IEEE Open Journal of Vehicular Technology

Received 22 November 2023; accepted 21 December 2023. Date of publication 19 January 2024;
date of current version 25 January 2024. The review of this article was coordinated by Editor Yong Zeng.

Digital Object Identifier 10.1109/OJVT.2023.3348658

A Survey on Reconfigurable Intelligent Surface for Physical Layer Security of Next-Generation Wireless Communications

RAVNEET KAUR [1], BAJRANG BANSAL [1] (Member, IEEE), SUDHAN MAJHI [2] (Senior Member, IEEE), SANDESH JAIN [3] (Member, IEEE), CHONGWEN HUANG [4] (Member, IEEE), AND CHAU YUEN [5] (Fellow, IEEE)

[1]Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida 201304, India
[2]Department of Electrical and Communication Engineering, Indian Institute of Science, Bangalore 560012, India
[3]Department of Electrical & Electronics Engineering, Center of Autonomous Systems, Atal Bihari Vajpayee-Indian Institute of Information Technology, Management, Gwalior 474015, India
[4]College of Information Science, Electronic Engineering, Zhejiang University, Zhejiang Provincial Key Laboratory of Info. Proc., Commun. &, Netw. (IPCAN), Hangzhou 310027, China
[5]School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798

CORRESPONDING AUTHOR: CHONGWEN HUANG (e-mail: chongwenhuang@zju.edu.cn).

This work was supported in part by SERB GoI, in part by Core Research Grant (CRG), under Grant CRG/2022/000529 in part by Empowerment And Equity Opportunities For Excellence In Science (EEQ) under Grant EEQ/2022/001018, in part by the China National Key R&D Program under Grants 2021YFA1000500 and 2023YFB2904800, in part by the National Natural Science Foundation of China under Grants 62331023 and 62101492, in part by the Zhejiang Provincial Natural Science Foundation of China, under Grant LR22F010002, in part by the Zhejiang University Global Partnership Fund, and Zhejiang University Education Foundation Qizhen Scholar Foundation, and in part by the Ministry of Education, Singapore, under its MOE Tier 2 Award Number MOE-T2EP50220-0019.

ABSTRACT Unprecedented growth in wireless data traffic, and ever-increasing demand for highly secured, and low-latency wireless communication has motivated the research community to move towards sixth-generation (6G) technology, where networks can cater to the rising need for ubiquitous secure wireless connectivity. One of the promising technologies for 6G wireless communication is the reconfigurable intelligent surface (RIS) concept that is proposed to successfully deal with increasing security threats by smartly controlling the wireless channel conditions. This survey paper presents a detailed literature review on RIS-assisted physical layer security (PLS) for next-generation wireless communications. Firstly, we briefly discuss the PLS concept, its importance, the PLS performance metrics, and its applicability in different wireless networks. Next, we discuss the applications of RIS in the 6G scenario. Then, a detailed and systematic classification of the various RIS-assisted wireless system topologies exhibiting multiple scenarios, system models, channel fading models, performance metrics and objectives is done. The existing state-of-art approaches for PLS such as secret key generation (SKG), optimization algorithms, namely semidefinite relaxation-successive convex approximation (SDR-SCA) to optimize RIS coefficients, and optimal placement of RIS units are discussed for single-input single-output (SISO) case. For multiple-input single-output (MISO) case, PLS strategies such as inducing artificial noise (AN), optimization algorithms, alternating optimization (AO), machine learning (ML) and deep learning (DL), and reflect matrices are discussed. Similarly, for multiple-input multiple-output (MIMO) setup, block coordinate descent (BCD) and AN induction are some of the PLS methods used to analyze the secrecy. Lastly, we present some of the technical challenges and future directions based on the survey.

INDEX TERMS Reconfigurable intelligent surface, physical layer security, MISO, MIMO, SISO.

I. INTRODUCTION

Steady growth in smaller and more portable wireless devices due to the emergence of many internet-based and mobile-based services have led to the need to develop firmly secured wireless communication systems [1]. Physical layer security (PLS) concept has emerged as a promising candidate

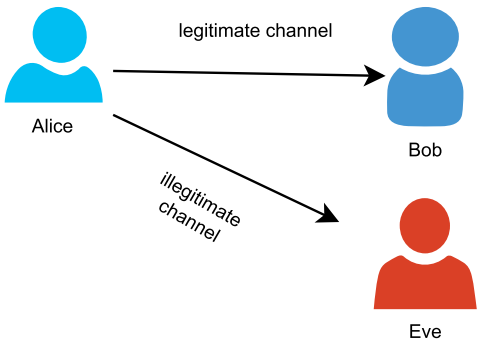

FIGURE 1. Wyner based PLS concept.

that exploits the wireless channel characteristics to ensure authentication and confidentiality in the physical layer, which was discovered by Wyner using a wiretap channel [2], [3], [4]. The basic concept of PLS includes three primary communication entities, as shown in Fig. 1.

The two legitimate nodes, i.e., transmitter, receiver, and one eavesdropper node referred to as Eve. The transmitter node, i.e., Alice, sends secret information to the receiver, i.e., Bob. Eve tries to decrypt the information to obtain the secret message.

PLS strategies have been proposed in the literature that aims to utilize the wireless channel characteristics such as fading, diversity, noise, and interference, for reducing the signaling overhead [5], [6]. They are more advantageous in decentralized networks since it does not require longer cryptographic key length as opposed to classical cryptography [7], [8], [9]. The concept of utilizing long secret key to attain perfect secrecy was successfully demonstrated by Shannon in 1949 [9]. This work inspired the research community to work on the idea of designing the robust and secured networks. The traditional cryptographic techniques may fail to provide robust security to the network for futuristic sixth-generation (6G) communication systems due to the unlimited computational capacity of quantum computing. The large amount of data that is collected by environmental, human-body sensors, etc. and the mobility features need more advanced security techniques that can be achieved by PLS combined with the advances in artificial intelligence (AI) algorithms. Hence, PLS has emerged as a promising technology for securing the network from eavesdroppers (Eves). Due to the aforementioned reasons, PLS-based methods are more suitable for providing robust security to emerging wireless technologies such as the Internet of Things (IoT), fifth-generation (5G)-Tactile Internet, vehicular communication for autonomous driving, remote surgery, etc., as these technologies are delay-sensitive, power-limited, and processing-restricted. It is likely to be best suited for critical applications such as financial services, mobile services, healthcare services, transport services, and AI-powered services which give utmost priority to strong security [1].

Nowadays, secured wireless communication is becoming more challenging due to the large number of users utilizing shared spectrum to improve spectrum efficiency such as cooperative communication and non-orthogonal multiple access (NOMA). Managing data security and privacy among billions of internet-connected devices is a significant challenge. Due to the rapid increase in IoT devices, the physical layer has become quite vulnerable to Eves due to hardware defects and physical signal features such as time, frequency, and modulation [10], [11]. The overall mobile data traffic figure anticipates reaching 5016 exabytes (EB)/month by 2030 as reported in International Telecommunication Union - Radiocommunication Report (ITU-R) [12]. There is a need to safeguard such a large volume of data from malicious users in wireless networks. Besides, securing such massive data, there are some other key performance indicators (KPIs) that motivate us to find new radical solutions for beyond 5G/6G based communication systems [13], [14]. The KPIs targeted for 6G are peak data rate (at least 1˜Tb/s) [15], user experience data rate (up to 1˜Gb/s), end-to-end latency (10 $\sim$100 μs) [16], mobility (at least 1000˜ km/hr), connection density (up to 107˜ devices/km^2), and area traffic capacity (up to 1˜Gbit/(s.m^2)).

Reconfigurable intelligent surface (RIS) is a planar surface that consists of a large number of low-power and low-cost passive elements as shown in Fig. 2. The outer layer comprises many reflecting elements, the middle layer is made of copper and the last layer has a circuit board that tunes the reflection coefficients. The RIS is operated by a smart controller. Each reflecting element is made up of positive-intrinsic-negative (PIN) diodes. The base station (BS) calculates the value of reflection coefficients depending on channel state information (CSI), which are provided to the RIS's controller through a feedback link. The key advantages of RIS are that it can improve the overall signal-to-interference-plus-noise ratio (SINR) without affecting the hardware, passively reflect the incident signals with optimal phase shifts, and reduce the number of antennas at the transmitter and receiver [17]. RIS is comparable to the half-duplex relay in terms of spectral efficiency performance and achieves the same and even better energy efficiency performance than a full-duplex relay. RIS does not require effective self-interference cancellation techniques or signal power amplification as compared to the conventional relay systems [18]. Also, due to its ability to get mounted on different surfaces, it is suitable for diverse application scenarios [17].

The RIS technology has several unique characteristics, such as it is nearly passive, unaffected by receiver noise, having complete frequency band response, being easily deployable, and does not need much signal processing [13], [19]. It also supports full-duplex transmission and adjusts the phase shifts to coherently combine the reflected, refracted, and scattered radio waves and minimizes the fading effect, thereby improving the performance [20]. The aforementioned features of RIS technology help in enhancing the quality of service (QoS) in terms of high data rate, support for a large number of users, ultra-high reliability, etc. [21], [22], [23]. Many existing PLS techniques, such as conventional beamforming, and artificial noise (AN), cannot provide complete security

