Received 14 March 2023; revised 8 April 2023; accepted 2 May 2023. Date of publication 9 May 2023; date of current version 6 June 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3273507

Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges

FAISAL NAEEM [1] (Member, IEEE), MANSOOR ALI [1] (Member, IEEE), GEORGES KADDOUM [1,2] (Senior Member, IEEE), CHONGWEN HUANG [3,4,5,6] (Senior Member, IEEE), AND CHAU YUEN [7] (Fellow, IEEE)

[1] Electrical Engineering Department, École de technologie supérieure, Montreal, QC H3C 1K3, Canada

[2] Cyber Security Systems and Applied AI Research Center, Lebanese American University, Beirut, Lebanon

[3] College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China

[4] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China

[5] Zhejiang–Singapore Innovation and AI Joint Research Lab, Hangzhou 310027, China

[6] Zhejiang Provincial Key Laboratory of Information, Processing, Communications and Networks, Hangzhou 310027, China

[7] School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore

CORRESPONDING AUTHOR: F. NAEEM (e-mail: faisal.naeem@nu.edu.pk)

This work was supported by the Ministry of Education, Singapore, under its MOE Tier 2 under Award MOE-T2EP50220-0019. The work of Chongwen Huang was supported in part by the China National Key R&D Program under Grant 2021YFA1000500; in part by the National Natural Science Foundation of China under Grant 62101492; in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR22F010002; in part by the Zhejiang University Global Partnership Fund; in part by the Zhejiang University Education Foundation Qizhen Scholar Foundation; and in part by the Fundamental Research Funds for the Central Universities under Grant 2021FZZX001-21.

ABSTRACT While sixth-generation (6G) wireless systems are expected to bring about an explosion of accessible user information and novel technologies, along with new threats to terrestrial and non-terrestrial networks, major concerns associated with the development of 6G networks are privacy and security. Reconfigurable intelligent surfaces (RISs), which have recently emerged as promising candidates to support 6G physical platforms, have proved to be capable of boosting security of next-generation wireless systems. However, due to their easy reconfigurability and low cost, RISs are vulnerable to several security threats, and this vulnerability has not yet been thoroughly addressed in previous research. To fill this gap in the literature, in this review, we aim to thoroughly analyze the security challenges affecting RIS-empowered 6G wireless networks. To this end, we review the attributes of RISs that distinguish them from other relevant technologies, such as multiple-input-multiple-output (MIMO), conventional relaying, backscatter communication (BackCom), as well as outline security and privacy attacks in RIS-assisted 6G applications. Our specific focus is on security and privacy threats associated with the use of RISs with different vital 6G technologies, including millimeter wave (mmWave), terahertz (THz), device-to-device (D2D) communication, Internet of Things (IoT) networks, multi-access edge computing (MEC), integrated sensing and communication (ISAC), simultaneous wireless information and power transfer (SWIPT), and non-terrestrial network. The review concludes with an outline of open research challenges and promising future directions to further increase secrecy of RIS-assisted 6G applications. The results of this review contribute to previous research on 6G network security, in general, and RIS-based 6G network security, in particular.

INDEX TERMS Reconfigurable intelligent surfaces, 6G, physical layer security, privacy, wireless communication.

I. INTRODUCTION

RECONFIGURABLE intelligent surfaces (RISs) have transformed traditional wireless networks into smart radio environments providing power-efficient, cost-effective services with high data rates for beyond fifth-generation (B5G) and sixth- generation (6G) networks [1], [2], [3], [4],

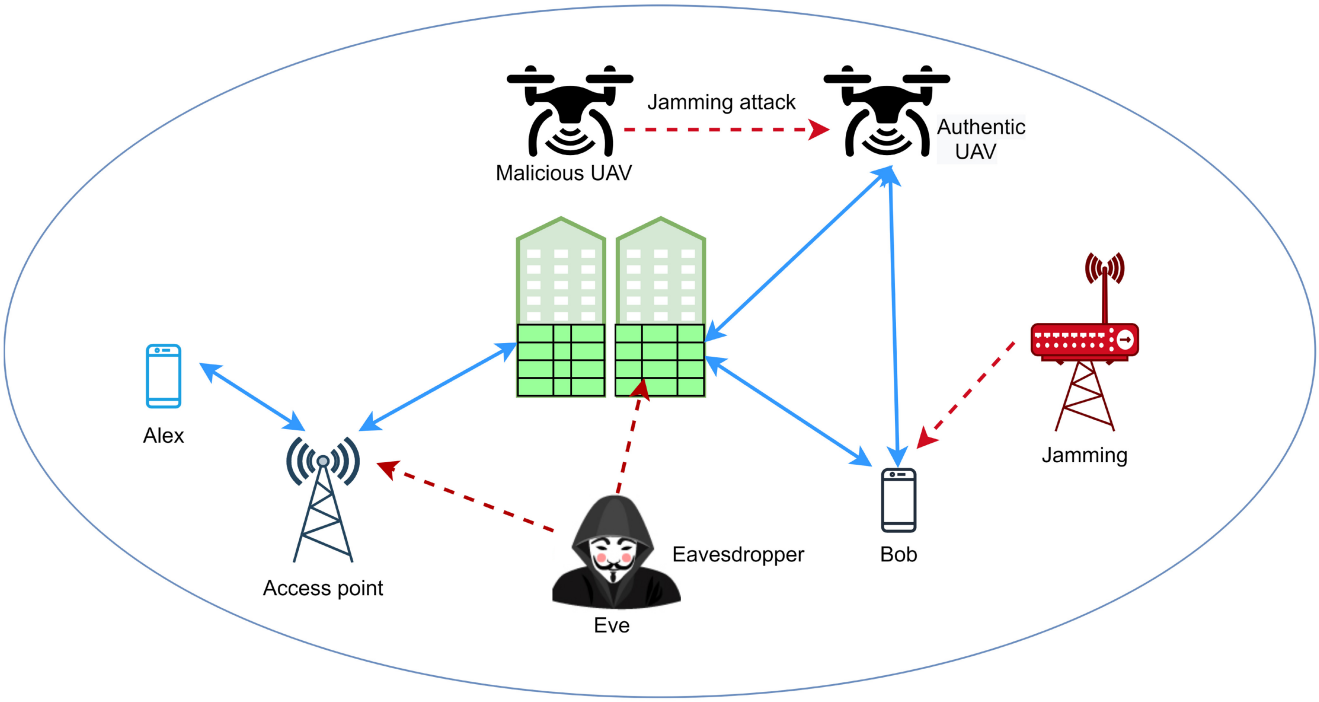

FIGURE 1. Security attacks on RIS-enabled wireless system.

[5], [6], [7], [8]. A RIS, also known as intelligent reflecting surface (IRS), is a digitally-controlled planar surface consisting of large amount of low-cost and passive reflecting elements that can intelligently tune the amplitudes and phase shifts of incident signals [8], [9]. As compared to traditional wireless techniques employed at transceivers, RISs can smartly reconfigure the wireless propagation channel towards the intended users, thus boosting the received signal power [10], [11], [12], [13]. Since RISs offer more freedom by intelligently adjusting the phase shift and amplitude of the RIS elements, RIS-enabled communications outperform existing wireless communications. Accordingly, an intelligent reconfiguration of the wireless propagation environment improves system performance [14], [15], [16], [17].

To date, there is robust evidence showing that RISs offer a considerable performance improvement in 6G applications such as terahertz (THz), millimeter wave (mmWave) [28], [29], [30], [31], [32], [33], [34], machine-to-machine (M2M), and device-to-device (D2D) communications, as well as in unmanned aerial vehicles (UAVs) [35], [36], satellite communications [37], integrated sensing and communication (ISAC) [38], and the Internet of Things (IoT) [39]. This evidence suggests that RISs can be meaningfully used in several ground-breaking applications of intelligent radio environments for future next-generation networks, such as B5G and 6G networks [8].

However, despite the recent ground-breaking advances in wireless technology, B5G and 6G networks remain to be vulnerable to several types of security threats, such as pilot contamination attacks (PCAs), jamming, and eavesdropping [40]. To address these concerns, different approaches to mitigate privacy and security threats to 6G networks have recently been proposed, such as physical key generation, RIS deployment, artificial noise generation, and frequency hopping. Among them, RISs were reported to be capable of reshaping wireless environments without incurring huge costs and adding complexity, which makes them suitable for deployment in B5G and 6G systems [41], [42].

According to several state-of-the-art reviews, RISs are useful in terms of improving physical layer security (PLS) performance metrics [43], [44], [45], [46], [47]. The RISs signal manipulation capability can enhance the PLS of the wireless networks by smartly reconfiguration of the channels of both the legitimate and eavesdropping users. Moreover, the RISs can also boost the signal beam at the intended receiver and suppress the beam at the eavesdropper making the wireless network secure. However, deploying RISs may create new security threats in the 6G network that must be tackled. E.g., instead of using RISs to enhance PLS and system performance, attackers or eavesdroppers (EAVs) can use them to deteriorate the performance of legitimate links or boost the performance of eavesdropping links, which can jeopardize security of the entire wireless system [48], [49], [50], [51]. Fig. 1 shows security attacks on a RIS-assisted wireless system consisting of the access point (AP) *Alex* that forwards traffic to the legitimate user (LU) *Bob* via RISs and UAVs in the presence of the eavesdropper *Eve* and a *jammer* attack. These attacks can severely degrade the performance of the RIS network. E.g., if *Eve* attacks the network, LU *Bob* cannot achieve a positive secrecy rate. Furthermore, the malicious jammer near the legitimate user *Bob* can attack a legitimate transmission by sending replayed

TABLE 1. Comparison of the existing survey in RIS-enabled 6G communication.

Reference	Area of focus
[18]–[21]	Motivates the applications and design of RISs for wireless communications systems with future research directions.
[22]	Outline the design of RISs for radio localization and mapping.
[23], [24]	Surveys the principles, applications and future research directions of RISs for emerging 6G.
[25]	Provides an overview of RIS-enabled covert communications
[26]	Provide a comprehensive review on physical layer security in LiFi-aided networks.
[27]	A systematic review of RIS-aided PLS in wireless systems
Contribution	Compared to previous surveys, our paper is the first to provide a comprehensive literature review on security and privacy attacks in RIS-assisted 6G applications such as mmWave, THz, D2D, IoT networks, MEC, SWIPT, ISAC, and UAVs. We also propose open research challenges and outline promising future directions to increase the secrecy of RIS-enabled systems in 6G applications.

or faked jamming signals to the *Bob* via RISs and UAVs, thus degrading the performance of LUs. This brings about new privacy and security threats arising from the deployment of RISs in 6G networks. Accordingly, in this paper, we aim to provide a comprehensive review of security and privacy threats from the perspective of RIS deployment in next-generation wireless systems.

Over the last several years, owing to the unprecedented benefits afforded by RISs, they have attracted a considerable scholarly attention. Numerous tutorials, surveys, reviews, and short magazine articles have introduced different aspects of RISs and their variants. Some of these works focused on general concepts and applications of RISs for wireless networks [6], [7], [18], [19], [20], [21]. Likewise, several articles investigated the applications of RISs with emerging 6G technologies [23], [25], [26], [52]. Furthermore, some reviews analyzed RIS-aided localization and mapping [22], as well as industrial viewpoints on RISs [53] and mathematical frameworks for RIS networks [9], [14], [54].

From the security and privacy perspective, there has been extensive research on the applications of RISs to enhance the privacy and security of wireless communications, including systematic reviews on RIS-aided covert communications [55], RIS-assisted physical layer security in wireless networks [26], [27], [56], [57], and RIS-aided security in energy harvesting networks [58]. However, to the best of our knowledge, none of the previous studies has thoroughly reviewed security and privacy challenges associated with integrating RISs in promising applications of 6G networks. Therefore, this review is the first to provide a comprehensive analysis of security threats associated with RISs for cutting-edge 6G technologies, including mmWave, THz, D2D communication, IoT networks, multi-access edge computing (MEC), simultaneous wireless information and power transfer (SWIPT), and UAVs. Table 1 compares the scope of previous reviews and that of this paper.

The remainder of the paper is organized as follows: Section II provides fundamental details about the operation and applications of RISs in 6G with various security attacks. Next, Section III identifies the types of attacks on RIS networks and different techniques used to improve RISs' security and privacy. In Section IV, we investigate the PLS for RIS-aided networks. The paper concludes with a discussion of challenges and future research directions (Section V) and conclusions (Section VI). Table 2 summarizes the list of key acronyms used throughout in the paper.

TABLE 2. List of main acronyms.

Acronyms	Definitions
6G	Sixth Generation
B5G	Beyond Fifth Generation
IRS	Intelligent Reflecting Surface
RIS	Reconfigurable Intelligent Surface
IRIS	Illegal Reconfigurable Intelligent Surface
PLS	Physical Layer Security
EAV	Eavesdropper
ML	Machine Learning
PSA	Pilot Spoofing Attack
PCA	Pilot Contamination Attack
ERA	Environment Reconfiguration Attack
M2M	Machine-to-Machine
D2D	Device-to-Device
MIMO	Multiple-Input-Multiple-Output
LU	Legitimate user
ECSI	Eavesdropper channel state information
CCC	Common control channel
SWIPT	Simultaneous wireless information and power transfer
CRs	Cognitive radios
PLS	Physical layer security
MTD	Moving target defence
IDS	Intrusion detection system
PSCA	Penalty successive convex approximation
AO	Alternate optimization
KGR	Key generation rate
AN	Artificial noise

II. RIS-AIDED 6G: APPLICATIONS AND SECURITY

A. RIS OPERATION

An RIS is a software-controlled planer surface consisting of several low-cost passive reflecting elements, each of which

TABLE 3. Security and privacy issues of different 6G applications.