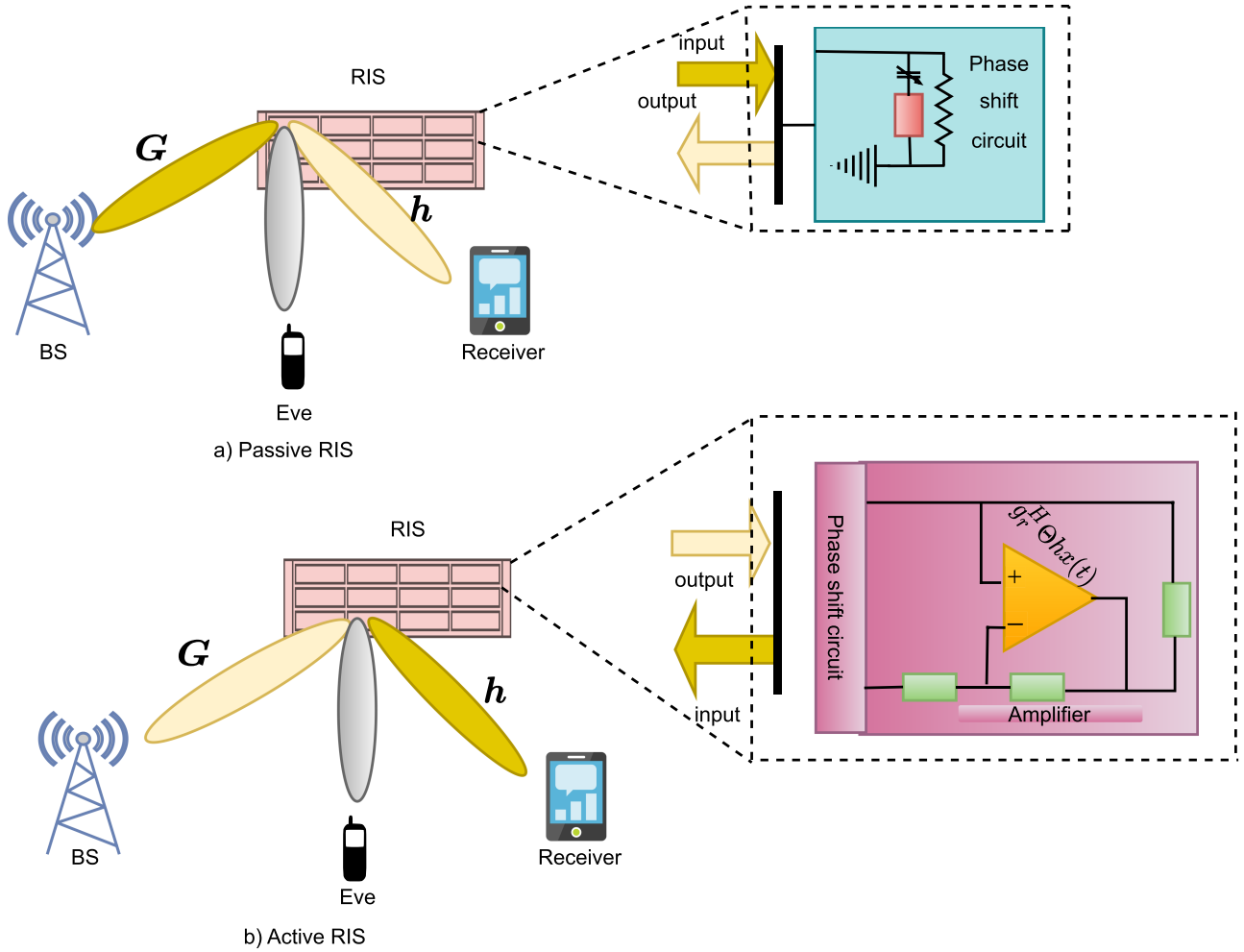

FIGURE 2. **RIS functionality.**

to the wireless network. The usage of RIS in conjunction with the PLS methods has been suggested in the literature to further enhance the overall security of communication between legitimate users [24], [25]. RIS's capability to perform passive beamforming increases the degree of freedom (DoF) that further enhances the system's performance, especially PLS. The main idea behind the design of RIS technology is the 2-Dimensional metasurface that can tune the wireless propagation environment by coherently combining the reflected, refracted, and scattered radio waves and directing them towards the legitimate receiver [26], [27]. In many research works, other terminologies for RIS such as intelligent reflecting surface (IRS) [28], [29], [30], [31], [32], intelligent wall [33], large intelligent surface (LIS) [22], have been used, though all these terms are based on the same principle of passive reflecting elements and perform same operation. A complete list of acronyms is given in Table 1.

As shown in Fig. 2, a multi-antenna BS with N antennas communicates with a single-antenna user via an M-element RIS in the presence of an Eve. RIS receives the signal $\mathbf{G}x(t)$ and delivers the resultant signal $\mathbf{h}^H\mathbf{\Theta}\mathbf{G}x(t)$ to the receiver by adjusting the reflection coefficient matrix denoted by Θ. Here, $x(t)$ is the input signal, $\mathbf{h}^H \in \mathbb{C}^{1\times M}$ represents the channel vector from RIS to the receiver, H is a Hermitian operator and $\mathbf{G} \in \mathbb{C}^{M\times N}$ is the channel matrix from transmitter to the RIS. The phase shift matrix Θ at RIS is given by $\Theta = diag(v)$, where $v = [e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_M}]^T$ and $\theta_i \in [0, 2\pi]$ represents the phase shift introduced by i^{th} element on the RIS. A PIN diode is embedded in each reflecting element and it can be switched ON and OFF by which a phase difference of π can be achieved [34]. RIS controller intelligently reconfigures the phase shifts of the RIS reflecting units [35] so that the reflected signal is constructively added to the LoS signal to maximize the total received power at the legitimate user and minimizing it at the Eve [36], [37]. This results in the enhancement of signal-to-noise ratio (SNR) at legitimate users and reduction at Eves, thus, improving the secrecy rate (SR). Both active as well passive configuration of RIS are shown. Besides modifying the phase shifts of RIS reflecting elements, active RIS can amplify the reflected signals due to the presence of integrated active reflection-type amplifier.

TABLE 1. List of Acronyms

Acronyms	Meaning	Acronyms	Meaning
PLS	Physical Layer Security	SDR-SCA	Semidefinite Relaxation-Successive Convex Approximation
6G	Sixth-Generation	AO	Alternating Optimization
IoT	Internet of Things	DL	Deep Learning
5G	Fifth-Generation	LiFi	Light Fidelity
AI	Artificial Intelligence	URLLC	Ultra-Reliable and Low Latency Communication
NOMA	Non-Orthogonal Multiple Access	ESC	Ergodic secrecy capacity
EB	Exabytes	BER	Bit Error Rate
SNR	Signal-to-Noise Ratio	SROCR	Sequential Rank-One Constraint Relaxation
KPI	Key Performance Indicator	TAaPSA	Tile-Allocation-and-Phase-Shift-Adjustment
RIS	Reconfigurable Intelligent Surface	KGR	Key Generation Rate
PIN	Positive-Intrinsic–Negative	ASR	Average Secrecy Rate
COP	Connection Outage Probability	AP-MRT	Access Point-Maximum Ratio Transmission
ESC	Ergodic Secrecy Capacity	PT	Primary Transmitter
PNSC	Probability of nonzero secrecy capacity	ST	Secondary Transmitter
IRS	Intelligent Reflecting Surface	THz	Terahertz
CSI	Channel State Information	ZFB	Zero-Forcing Beamforming
SINR	Signal-to-Interference-Noise Ratio	SDP	Semidefinite Programming
LIS	Large Intelligent Surface	SD	Successive Design
QoS	Quality of Service	JD	Joint Design
BS	Base Station	MM/MO	Majorization-Minimization/Manifold Optimization
SR	Secrecy Rate	CCT-SDR	Charnes-Cooper Transform and Semidefinite Relaxation
WTC	Wiretap Channel	UAV	Unmanned Aerial Vehicle
ASC	Average Secrecy Capacity	CRN	Cognitive Radio Networks
PU	Primary User	SU	Secondary User
MIMO	Multiple-Input Multiple-Output	LoS	Line-of-Sight
MISO	Multiple-Input Single-Output	IIoMT	Intelligent Internet of Medical Things
SISO	Single-Input-Single-Output	V2V	Vehicle-to-Vehicle
SOP	Secrecy Outage Probability	V2I	Vehicle-to-Infrastructure
ML	Machine Learning	RF	Radio Frequency
AN	Artificial Noise	VLC	Visible Light Communication
BCD	Block Coordinate Descent	SKG	Secret Key Generation

RIS combined with PLS dramatically improves the secrecy performance of wiretap channels (WTCs) [28], [29], [38], [39], [40], [41], [42], [43], [44]. The authors in [28] maximized the secrecy rate of RIS-assisted multi-antenna wireless communication system by applying alternating optimization. In [38], a more practical scenario is considered where the CSI of the Eve is unknown to the transmitter. By applying the joint beamforming and jamming scheme and effective utilization of RIS, the authors demonstrated the enhancement in secrecy rate. In [29], the authors considered an RIS-assisted Gaussian multiple-input multiple-output (MIMO) wiretap channel and maximized the secrecy rate by jointly designing the transmit covariance matrix at the transmitter and the phase-shift matrix at the RIS. The authors in [40] provided the asymptotic secrecy outage probability (SOP) analysis to study the impact of the increase in the number of reflecting elements of RIS and average SNRs. It is shown that the secrecy performance is enhanced by utilizing the characteristics of RIS. Then, in [41], [42], the authors utilized the concept of physical layer secret key generation by using RIS to maximize the secret key rate. Several research works have examined PLS scenarios for the cases of both known and unknown CSI of the Eve to the legitimate transmitter. In [43], the authors proposed an active RIS assisted system to minimize transmission power at UAV-borne BS and enhance achievable secrecy rate. In [44], the authors considered a active-RIS assisted MISO system with an eavesdropper and achieved enhanced secrecy performance gain by not only modifying the phase shifts but also by amplification of signal amplitudes.

There are some articles in the literature that address the related issue of PLS with brief discussion on RIS for some wireless networks [45], [46], [47], [48], [49], [50]. In [45], the authors have done a short survey by reviewing the research works related to RIS-assisted PLS and also suggested some of the open research challenges in RIS-assisted PLS scenarios. In [46], the authors have discussed about the various challenges, solutions and applications of PLS in beyond-5G systems, including cell-free massive MIMO, RIS, light fidelity

(LiFi), or distributed and cooperative protocols. In [47], the authors discussed different use cases demonstrating the impact of RIS in enhancing the PLS of unmanned aerial vehicle (UAV) networks. In another survey [48], the authors have presented a systematic classification of key less PLS schemes. They have also concisely discussed about AI in PLS and RIS for PLS in the context of key less PLS. In [49], the authors have presented a comprehensive survey on different RIS applications in ground-based vehicular communications and aerial vehicular communications. In [50], the authors presented a comprehensive analysis on security and privacy challenges faced by RIS-assisted 6G technologies.

The aforementioned existing survey articles [45], [46], [47], [48], [49], [50] have not provided detailed discussion on RIS-assisted PLS systems. To the best of the authors' knowledge, this is the first survey article that addresses in detail about the wide range of research works focused on RIS-assisted PLS systems for improving the overall secrecy performance. Specifically, this work presents an in-depth analysis of how RIS is utilized to enhance the PLS for different wireless networks with different topologies. Additionally, this survey article aims to discuss RIS coupled with various promising 6G communication technologies such as RIS-assisted energy-efficient and extremely-high reliability and low latency with security (eRLLCS), RIS-assisted visible light communication (VLC) systems [51], RIS-UAV [52], RIS-NOMA [53], RIS-assisted intelligent transportation systems, and RIS-assisted smart healthcare. The major contributions of this survey article are detailed as follows:

- A detailed and systematic classification of various RIS-assisted models is provided based on system model, fading distribution, type of eavesdropping attacks (active or passive), methodology adopted and performance metric evaluated.
- Some promising essential technologies for 6G that use RIS to reduce eavesdropping and improve secrecy are discussed in this article.
- This survey article also discuss various performance metrics required to evaluate the secrecy performance of RIS-assisted wireless networks.
- A tutorial with an emphasis on key design issues, namely, PLS performance metrics, RIS placement in different communication scenarios, and RIS passive reflection optimization techniques from a security perspective, to help researchers, engineers, cyber-security practitioners, system designers, students, in clearly grasping the big picture of the role of RIS in enhancing PLS, is presented.
- Lastly, possible research directions that could be further worked upon for the betterment of security in RIS-assisted PLS systems are suggested.