6G Applications	Privacy Issues	Security Issues	Key Solutions
Metaverse [75]	Leakage of private data, identity forgery, digital assets theft, Intercept, impersonation privacy	Remote access vulnerabilities, phishing, replay attack, thread hijacking	Blockchain, federated learning, light-weight differential privacy
Holographic Telepresence [76], [77]	Expose biometric data, social habits, personal behavior	Deepfake agent, eavesdropping, DoS attack	Moving target defense(MTD)/intrusion detection system (IDS), PLS
Tactile Interaction [78], [77]	Expose biometric data	Man-in-the-middle attacks, DoS against tactile applications	MTD/IDS, PLS, quantum-safe communications
Autonomous vehicle [79]	Compromised credentials, location tracking	Sudden crash, eavesdropping, DoS attack, jamming V2X	MTD/IDS, physical security isolation, PLS, distributed ledgers, blockchain
Smart Robots [80]	Exposure of private data	Malware injection for physical damage or device malfunction	IDS/MTD, PLS

can reconfigure the incident signal phase to create a favorable wireless transmission environment [16], [17], [59], [60], [61]. For instance, a smart controller based on a field-programmable gate array (FPGA) controls RIS reflection adaptation. The controller serves as a gateway for communicating and coordinating with the base station (BS) through a separate wired or wireless link. The RIS first receives a signal from the BS and then reflects the incident signal through induced phase variations regulated by the controller. Eventually, the reflected signal and direct BS signal can be coherently added to either attenuate or boost the overall strength of the signal at the receiver. Overall, RIS architecture can be categorized into passive and active. Passive RISs do not process any information and only reflect the incident signal to facilitate communication between the receiver and transmitter. Passive RISs use passive reflecting elements to fully control the beamforming without amplification and are not associated with additional power consumption [62], [63], [64]. By contrast, active RISs can amplify reflected signals via amplifiers embedded in their elements [36], [65], [66], [67], [68].

RISs have several potential advantages over other wireless technologies, such as multiple-input-multiple-output (MIMO) relaying, backscatter communication (BackCom), and conventional relaying [50], [69], [70]. For instance, conventional relaying requires additional power in order to transmit, amplify, and regenerate the signal. By contrast, a RIS passively reflects the incident signal by inducing phase shifts without requiring any additional radio frequency (RF). Furthermore, the RIS functions in the full-duplex (FD) mode that is free of self-interference and noise amplification. Furthermore, unlike conventional BackCom like RF identification (RFID) tags, the RIS modulates information on the incident signal, and then the modulated signal is backscattered to the receiver.

Furthermore, contrary to MIMO relaying, RISs are associated with relatively low power consumption and hardware costs. Although MIMO relaying can achieve a higher signal-to-noise ratio (SNR) than the RISs [24], [71], [72], the SNR of an RIS-aided system can be improved by increasing the number of reflecting elements. In addition, the cost of one reflecting element of an RIS is considerably lower than that of one antenna element in MIMO relaying. Finally, due to the conformal geometry, RISs are lightweight and can be mounted on building facades, walls, ceilings, and so forth, which makes them a promising approach to improve the capacity of future 6G networks [73], [74].

B. SECURITY AND PRIVACY IN RIS-ASSISTED 6G APPLICATIONS

The RIS-assisted 6G network will require modification in its security architecture with the integration of space-air-ground-sea integrated network (SAGIN) architecture to satisfy the requirements of novel applications [40]. In particular, the third-generation partnership project (3GPP) considered the architectural design for the non-terrestrial networks, anticipating a close integration between aerial, satellite, and terrestrial networks [81]. Specifically, 3GPP release 16 defined the standardization of non-terrestrial networks for the next-generation network [83]. Moreover, new security aspects and modifications were also defined by 3GPP in release 18 [82]. Moreover, new security aspects and modifications have been also defined by 3GPP in the release 18 [83].

As can be seen in Table 3, robust PLS can be a game-changer for protecting 6G networks from several security

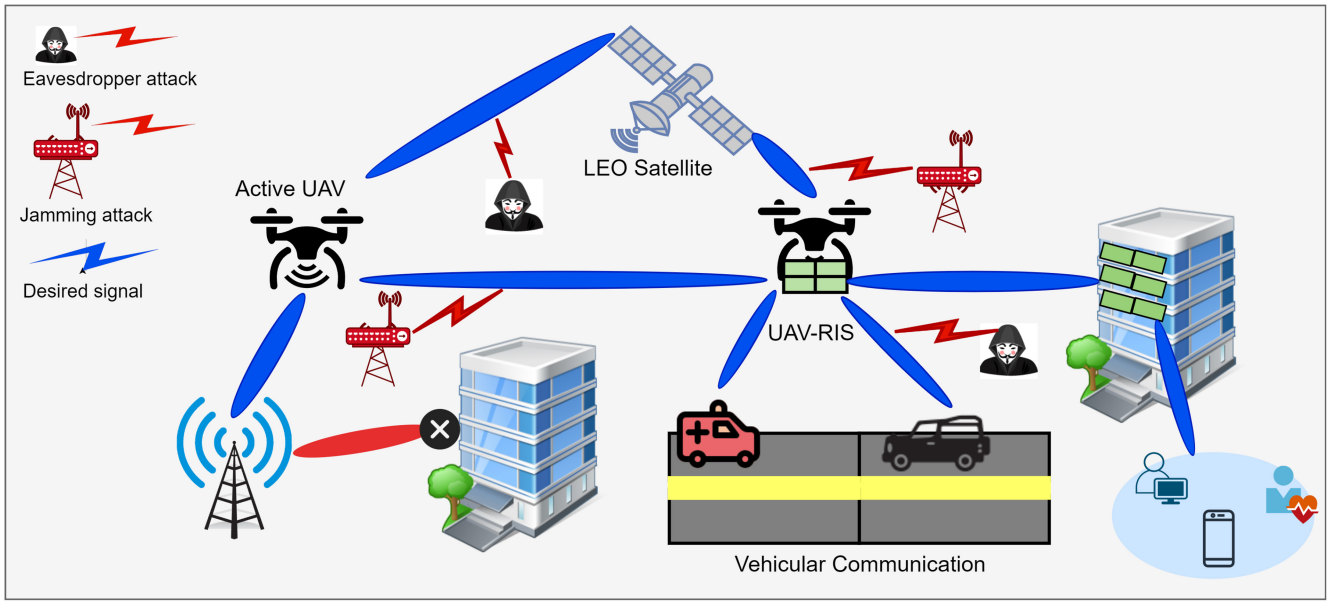

FIGURE 2. RIS-empowered non-terrestrial network: security and privacy attacks.

threats [84], [85], [86], [87]. Since the physical layer is a keystone of wireless communications, numerous traditional security attacks, such as jamming and eavesdropping that affect almost all 6G applications, can be prevented by protecting physical-layer information. A recent study that evaluated the advantages of RISs in terms of wireless security improvement found that RISs can improve PLS by reconfiguring the phase shift and amplitude of reflecting elements to add wireless signals destructively at a potential EAV and constructively at a legitimate receiver (LR) [88].

Furthermore, RISs were also reported to be a promising approach to preserve privacy during wireless communication [55], [89]. This can be achieved by using the low probability-of-detection or covert communication [90], which attempts to hide wireless transmissions (e.g., hide the location of the transmitter or avoid exposing a transmitter) from a warden, thereby attaining a high level of privacy. RISs can also adjust the amplitude or phase shift of their reflecting elements to intentionally create a spatial null around the warden and, by doing so, achieve a high communication covertness [88].

However, despite the benefits of RISs briefly reviewed above, RIS deployment in 6G networks is subject to certain security constraints [40], [63], [91], [92]. For instance, when EAVs and LUs have highly correlated links, the secrecy rate attainable using RISs is quite limited [93]. RISs add beamformed signals destructively at the EAVs and constructively at the intended user. However, this processing approach is not always trivial and can complicate the entire system. Moreover, this approach additionally requires the use of other signal processing techniques to detect incoming symbol vectors from the user, estimate the channel between the RIS and the user, and track the user's location. In the absence of the corresponding sophisticated algorithms, an accurate signal beamforming is not attainable, and the entire system is exposed to several security risks. Furthermore, RIS security also needs to be addressed for 6G network PLS, as an attacker can physically or remotely access the RIS controller and modify configuration parameters. Furthermore, the attacker can put itself close to the RIS and use the correlated channel to eavesdrop on the incoming signals [93]. In the next section, we review different types of security and privacy threats on perspective applications of RIS-enabled 6G networks.

C. APPLICATIONS OF RISs IN 6G FROM SECURITY PERSPECTIVE

The evolving RIS-enabled wireless network was previously reported to have promising applications in various scenarios (see Figs. 2 and 3). In what follows, these scenarios are discussed in further detail. Table 4 summarizes major types of security and privacy attacks in RIS-assisted 6G applications.

1) *THz and mmWave:* The first scenario involves completely blocked users unable of communicating with the BSs. In such conditions, RISs can create a strong LOS channel between the sender and the receiver and combat the transmission distance constraint. This capability of RISs is particularly helpful in addressing the coverage extension issues arising in THz and mmWave communication systems because of these bands' unfavorable omnidirectional path losses. Moreover, RISs also increase the channel rank, received power and, consequently, spatial diversity required for outdoor systems. However, in mmWave/THz scenarios, RISs can also lead to security attacks such as eavesdropping attacks where eavesdroppers can attack the RIS to user link and transmitter to RIS. Several previous studies on EAV attacks on a single RIS

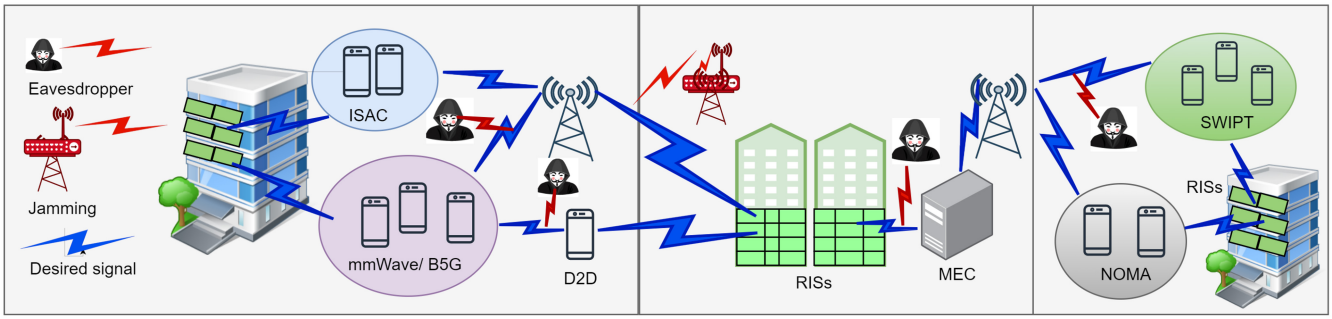

FIGURE 3. RIS-empowered 6G applications: security and privacy attacks.

TABLE 4. Security and privacy attacks in RIS-assisted 6G applications.

Application	Types of attacks
THz and mmWave	Eavesdropper attacks RIS links due to imperfect eavesdropper channel state information.
Cell-edge	Malicious jamming attacks can interfere with users' transmission quality.
Device to Device	Passive eavesdropper and jamming attacks can leak the information in a downlink transmission scenario.
Internet of Things	The MJs can perform cooperative attacks (e.g., jamming attacks) to the RISs and BSs, thus complicating the decoding of information.
NOMA	The NOMA users with high power are exposed to external EAVs, while the broadcasted information by the NOMA users can be leaked to the internal untrusted EAVs due to successive interference cancellation.
Cognitive radio	RIS-enabled CRs are exposed to jamming and eavesdropping attacks on the CSIs of the wiretap links in RIS-CRs.
Multi-access edge computing	The offloading of data can be attacked by the malicious eavesdropper, thus resulting in data leakage due to broadcasting nature of EM signals.
UAVs	The eavesdropper and unreliable UAVs can perform security and privacy attacks such as cooperative jamming attacks.
SWIPT	SWIPT networks are exposed to active and passive jamming attacks.
Satellite communication	The eavesdropper can breach the security of the RIS-assisted satellite communication when deployed near a legitimate node.
Integrated sensing and communication	RIS-assisted ISAC is exposed to jamming and eavesdropping attacks due to LOS-dominated air-ground communication channels.

environment assumed a perfect eavesdropper channel state information (ECSI) for THz system (e.g., [94], [95],[96]). However, in practice, obtaining a perfect ECSI for the envisioned 6G environments is impossible due to channel estimation errors or untrustworthy behaviors of the eavesdropper. Moreover, due to imperfect ECSI, the narrow beam width characteristics of THz waves can cause information leakage.

2) *Cell edge:* The second application scenario consists of a RIS-assisted network where users are located at the edge of the cell that can experience co-channel interference from neighboring BSs and a high signal attenuation from its BS [97]. In this scenario, the RIS can mitigate eavesdroppers' impact by properly cancelling their signal and thus boosting the communication system's security. For instance, the RIS technology was previously used to improve communication system security and mitigate jamming interference [98]. However, in such scenarios, users at the cell edge can suffer from the NLOS communication channel, and malicious multi-antenna jamming attacks can interfere with transmissions by sending replayed or faked jamming signals [99].

3) *Device to Device:* The third scenario involves D2D networks [100] where the RISs are used to support the requisite low-power transmission, cancel interference, and enhance individual data links. The RIS-enabled D2D network in a downlink transmission scenario can be exposed to passive eavesdropper and

jamming attacks where the D2D transmitter forwards information symbols to the D2D receiver and BS.

4) *IoT networks:* The fourth scenario involves RIS-assisted IoT systems (e.g., [101]) that can alleviate energy budget issues in energy-constrained IoT networks and compensate for power losses over long distances through passive RIS beamforming. However, RIS-assisted IoT networks are vulnerable to cooperative attacks between EAVs and malicious jammers (MJs) capable of degrading the system performance. Specifically, the MJs can perform jamming attacks on RISs and BSs, thus complicating the decoding of information [102].
5) *NOMA:* The fifth scenario involves 6G NOMA systems (e.g., [97], [103]). In these systems, RISs can help to increase the number of served users and improve the communication rate, which is a key requirement for these systems. Yet, RIS-assisted NOMA networks are exposed to internal and external eavesdropping security attacks. NOMA users with high power are exposed to external EAVs, while their broadcasted information can be leaked to the internal untrusted EAVs due to successive interference cancellation [104].
6) *Cognitive radio:* The sixth scenario is related to cognitive radio (CR) networks [105] where RISs can be employed to increase the degree of freedom so as to further boost network performance [106]. As secondary users share the channel sensing via a common control channel (CCC), intruders can perform jamming attacks such as denial-of-service (DoS) on the CCC in RIS-assisted CRs (RIS-CRs) [107]. Moreover, EAVs can perform security attacks and obtain the CSIs of the wiretap links in RIS-CRs.
7) *Multi-access edge computing:* The seventh scenario includes using RISs in MEC systems, wherein RIS deployment is used to improve spectral efficiency and energy efficiency (EE). For instance, as reported in several previous studies, mobile users' transmit power can be minimized by considering an infrastructure in which machine learning tasks are offloaded to MEC server [108], [109]. However, due to broadcasting nature of EM signals from RIS-MEC network, the offloading of data can be intercepted by the malicious eavesdropper [110].
8) *UAV:* The eighth scenario involves the UAV networks where RISs can be deployed to improve the quality of communication between ground users and the UAV, which can result in system performance optimization [111]. In a RIS-assisted UAV network, the eavesdropper and unreliable UAVs can perform security and privacy attacks (e.g., cooperative jamming attacks) and degrade network performance [112].
9) *SWIPT:* The ninth scenario of RIS-assisted communication pertains to the SWIPT (see Fig. 3). In such systems, the RIS phase-shift matrix can be formulated to improve the strength of the signal at the energy receivers in the charging zone to ensure compliance with the energy harvesting requirements [113]. SWIPT networks are exposed to two types of EAD attacks: active and passive [114], [115]. In the active EAD attack, attackers can mislead the BS to forward the signal to the EAD instead of LUs. Moreover, the EAD can act as a LU and forward the pilot signal to the BS in SWIPT systems. The passive attack is challenging, since, due to imperfect CSI, EADs cannot be detected at the BS.
10) *Satellite networks:* The next scenario is related to the deployment of low earth orbit satellites and high-altitude platforms that have emerged as a potential solution for low-latency and ubiquitous communications. However, constraints of such deployment include dynamic propagation environment and high probability of blockage. These concerns could be addressed by using RISs-assisted non-terrestrial communication as a cost-effective solution. Specifically, RISs can provide controllable propagation environment and bypass blockages to improve capacity in satellite communication [116], [117]. In the scenario when the eavesdropper is very close to the legitimate node, satellite communication is exposed to eavesdropping attacks [118]. In that case, the communication channel between the space wiretap channel and space legitimate channel are similar and are exposed to eavesdropper attack.
11) *Integrated sensing and communication:* Finally, the deployment of RISs in ISAC provides significant performance improvements with regard to spectral efficiency, interference suppression, and target detection [119], [120]. RIS-aided ISAC improves target parameter interference suppression and NLOS target detection. However, due to LOS-dominated air-ground communication channels, RIS-assisted ISAC is vulnerable to jamming and eavesdropping attacks. Moreover, malicious and unauthorized UAVs also pose new security attacks to ground ISAC communication networks [121].

III. ATTACK AND THREATS IN RIS-AIDED WIRELESS SYSTEMS

Exploitation of RISs by malicious sources may pose various privacy and security threats to future wireless systems. In this section, we discuss different security threats that RISs can face. Furthermore, a discussion of PLS is most important here, as major beamforming operations occur in the physical layer of RIS devices. In addition, we also review security issues associated with network layers. The major reason of this review is that most of the data from IoT and sensing devices associated with UAVs are processed by the network layer in accordance with the corresponding protocols to successfully transmit the information to destination. However, if the attacker tampers the destination address, the data will be transmitted to the wrong address, and the RIS

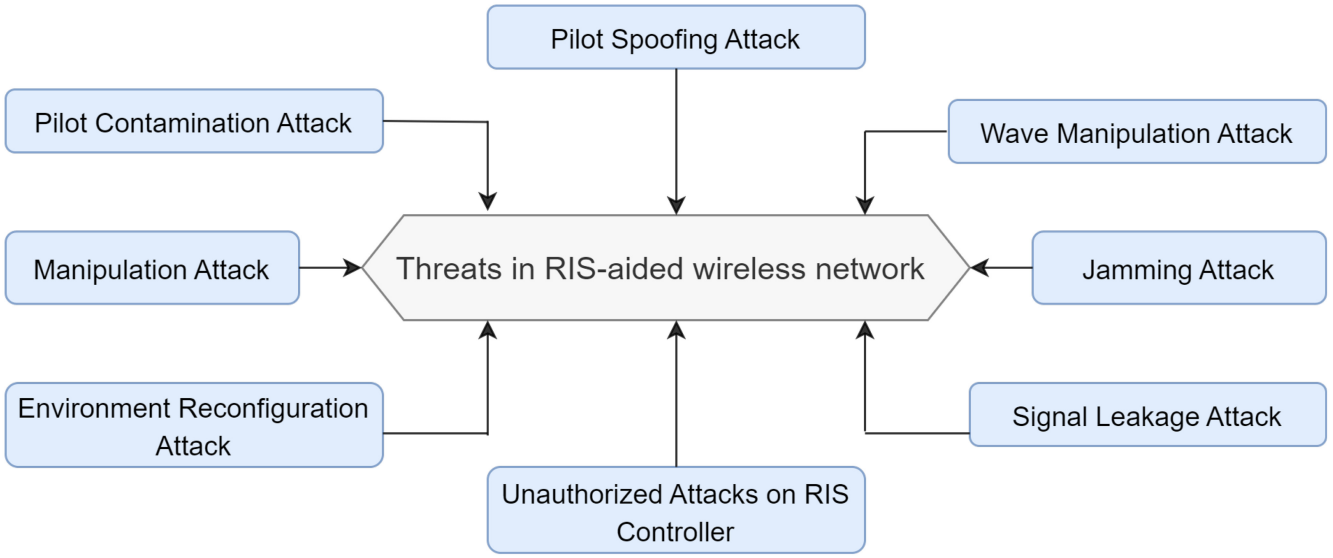

FIGURE 4. Security attacks on RIS-assisted wireless networks.

will be used for an unintended signal transmission. Table 5 summarizes potential RIS-based security threats and possible countermeasures.

A. PILOT CONTAMINATION ATTACK (PCA)

In previous research, RISs were reported to demonstrate a great potential in offering more flexibility for wireless communications. Namely, owing to their no power consumption and no added thermal noise during reflection, RISs can enhance energy and spectrum efficiency [19]. However, more threats to multiple-antenna systems can emerge. Theoretically, the reverse pilot transmission phase involves capturing the CSI of RISs [131]. In a recent study, Huang and Wang [122] proposed a novel PCA strategy during the pilot training phase where *Eve* exploited an RIS to perform a PCA. The results of this study revealed that *Eve* might use an RIS to deteriorate performance of the wireless system. *Eve* can also use RISs to attack the reverse pilot transmission phase of a time division duplex system without any information about the pilot sequence, as well as to reflect pilot sequence transmitted to LU *Alex* by LU *Bob*.

Technically, the existing random orthogonal pilot [132], [133], artificial noise or random data [134], [135], and random modulation [136], [137] methods fall short of the RIS- assisted PCA (RIS-PCA) scheme, as all these methods require a difference in the signal sequence sent by *Bob* and *Eve*. Furthermore, an RIS-PCA attack alters channel estimation results, which then deteriorates transmission performance in the downlink transmission phase and thus enables the eavesdropper to obtain confidential details using a pilot spoofing attack.

Considering seriousness of the threat presented by PCAs to multiple-antenna systems, different approaches were previously proposed to detect PCAs and ensure secure transmission under such attacks [136], [137], [138]. However, existing countermeasures for PCAs do not work for RIS-based PCAs, as *Eve* is not required to have details about the pilot sequence of *Bob*, thereby posing serious security threats to the legitimate wireless network. Because of the notable differences between classic PCAs and RIS-based PCAs, it is essential for the RIS-based variant to identify possible countermeasures. Inspired by these observations, Huang and Wang [122] proposed a novel generalized cumulative sum (GCUSUM) scheme—namely, a sequential process for detecting the occurrence of RIS-based PCAs. In the analysis of the worst-case average wiretapping throughput gain, worst-case average detection delay, and average run length to false alarm of the GCUSUM scheme, the authors obtained noteworthy results. Moreover, Huang and Wang [122] also presented a cooperative channel estimation scheme to ensure secure transmission when under an RIS-based PCA.

B. PILOT SPOOFING ATTACK (PSA)

A PSA attack introduces novel challenges for secure transmission at the physical layer. A PSA attack is a type of active eavesdropping wherein the identical training sequences are launched to manipulate the channel estimation result during the pilot training phase [139]. While this technique cannot be performed without detailed information regarding the pilot sequence, a random pilot sequence can be created to detect a PSA. However, RISs and the real-time-programmable attributes of wireless channels offer innovative opportunities for efficient pilot spoofing. Owing to the ease of accessibility of the communication protocol, an RISs control method might be seamlessly embedded in the protocol that allows malicious individuals to use RISs to manipulate the wireless channel. After tempering the protocols, the reciprocity of the downlink and uplink channels can

TABLE 5. RIS-based Security Attacks and Countermeasures.

Ref.	Type of Attack	Description	Countermeasures / Proposed solution
[122]	Pilot Contamination Attack (PCA)	RIS-based PCA attack can modify the channel estimation outcome, which deteriorates the transmission performance in the downlink phase and facilitates the eavesdropper in capturing information through spoofing	A GCUSUM detection scheme to detect PCA for enabling secure transmissions under RIS-based PCA
[123]	Pilot Spoofing Attack (PSA)	An active eavesdropping where an identical training sequence is launched to manipulate the channel estimation outcome during the pilot training phase	AO algorithm and Charnes-Cooper transformation procedure to address the PSA attack on RIS-assisted systems
[124]	Jamming Attack	RIS deployed as a jammer to degrade the SINR at the LR	A SDR optimization technique to reduce SINR at the LR
[125]	Manipulation Attack	An attack where the RIS phase is rapidly changed by the Eve to manipulate the wireless environment to reduce KGR	A slewing rate detection process where the compromised path is removed from the time domain, and a flexible quantization scheme is employed for KGR maximization
[126]	Environment reconfiguration attack (ERA)	A new form of jamming attack wherein an attacker exploits the RIS to rapidly vary the electromagnetic propagation environment for disturbing LRs	Formulating an ILP for RIS environment that can quickly modulate the channel response of victim wireless communication parties
[51]	Signal leakage and interference attack	Signal leakage attack leverages IRIS to augment the eavesdropping data rate while interference attack involves the use of IRIS to transmit the interference signal	An AN-assisted solution based on joint optimization to alleviate the security damage caused by IRIS
[127]	Eavesdropping	The adversary tries to intercept the information flow between the nodes	Cooperative jamming where control center jams the communication channel for eaves
[128]	Unauthorized access to RIS controller	With no identification system installed on RISs, the malicious signal is transmitted to the users, affecting end-usersâ^{TM} decision- making process	ANN-based advanced intelligent framework for signal classification and identification
[129]	Attack on RIS controller and tunable chips	The adversary can get remote access to RIS controller that controls chip parameters for phase and amplitude through malware injection	Optimization-based techniques to re-tune the chips parameters while detecting variations caused by disturbances
[130]	Wave manipulation	The attacker can adjust the controller functions to control the movement of RISs to elicit destructive interference among electromagnetic waves	An advanced FPGA based controller with genetic algorithm in order to adjust itself to create desirable radiation under attack scenarios

be obliterated, thereby leaving to potential additional threats to the legitimate communication [123].