Fig. 3 shows the systematic representation of the survey. The rest of this paper is summarized as follows: Section II presents the PLS concept and the performance metrics to evaluate the secrecy performance of the given system. It discusses how PLS is useful in the development of highly secured and robust future wireless systems. Different kinds of privacy, minimization of active and passive attacks, and ultra-reliable and low latency communication (URLLC) are some of the PLS crucial features which are discussed in this Section. Section III provides a brief description of RIS and its applicability in the 6G scenario. Section IV summarizes the existing state-of-the-art methods for secrecy enhancement in RIS-assisted wireless systems. There is a discussion of technical challenges and future directions in Section V. Finally, we conclude the survey in Section VI.

II. PLS AND ITS APPLICABILITY IN OTHER NETWORK SCENARIOS

In this Section, we briefly discuss PLS, various performance metrics of PLS and its applicability in different wireless networks as shown in Table 2. Due to the anticipated trillions of IoT devices connected to the backbone network in the presence of a highly mobile and distributed environment, it has become crucial to adopt PLS techniques [54]. As discussed earlier, the PLS techniques exploit the channel characteristics, i.e., noise and fading, and transceiver architecture features such as synchronization and hardware impairment, to fully support legitimate communication by providing double-layer security [55]. Connecting more wireless devices increases the risk for future wireless networks [1].

Some of the critical aspects of future wireless networks in which PLS has a crucial role to play are as follows:

- *Privacy and authentication:* Privacy is one of the most crucial elements which needs to be considered in wireless communication [56]. There are three different types of privacy: data privacy, location privacy, and identity privacy. Due to the demand for data-intensive on-demand services by the users, the service providers get access to their private information, which is stored and utilized by other collaborators, and adversarial entities in designing their recommendation systems [57]. So, in order to prevent illegal data access by service providers and securely implement the smart city concept, there is a need to ensure the privacy of users' data. User authentication is also essential in order to prevent the wireless network from impersonation threats [2], [56].
- *Enhancing secrecy capacity in MIMO system:* With the help of PLS characteristics in [58], the authors achieved a large secrecy capacity between the source and destination. Antenna array beamforming techniques enhance communications between legitimate users while jamming Eve's signals. Multi-antenna deployments and cooperative relays can increase the SR performance of the system [3], [59], [60].
- *Minimize active and passive attacks:* Interference and jamming are the two kinds of active attacks. These attacks use transmission power to interfere with the original signal. Jamming is of four types: spot, sweep, barrage, and deceptive jamming. Similarly, interference can persist by random and on-demand interference. Passive attacks include eavesdropping and traffic analysis.

TABLE 2. Summary of the Existing Surveys on PLS Schemes in Different Wireless Networks

Ref.	Year	Area of Focus	Performance Metrics	Technologies/scenarios discussed
[46]	2021	6G networks	Secrecy capacity, Secrecy throughput	Both dry and wet nano-scale devices, Massive cell free MIMO, RIS, VLC, phy-sec based crypto-key for symmetric encryption, Distributed and cooperative protocols
[47]	2022	UAV with RIS networks	Secrecy capacity	Four use cases, namely, non-LoS scenarios, satellite communication. mobile-RIS enhanced UAVs, cooperative jamming, optimizing PLS for multiple eavesdroppers case
[76]	2018	5G wireless networks	Secrecy capacity, secrecy gain, SOP, secrecy throughput, ESC, COP, secrecy energy efficiency	Device authentication schemes, key generation, data confidentiality schemes, source authentication and data integrity schemes
[77]	2018	OFDM	Secrecy capacity	A detailed study on various OFDM-based PLS techniques targeting key generation and distribution, data confidentiality, authentication, integrity and availability
[78]	2020	Smart Radio environment	Secrecy rate	Electromagnetic properties of RIS, Optimization models and solution methods for RIS-assisted wireless systems considering rate maximization, power minimization problems
[5]	2016	Multiple-antenna techniques	Secrecy capacity, SOP, ESC, interception probability, secrecy energy efficiency	Point-to-point, dual-hop relaying, multiuser, and heterogeneous networks.
[79]	2014	Multiuser Wireless Networks	Secrecy capacity, secrecy throughput, secrecy sum capacity, ESR	Practical secrecy-preserving code design and inter-disciplinary approaches for security, secure transmission strategies from point-to-point channels to larger multiuser networks
[80]	2019	Optimization and signal processing	Secrecy rate, SOP, secure energy efficiency, ESC, secrecy sum rate, secrecy gap	PLS literature categorized on the basis of secrecy rate maximization, secrecy outage probability minimization, power consumption minimization, and secure energy efficiency maximization
[81]	2020	VLC systems	Secrecy capacity, SOP	unified survey covering different channel models, network configurations, input distributions, secrecy capacity and information rates
[82]	2019	UAV systems	Secrecy capacity, SOP	Trajectory design, resource allocation, and cooperative UAVs to fight against both active and passive eavesdropping
[1]	2019	Techniques for Confidentiality	Secrecy capacity, SOP	Detailed classification of PLS techniques against passive eavesdropping
[83]	2018	Cooperative relaying and jamming strategies	Secrecy capacity, equivocation rate, perfect secrecy, SOP, intercept probability	Latest hybrid techniques that utilize both cooperative relaying and jamming.
[84]	2019	5G IoT networks	SOP, secrecy sum rate	Physical layer threats in 5G IoT networks involving massive MIMO, NOMA, VLC, energy harvesting (EH) communications.
[85]	2020	Space Information Networks	Secrecy capacity, ESC, probability of nonzero secrecy capacity, SOP, secrecy energy efficiency	PLS in satellite communications categorized based on different architectures such as land mobile satellite communication networks, hybrid satellite-terrestrial relay networks, etc.
[86]	2016	Information reconciliation schemes	Secrecy capacity	Interactive information reconciliation protocols and a reconciliation layer model to structure them.
[87]	2015	Massive MIMO	Secrecy capacity, ESC	Active and passive attacks as well as detection schemes
[88]	2021	CRN	Secrecy capacity, SOP, PNSC	Physical layer attacks of CRN and their certain countermeasures
[89]	2016	Uncertain Channel state information at transmitter (CSIT)	Secrecy capacity, SOP, ESC, secrecy diversity gain, secrecy multiplexing gain, Secrecy sum-rate, ergodic secrecy sum-rate, PNSC	PLS with CSIT uncertainty considering both scenarios, i.e. when CSI of an eavesdropper is known/unknown to transmitter.
[90]	2021	Fading channels	Secrecy capacity, secure energy efficiency	Classification based on CSI of eavesdroppers and incorporating PLS aspects over fading channels.
[91]	2019	Finite-Alphabet Signalling	Secrecy capacity, SOP, ESR, security gap, secrecy gain, achievable secrecy rate	PLS with discrete signalling for various scenarios, different transmit signal design algorithms for single as well as multi-antenna wiretap channels
[92]	2021	ML	Secrecy capacity, secrecy rate, equivocation rate, interception probability, SOP, ESC, average secrecy outage duration, amount of secrecy loss	Intelligent wireless physical layer security (WPLS) technology enhancement methods, i.e., relay node selection, antenna selection, and authentication and their process of integration with ML, ML techniques for WPLS.

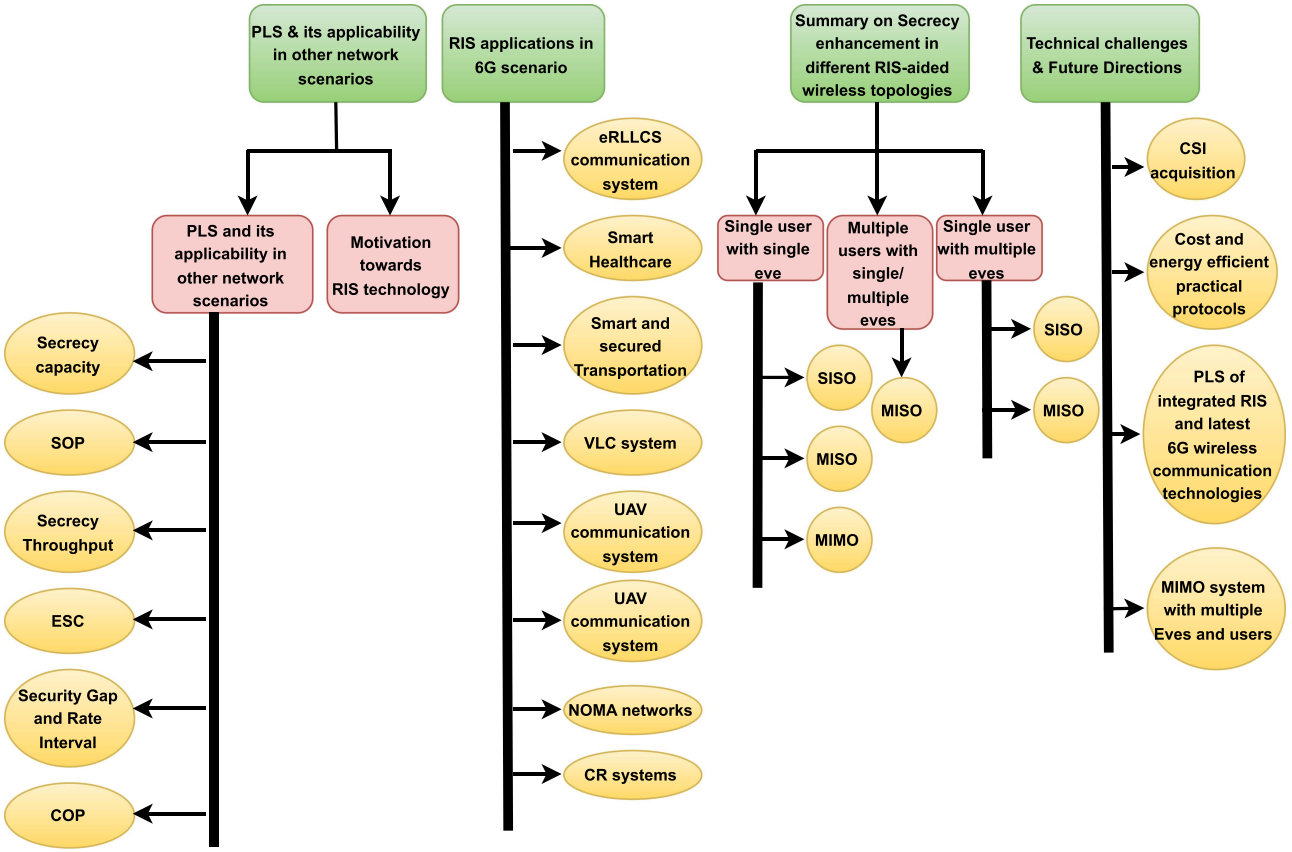

FIGURE 3. Systematic representation of the survey.

By applying different PHY layer security techniques, such as beamforming, AN, and directional antennas, the wireless networks can be prevented from such attacks to a certain extent [61].

Here, we briefly discuss some performance metrics.