While Huang and Wang [122] already mentioned the idea of an RIS- assisted spoofing attack, they did not find anything the maximization of wiretapping capability. Yang et al. [123] proposed a new pilot attack strategy that uses an RIS in a three-node model. In this model, the RIS is placed close to the LUs to passively reflect the legitimate signal. The control scheme is embedded in the communication process in the time division duplex mode to facilitate the eavesdropper conducting pilot spoofing. Channel reciprocity fades away because the RIS phase shifts are varied during the downlink and uplink phases, and the beamforming vector's bias towards the EAVs is increased. Yang et al.'s [123] results indicated that this approach can generate severe security threats with no energy footprints. Furthermore, the internal users' lack of proper RIS employment was found to potentially lead to other serious concerns.

Overall, countering the RIS-aided PSA attacks is associated with two major challenges: (i) uncertainty in terms of noise present during PSA detection that can damage the known energy-based signals detectors; and (ii) uncertainty in channel distribution information that invalidates the statistic feature- based PSA detection schemes. With this in mind, Liu et al. [140] devised a three-step training procedure to address PSA attacks on RIS-assisted systems. In this study, the detector was used to examine the signal power levels received at the transmitter to reliably detect the PSAs. The proposed three-step training method did not need any prior information about the noise variance and could acquire the CSI of illegitimate and legitimate backscatter channels. Although the theoretical analysis of the proposed scheme's efficacy was conducted, the scheme was a prototype. Accordingly, further research is needed to address several practical concerns, such as the efficient design of a feedback process in a backhaul link or the random binary sequence for RIS-enabled MISO systems.

C. JAMMING ATTACK

In an important recent study, Lyu et al. [124] presented another adverse RIS application for modern wireless systems involving an RIS used as a green jammer to attack the communication between two authorized parties. Contrary to several recent studies where RISs were adopted to boost the secrecy rate at the LR [93], [141], [142], Lyu et al. proposed using RIS-assisted jammer to degrade the signal-to-interference-plus-noise ratio (SINR) degradation at the LR. Furthermore, unlike in the traditional active jamming attacks that use their internal energy to bombard the victim system with strong noise signals, the RIS-enabled jammer proposed by Lyu et al. used the victim system's signals for the attack by altering their phase shifts and reflection coefficients. The RIS-based jamming attack left no footprint as it interfered with the system, which made its detection and prevention more tricky and cumbersome. Lyu et al. [124] showed that, under certain circumstances, their proposed RIS-based jammer outperformed classic jamming attacks, particularly when there was a small distance ($<$10 m) between *Bob* and the RIS.

Overall, cooperative jamming is a technique used to tackle eavesdropping and jamming attacks so as to increase communication network security. In this jamming technique, the main station transmits the information signal to the LUs. By contrast, the relay node transmits the jamming signal to interrupt the communications channel for EAVs. Cooperative relaying or jamming differs from normal jamming in that it increases network security by establishing a secure channel between end nodes. Several known cooperative relaying or jamming techniques include decode-and-forward and amplify-and-forward.

D. ENVIRONMENT RECONFIGURATION ATTACK (ERA)

Staat et al. [126] introduced a new type of jamming attack on modern wireless network, named the environment reconfiguration attack (ERA). In this attack, an RIS is exploited by an adversary to swiftly change the electromagnetic propagation environment and create disturbance for LRs. Through reflecting available legitimate signals, the RIS provides the adversary with a significant advantage over conventional jamming. Accordingly, the adversary no longer needs to actively emit of jamming signals. Staat et al. [126] proposed orthogonal frequency division multiplexing (OFDM) modulation to comprehensively examine the ERA. The authors also presented an optimization algorithm to improve the ERA's jamming performance. The results of the aforementioned study revealed that, even with a very small RIS, the ERA could severely degrade the available data rates.

Staat et al. [126] further argued that their ERA has a higher practical value than the previously proposed RIS-based jamming techniques [124] that require the attacker to know all details about the involved channel states. Indeed, as documented in the literature [7], [9], [19] [126], obtaining such details is not feasible. Thus, the ERA approach [126] eliminates this impractical channel knowledge requirement for the attacker and achieves a significantly better jamming performance.

E. MANIPULATION ATTACK

In another relevant study, Hu et al. [125] presented a novel RIS-aided manipulation attack to reduce the key generation rate (KGR); in this attack, the active attacker *Eve* performs rapid RIS phase changes to manipulate the wireless environment. To analyze the weakness of conventional key generation technology subject to this type of attack, the authors used the channel frequency response coefficient. Hu et al. [125] introduced a path-separation-based slewing rate detection process to counter RIS-enabled manipulation attacks. This process involves removing the compromised path from the time domain and using a flexible quantization method for KGR maximization. The simulation results showed promising performance of the proposed process in terms of successful detention of the attacked path; the authors also argued for further improvement of their process improved upon in future studies.

F. SIGNAL LEAKAGE AND INTERFERENCE ATTACK

Wang et al. [51] proposed a novel concept-illegal reconfigurable intelligent surface (IRIS) involving the illegitimate use of an RIS. Two important security issues—namely, interference and signal leakage—were investigated in the case of IRIS presence.

Signal leakage represents the scenario where an IRIS is used to improve the eavesdropping data rate and increase the information leakage to the EAV. In a traditional wireless system, an IRIS can be used by the EAV to reflect the environmental signal, as well as to collect the transmission signal that cannot be received earlier. The IRIS can passively enhance communication quality of illegal links and degrade the performance of PLS without generating an extra RF signal. Therefore, it is rather difficult to detect and prevent signal leakage. The concept pf signal leakage mainly focuses on acquiring more legal signals leaked from the AP to boost the EAV's wiretapping capability. This is different than RIS-based jamming [124] where the signal power received at the LU is reduced through the destructive addition of signals from the RIS and AP.

While RISs are used for PLS improvement, it is difficult to achieve a good system performance, as the legitimate system cannot control IRIS-aided interference links. Moreover, using an IRIS to transmit interference signals—referred to as *interference* attack—can severely degrade the SINR at the LU. Likewise, it is almost impossible to cancel interference signals from IRIS. This situation can severely hinder the channel estimation and data transmission process. While a pilot symbol is sent to the LU by the AP during the channel estimation process, the attacker can use the IRIS to send another pilot symbol. If the attacker uses a high transmit power and the IRIS is reasonably optimized, it can control the training phase and degrade the channel estimation accuracy [51].

Another major challenge to is IRIS-based interference and signal leakage attacks, i.e., joint optimization of the beamforming vector at the AP and imperfect CSI-based RIS phase shifts. In most previous studies on RIS-aided PLS optimization, the CSI of illegitimate and legitimate links was assumed to be perfectly known [41], [42], [143]. Therefore, joint optimization for wireless networks that incorporates IRIS and RIS has to be redesigned assuming imperfect CSI for legitimate links and no CSI for illegitimate ones. Admittedly, addressing this concern will increase the complexity of the optimization problem and severely restrict the improvement in the performance attained through joint optimization. In addition, IRIS deployment further improves communication quality of illegitimate wireless systems and, in turn, further degrades PLS performance. The simple joint optimization of RIS phase shifts, and beamforming vector at AP is not sufficient to relieve the considerable effect brought by IRIS. In this context, in order to safeguard transmission in IRIS-based threats, it becomes imperative to investigate innovative ideas. In one study seeking to do so, Wang et al. [51] introduced an artificial noise (AN) assisted solution based on joint optimization to alleviate PLS degradation caused by the IRIS. The basic concept behind the AN technology was integrating the noise signal with the information signal. The legitimate channel and noise channel were kept orthogonal. Without affecting LUs, the noise signal only obstructed all possible EAVs regardless of the location detection of IRIS and EAVs. This would eventually improve the wireless system secrecy rate, reduce the data rate at EAVs, as well as secure the transmissions against IRISs and EAVs.

G. UNAUTHORIZED ACCESS AND ATTACKS ON RIS CONTROLLER

RISs may be subjected to many incident signals from different network nodes, including those generated and transmitted by malicious users. If a network's RISs are not equipped with a proper identification system, a malicious signal transmitted to LUs will affect their decision-making. For instance, if false information about traffic is transmitted to and used by an ambulance, the patient's condition might further deteriorate [128], and a tactical situation might get complicated if unauthorized personnel use RISs in a tactical network.

Moreover, intruders can also attack tunable chips of the RIS. The primary function of these chips is to reconfigure the phase and amplitude of signals to successfully reach their destination. The role of the adversary is to change the parameters so that the signals containing information get diverted from their original propagation path [129]. The adversary can gain remote access to the RIS controller that controls chip parameters through malware injection. Similarly, using meta-surface control functions, the eavesdropper can also attack wave manipulation or modulation techniques used to create multiple reflections of the incoming signal, with different phases and amplitudes. By adjusting the controller functions, the adversary can change the movement of RISs so as to cause a destructive interference. This will completely corrupt informative signals, and the end user will receive only disrupted signals containing noises [130].

IV. PHYSICAL LAYER SECURITY FOR RIS-ASSISTED NETWORKS

Available research on RIS-related security threats is still in its infancy. To date, very few studies have addressed possible countermeasures for the potential threats to RISs. In this section, these studies are reviewed in further detail. Tables 6 and 7 summarizes the PLS in RIS-enabled wireless and non-terrestrial networks.

A. RIS-ASSISTED WIRELESS NETWORKS

Wang et al. [144] proposed a semi-definite programming relaxation technique for robust cooperative jamming and beamforming design with eavesdroppers under an imperfect CSI to maximize EE. The proposed technique achieved a higher EE in an imperfect CSI with eavesdroppers. In another relevant study, an alternating optimization algorithm was proposed to design an optimal phase shift of RIS and beamforming for BS [41]. This system model considered a RIS-assisted wireless network with multi-antenna eavesdropper and a single-antenna LU. Simulation results revealed that the model achieved a higher secrecy rate even in the presence of eavesdropper. Furthermore, Chen et al. [42] proposed an AO technique to maximize the SR in a downlink MISO broadcast network with multiple eavesdroppers. According to the results of simulations conducted under various practical constraints on RIS reflecting elements, the proposed technique achieved a higher SR with an improved PLS. A semidefinite programming relaxation and policy gradient descent technique was proposed to achieve higher secrecy rate while minimizing the transmission power [145]. The simulations were conducted in rank-one and rank-rank channels scenarios in the RIS-MISO model. The results showed an improved PLS and an improvement for the transmission power and secrecy rate. Furthermore, aiming to maximize the SR while satisfying the unit-modulus constraint on passive beamforming at RIS and transmit power constraint at the beamforming of BS, Zhou et al. [146] proposed successive convex approximation (SCA) to design a robust secure system under the transceiver hardware constraints. Simulation results showed that proposed technique achieved a higher SR and was more robust to the hardware constraints than the traditional techniques that do not consider the effect of hardware impairments. Finally, Si et al. [147] formulated the problem of maximizing the covert transmission rate as SDR to jointly optimize the RIS phase shift and transmit beamforming. Numerical results revealed that proposed optimization technique achieved a higher covert transmission rate and improved the PLS of RIS-assisted wireless network.

B. RIS-AIDED INTEGRATED SENSING AND COMMUNICATIONS

Deployment of RISs in ISAC networks yielded promising results, as it can create a virtual LOS communication links

TABLE 6. RIS-assisted eavesdropper attack in 6G applications.

Reference	Application	Algorithm	Contributions	Performance
[144]	Wireless	Semidefinite programming relaxation	Development of a robust cooperative jamming and beamforming design under an imperfect CSI to maximize EE	Maximizing energy efficiency and secrecy rate.
[41]		Manifold optimization and fractional programming	Proposal of an alternating optimization technique to design optimal phase and beamforming design to maximize secrecy rate	Higher secrecy rate.
[42]		Path following and alternating optimization	Maximization of SR based on zero-forcing beamforming and path-following algorithm	Achieving minimum secrecy rate.
[145]		Semidefinite programming relaxation and policy gradient descent	Minimizing the transmit power and improving SR in RIS for rank-one and rank-rank channels	Higher secrecy performance.
[146]		Successive convex approximation	Maximizing the SR while guaranteeing unit-modulus constraint on passive beamforming at the RIS under hardware impairment constraint	Robust secrecy rate with hardware impairments.
[147]		Gaussian randomization, SDR and AO	Formulating a joint transmit beamforming and RIS phase shift under partial CSI.	Maximizing covert transmission rate.
[89]	Covert	Penalty successive convex approximation (PSCA)	The PSCA algorithm to design the RIS reflecting coefficient and transmit power to improve covertness performance	Higher SNR.
[9]		One-dimensional search	Development a robust design to achieve optimal RIS reflection amplitude and transmit power	Improved achievable covertness.
[148]		SDR, Gaussian random	Maximizing covert communication with the presence of both noise information uncertainty and channel information uncertainty at the eavesdropper	Higher covert rate performance.
[55]	MIMO	Integer linear program (ILP)	An ILP to maximize the covert communication	Improvement of covert rate performance.
[149]		SCA	Optimizing active and passive beamformers for the maximization of covert rate in presence of warden	Higher covert rate gain.
[59]		AO	AO algorithm to design the beamforming of RIS and UAV BS to maximize the SR for RIS-assisted mmWave network	Minimizing SINR at the Eavesdropper.

for both sensing and communication to enhance the capacity. While several previous studies investigated the role of RIS in ISAC and their potential in increasing the target sensing capability [156], [157], [158], in most of this research, it was assumed that the target cannot intercept the transmitted signals. In ISAC networks, the transmitted signal contains both sensing and communication signals that can be intercepted by intruders. Furthermore, employing AN at the transmitting nodes, Su et al. [159] developed a PLS framework and formulated the optimization problem as fractional programming (FP) to minimize the SINR at the radar targets and to maximize the secrecy rate in the ISAC network. The numerical results revealed that, although highest secrecy rate was achieved, the model considered that both perfect CSI and precise location of the target were known at BS. This makes the PLS techniques developed for the traditional ISAC networks not applicable in the presence of RIS. In another relevant study, Hua et al. [160] investigated the RIS-assisted ISAC system for improving the PLS while considering the communication and sensing mechanism. A penalty-based algorithm was proposed to jointly optimize radar beamformers, RIS phase shifts, and communication beamformers to maximize communication and sensing considering multiple communication users and an eavesdropping target. The simulations results achieved tolerable information leakage to the eavesdropping target and minimum SINR for users.