A. SECRECY CAPACITY

The secrecy capacity is the difference between the capacity of the main channel and the Eve's channel [4], [62] and is given by

$$C_{\mathrm{S}} = C_{\mathrm{M}} - C_{\mathrm{W}}, \tag{1}$$

where C_M is the main channel's capacity and C_W is the Eve channel's capacity, all in bits/s. The mathematical expressions for C_M and C_W are given by

$$C_{\mathrm{M}} = \frac{1}{2}\log_2\left(1 + \frac{P}{N_{\mathrm{M}}}\right), \tag{2}$$

and

$$C_{\mathrm{W}} = \frac{1}{2}\log_2\left(1 + \frac{P}{N_{\mathrm{W}}}\right), \tag{3}$$

where P is the signal power, N_M, and N_W are Gaussian noise powers corresponding to the main and Eve channel respectively [63]. When the main channel capacity becomes smaller than the Eve channel capacity, i.e., secrecy capacity falls below zero, then its occurrence probability is called intercept probability [64].

B. SOP AND CONNECTION OUTAGE PROBABILITY (COP)

SOP is defined as the probability that the target rate becomes higher than the instantaneous code rate. It can be expressed as

$$p_{\mathrm{out}} = P(C_{\mathrm{S}} < R_{\mathrm{S}}), \tag{4}$$

where R_S is the target rate and C_S is the instantaneous secrecy capacity. SOP signifies that if the instantaneous code rate becomes lower than the required communication rate, the information-theoretic secrecy of the system will no longer be supported [63].

COP is defined as the probability that the Eve receives the message successfully. Connection outage occurs when the amount of mutual information accumulated for legitimate channel is less as compared to the code rate.

C. SECRECY THROUGHPUT

It is the average amount of confidential information received without a secrecy outage at the receiver. Mathematically, it is given as the product of target SR and the secrecy probability [65]. Effective secrecy throughput depends on the CSI accuracy at transmitter. It increases with increase in accuracy

of CSI availability upto a certain extent. Then it decreases since higher value of CSI accuracy will also enhance the Eve's decoding capability leading to rise in SOP as well [66]. Effective secrecy throughput can be defined as

$$T_{eff} = (R_{code} - R_{red})P_r(C_L - C_{eve}, C_{eve} < R_{eve}) \quad (5)$$

where R_{code} and R_{red} represent the codeword rate and redundancy rate respectively. C_L and C_{eve} denote the legitimate channel and eavesdropper's channel capacities respectively. $(R_{code} - R_{red})$ signifies the largest secrecy rate i.e. R_s and the expressions $P_r(C_L - C_{eve}, C_{eve} < R_{eve})$ indicates the probability that there is secured and reliable transmission of information from transmitter and receiver.

D. ERGODIC SECRECY CAPACITY (ESC)

Ergodic secrecy capacity is the capacity of fading channels calculated in an average sense, (which is an important parameter in PLS) since the received SNR varies with time for a faded scenario [67]. From the transmitter node to the jth legitimate receiver and the worst-case Eve, the ergodic capacity of the legitimate channel is expressed as [67], [68]

$$R_{T:j} = E_{h_j,r_j}\left[log_2\left(1 + |h_j|^2 P/\left(r_j^{\alpha}\sigma_s^2\right)\right)\right], \quad (6)$$

and the ergodic capacity of the eavesdropping channel is given as

$$R_{T:e} = E_{h_e,r_e}[log_2(1 + |h_e|^2 P/(r_e^{\alpha}\sigma_e^2))], \quad (7)$$

where $R_{T:j}$ is ergodic capacity of the transmitter and jth receiver link and $R_{T:e}$ is the ergodic capacity of the transmitter and worst-case Eve link. E is the expectation operator. h_j corresponds to the fading coefficient between the transmitter and the jth legitimate receiver and h_e corresponds to the fading coefficient between the transmitter and the worst-case Eve. r_j is the distance between the transmitter and jth legitimate receiver and r_e is the distance between the transmitter and the best Eve. σ_s^2 and σ_e^2 denote the variance of noise at the legitimate transmitter and the worst-case Eve, respectively. Assuming that the worst-case Eve achieves the highest channel gain, the above set of equations is the analytical upper bound on the ergodic secrecy capacity for the worst-case Eve. Mathematically, the ergodic secrecy capacity is given by

$$C_{T:j} = \left[R_{T:j_{min}} - R_{T:emax}\right]^+, \quad (8)$$

where $[a]^+$ is max $(0, a)$, $R_{T:j_{min}}$ is the minimum ergodic capacity obtained from a group of receiver nodes and $R_{T:emax}$ is the maximum ergodic capacity obtained from a group of eavesdropping nodes.

E. SECURITY GAP AND RATE INTERVAL

Security gap and rate interval can assess the PLS in URLLC. The security gap can be defined as

$$\text{Security gap} = \frac{\text{SNR}_{\text{Bmin}}}{\text{SNR}_{\text{Bmax}}} \quad (9)$$

where SNR_{Bmin} is reliability threshold and SNR_{Bmax} is security threshold. SNR_{Bmin} is given as the lowest SNR of the main channel that satisfies the condition, $P_{\text{BER}}^{\text{B}} \leq P_{\text{BER(max)}}^{\text{B}}$, where $P_{\text{BER}}^{\text{B}}$ is the average bit error rate (BER) at the sender, $P_{\text{BER(max)}}^{\text{B}} \approx 0$ is the maximum average BER needed for guaranteed reliable communication between the sender and the receiver. The security threshold is given as the highest SNR of the Eve's channel that satisfies the condition, $P_{\text{BER}}^{\text{E}} \geq P_{\text{BER(min)}}^{\text{E}}$, where $P_{\text{BER}}^{\text{E}}$ is the average BER at Eve where $P_{\text{BER(min)}}^{\text{E}} \approx 0.5$ is the minimum average BER needed for guaranteed secrecy level between the sender and the receiver. The rate interval is given as

$$\delta R = R_{\text{tr}} - R_{\text{inf}}, \quad (10)$$

where R_{tr} is defined as the highest allowable transmission rate that satisfies the condition, $P_{\text{BER}}^{\text{B}} \leq P_{\text{BER(max)}}^{\text{B}}$, and R_{inf} is defined as the lowest allowable transmission rate that satisfies the condition $P_{\text{BER}}^{\text{E}} \geq P_{\text{BER(min)}}^{\text{E}}$. If δR is positive, reliable and secure communication is possible between sender and receiver. If δR is negative then it is not possible [69].

F. INTERCEPT PROBABILITY AND PROBABILITY OF NONZERO SECRECY CAPACITY (PNSC)

The probability by which the secrecy capacity, C_s falls below zero is called intercept probability [70], [71], [72].

$$P_{inter} = P_r(C_s < 0) \quad (11)$$

Passive eavesdropper intercept legitimate channel's information without modifying it whereas active eavesdropper have the ability to modify it and cause severe decoding errors.

PNSC can be defined as the probability that secrecy capacity is maintained above zero level since the wireless channel is variable. The secrecy of the channel can be maintained only till the legitimate channel's quality is better than the eavesdropper's channel.

$$P_r(C_s > 0) = P_r(\gamma_L - \gamma_{eve}) \quad (12)$$

where γ_L and γ_{eve} are signal-to-noise ratio corresponding to legitimate and eavesdropper's channel respectively. The performance of RIS-assisted secure communication system is evaluated in terms of average secrecy rate, PNSC and SOP [73].

G. SECURE ENERGY EFFICIENCY

The energy efficiency of secured transmission over physical layer can be evaluated by the help of two performance metrics. One is the secure energy efficiency and the other is energy per secret bit. Secure energy efficiency can be defined as the amount of confidential information transmitted with a specified amount of energy consumed in duration δT. The ratio can be calculated as

$$EE = \frac{R_{sec}\delta T}{\delta E} = \frac{Rsec}{P}(bits/Joule) \quad (13)$$

where R_{sec} is the achievable secrecy rate. This metric is used in literature [74], [75] to measure the energy efficiency of physical layer. Another metric is the reciprocal of secure energy efficiency and is referred to as energy per secret bit It can

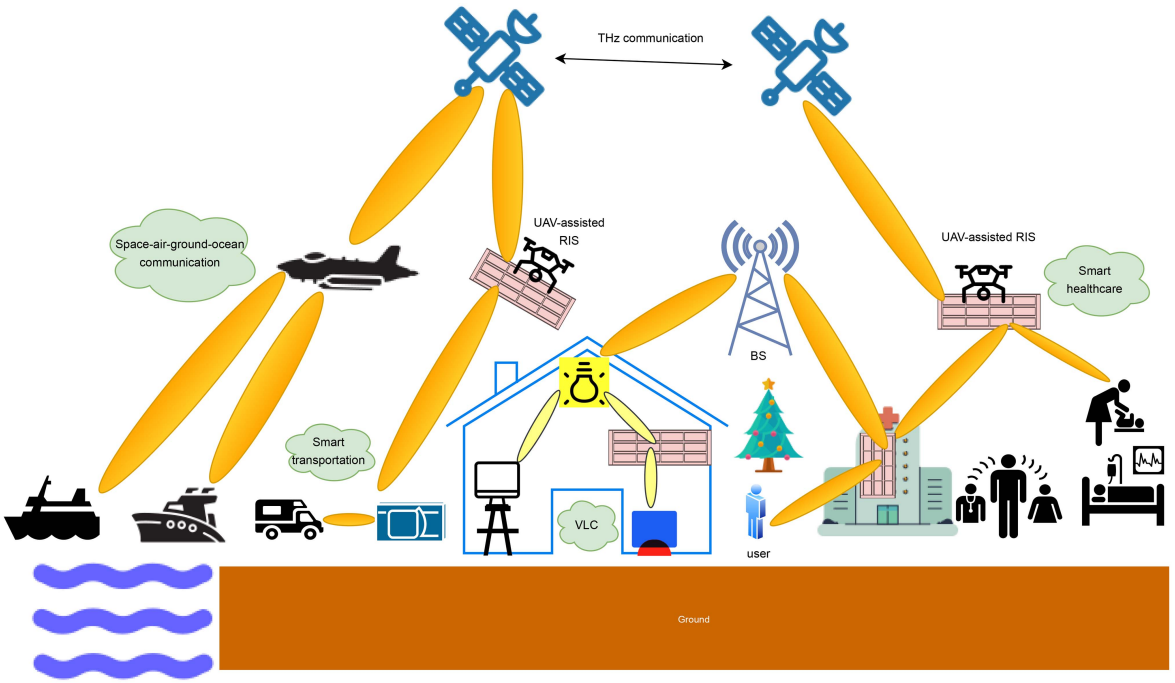

FIGURE 4. RIS-based 6G communication scenario.

be calculated as the minimum energy needed to transmit one bit securely.

$$E_{bit} = \frac{P}{R_{sec}}(Joules/bit) \tag{14}$$

The suitability of the performance metric depends on the system scenarios and the channel conditions.

Table 2 summarizes the existing surveys on PLS schemes in different wireless networks. In [76], the authors discussed PLS research on various 5G technologies including MIMO, NOMA, millimeter-wave communications, etc. and not particularly on RIS. The authors in [5] focussed on various multiple-antenna techniques to enhance PLS for different systems. Similarly, the authors in [79] have provided a detailed review on various secure transmission strategies from point-to-point channels to larger multi user networks Then, in [80], the authors presented a detailed survey on various PLS optimization strategies to maximize secrecy performance of the system. The authors in [81] and [82] focused particularly on PLS for VLC and UAV systems, respectively. Similarly, in [85], the authors presented an exhaustive survey on PLS in satellite communications. However, the aforementioned works in [5], [79], [80], [81], [82], [85] have not considered the important fact that besides controlling the transmitter and receiver, the propagation channel parameters can also be finely tuned. RIS has the capability to smartly control channel parameters thereby improving the SNR, security, spectral and energy efficiency. It can be integrated with other existing networks by modifying the network protocol. Also, it is nearly passive, light in weight and small in size due to which it can be easily deployed. All these unique characteristics can help in realizing an intelligent network in 6G scenario. The role of RIS in 6G PLS is discussed in following Section.

III. RIS AND ITS APPLICABILITY IN 6G PHYSICAL LAYER SECURITY SCENARIO

As shown in Fig. 4, the deployment of RIS in smart offices/homes, not only improves the connectivity but also compensates for the power loss by reflecting beamforming to nearby devices [93]. In order to enhance the coverage in an indoor environment such as airports, shopping malls, educational institutions, and factories, RIS can be fixed to walls, ceilings, and even furniture, which is quite practically feasible [94]. Similarly, the connectivity can be enhanced in outdoor environments by coating RIS on building exteriors, lampposts, high-speed moving vehicles, road signs, etc., in order to control the transportation system smartly and thus make the propagation environment intelligent [19], [78], [94], [95], [96], [97]. RISs can be deployed in high-security areas where BSs cannot be installed [98]. With the rapid evolution of 6G emerging technologies, i.e., THz communication, AI, intelligent wearables, implants, RIS, optical wireless communication (OWC), 3D networking, proactive caching, UAV, and wireless power transfer, the number of wireless devices has increased manifold [99], [100].

Table 3 shows the summary of representative works on RIS and its role in 6G PLS scenario. To support ubiquitous connectivity all over the world, including deserted places, as well as to satisfy the 6G KPIs in terms of data rate upto Tbps, RIS is an excellent option. It is due to its nearly passive nature, its ability to control the wavefront intelligently such that additional reflected paths are available at high frequency

TABLE 3. A Summary of Representative Works on RIS and Its Role in 6G PLS Scenario

Area of Main Focus	Ref.	System Scenario	Major Contributions
Smart healthcare	[13]	Proposed system with RIS and smart sensors	Proposed that by embedding RIS and smart sensors, secured and wearable body area network can be designed.
Smart and secured transportation	[105]	V2I networks	Average secrecy capacity is analyzed and compared for the decode-and-forward relay, the amplify-and-forward fixed gain relay, and the RIS.
	[106]	First scenario - V2V network with RIS-based access point for transmission, Second scenario - VANET comprising a RIS-based relay	RIS used as a reflector and a transmitter. ASC and SOP are analyzed.
	[107]	First scenario - V2V network with RIS as a relay, Second scenario - V2I network with RIS as a receiver	Improved SOP is obtained due to presence of RIS.
VLC systems	[108]	SISO	By smartly adjusting mirrors of an intelligent controllable integer array, secrecy performance is improved.
	[109]	Multi-user	Improved secrecy rate due to RIS as compared to other benchmark schemes, i.e., random assignment case and without RIS case.
	[110]	Dual-hop SISO-based VLC/RF hybrid network	Closed-form expressions of SOP and strictly positive secrecy capacity are obtained.
UAV communication system	[111]	RIS-assisted UAV system composed of rotary-wing UAV, ground user, and an Eve	Average worst SR is maximized by joint uplink/downlink optimization.
	[112]	UAV-mounted BS, a legitimate receiver and a passive Eve	Maximize ASR in the presence of RIS by joint optimization and by applying SCA scheme.
	[113]	Uplink communication system composed of RIS-assisted UAV, BS, multiple users	Maximized the fair secrecy energy efficiency by joint optimization of UAV's trajectory, phase shifts of RIS, and transmit power.
NOMA	[114]	Two single-antenna users, multi-antenna BS, multi-antenna Eve	Utilized robust active and passive beamformi9266086ng for secured communication. SROCR based AO algorithm is applied to optimize RIS reflection coefficients and transmit power.
	[115]	Downlink MISO	Enhancement of heterogeneous internal secrecy requirements and SDP and SCA-based iterative algorithms are proposed
	[53]	First scenario - Two NOMA users with internal eavesdropping, second scenario - Two NOMA users with both both external and internal eavesdropping	Secrecy performance is enhanced by applying joint beamforming and power allocation scheme
	[116]	Multi-antenna BS, passive Eve, multiple users	By joint optimization of transmit beamforming, artificial jamming, and RIS reflecting vectors, SR, sum SR and eavesdropping rate are optimized.
	[117]	Two legitimate users, BS, and an Eve	Performance evaluation in terms of SOP and ASC under a generalized Nakagami-m fading channel model is done.
CR systems	[118]	Underlay MIMO-CRN with a relay node	Proposed a bi-directional zero-forcing beamforming scheme to improve ergodic secrecy capacity and SOP of network.
	[119]	Gaussian CR MISO system	Secrecy rate of secondary user (SU) is improved by applying joint optimization done by AO algorithm in the presence of RIS.
	[120]	MIMO CR WTC model	SU's secrecy performance is enhanced by proposed AO algorithm which has faster monotonic convergence too.
	[121]	CR MISO WTC model	Enhanced secrecy rate for SU is achieved considering three different CSI availability conditions for Eve, i.e., full CSI, imperfect CSI, and no CSI.
	[122]	Multi-antenna cognitive BS, primary user (PU) and SU, multiple coordinated eavesdroppers	Enhanced spectral efficiency, energy efficiency, and security is achieved.

and visible light spectrum, and its easy deployment in the existing infrastructure [11], [13], [98], [101]. In [102], the authors investigated the performance of RIS-assisted THz massive MIMO system and by exploiting the use of RIS, the bit-error rate performance is improved by combating the large free space path-loss. It can provide a robust non-line-of-sight (NLoS) link in areas where obstacles block the line-of-sight (LoS) path [103]. The indoor RIS can be connected to the outdoor RIS which facilitates cooperative communication between the household environment and outside the public domain. As discussed in [104], intelligent Omni-surface, which is a specimen of RIS, can be utilized to provide ubiquitous service connectivity to mobile users. In the future, this ubiquitous wireless connectivity requires authentication and complete security from eavesdropping and man-in-the-middle attacks. It is possible with the help of RIS-assisted PLS techniques, which aim to redirect undesirable signals in such a way that the communication between legitimate users is strongly secured [45], [46], [101].

Some of the PLS applications of RIS in 6G are discussed as follows:

A. RIS-ASSISTED ERLLCS COMMUNICATION SYSTEM

The smart city concept composed of advanced industries, schools/universities, and critical areas such as health care, defense sector, surveillance, etc., require less delay and secure connectivity that is free from Eves. The smart city model comprises applications as the upper layer, followed by an open-access platform and massive IoT infrastructure that forms the lower layer. These layers utilize the wireless medium to communicate with each other [123]. So, one must safeguard the interaction between the layers in a massive IoT against malevolent users regarding privacy, confidentiality, integrity, and interoperability. The next generation of communication systems will consist of massive self-organizing and self-healing robots. Many IoT devices, including personal IoT, healthcare IoT, and industrial IoT, require high computational power and, therefore, need more energy. So, in order to ensure an eco-friendly communication network design, bit-per-Joule energy efficiency (EE) is also a crucial performance criterion. It decides the applicability of a particular wireless technology for creating the green and sustainable network [124]. PLS exploits the inherent characteristics of the physical channel and does not involve any complex encryption/decryption process, due to which it becomes beneficial in providing security to delay-sensitive applications. It satisfies the ultra-low latency requirement of the given network while maintaining its security and privacy [69]. Authors in [125] applied the friendly jamming technique, which is one of the promising PLS techniques, to prevent the data from getting decoded by Eves. RIS turns out to be a powerful hardware technology for the upcoming 6G networks due to the presence of many low-cost and passive reflecting elements. It can play an important role in achieving PLS by carefully utilizing the channel conditions and by optimization of phase shifts of reflecting elements of RIS to enhance the data rate and energy efficiency compared to the traditional amplify-and-forward relay in communication networks [124], [126]. By configuring RIS to redirect the signals such that they produce destructive interference towards Eves and add constructively at desired users, the security of the system can be enhanced [123]. RIS maintains a trade-off between security, complexity, and energy while designing PLS protocols for IoT-based networks [127]. One of the methods used in conjunction with the RIS to improve network security is cooperative jamming [31].

B. RIS-ASSISTED SMART HEALTHCARE SYSTEM

The smart healthcare system is a data-intensive service that requires very high data rates, ultra-high reliability, and very low end-to-end delays that can be made possible by using 6G network [126]. As shown in Fig. 4, a smart healthcare system consists of intelligent internet of medical things (IIoMT) which are wearable devices and sensors that can intelligently monitor real-time data and securely send the patient's information to the medical staff via the internet. It is required to prevent the patients' privacy and access to the massive volume of critical information from eavesdropping, jamming, and spoofing [128]. Remote healthcare has become very crucial, especially in pandemic times when it is required to follow strict protocols and maintain social distancing to minimize the infection spread. It facilitates hospital-to-home (H2H) facility, thus reducing patient load at the hospital and supporting the elderly population who need continuous health monitoring to ensure well-being. For IIoMT devices, energy efficiency is the most crucial parameter. In order to send and receive confidential data securely and efficiently, reliable connectivity is also critical. Due to the boundless spread of a large amount of medical data, there is a need to address the security and privacy issue of this humongous information in order to form a fully connected and secured digital world [66]. In [129], the authors briefly discuss the three main classifications in which the PLS techniques can be categorized based on the kind of authenticity attack. These are cryptography, anomaly detection, and "friendly" jamming.

A PLS technique to ensure authentication and improve channel estimation for Wireless Implantable Devices is proposed. In the future, RIS-assisted PLS techniques can be used effectively to protect private medical and health data from Eves. It can be deployed for seamless connectivity and enhance the security of the legitimate link from malicious users. Also, due to its passive reflection mechanism, it is applicable for almost the whole frequency range, which makes it a cost-effective solution for 6G applications [130]. The capability of RIS to modify the propagation channel conditions can be effectively utilized to enhance reliability and sensing accuracy which are the prime concerns in the medical field [131]. In [13], the authors have proposed a design to create wearable body area network to monitor the health of people in real time by using RIS and smart sensors. The sixth generation of wireless communication networks can satisfy all these requirements, which are beyond 5G capabilities [132].