TABLE 7. RIS-assisted eavesdropper attack in non-terrestrial networks.

Reference	Application	Algorithm	Contributions	Performance
[150]	UAV	Iterative algorithm	An iterative technique to optimize the trajectory of UAV and phase shift of RIS under the eavesdropper	Maximizing secrecy rate.
[151]		SDR, SCA, and S-procedure	A robust and secure framework to maximize the SR in an imperfect CSI	Maximizing the average worst-case secrecy rate.
[152]		Convex approximation	Secure EE and PLS of the network	Higher secrecy rate.
[153]		AO	Formulation of an AO to optimize the UAV trajectory and transmit power, phase shift of RIS with eavesdropper	Maximizing secrecy rate.
[60]	Satellite	AO algorithm	An AO technique to minimize the SINR at the destination eavesdropper	Higher secrecy gain and reduced target SINR.
[154]		RIS deployment	Deployed RIS with SAGIN to improve the connectivity, wireless coverage, and the PLS	Higher transmission rate.
[155]		Two-hop algorithm	A two-hop RIS-assisted algorithm to improve the secrecy rate from the ground station to satellite communication	Maximizing secure transmission probability.

C. RIS-ASSISTED NON-TERRESTRIAL NETWORKS

Next-generation communication networks can achieve ubiquitous and user-centric connectivity for 6G networks through orchestration of non-terrestrial and terrestrial networks [161]. In what follows, we discuss PLS for non-terrestrial networks from UAV and satellite communication perspectives.

1) UAV NETWORKS

Fang et al. [150] proposed an iterative technique for a robust design to optimize the trajectory of UAV and phase shift of RIS under the eavesdropper. The RIS-assisted UAV framework achieved an improved secrecy rate for the transmission and improved the PLS security. Furthermore, Li et al. [151] presented three algorithms—namely, S-procedure, SCA, and SDR—to improve the PLS and secrecy rate of the network. The proposed algorithm was found to optimize the users' transmit power, beamforming of RIS, and trajectory of UAV in the presence of eavesdropper under an imperfect CSI. A convex approximation technique was proposed to optimize the phase shift of RIS and trajectory of UAVs under the eavesdropper [152]. The proposed algorithm maximized the secure EE and PLS of the network. In another study, Fang et al. [153] developed a robust secure framework to improve the PLS of RIS-assisted UAV framework to maximize the secrecy rate, proposing the AO to optimize the UAV trajectory and transmit power, and phase shift of RIS with the presence of an eavesdropper. Numerical results showed an improved secrecy rate in RIS- assisted UAV network. Furthermore, Sun et al. [59] proposed an AO algorithm to design the beamforming of RIS and UAV BS for RIS-UAV assisted mmWave network to maximize the SR in the presence of eavesdropper. The results showed that, as compared to other techniques, the proposed approach achieved a higher secrecy rate.

2) SATELLITE NETWORKS

Xu et al. [60] developed an AO technique to minimize the destination SINR at the eavesdropper to limit the maximum interference at the satellite user and guarantee reliable signal strength at the terrestrial network user. The simulation results achieved a higher secrecy gain and significantly reduced the target SINR at the eavesdropper. In an another study on the role of integrating RIS with space-air-ground integrated network (SAGIN), Xu et al. [154] found that RIS-aided SAGIN can significantly improve the connectivity, wireless coverage as well as the PLS. Furthermore, in an investigation on the deployment of RISs to improve the PLS in satellite communication system, Ngo et al. [155] proposed a two-hop content delivery technique to improve the secrecy rate from the ground station to satellite communication by deploying RIS.

The aforementioned PLS technique developed for RIS network assumes protecting the transmitted data against the eavesdropping. However, privacy issues cannot be addressed by merely considering the presence of transmissions. To properly address the issue, the covert communication paradigm capable of preserving a high level privacy and security in RIS was introduced [90].

D. RIS-ASSISTED COVERT COMMUNICATION

In a study introducing a penalty successive convex approximation (PSCA) algorithm to design the RIS reflecting coefficient and transmit power considering the covertness communication without Willie's instantaneous CSI and global CSI, Zhou et al. [89] found that RIS-assisted networks

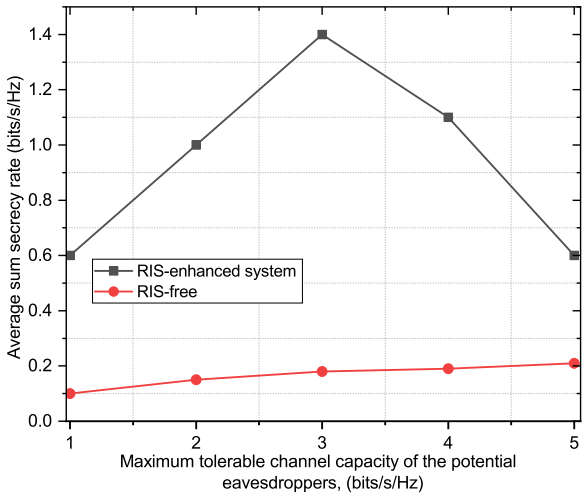

FIGURE 5. Performance of average secrecy rate (bits/s/Hz) with potential eavesdroppers.

can outperform traditional networks in the context of covert communication. Furthermore, Wu et al. [9] proposed a one-dimensional search method to optimize the optimal RIS reflection amplitude and transmit power in RIS-aided covert network. The model assumed that Willies statistical CSI is available globally. Numerical results showed that the proposed technique achieved maximum covertness as compared to the condition without the use of the RIS approach. Several other studies proposed an RIS-assisted framework for covert communication in NOMA network [55], [149]. The proposed approach was found to be capable of varying the legitimate information transmission environment from the malicious detection and increasing covert communication. Extant research on RIS-enabled covert communication considers only either the presence of channel information uncertainty or noise information uncertainty at the eavesdropper. Moreover, in another paper, [148] considered channel information uncertainty at the legitimate transmitter and noise information uncertainty at the eavesdropper. However, due to calibration error, as well as variation in the environmental noise and temperature, channel information uncertainty and noise information uncertainty at the eavesdropper could not be avoided. To address the issue, Zou et al. [148] proposed a SDR technique for covert communication under the noise information and channel information uncertainty constraint at the eavesdropper. The corresponding simulation results revealed that, as compared to baseline schemes, the proposed technique achieved a higher covert communication.

E. CASE STUDY

The performance of PLS with a RIS-empowered system is evaluated in terms of the average secrecy rate compared to the baseline scheme without RIS architecture. The scenario allows a maximum tolerable channel capacity for all eavesdroppers. We assume an equal maximum tolerable channel capacity for all eavesdroppers. Fig. 5 shows that the system secrecy rate is almost zero when RIS is not deployed. This is due to the weak LOS between legitimate users and AP. In other words, secure wireless communication cannot be achieved for blocked users due to an unfavorable wireless propagation environment. Furthermore, the RIS-empowered wireless system achieves a higher average secrecy rate than the RIS-free environment, which confirms that deployment of RIS can make the wireless system more secure.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

6G network can be a promising paradigm to significantly boost privacy and security of wireless communications. Emerging as a potential solution for B5G and 6G networks, RISs can improve communication performance by dynamically tuning phase shifts of the transmission signal. However, due to RIS elements' simpler configuration and cost-effectiveness, RIS-enabled systems are vulnerable to several types of security threats. In this section, we provide a succinct summary of current challenges and future research directions to address privacy and security concerns of RIS-enabled 6G communication systems (see Table 8 for a summary).

A. AI-ENABLED PRIVACY PRESERVING TECHNIQUES

The evolution of 6G technology is expected to lead to a massive increase in AI-based smart applications that will require customized context-aware privacy solutions. Because of complexity and diversity of new privacy challenges, traditional privacy-preserving techniques might not perform well for RIS-assisted next-generation wireless applications. In this context, in order to adequately address the growing privacy and security concerns in modern wireless networks, it is imperative to identify innovative ideas.

One such promising solution to preserve privacy of RIS-enabled future wireless systems is distributed ledger technologies, such as Blockchain. Blockchain offers many privacy and security features, including anonymity, verifiability, transparency, and immutability. It also provides access control optimization, secure data sharing, effective monitoring, traceability, as well as ensures integrity of data and efficient accountability [162].

Another actively investigated research topic to ensure privacy protection is federated learning (FL) [163]. FL is a distributed ML technique that can locally train models using a generated source with a massive volume of data. Instead of sending a raw dataset for training, each learner in local networks forwards their aggregated weights to a global FL model. By means of following the idea of bringing the code to the data, instead of the data to the code, FL can address some of the major challenges associated with data locality, data ownership, and data privacy [164], [165]. Several recent studies [166], [167] have leveraged FL algorithm in RIS-aided systems and obtained promising results. Owing to their privacy-preserving characteristic, FL algorithm is expected to yield noteworthy results in terms of secure design and

TABLE 8. Summary of challenges and future research directions of security attacks in future RIS-assisted 6G networks.

Challenge	Description	Research directions
Context-aware privacy solutions	Traditional AI techniques for privacy preservation cannot perform well for RIS-assisted communication due to the diversity and complexity of new privacy challenges	Novel ML techniques such as federated learning, differential privacy, and distributed ledger technologies (e.g., Blockchain) to address security constraints
Channel state information	Multi-RISs deployment in noisy and random networks will result in under- estimation of network states and difficulty in predicting security threats	Novel multi-agent RL frameworks and digital twin techniques to accurately predict security threats in RIS networks
Physical layer security	Multi-RISs deployment in a cell will result in channel fading and noise in the signal and potentially lead to misclassification at the AP side between an eavesdropper and an illegitimate user	Novel deep learning, molecular communication, PLS solutions, and federated RL techniques to increase RIS network privacy
End-to-End network security	RIS-assisted network requires intelligent programmable interfaces to deploy security policies	Novel network function virtualization (NFV) and software-defined networking (SDN) frameworks to proactively detect RIS network security threats
Complex and dynamic wireless environment	RIS networks will be based on UAVs, and highly mobile and heterogeneous networks and existing optimization techniques cannot detect the security threats	Novel multi-agent reinforcement learning integrated with FL techniques to mitigate security and privacy attacks
Illegal Reconfigurable Intelligent Surfaces (IRIS)	IRIS will be exposed to leakage/interference and passive jamming attacks that need to be mitigated	Novel multi-agent reinforcement learning (MARL) and cooperative nodes paradigm to detect security attacks

deployment of multiple RISs in 6G systems, which makes these algorithms a potential domain for further research. In the context of attempts to achieve a higher accuracy along with privacy in 6G networks, deep reinforcement learning (DRL)-based FL and transfer FL techniques are getting more scholarly attention. The main reason for using DRL-based FL techniques for privacy is that these techniques can explore the environment and provide a real-time remedial solution for privacy preservation when under attack.

Another possible solution to address the challenges anticipated in future 6G applications is privacy protection using differential privacy (DP) schemes [168], [169]. The DP operation involves perturbing actual data using artificially designed random noise functions prior to transmitting the final output to the allocated server, thus preventing attackers from conducting received data analysis and capturing personal details from user data. Integrating RISs with DP techniques can preserve end users' privacy while maintaining quality communication. However, while further research in this direction may lead to significant improvements in the performance of 6G systems while ensuring user privacy, available research on this topic remains very limited [91]. Another way to secure communications is using homomorphic encryption techniques where public and private keys are distributed among LUs. In that case, even if RISs are compromised and used to direct the signals to the unintended user, the adversary will not be able to decrypt the information.

B. INTEGRATED SENSING AND COMMUNICATIONS

In the ISAC network, both radar and communication signals are transmitted on the same frequency band, which makes data transmission to both radar targets and communication users more complex because of the higher risks of security threats by eavesdropper or unauthorized users. The use of RIS, which allows for intelligent tuning of the amplitude and phase shifts of the RIS elements to increase the LOS signal towards the legitimate user instead of the eavesdropper, can significantly enhance the PLS. However, existing RIS-aided ISAC networks assume known location and knowledge of RIS parameters and locations, which are challenging to acquire for mobile next-generations networks, such as the emerging THz and mmWave networks. In this respect, data-driven techniques such as DL, RL and DT can be effective to learn the dynamic characteristics and parameters of the RIS-assisted ISAC networks to increase the PLS.