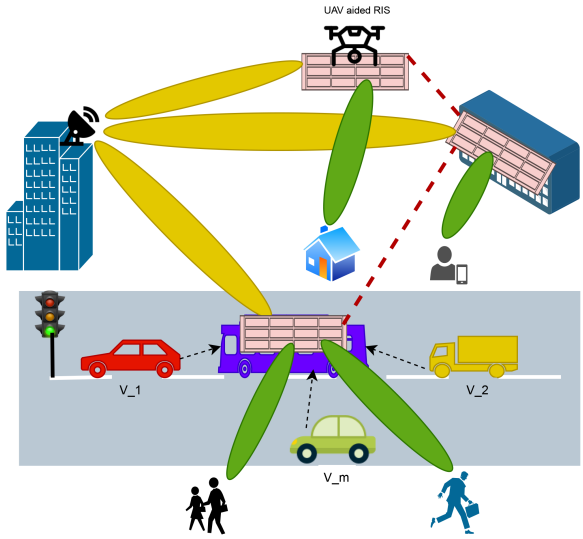

FIGURE 5. RIS-assisted vehicular network.

C. RIS-ASSISTED SMART AND SECURED TRANSPORTATION

Smart transportation aims to enhance the cellular user's quality of service (QoS), road safety, traffic congestion, cost and energy efficiency by deploying the latest wireless technologies in the current transportation system [133]. It focuses the desired signal towards the intended receiver by adjusting the phase shifts and amplitudes of incident waves such that the desired information and energy is transmitted to the receiver [134]. Security issues in vehicle-to-infrastructure (V2I) networks are addressed by deploying RIS keeping in mind that it should be 1) optimally placed, 2) able to estimate the CSI in a highly dynamic vehicular environment, 3) able to reflect optimally, and 4) able to adapt to varied spectrum ranges. The intelligent transportation system needs to protect the communication links between different wireless vehicular network entities from Eve attacks as shown in Fig. 5. $V_1, V_2, \ldots, V_m$ are interfering vehicles and there is a direct link between vehicle vehicle V and UAV-assisted RIS. It is demonstrated that RIS provides the highest average secrecy capacity as compared to the decode-and-forward (DF), amplify-and-forward fixed gain relays in presence of an Eve [105]. Due to the enormous increase in intelligent devices that require frequent recharging, it is essential to make arrangements for such facilities in future vehicles. One such concept is wireless energy transfer (WET) which utilizes RIS to provide recharging of intelligent devices within the vehicle. In order to effectively transmit energy via radio frequency (RF) signals in a poor propagation environment, passive RIS elements are coated within the vehicle to reconfigure the environment. In [105], the authors discussed that machine learning (ML) can be used to design more effective RIS-assisted PLS techniques as it can provide more accurate CSI [135].

In [106], the authors utilized RIS for both PLS as well as vehicle-to-vehicle (V2V) communication. In previous works, the researchers either did not consider RIS in the vehicular networks [136], [137], [138], [139], [140] or the system was a non-vehicular RIS-assisted PLS system. In [106], two scenarios are considered. In the first scenario, the authors considered a V2V network consisting of a RIS-based access point for transmission, and in the second scenario, they considered a vehicular ad-hoc network (VANET) comprising a RIS-based relay. The main idea is to utilize RIS as a reflector and a transmitter. Mobile nodes are considered and also the effects of fading. They showed that the parameters such as source power, Eve distance, the distance between source and relay, secrecy threshold, and the number of RIS cells had a great impact on the system's performance. The average secrecy capacity (ASC) and SOP of the system were analyzed. Similarly, in [107], the authors considered two realistic scenarios; one is V2V communication in which RIS acts as a relay as shown in Fig. 5, and the other is V2I, in which RIS acts as a receiver. SOP is analyzed, and the system's performance improves due to RIS's presence in the network.

D. RIS-ASSISTED VLC SYSTEMS

VLC is a high-speed communication technique that utilizes existing illumination systems which makes it cost-effective. It operates within the frequency range of 400–800 THz, which makes it a suitable technique for the 6G scenario [141]. RIS's ability to re-configure the wireless propagation channel to compensate for the blocked LoS path is greatly utilized in enhancing the communication performance [142]. By intelligently controlling the reflection coefficients, a fine-grained three-dimensional (3D) passive beamforming toward the desired user can be achieved. This feature also helped in improving the secrecy performance of the single-input single-output (SISO) VLC system [108]. RIS is implemented as an intelligent controllable mirror array and by smartly controlling the orientation of each mirror, the difference between the channel gains of transmitter and receiver is increased, and thus the secrecy performance is improved. Now, in [109], the authors investigated the secrecy performance of a multi-user RIS-assisted VLC system. The system model is composed of multiple transmitters, multiple receivers, and an Eve. By adopting an additive channel model [143] instead of optimizing the mirror orientation as discussed above [108], the secrecy rate is significantly improved as compared to the other benchmarks, namely, random assignment case and without RIS case.

In [28], the authors considered maximizing the SR of a RIS-assisted RF multi-antenna system with a single antenna Eve. Most of the research works are focused on enhancing the secrecy performance of RIS-assisted standalone VLC or RF network [28], [108], [109]. So, the authors in [110] discussed the PLS of RIS-assisted dual-hop SISO-based VLC/RF hybrid network in the presence of an Eve eavesdropping from the relay. The first hop is the VLC link that transmits information in an electromagnetic-sensitive environment and the second hop corresponds to the RF link that further increases the communication coverage with the help of RIS and relay nodes. Closed-form expressions of SOP and strictly positive secrecy capacity are derived and verified via simulations. Further

research can be done in RIS-assisted PLS systems considering multiple-input single-output (MISO) systems, MIMO systems, multiple RISs, Nakagami fading channels, etc.

E. RIS-ASSISTED UAV COMMUNICATION SYSTEMS

UAV-based communication systems have emerged as one of the most innovative and upcoming wireless technologies, which is getting popularity due to its flexible networking architecture and affordable deployment cost [144], [145], [146], [147], [148]. They are needed in order to cater to explosive growth in wireless traffic, especially in high altitude areas or difficult terrains where either the BS is inoperative or is not possible to build [149], [150], [151], [152]. By optimization of rotation angles and RIS location, which can be adjusted by UAV, the ergodic capacity is improved [153].

By deploying a UAV relay with a RIS between users and BS, stronger legitimate links with ground nodes can be made, and also more potential Eves can be determined [154] as shown in Fig. 5. In [111], the authors investigated the performance of a RIS-assisted UAV secure communication systems that consists of rotary-wing UAV, ground user, and an Eve. Time division multiple access (TDMA) protocol is used in order to ensure legitimate communication between ground user and UAV. Building-mounted RIS is used to further assist secure data communication. Rician fading is assumed for all links. Imperfect CSI of the Eve is available to the transmitter. To maximize the average worst SR, joint uplink/downlink optimization is done by the proposed algorithm. The performance improvement is observed in simulation results due to the joint design of UAV trajectory, RIS's passive beamforming and transmit power of legitimates. The authors in [112] proposed a RIS-assisted UAV communication system that consists of UAV-mounted BS and a legitimate receiver to maximize the average secrecy rate. Passive Eve is considered, so, the small scale fading between the RIS and the passive Eve is difficult to achieve. Joint optimization of the trajectory, transmit power of UAV, and phase shifters of RIS is done and the SCA scheme is applied. It is demonstrated that with the help of RIS, the secrecy performance of the system is significantly improved. In [113], the authors maximized the fair secrecy energy efficiency which is calculated by taking the ratio of the minimum secrecy rate to the total power utilized. This is done by jointly optimizing the UAV's trajectory, phase shifts of RIS, and transmit power.

From these studies, it can be concluded that significant secrecy performance improvement can be achieved over the traditional schemes as in [113]. For efficient utilization of bandwidth resources, RIS can be deployed to enhance the spectral efficiency by integrating the index modulation [126]. By utilizing the THz and visible band, and deploying RIS, the spectral efficiency of the wireless communication system can be further increased [155], [156]. From the point of view of PLS, RIS aims to maximize the SR in the UAV-assisted networks, besides improving spectral efficiency [52], [157].

F. RIS-ASSISTED NOMA NETWORKS

NOMA is one of the crucial schemes for 5G and beyond wireless networks, because it has high spectral efficiency, low latency, supports a massive number of users, etc. [158], [159]. However, this scheme is quite prone to eavesdropping. So, there is a need to fully secure from malicious users [1], [160]. So, designing PLS techniques for NOMA is very critical for the security of the network [161]. The work in [161] focuses on PLS for downlink NOMA considering both kinds of Eves, i.e., 1) external Eves and 2) internal Eves.

The authors of [114] focused on securing wireless transmission in NOMA networks with RIS assistance. Rayleigh fading channel was used. The work utilized robust active and passive beamforming for the secure wireless transmission of data and to minimize overall transmission power. AN was introduced to degrade the information reception capability of the Eve. A sequential rank-one constraint relaxation (SROCR) based alternating optimization (AO) algorithm is applied to optimize the RIS reflection coefficients and transmit power efficiently. A robust beamforming design was analyzed mathematically and it was demonstrated that by carefully increasing the number of antennas at BSs, the transmit power decreases, and beamforming gain for secured communication in NOMA improves. It was shown that with the increase in the eavesdropping rate, the security requirement reduces due to which less AN is needed. The proposed AO algorithm performs better in terms of transmit power than two baseline schemes, i.e., random phase and equal power allocation (EPA). It consumes the least power of all. In article [115], the authors enhanced the heterogeneous internal secrecy requirements of NOMA users and minimized the total transmit power. They proposed SDP and SCA-based iterative algorithms to optimize active beamforming and passive phase shifts to minimize power consumption. A significant improvement in power consumption compared to conventional NOMA (C-NOMA), NOMA without RIS, and OMA with or without RIS is demonstrated. Then in [53], the authors investigated the performance of RIS-assisted downlink NOMA transmission system having two NOMA users. Two scenarios are considered. In the first one, internal eavesdropping is present, and in the second case, it extends to both external and internal eavesdropping. The authors further considered two sub-scenarios, one is the sub-scenario without CSI of Eve, and in another case, the Eve's CSI is available. Joint beamforming and power allocation scheme were applied to enhance the secrecy performance. Also, by increasing the number of reflecting elements of RIS, the secrecy performance is improved.

The authors in [116] optimized the SR, sum SR, and eavesdropping rate by jointly optimizing the transmit beamforming, artificial jamming, and RIS reflecting vectors. The jamming and NOMA signals are transmitted together to suppress eavesdropping and apply successive interference cancellation (SIC). In another article, [117], the secrecy performance of RIS-assisted NOMA networks consisting of two legitimate users, BS, and an Eve is evaluated in terms of SOP and ASC

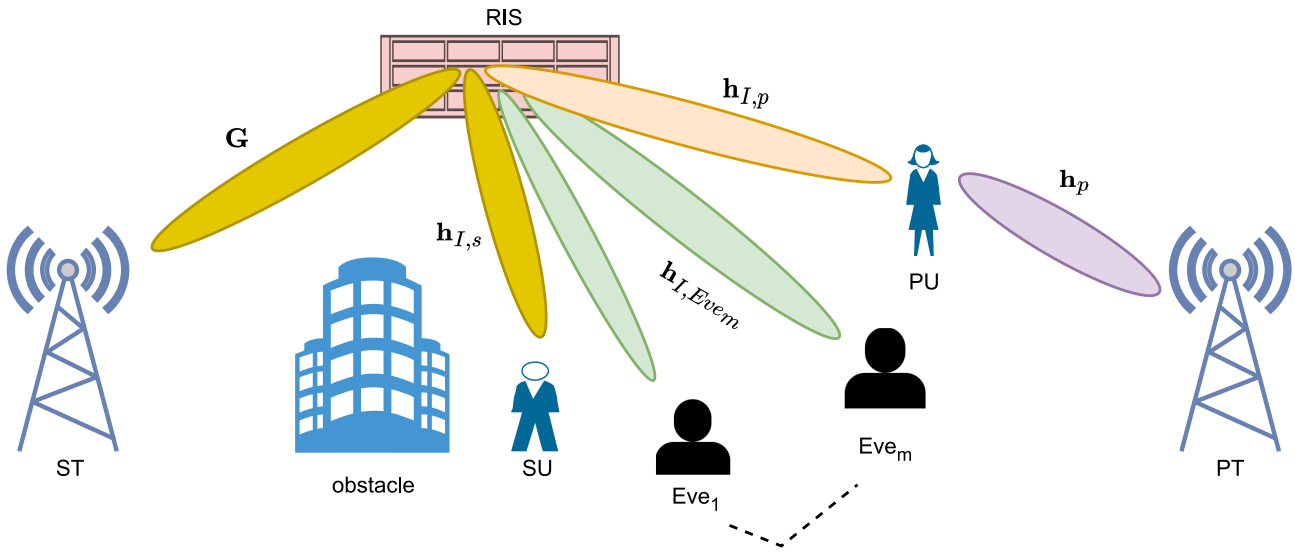

FIGURE 6. RIS-assisted CRN.

under a generalized Nakagami-m fading channel model. The secrecy diversity orders and high SNR slopes are also determined in [117].

G. RIS-ASSISTED CR SYSTEMS

In this Section as shown in Fig. 6, we discuss CR systems which are deployed in order to cater to the ever increasing bandwidth demand of users and thus solve the spectrum scarcity issues. These are prone to eavesdropping, jamming, and spectrum sensing data falsification and need to be fully protected by applying PLS techniques [119]. The authors in [118] considered an underlay MIMO-CRN with a relay node to effectively utilize the spectrum and cater to a huge number of users. Both primary users (PUs) and secondary users (SUs) intelligently use the same spectrum in underlay MIMO-CRN due to which there is less interference to PU data. But to fully preserve the privacy of PU's and SU's data and maintain their data rate, the authors propose a bi-directional zero-forcing beamforming scheme to enhance the secrecy capacity of the network. Highly secured communication is achieved for both PUs and SUs and the results are demonstrated in terms of ergodic secrecy capacity and SOP. As shown in Fig. 6, RIS is combined with PLS to prevent the network from eavesdropping and to make it energy-efficient. Here $\mathbf{G} \in \mathbb{C}^{M\times N}$ is the channel matrix from secondary transmitter (ST) to the RIS. $\mathbf{h}_{I,s} \in \mathbb{C}^{M\times 1}$ denote channel vector from RIS to SU, $\mathbf{h}_{I,Eve_m} \in \mathbb{C}^{M\times 1}$ denote channel vector from RIS to m^{th} eavesdropper and $\mathbf{h}_{I,p} \in \mathbb{C}^{M\times 1}$ represent the channel vector RIS to PU respectively. RIS's ability to constructively add the signals at desired receiver, destructively at the Eve, and its energy-efficient passive nature makes it extremely important entity while designing wireless networks.

In [119], the authors considered a RIS-assisted gaussian CR MISO system and aim to enhance the secrecy rate of the SU. Joint optimization of transmit covariance at transmitter and phase shift coefficients at RIS is done by applying AO and improved results with RIS are reported in terms of secrecy rate. Similarly, in [120], the authors considered a RIS-assisted multiple-input-multiple-output cognitive radio wiretap channel (MIMO CR WTC) model and aim to enhance the secrecy rate of the SU. An AO is proposed for joint optimization of transmit covariance at the base station and phase shift coefficients at RIS. So, the secrecy rate of the SU is enhanced over other benchmark schemes and the proposed algorithm has fast monotonic convergence too. Then in [121], the authors considered a CR MISO WTC and aim to enhance the secrecy rate at SU under certain power constraints. It is assumed that complete CSI of PU and SU is available and for Eve, three different conditions of CSI are considered, namely, full CSI, imperfect CSI, and no CSI. To get the enhanced secrecy rate in each scenario, different optimization algorithms are proposed and optimized secrecy rates are obtained for each case. The authors in [122] considered a RIS-assisted cognitive radio network (CRN) that utilizes RIS to enhance its spectral efficiency, energy efficiency, and security.

IV. STUDIES ON SECRECY ENHANCEMENT IN VARIOUS RIS-ASSISTED WIRELESS SYSTEM TOPOLOGIES

The major research works on secrecy performance in RIS-assisted wireless networks are summarized in this Section. The organization is done based on the system design, specifically how RIS relates to the network's topology. The research works presented are classified according to the four main categories, i.e., single/multiple users with single/multiple Eves. Further, they are analysed in terms of performance metrics obtained, antenna system deployed, number of RIS present, channel model used, and the major contributions in the research field. Table 4 presents a summary of representative

TABLE 4. A Summary of Representative Works on Secrecy Enhancement of RIS-Assisted Wireless Networks With Single/Multiple Users and Single/Multiple Eves

Related Works		Metric	Antenna system	Number of RIS	Channel fading	Major Contributions
Single user with one eve	[40]	SOP	SISO	Single	Rayleigh	Analytical SOP derived and validated
	[163]	Secret key capacity	SISO	Single	-	Proposed scheme improves secret key capacity over random placement scheme
	[173]	SR	MISO	Single	One rank channel model	Closed-form beamforming solution was derived and SR improved
	[162]	SOP and average SR	SISO	Single	Legitimate/wiretap (a) FN/Rayleigh (b) Beckmann/Rayleigh, (c) Nakagami/Rayleigh	Different scaling laws for legitimate and Eve's SNRs improves PLS performance
	[174]	SR	MISO	Single	Clustered channel model based on extended Saleh Valenzuela model	Two high-quality sub-optimal designs i.e., close-form SD and iterative JD proposed and significant improvement obtained
	[164]	KGR	SISO	Multiple	Fast fading	Proposed scheme outperforms random phase shifted RIS, no-RIS scheme
	[38]	Average SR	MISO	Single	Rayleigh	Proposed scheme improves average SR even without Eve's CSI
	[51]	Average SR	MISO	Single	Quasi-static flat fading	Proposed AO based joint active and passive beamforming scheme outperforms other benchmark schemes i.e AP-MRT with RIS, upper bound, no-RIS
	[175]	SR	MISO	Single	Rician	Performance comparison of proposed-MM, proposed-MO with CCT-SDR and heuristic approaches is done numerically and via simulations; proposed algorithms perform better
	[176]	SR	MIMO	Single	Direct path-Rayleigh fading, RIS related paths-Rician fading	Proposed BCD-MM algorithm provides improved security gains over No-RIS, Rand-Phase and BCD-QCQP-CCP schemes
	[28]	SR	MISO	Single	Rayleigh	Proposed AO scheme with RIS performs better than system without RIS
	[51]	Average SR	MISO	Single	Rayleigh	Proposed algorithm based on alternating optimization, SDR and Gaussian randomization methods perform better over the case without using RIS
	[177]	SR	MIMO	Single	Quasi-static flat-fading channel	Proposed SCA-based algorithm outperforms the other benchmark schemes, namely, no-RIS and random-RIS
	[178]	Average SR	MISO	Single	Rayleigh	Proposed element-wise BCD and AO with minorization-maximization techniques with RIS perform better than non-RIS case
	[32]	ASR	MIMO	Single	Large scale fading	Proposed "MIMO RIS with AN" scheme provides higher ASR as compared to "MIMO RIS without AN" scheme, "MIMO with AN and without RIS" scheme and "MIMO without AN and without RIS" scheme
	[30]	Average SR	MISO	Single	Quasi-static flat fading	Generic multi-objective AO with RIS performs better than non-RIS case

TABLE 4. *(Continued.)*

Related Works		Metric	Antenna system	Number of RIS	Channel fading	Major Contributions
Single user with multiple eves	[179]	SOP and ASR	SISO	Single	Rice	GA-based TAaPSA strategy improved ASR and its accuracy is verified by simulation results
	[67]	ESC	SISO	Single	-	Asymptotic analysis of obtained ESC shows that ESC scales with log N in presence of both colluding and non-colluding Eves
	[41]	Secret key capacity	MISO	Single	Rayleigh	Proposed SCA-SDR optimization algorithm with RIS outperforms technique without RIS
	[31]	Achievable SR	MISO	Single	Quasi-static flat fading	Proposed RIS-assisted cooperative jamming scheme provides good trade-off between energy efficiency and secrecy rate
	[180]	ASR	MISO	Single	Large scale and small scale fading	Proposed AO based RSBF scheme performs better than MRT-based scheme, perfect CSI based scheme and average based scheme
	[181]	SR	MISO	Single	Rayleigh	By joint transmit beamforming with AN and RIS reflect beamforming, SR is maximized
Multiple users with one eve	[182]	ASR	MISO	Single	Quasi-static block fading	Proposed user scheduling scheme improves ASR and lower bound on ASR and its scaling laws are also derived
	[114]	SR	MISO	Single	Rayleigh	Proposed SROCR based AO algorithm performs better than random phase and EPA; Security effectiveness validated numerically
Multiple users with multiple eves	[183]	Minimum SR	MISO	Single	Rician	Joint optimization by AO and ZFB to maximize minimum SR
	[184]	System sum-rate and avg. sum SR	MISO	Multiple	Rician	Proposed AO algorithm is robust and uniform distribution of reflecting elements among multiple RISs improves PLS

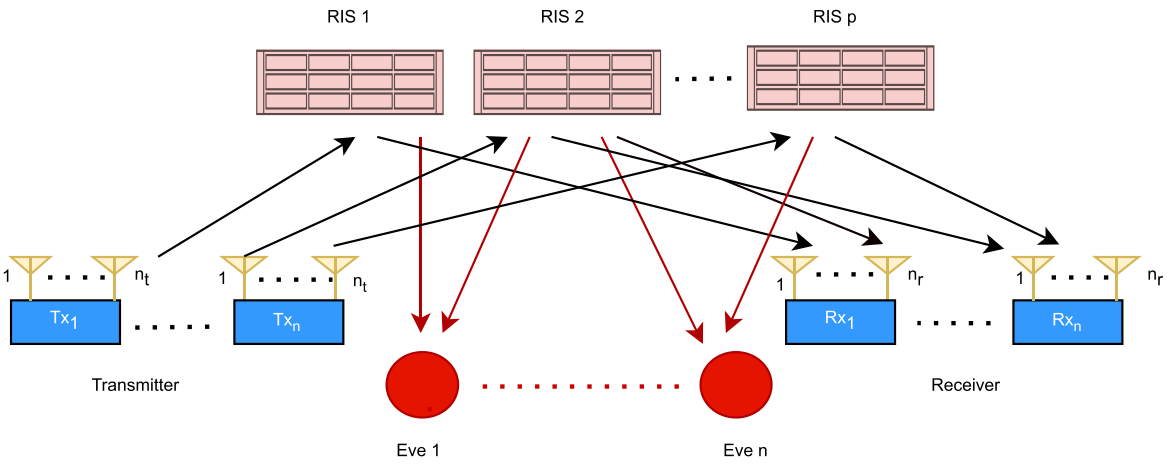

FIGURE 7. Generic RIS-assisted System Setup.

works on secrecy enhancement of RIS-assisted wireless networks with single/multiple users and single/multiple Eves.