C. NON-TERRESTRIAL NETWORKS

Non-terrestrial networks will have highly mobile and dynamic characteristics due to mobility of space and aerial

platforms, as well as random time-varying channels in underwater and maritime propagation media. Developing PLS is more challenging for RIS-assisted non-terrestrial networks, as it requires accurate channel estimation. Accordingly, further research on the role of intelligent signal processing and data-driven techniques such as DL, FL and RL would be needed for an accurate channel estimation in dynamic non-terrestrial networks.

D. DIGITAL TWIN

An important candidate for bridging the connection gap between digital systems and physical spaces is the digital twin, which involves the construction of digital replicas of physical units (e.g., physical objects, machines, devices, etc.) at the server based on their real-time running status and historical data [170]. A digital twin can facilitate reliable communication and real-time interactions between physical entities and digital space, thus leading to the operation optimization of physical systems. Although RIS is a key technology for 6G, an important challenge that remains is the optimal configuration of a large number of RIS elements. A digital-twin framework for RIS-enabled 6G wireless networks can allow for an optimally controlled automation at different granularities [171]. Digital-twin technology can also be used for the development of a practical RIS solution ensuring an improved security, privacy, and overall performance of RIS-assisted 6G systems. Accordingly, the RISs controller can be trained in a virtual environment under different attack scenarios to find out how to counter those attacks to ensure secure and stable communication between LUs.

E. SOFTWARE-DEFINED NETWORKING AND NETWORK FUNCTION VIRTUALIZATION

RIS-assisted 6G systems can unify the concepts of artificial intelligence, network function virtualization, and software-defined networking in a complex environment to not just provide the requisite services, but, most importantly, to ensure end-to-end network security [172]. Using AI to proactively detect threats and initiate the transfer of security functions throughout the RIS-assisted network, programmable interfaces may allow for the deployment of security functions, similar to virtualized network functions (VNFs), in a virtual environment using AI.

F. MULTI AGENT REINFORCEMENT LEARNING

Several recent studies have used reinforcement learning to achieve smart beamforming at the base station against eavesdroppers in complicated scenarios (RL) [2], [3], [173], [174]. However, RIS-assisted secure systems require the optimization of BS's transmitting beamforming and the RISs reflecting beamforming. Considering an imperfect CSI and multiple eavesdroppers, neither DRL nor RL has been explored for the optimization of the aforementioned two types of beamforming. In a recent study on an RIS-enabled secure communication system, Yang et al. [175] proposed a novel DRL-based secure beamforming strategy to maximize the secrecy rate of the system in the presence of multiple eavesdroppers while considering the LU's QoS requirements. This approach yielded promising results that pave a path for further research on the adoption of multi-agent RL to achieve improved secrecy rates in RIS-aided 6G communication systems.

G. QUANTUM COMMUNICATION

Another promising communication technology for 6G networks that can considerably improve the reliability and security of data transmission is quantum communication. An attacker's attempts to eavesdrop or replicate something in quantum communication results in an evident impact on the quantum state, so the recipient instantly becomes aware of the attacker's interference [176].

Theoretically, quantum communication can offer high-level security for long-distance communications [177]. However, not all privacy and security problems can be solved using quantum communication. Despite substantial developments in implementing quantum cryptography, several major challenges in the materialization of long-distance quantum communications operation remain, such as errors and fiber attenuation. In this respect, Hu et al. [178] speculated that different innovative techniques and varied quantum encryption modes, such as quantum dense coding, quantum teleportation, quantum secure direct communication, quantum secret sharing, quantum key distribution, among others, might be required to ensure secure quantum communication. In another recent study, several quantum schemes that employ quantum key distribution models to protect key security were elaborated [179]. Incorporation of quantum technology in RIS-assisted 6G networks can also elevate the quality of communication to a level unattainable for conventional communication systems. However, research in this area is currently in its infancy, and plenty of work needs to be done.

H. PHYSICAL LAYER SECURITY

Security procedures embedded across different network layers might be jointly used to implement redundant protection. The evolving 6G technology can leverage PLS mechanisms to provide an additional protection layer in RIS-assisted systems with regard to novel enabling technologies. A budding technology for 6G in the healthcare domain is molecular communication. The main concept behind molecular communication involves the use of biochemical signals to transmit information [162]. Molecular communication handles very sensitive data with various privacy and security challenges associated with the encryption, authentication, and communication processes, which makes it indispensable to increase security of this technology. However, while several studies have identified key directions for secure molecular communication [180], [181], in order to achieve the results that the existing systems cannot offer, intensive research is needed

to develop practical molecular communication schemes for RIS-assisted 6G networks.

Among the leading technologies for improving security in RIS-assisted 6G networks are THz communications (1GHz -10 THz). This frequency band is associated with an increase in the transmitted signals' directionality, which enables the confinement of illegitimate users on the similar constricted route of LUs for the signal interception and thus improves the physical layer security. Yet, vulnerabilities of THz communications include data transmission exposure, malicious behavior, and access control attacks. Accordingly, in order to secure THz transmissions, novel PLS solutions, such as the employment of devices at THz frequencies and electromagnetic signature of materials for authentication mechanisms, are needed [3], [182].

I. MEASURES AGAINST ILLEGAL RECONFIGURABLE INTELLIGENT SURFACES

In order to safeguard 6G communication against IRIS-based attacks, several open research challenges need to be addressed. Some of these challenges include (1) passive jamming where an IRIS might be employed directly in authorized systems as a passive jammer to silently affect the PLS [124]; and (2) hybrid interference/leakage attack that is volatile and may result in catastrophic threats to PLS. What worsens the situation is that the traditional beamforming and channel estimation become non-functional under such attack.

Although AN technology has demonstrated significant results in countering IRIS-based threats [51], the impact of IRIS can be considerably stronger for the complex 6G systems. Therefore, preventing illegal deployment of RISs requires more powerful and effective countermeasures. Several potential directions include random phase-shift keying symbols-based detection mechanisms, angle-of-arrival-based detection schemes, and so on. One more solution is the adoption of DRL, which is particularly useful for systems with time-varying and uncertain channels. In the DRL architecture, a decision to enhance the system's performance is made based only on the CSI of legitimate links and the current secrecy rate. If a proper learning strategy and valid neural networks are implemented, the CSI of illegal links may not be necessary for attaining optimum phase shifts configuration and beamforming policy. Yet another emerging technology for combating IRIS-aided attacks is using cooperative nodes that broadcast a joint orthogonal pilot sequence at UL channel estimation, which then mutually tries to reduce pilot contamination within the network.

VI. CONCLUSION

Privacy and security are key performance indicators of a wireless system. The enhanced Internet access of future wireless networks will massively connect those networks with heterogeneous networks of terrestrial nodes, satellites, physical and virtual telecom networks, enterprises, and so forth. In recent years, RIS has emerged as a key enabler technology for 6G, showing promising results in enhancing the overall security and privacy of wireless systems. However, RIS remains vulnerable to different security threats, and its use may result in detrimental interferences to wireless communications. This makes RIS a noteworthy example of how novel technologies can bring a shift in attack taxonomies, as previously complicated attacks become tractable. To date, exploitation of RIS as a malicious tool to attack wireless communication systems has not been sufficiently investigated in the literature. In this study, we analyzed unavoidable security threats to 6G networks arising from the illegal deployment and malicious use of RISs and, based on the results, identified open research challenges and potential future directions in this area. Accordingly, this study may serve as an important reference future research on 6G security, in general, and RIS-aided 6G systems, in particular.

ACKNOWLEDGMENT

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the Ministry of Education, Singapore.

REFERENCES

[1] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[2] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, Aug. 2020.

[3] C. Huang et al., "Multi-hop RIS-empowered terahertz communications: A DRL-based hybrid beamforming design," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1663–1677, Jun. 2021.

[4] L. Wei, C. Huang, G. C. Alexandropoulos, C. Yuen, Z. Zhang, and M. Debbah, "Channel estimation for RIS-empowered multi-user MISO wireless communications," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4144–4157, Jun. 2021.

[5] L. Wei et al., "Joint channel estimation and signal recovery for RIS-empowered multi-user communications," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4640–4655, Jul. 2022.

[6] X. Yuan, Y.-J. A. Zhang, Y. Shi, W. Yan, and H. Liu, "Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 136–143, Apr. 2021.

[7] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[8] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[9] C. Wu, S. Yan, X. Zhou, R. Chen, and J. Sun, "Intelligent reflecting surface (IRS)-aided covert communication with Warden's statistical CSI," *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1449–1453, Jul. 2021.

[10] B. Zheng, C. You, W. Mei, and R. Zhang, "A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1035–1071, 2nd Quart., 2022.

[11] C. Pan et al., "An overview of signal processing techniques for RIS/IRS-aided wireless systems," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 883–917, Aug. 2022.

[12] T. Zhou, K. Xu, Z. Shen, W. Xie, D. Zhang, and J. Xu, "AoA-based positioning for aerial intelligent reflecting surface-aided wireless communications: An angle-domain approach," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 761–765, Apr. 2022.

[13] C. You, B. Zheng, W. Mei, and R. Zhang, "How to deploy intelligent reflecting surfaces in wireless network: BS-side, user-side, or both sides?" *J. Commun. Inf. Netw.*, vol. 7, no. 1, pp. 1–10, 2022.

[14] R. Alghamdi et al., "Intelligent surfaces for 6G wireless networks: A survey of optimization and performance analysis techniques," *IEEE Access*, vol. 8, pp. 202795–202818, 2020.

[15] P. Zeng, D. Qiao, Q. Wu, and Y. Wu, "Throughput maximization for active intelligent reflecting surface-aided wireless powered communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 992–996, May 2022.

[16] X. Shao, C. You, W. Ma, X. Chen, and R. Zhang, "Target sensing with intelligent reflecting surface: Architecture and performance," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 7, pp. 2070–2084, Jul. 2022.

[17] W. Mei, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless networks: From single-reflection to multireflection design and optimization," *Proc. IEEE*, vol. 110, no. 9, pp. 1380–1400, Sep. 2022.

[18] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[19] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[20] M. Zeng et al., "IRS-empowered wireless communications: State-of-the-art, key techniques, and open issues," 2021, *arXiv:2101.07394*.

[21] S. Gong et al., "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 4th Quart., 2020.

[22] H. Wymeersch, J. He, B. Denis, A. Clemente, and M. Juntti, "Radio localization and mapping with reconfigurable intelligent surfaces: Challenges, opportunities, and research directions," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 52–61, Dec. 2020.

[23] N. Rajatheva et al., "Scoring the terabit/s goal: Broadband connectivity in 6G," 2020, *arXiv:2008.07220*.

[24] C. Pan et al., "Multicell MIMO communications relying on intelligent reflecting surfaces," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5218–5233, Aug. 2020.

[25] J. Zhao, "A survey of intelligent reflecting surfaces (IRSs): Towards 6G wireless communication networks with massive MIMO 2.0," 2019, *arXiv:1907.04789*.

[26] H. Abumarshoud, L. Mohjazi, O. A. Dobre, M. Di Renzo, M. A. Imran, and H. Haas, "LiFi through reconfigurable intelligent surfaces: A New Frontier for 6G?" 2021, *arXiv:2104.02390*.

[27] A. Almohamad et al., "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, 2020.

[28] X. Ma et al., "Intelligent reflecting surface enhanced indoor terahertz communication systems," *Nano Commun. Netw.*, vol. 24, May 2020, Art. no. 100284.

[29] J. Qiao, C. Zhang, A. Dong, J. Bian, and M.-S. Alouini, "Securing intelligent reflecting surface assisted terahertz systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8519–8533, Aug. 2022.

[30] Y. Zhu, B. Mao, and N. Kato, "Intelligent reflecting surface in 6G vehicular communications: A survey," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 266–277, 2022.

[31] W. Jiang and H. D. Schotten, "Dual-beam intelligent reflecting surface for millimeter and THz communications," in *Proc. IEEE 95th Veh. Technol. Conf. (VTC-Spring)*, 2022, pp. 1–6.

[32] B. Ning, T. Wang, P. Wang, Z. Chen, and J. Fang, "Space-orthogonal scheme for IRSs-aided multi-user MIMO in mmWave/THz communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2022, pp. 3478–3483.

[33] Y. Xing, F. Vook, E. Visotsky, M. Cudak, and A. Ghosh, "Raytracing-based system performance of intelligent reflecting surfaces at 28 GHz," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2022, pp. 498–503.

[34] S. Noh, J. Lee, G. Lee, K. Seo, Y. Sung, and H. Yu, "Channel estimation techniques for RIS-assisted communication: Millimeter-wave and sub-THz systems," *IEEE Veh. Technol. Mag.*, vol. 17, no. 2, pp. 64–73, Jun. 2022.

[35] T. Sharma, A. Chehri, and P. Fortier, "Reconfigurable intelligent surfaces for 5G and beyond wireless communications: A comprehensive survey," *Energies*, vol. 14, no. 24, p. 8219, 2021.

[36] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6G wireless networks," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 184–191, Dec. 2021.

[37] B. Zheng, S. Lin, and R. Zhang, "Intelligent reflecting surface-aided LEO satellite communication: Cooperative passive beamforming and distributed channel estimation," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 10, pp. 3057–3070, Oct. 2022.

[38] A. M. Elbir, K. V. Mishra, M. B. Shankar, and S. Chatzinotas, "The rise of intelligent reflecting surfaces in integrated sensing and communications paradigms," *IEEE Netw.*, early access, Dec. 26, 2022, doi: 10.1109/MNET.128.2200446.

[39] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, 2019.

[40] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[41] K. Feng, X. Li, Y. Han, S. Jin, and Y. Chen, "Physical layer security enhancement exploiting intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 734–738, Mar. 2021.

[42] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[43] S. Sun, F. Yang, J. Song, and Z. Han, "Optimization on multiuser physical layer security of intelligent reflecting surface-aided VLC," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1344–1348, Jul. 2022.

[44] Z. Tang, T. Hou, Y. Liu, J. Zhang, and L. Hanzo, "Physical layer security of intelligent reflective surface aided NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7821–7834, Jul. 2022.

[45] Y. Wang, W. Shi, M. Huang, F. Shu, and J. Wang, "Intelligent reflecting surface aided secure transmission with colluding eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 10155–10160, Sep. 2022.

[46] M. F. Ahmed, K. P. Rajput, N. K. D. Venkategowda, K. V. Mishra, and A. K. Jagannatham, "Joint transmit and reflective beamformer design for secure estimation in IRS-aided WSNs," *IEEE Signal Process. Lett.*, vol. 29, pp. 692–696, 2022.

[47] L. Jin, X. Xu, S. Han, J. Liu, R. Meng, and H. Chen, "RIS-assisted physical layer key generation and transmit power minimization," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 2065–2070.

[48] S. Sarp, H. Tang, and Y. Zhao, "Use of intelligent reflecting surfaces for and against wireless communication security," in *Proc. IEEE 4th 5G World Forum (5GWF)*, 2021, pp. 374–377.

[49] H. Tang, S. Sarp, Y. Zhao, W. Wang, and C. Xin, "Security and threats of intelligent reflecting surface assisted wireless communications," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2022, pp. 1–9.

[50] W. Shi, W. Xu, X. You, C. Zhao, and K. Wei, "Intelligent reflection enabling technologies for integrated and green Internet-of-Everything beyond 5G: Communication, sensing, and security," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 147–154, Apr. 2023.

[51] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, Jun. 2022.

[52] M. Munochiveyi, A. C. Pogaku, D.-T. Do, A.-T. Le, M. Voznak, and N. D. Nguyen, "Reconfigurable intelligent surface aided multi-user communications: State-of-the-art techniques and open issues," *IEEE Access*, vol. 9, pp. 118584–118605, 2021.

[53] R. Liu, Q. Wu, M. Di Renzo, and Y. Yuan, "A path to smart radio environments: An industrial viewpoint on reconfigurable intelligent surfaces," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 202–208, Feb. 2022.

[54] X. Yu, V. Jamali, D. Xu, D. W. K. Ng, and R. Schober, "Smart and reconfigurable wireless communications: From IRS modeling to algorithm design," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 118–125, Dec. 2021.

[55] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang, and D. Niyato, "Intelligent reflecting surface enabled covert communications in wireless networks," *IEEE Netw.*, vol. 34, no. 5, pp. 148–155, Sep./Oct. 2020.

[56] J. Xu et al., "Reconfiguring wireless environment via intelligent surfaces for 6G: Reflection, modulation, and security," *Sci. China Inf. Sci.*, vol. 66, Nov. 2022, Art. no. 130304.

[57] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2018.

[58] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2658–2693, 4th Quart., 2020.

[59] S. Sun, T. Wang, F. Yang, J. Song, and Z. Han, "Intelligent reflecting surface-aided visible light communications: Potentials and challenges," *IEEE Veh. Technol. Mag.*, vol. 17, no. 1, pp. 47–56, Mar. 2022.

[60] S. Xu, J. Liu, Y. Cao, J. Li, and Y. Zhang, "Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 2007–2011, Feb. 2021.

[61] M. Jian et al., "Reconfigurable intelligent surfaces for wireless communications: Overview of hardware designs, channel models, and estimation techniques," *Intell. Converg. Netw.*, vol. 3, no. 1, pp. 1–32, 2022.

[62] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.

[63] W. Song, S. Rajak, S. Dang, R. Liu, J. Li, and S. Chinnadurai, "Deep learning enabled IRS for 6G intelligent transportation systems: A comprehensive study," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 24, 2022, doi: 10.1109/TITS.2022.3184314.

[64] Z. Kang, C. You, and R. Zhang, "Active-passive IRS aided wireless communication: New hybrid architecture and elements allocation optimization," 2022, *arXiv:2207.01244*.

[65] C. You and R. Zhang, "Wireless communication aided by intelligent reflecting surface: Active or passive?" *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2659–2663, Dec. 2021.

[66] R. Long, Y.-C. Liang, Y. Pei, and E. G. Larsson, "Active reconfigurable intelligent surface-aided wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4962–4975, Aug. 2021.

[67] Y. Liu et al., "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021.

[68] Y. Ge and J. Fan, "Beamforming optimization for intelligent reflecting surface assisted MISO: A deep transfer learning approach," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3902–3907, Apr. 2021.

[69] S. Yin, Y. Li, Y. Tian, and F. R. Yu, "Intelligent reflecting surface enhanced wireless communications with deep-learning-based channel prediction," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 1049–1053, Jan. 2022.

[70] M. Noor-A-Rahim et al., "Towards industry 5.0: Intelligent reflecting surface (IRS) in smart manufacturing," *IEEE Commun. Mag.*, vol. 60, no. 10, pp. 72–78, Oct. 2022.

[71] E. Björnson and L. Sanguinetti, "Power scaling laws and near-field behaviors of massive MIMO and intelligent reflecting surfaces," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1306–1324, 2020.

[72] L. Zhang, Y. Wang, W. Tao, Z. Jia, T. Song, and C. Pan, "Intelligent reflecting surface aided MIMO cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11445–11457, Oct. 2020.

[73] P. Zeng, D. Qiao, H. Qian, and Q. Wu, "Joint beamforming design for IRS aided multiuser MIMO with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10729–10743, Oct. 2022.

[74] M. AlaaEldin, E. Alsusa, and K. G. Seddik, "IRS-assisted physical layer network coding over two-way relay fading channels," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8424–8440, Aug. 2022.

[75] J. Sun, W. Gan, Z. Chen, J. Li, and P. S. Yu, "Big data meets metaverse: A survey," 2022, *arXiv:2210.16282*.

[76] 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 Veh. Technol. Mag.*, vol. 14, no. 3, pp. 18–27, Sep. 2019.

[77] N. Promwongsa et al., "A comprehensive survey of the tactile Internet: State-of-the-art and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 472–523, 1st Quart., 2020.

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

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

[80] C. Huang et al., "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[81] F. Rinaldi et al., "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165178–165200, 2020.

[82] 3GPP. "Solutions for NR to support non-terrestrial networks (NTN)." 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/Arch./38_series/38.821/

[83] "3GPP release 18." 2022. [Online]. Available: https://www.3gpp.org/release18

[84] A. Chorti et al., "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[85] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, and F. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451–4463, May 2021.

[86] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for beyond 5G: Ultra secure low latency communications," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2232–2242, 2021.

[87] S. Soderi and R. De Nicola, "6G networks physical layer security using RGB visible light communications," *IEEE Access*, vol. 10, pp. 5482–5496, 2022.

[88] S. Yan, X. Zhou, D. W. K. Ng, J. Yuan, and N. Al-Dhahir, "Intelligent reflecting surface for wireless communication security and privacy," 2021, *arXiv:2103.16696*.

[89] X. Zhou, S. Yan, Q. Wu, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 532–547, Jan. 2022.

[90] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 19–25, Oct. 2019.

[91] Q. Pan, J. Wu, X. Zheng, W. Yang, and J. Li, "Differential privacy and IRS empowered intelligent energy harvesting for 6G Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22109–22122, Nov. 2022.

[92] Z. Chen, X. Ma, C. Han, and Q. Wen, "Towards intelligent reflecting surface empowered 6G terahertz communications: A survey," *China Commun.*, vol. 18, no. 5, pp. 93–119, 2021.

[93] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[94] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1743–1747, Oct. 2020.

[95] B. Ning, Z. Chen, W. Chen, and L. Li, "Improving security of THz communication with intelligent reflecting surface," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[96] R. W. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[97] Z. Ding and H. V. Poor, "A simple design of IRS-NOMA transmission," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1119–1123, May 2020.

[98] H. Yang et al., "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1963–1974, Mar. 2021.

[99] W. Khalid, H. Yu, D.-T. Do, Z. Kaleem, and S. Noh, "RIS-aided physical layer security with full-duplex jamming in underlay D2D networks," *IEEE Access*, vol. 9, pp. 99667–99679, 2021.

[100] H. A. U. Mustafa, M. A. Imran, M. Z. Shakir, A. Imran, and R. Tafazolli, "Separation framework: An enabler for cooperative and D2D communication for future 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 419–445, 1st Quart., 2016.

[101] M. Jung, W. Saad, M. Debbah, and C. S. Hong, "Asymptotic optimality of reconfigurable intelligent surfaces: Passive beamforming and achievable rate," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.

[102] C. So-In et al., "Performance analysis of an energy-harvesting IoT system using a UAV friendly jammer and NOMA under cooperative attack," *IEEE Access*, vol. 8, pp. 221986–222000, 2020.

[103] B. Tahir, S. Schwarz, and M. Rupp, "RIS-assisted code-domain MIMO-NOMA," in *Proc. IEEE 29th Eur. Signal Process. Conf. (EUSIPCO)*, 2021, pp. 821–825.

[104] W. Wang et al., "Secure beamforming for IRS-enhanced NOMA networks," *IEEE Wireless Commun.*, vol. 30, no. 1, pp. 134–140, Feb. 2023.

[105] J. Yuan, Y.-C. Liang, J. Joung, G. Feng, and E. G. Larsson, "Intelligent reflecting surface-assisted cognitive radio system," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 675–687, Jan. 2021.

[106] D. Pérez-Adán, Ó. Fresnedo, J. P. González-Coma, and L. Castedo, "Intelligent reflective surfaces for wireless networks: An overview of applications, approached issues, and open problems," *Electronics*, vol. 10, no. 19, p. 2345, 2021.

[107] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," 2021, *arXiv:2101.00292*.

[108] S. Huang, S. Wang, R. Wang, M. Wen, and K. Huang, "Reconfigurable intelligent surface assisted mobile edge computing with heterogeneous learning tasks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 2, pp. 369–382, Jun. 2021.

[109] X. Cao et al., "Massive access of static and mobile users via reconfigurable intelligent surfaces: Protocol design and performance analysis," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1253–1269, Apr. 2022.

[110] S. Mao et al., "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6647–6660, Jun. 2022.

[111] Y. Chen, Y. Wang, and L. Jiao, "Robust transmission for reconfigurable intelligent surface aided millimeter wave vehicular communications with statistical CSI," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 928–944, Feb. 2022.

[112] W. U. Khan et al., "Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces," 2022, *arXiv:2203.16907*.

[113] W. Yan, X. Yuan, Z.-Q. He, and X. Kuai, "Passive beamforming and information transfer design for reconfigurable intelligent surfaces aided multiuser MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1793–1808, Aug. 2020.

[114] M. R. Khandaker, C. Masouros, K.-K. Wong, and S. Timotheou, "Secure SWIPT by exploiting constructive interference and artificial noise," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1326–1340, Feb. 2019.

[115] G. Zhou, C. Pan, H. Ren, K. Wang, K. K. Chai, and K.-K. Wong, "User cooperation for IRS-aided secure MIMO systems," *Intell. Converg. Netw.*, vol. 3, no. 1, pp. 86–102, Mar. 2022.

[116] K. Tekbiyik, G. K. Kurt, A. R. Ektı, and H. Yanikomeroglu, "Reconfigurable intelligent surfaces empowered THz communication in LEO satellite networks," *IEEE Access*, vol. 10, pp. 121957–121969, 2022.

[117] K. Tekbıyık, G. K. Kurt, A. R. Ekti, and H. Yanikomeroglu, "Reconfigurable intelligent surfaces in action for nonterrestrial networks," *IEEE Veh. Technol. Mag.*, vol. 17, no. 3, pp. 45–53, Sep. 2022.

[118] C. Jiang, C. Zhang, L. Mu, Z. Zhang, and J. Ge, "Aerial RIS-aided physical layer security design for satellite communication among similar channels," *J. Inf. Intell.*, to be published.

[119] X. Wang, Z. Fei, J. Huang, and H. Yu, "Joint waveform and discrete phase shift design for RIS-assisted integrated sensing and communication system under Cramér–Rao bound constraint," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 1004–1009, Jan. 2022.

[120] H. Luo, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint beamforming design for RIS-assisted integrated sensing and communication systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13393–13397, Dec. 2022.

[121] K. Meng, Q. Wu, J. Xu, W. Chen, and Z. Feng, "UAV-enabled integrated sensing and communication: Opportunities and challenges," 2022, *arXiv:2206.03408*.

[122] K.-W. Huang and H.-M. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 345–359, Jan. 2021.

[123] J. Yang, X. Ji, F. Wang, K. Huang, and L. Guo, "A novel pilot spoofing scheme via intelligent reflecting surface based on statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12847–12857, Dec. 2021.

[124] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "IRS-based wireless jamming attacks: When jammers can attack without power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1663–1667, Oct. 2020.

[125] L. Hu, G. Li, H. Luo, and A. Hu, "On the RIS manipulating attack and its countermeasures in physical-layer key generation," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC-Fall)*, 2021, pp. 1–5.

[126] P. Staat, H. Elders-Boll, M. Heinrichs, C. Zenger, and C. Paar, "Mirror mirror on the wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces," 2021, *arXiv:2107.01709*.

[127] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022.

[128] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: Security issue in IoT network," in *Proc. IEEE 2nd Int. Conf. IoT Soc. Mobile Anal. Cloud (I-SMAC)*, 2018, pp. 104–107.

[129] H. Yang et al., "A programmable metasurface with dynamic polarization, scattering and focusing control," *Sci. Rep.*, vol. 6, no. 1, pp. 1–11, 2016.

[130] E. Basar, "Index modulation techniques for 5G wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 168–175, Jul. 2016.

[131] Y.-C. Liang, R. Long, Q. Zhang, J. Chen, H. V. Cheng, and H. Guo, "Large intelligent surface/antennas (LISA): Making reflective radios smart," *J. Commun. Inf. Netw.*, vol. 4, no. 2, pp. 40–50, 2019.

[132] X. Hou, C. Gao, Y. Zhu, and S. Yang, "Detection of active attacks based on random orthogonal pilots," in *Proc. IEEE 8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2016, pp. 1–4.

[133] H.-M. Wang, K.-W. Huang, and T. A. Tsiftsis, "Multiple antennas secure transmission under pilot spoofing and jamming attack," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 860–876, Apr. 2018.

[134] D. Hu, W. Zhang, L. He, and J. Wu, "Secure transmission in multi-cell multi-user massive MIMO systems with an active eavesdropper," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 85–88, Feb. 2018.

[135] Y. Wu, C.-K. Wen, W. Chen, S. Jin, R. Schober, and G. Caire, "Data-aided secure massive MIMO transmission under the pilot contamination attack," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4765–4781, Jul. 2019.

[136] X. Wang, M. Liu, D. Wang, and C. Zhong, "Pilot contamination attack detection using random symbols for massive MIMO systems," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, 2017, pp. 1–7.

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

[138] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.

[139] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.

[140] X. Liu, Y. Tao, C. Zhao, and Z. Sun, "Detect pilot spoofing attack for intelligent reflecting surface assisted systems," *IEEE Access*, vol. 9, pp. 19228–19237, 2021.

[141] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[142] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[143] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[144] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy efficient robust beamforming and cooperative jamming design for IRS-assisted MISO networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2592–2607, Apr. 2021.

[145] B. Feng, Y. Wu, and M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system," in *Proc. IEEE 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2019, pp. 1–6.
[146] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO system with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1309–1313, Jun. 2021.
[147] J. Si et al., "Covert transmission assisted by intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5394–5408, Aug. 2021.
[148] L. Zou, D. Zhang, M. Cui, G. Zhang, and Q. Wu, "IRS-assisted covert communication with eavesdropper's channel and noise information uncertainties," *Phys. Commun.*, vol. 53, Aug. 2022, Art. no. 101662.
[149] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, "Intelligent reflecting surface-assisted multi-antenna covert communications: Joint active and passive beamforming optimization," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3984–4000, Jun. 2021.
[150] J. Fang, Z. Yang, N. Anjum, Y. Hu, H. Asgari, and M. Shikh-Bahaei, "Secure intelligent reflecting surface assisted UAV communication networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2021, pp. 1–6.
[151] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust secure UAV communications with the aid of reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402–6417, Oct. 2021.
[152] W. Wang, H. Tian, W. Ni, and M. Hua, "Intelligent reflecting surface aided secure UAV communications," 2020, *arXiv:2011.04339*.
[153] S. Fang, G. Chen, and Y. Li, "Joint optimization for secure intelligent reflecting surface assisted UAV networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 276–280, Feb. 2021.
[154] S. Xu, J. Liu, T. K. Rodrigues, and N. Kato, "Envisioning intelligent reflecting surface empowered space-air-ground integrated network," *IEEE Netw.*, vol. 35, no. 6, pp. 225–232, Nov./Dec. 2021.
[155] Q. Ngo, K. Phan, A. Mahmood, and W. Xiang, "Physical layer security in IRS-assisted cache-enabled hybrid satellite-terrestrial networks," TechRxiv, 2022.
[156] X. Song, D. Zhao, H. Hua, T. X. Han, X. Yang, and J. Xu, "Joint transmit and reflective beamforming for IRS-assisted integrated sensing and communication," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 189–194.
[157] R. Liu, M. Li, Y. Liu, Q. Wu, and Q. Liu, "Joint transmit waveform and passive beamforming design for RIS-aided DFRC systems," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 995–1010, Aug. 2022.
[158] Z.-M. Jiang et al., "Intelligent reflecting surface aided dual-function radar and communication system," *IEEE Syst. J.*, vol. 16, no. 1, pp. 475–486, Mar. 2022.
[159] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 83–95, Jan. 2021.
[160] M. Hua, Q. Wu, W. Chen, O. A. Dobre, and A. L. Swindlehurst, "Secure intelligent reflecting surface aided integrated sensing and communication," 2022, *arXiv:2207.09095*.
[161] K. Tekbiyik, A. R. Ekti, G. K. Kurt, A. Gorcin, and H. Yanikomeroglu, "A holistic investigation of terahertz propagation and channel modeling toward vertical heterogeneous networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 14–20, Nov. 2020.
[162] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, 2020.
[163] M. Chen, N. Shlezinger, H. V. Poor, Y. C. Eldar, and S. Cui, "Communication-efficient federated learning," *Proc. Nat. Acad. Sci. USA*, vol. 118, no. 17, 2021, Art. no. e2024789118.
[164] K. Bonawitz et al., "Towards federated learning at scale: System design," in *Proc. Mach. Learn. Syst.*, vol. 1, 2019, pp. 374–388.
[165] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 46–51, Jun. 2020.
[166] L. Li et al., "Enhanced reconfigurable intelligent surface assisted mmWave communication: A federated learning approach," *China Commun.*, vol. 17, no. 10, pp. 115–128, 2020.
[167] W. Ni, Y. Liu, Z. Yang, H. Tian, and X. Shen, "Federated learning in multi-RIS aided systems," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9608–9624, Jun. 2022.
[168] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[169] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for Industrial Internet of Things: Opportunities, applications, and challenges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10430–10451, Jul. 2021.
[170] D. M. Botín-Sanabria et al., "Digital twin technology challenges and applications: A comprehensive review," *Remote Sens.*, vol. 14, no. 6, p. 1335, 2022.
[171] B. Sheen, J. Yang, X. Feng, and M. M. U. Chowdhury, "A digital twin for reconfigurable intelligent surface assisted wireless communication," 2020, *arXiv:2009.00454*.
[172] I. Ahmad et al., "The challenges of artificial intelligence in wireless networks for the Internet of Things: Exploring opportunities for growth," *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 16–29, Mar. 2021.
[173] C. Li, W. Zhou, K. Yu, L. Fan, and J. Xia, "Enhanced secure transmission against intelligent attacks," *IEEE Access*, vol. 7, pp. 53596–53602, 2019.
[174] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep reinforcement learning-enabled secure visible light communication against eavesdropping," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6994–7005, Jan. 2021.
[175] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 375–388, Jan. 2021.
[176] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.
[177] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart., 2018.
[178] J.-Y. Hu et al., "Experimental quantum secure direct communication with single photons," *Light Sci. Appl.*, vol. 5, no. 9, pp. e16144–e16144, 2016.
[179] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.
[180] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110687–110697, 2019.
[181] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 198–207, Sep. 2014.
[182] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. IEEE Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627.

FAISAL NAEEM (Member, IEEE) received the Ph.D. degree in electrical engineering from the National University of Computer and Emerging Sciences. He is currently working as a Postdoctoral Research Fellow with the Resilient Machine Learning Institute Centre, École de technologie supérieure, Montreal, Canada. His research interests are focused on developing artificial intelligence-based techniques specifically federated learning, semi-supervised learning, and reinforcement learning for resource management and security in reconfigurable intelligent surface and B5G/6G networks.

MANSOOR ALI (Member, IEEE) is working as a Postdoctoral Research Fellow with the Electrical Engineering Department, École de technologie supérieure, University of Quebec, Montreal, Canada. His research interests include the load forecasting in a power system network, fuzzy control, smart grids, security and privacy for cyber–physical systems, and digital twins.

GEORGES KADDOUM (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the École nationale supérieure de techniques avancées (ENSTA Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne (ENSTB), Brest, in 2005, and the Ph.D. degree (with Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. He is currently a Professor and the Tier 2 Canada Research Chair with the École de technologie supérieure (ÉTS), Université du Québec, Montreal, Canada, and a Faculty Fellow with the Cyber Security Systems and Applied AI Research Center, Lebanese American University. In 2014, he was awarded the ÉTS Research Chair in physical-layer security for wireless networks. Since 2010, he has been a Scientific Consultant in the field of space and wireless telecommunications for several U.S. and Canadian companies. He has published over 300 journals, conference papers, two chapters in books, and has eight pending patents. His recent research activities cover wireless communication networks, tactical communications, resource allocations, and security. He received the Best Papers Awards at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications, with three coauthors, and at the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications, with four coauthors. Moreover, he received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award in 2015, 2017, and 2019. In addition, he received the Research Excellence Award of the Université du Québec in 2018. In 2019, he received the Research Excellence Award from ÉTS in recognition of his outstanding research outcomes. He is currently serving as an Area Editor for the IEEE TRANSACTIONS ON MACHINE LEARNING IN COMMUNICATIONS AND NETWORKING and an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON COMMUNICATIONS, and IEEE COMMUNICATIONS LETTERS.

CHONGWEN HUANG (Senior Member, IEEE) received the B.Sc. degree from Nankai University in 2010, the M.Sc. degree from the University of Electronic Science and Technology of China in 2013, and the Ph.D. degree from the Singapore University of Technology and Design in 2019, where he was a Postdoctoral Fellow from October 2019 to September 2020. In September 2020, he joined into Zhejiang University as a Tenure-Track Young Professor, and he is also with Xidian University, and with Zhejiang–Singapore Innovation and AI Joint Research Lab and Zhejiang Provincial Key Laboratory of Information, Processing, Communications and Networks since September 2022. He is the recipient of the 2021 IEEE Marconi Prize Paper Award, the 2023 IEEE Fred W. Ellersick Prize Paper Award, and the 2021 IEEE ComSoc Asia–Pacific Outstanding Young Researcher Award. He has been serving as an Editor for IEEE COMMUNICATIONS LETTER, *Signal Processing* (Elsevier), *EURASIP Journal on Wireless Communications and Networking*, and *Physical Communication* since 2021. His main research interests are focused on holographic MIMO surface/reconfigurable intelligent surface, B5G/6G wireless communications, mmWave/THz communications, and deep learning technologies for Wireless communications.

CHAU YUEN (Fellow, IEEE) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively.

He was a Postdoctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, in 2005, and a Visiting Assistant Professor with The Hong Kong Polytechnic University in 2008. From 2006 to 2010, he was with the Institute for Infocomm Research, Singapore. From 2010 to 2023, he was with the Engineering Product Development Pillar, Singapore University of Technology and Design. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. He has three U.S. patents and published over 500 research papers at international journals or conferences.

Dr. Yuen received the IEEE Communications Society Fred W. Ellersick Prize in 2023, the IEEE Marconi Prize Paper Award in Wireless Communications in 2021, and the EURASIP Best Paper Award for *Journal on Wireless Communications and Networking* in 2021. He was a recipient of the Lee Kuan Yew Gold Medal, the Institution of Electrical Engineers Book Prize, the Institute of Engineering of Singapore Gold Medal, the Merck Sharp and Dohme Gold Medal, and twice a recipient of the Hewlett Packard Prize. He received the IEEE Asia–Pacific Outstanding Young Researcher Award in 2012 and the IEEE VTS Singapore Chapter Outstanding Service Award in 2019. He currently serves as an Editor-in-Chief for *Computer Science* (Springer Nature) and an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE SYSTEMS JOURNAL, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, where he was awarded as an IEEE TNSE Excellent Editor Award and a Top Associate Editor for TVT from 2009 to 2015. He also served as the Guest Editor for several special issues, including IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *IEEE Wireless Communications Magazine*, *IEEE Communications Magazine*, *IEEE Vehicular Technology Magazine*, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and *Applied Energy* (Elsevier). He is a Distinguished Lecturer of the IEEE Vehicular Technology Society, a Top 2% Scientist by Stanford University, and also a Highly Cited Researcher by Clarivate Web of Science.