A. SECURED TRANSMISSION FOR A SINGLE USER WITH ONE EVE

In Fig. 7, we consider a generic RIS-assisted system setup consisting of t transmitters, k receivers, n Eves, and p number of RISs each with L reflecting elements. Each transmitter and receiver is composed of n_t and n_r number of antennas respectively.

1) SISO

For SISO wireless network configuration with a single transmitter, single receiver, single RIS, and an Eve, we consider $t = 1, k = 1, n = 1, p = 1, n_t = 1$ and $n_r = 1$. Table 3 presents a representative study considering this setup. Authors in [40] have derived an asymptotic expression for SOP

of RIS-assisted communication system in the presence of a passive Eve, and verified by simulations. SOP versus average SNR results for different RIS elements is presented. The authors in [162] discussed the PLS performance of RIS-assisted communication systems with imperfect phase compensation. A channel model for legitimate and wiretap links is used to formulate three scenarios. The first scenario considered folded normal and Rayleigh distributions for legitimate and illegitimate links, respectively, assuming no phase errors. In the second and third scenarios, legitimate links are modeled by Beckmann and Nakagami distributions, respectively, whereas illegitimate links are modeled by Rayleigh distribution, assuming phase errors in both cases. Both active as well as passive eavesdropping cases are considered. The authors derived the analytical expressions of SOP and average SR for each scenario and provided an open problem for investigating the secrecy performance of the multi-antenna system.

Recently, secret key generation (SKG) has gained popularity in safeguarding legitimate data communication from eavesdropping [41], [163]. Several research works have been reported in the literature [41], [42], [163], [164], [165], [166] for SKG and the secret key rate maximization in RIS-assisted wireless networks. SKG approach proves to be a lightweight PLS technique that uses shared keys among legitimate users to secure the privacy of the data communication from malicious users. Hence, Eves face difficulty in decoding the information because there is a low correlation between legitimate channels and Eves. In [163], the authors aim to increase the secret key capacity of the RIS-assisted system by optimizing the location of intelligent RIS units. The system model is composed of a single antenna transmitter, receiver, and Eve. The secret key capacity formula is derived, and besides enhancing the secret key capacity, the bit inconsistency rate is also reduced. In [41], [163], the authors have utilized RIS for SKG in order to enhance the secret key capacity. In [163], the authors consider a single Eve whereas [41] dealt with multiple non-colluding Eves. The Eves in both [41] and [163] are not completely passive, so, their CSI statistics are available to the transmitter as well as to the receiver. The authors in [167] investigated both constructive and destructive impact of RIS on physical layer key generation (PKG) scheme. The system setup is composed of a transmitter, receiver, RIS and an eavesdropper which can be active or passive. The experimental results demonstrated the improvement in sum secrecy rate.

The authors in [168] investigated the environment reconfiguraton attack (ERA) which is a wireless jamming attack primitive. The system setup is composed of legitimate transmitter, receiver and an eavesdropper that employ OFDM modulation technique along with RIS. RIS behaves as a practical low-cost toolkit for attackers and helps in disturbing legitimate receivers and thus randomness increases. Analytical, simulation as well as experimental results are presented. The results demonstrate that ERA is able to severely degrade available data rates even with small RIS. So, RIS acts as a powerful attacker tool that can deal with physical layer attacks against wireless communications. The authors in [169] designed a countermeasure against adversarial wireless sensing that is referred to as IRShield that acts as a plug-and-play privacy-preserving extension to the existing wireless infrastructure. The experimental evaluation of the designed system demonstrated that the adversarial motion detection rates from passive eavesdropping of wireless signals are lowered to 5% or less.

The authors in [170] analysed the security gap concept for Gaussian channels and for the discrete memoryless channels (DMCs) for any finite codelengths under any reliability/security conditions and at any transmission rates. The authors in [171] have proposed a suitable performance metric for URLLC networks, i.e., COP that maintains a trade-off between latency, reliability, security and network throughput. In another research work [172], the authors have analysed the performance of PLS in RIS-assisted hybrid automatic repeat request (HARQ) system. The system setup is composed of single antenna transmitter, receiver, Eve and an RIS in non-LoS scenario. The closed form expressions for COP and SOP are obtained in RIS-assisted hybrid automatic repeat request with chase combining (HARQ-CC) and hybrid automatic repeat request with incremental redundancy (HARQ-IR) systems and the numerical results are verified by simulation results.

2) MISO

For MISO configuration with a single transmitter, receiver, RIS, and an Eve, we consider n_t number of transmit antennas, $n_r = 1$, $t = 1$, $k = 1$, $n = 1$ and a RIS i.e. $p = 1$ with L reflecting elements. The representative works considering this setup are given in Table 3 and discussed here. The authors in [38] and [114] investigated the secrecy performance of the RIS-assisted communication system when the Eve's CSI is not known and AN is utilized to prevent the leakage of information to the Eve, i.e. the Eve is completely hidden and does not exchange CSI with transmitter. In [38], the authors aimed to minimize the transmit power such that the desired QoS is satisfied at the receiver and utilize the remaining power for generating AN to jam the Eve's receiver. Two algorithms, namely, oblique manifold (OM) and minorization-maximization, are applied to solve the non-convex optimization problem, and the simulation results are reported in terms of average SR versus QoS threshold. Though SR is less compared to the scenario when the Eve's CSI is known, the level of secrecy is still appreciable. In [114], RIS-assisted NOMA transmission is considered and the CSI of multi-antenna Eve is imperfectly known. A Sequential rank-one constraint relaxation (SROCR) AO algorithm is proposed to efficiently optimize the RIS reflection coefficients and the transmit power. In [28], the authors considered maximizing the SR of RIS-assisted multi-antenna system with a single antenna Eve and then extended it to a multi-antenna Eve. They presented an alternating algorithm to jointly optimize the transmit covariance matrix and RIS's phase shift matrix under Rayleigh's fading channel model.

It is demonstrated via simulations that their RIS-assisted network improves the SR compared to the conventional technique without RIS. Furthermore, the impact of horizontal distance between the transmitter and the receiver is observed on the SR performance of the proposed method in [28]. As observed from the presented simulations, the SR increases with the increase in horizontal distance between the transmitter and the receiver, which is attributed to the receiver's closer proximity to RIS, thereby resulting in stronger reflect beamforming.

On a comparable basis, in [178], the authors aimed to maximize the SR of the network consisting of a multi-antenna transmitter, receiver, and Eve. Assuming that CSI is perfectly known to to the transmitter and the RIS. The differences are in the optimization techniques used at the transmitter and RIS. They have proposed two techniques, namely, element-wise block coordinate descent (BCD) and AO with minorization-maximization. The first is more suitable for small-scale RISs, while the second is more suitable for large-scale fading RISs. In [178], Rayleigh fading channels are employed. The simulation results indicate that the average SR performance for both BCD and AO algorithms is similar for wide range of transmit power values. The average SR performance is also compared with the no RIS scenario and demonstrates that the average SR improves significantly by employing the RIS. Similarly, in [185], the authors presented a power-efficient scheme that aimed to minimize the transmit power subject to secrecy constraints. A multi-antenna BS communicates with a single-antenna receiver in the presence of a single-antenna passive Eve. They employed an AO algorithm and semidefinite programming (SDP) relaxation to obtain an optimal secure transmit beamformer and reflecting beamformer design at RIS. The authors demonstrated that it outperforms when there is no RIS in terms of secure transmit power.

However, in prior works, the scenario like in [51] has rarely been thoroughly investigated, where the average power of a legitimate communication link is lesser than the Eve link. The considered channel in [51] is a quasi-state flat fading one. The average secrecy rate (ASR) is maximized by joint optimization of the access point (AP) transmit beamforming vector, and RIS reflect beamforming vector. An efficient algorithm based on alternating optimization (AO) maximizes the SR. The authors compared the performance of the proposed 'alternating optimization' based joint active and passive beamforming scheme with access point-maximum ratio transmission (AP-MRT) with RIS, without RIS. Furthermore, the proposed scheme in [51] was also validated by the analytical upper bound on SR, which agrees well with the simulation results. Using the presented simulation results in [51], it is shown that their scheme outperforms the existing benchmarks like AP-MRT in achieving secrecy.

The aforementioned research works studied the performance of single RIS-based wireless networks considering both large and small-scale RISs [178]. The SR performance can be further analyzed for multiple RISs scenarios. There are a few research works in which multiple RISs are considered to increase the communication links between the legitimate parties, which results in improved SR performance as demonstrated in [186], [187], [188], [189]. The multiple RISs are considered in order to make the data transmission more robust and secured [186]. Deep Reinforcement Learning approaches are also applied to smart radio environment composed of multiple RISs for the orchestration of tunable reflecting elements [190].

RIS can be used either as legitimate or eavesdropping in order to enhance the privacy of confidential information [187]. By deploying multiple RISs, the number of transmission paths between the legitimate receiver and the BS increases, which results in an improvement in the received signal power, thereby improving the overall SR performance [188]. The authors in [186] maximized the SR of the system in which multiple RISs cater to the users. When Eve is active, its CSI is available at AP. The switch state of each RIS is adjusted according to the system load. RIS phase shifts, AP transmit beamforming, and RIS switch state vector are jointly optimized to maximize SR under a given power constraint. They demonstrated that the proposed distributed RISs assisted scheme performs better in terms of SR than the conventional RIS-assisted scheme. In another research [187], the authors investigated the SR performance of multistream MIMO PLS system considering two RISs, i.e., one legitimate and the other eavesdropping RIS. The simulation system comprises a multi-antenna BS, a multi-antenna legitimate receiver, and a legitimate RIS. Within proximity of the legitimate communication link lies a multi-antenna Eve with an eavesdropping RIS to assist in decoding legitimate information. It was assumed that BS knows about the Eve but is unaware of the eavesdropping RIS. Similarly, the Eve is unaware of the deployment of the legitimate RIS. Frequency flat Rayleigh fading channels are considered. They showed that even with a minimal RIS size compared to an eavesdropping one, the SR increases over the whole range of SNR. In [189], the authors maximized the SR at the user in the network having RIS-assisted channel with inter-surface signal reflection. They apply the AO algorithm for joint optimization of the beamformer at transmitter and phase shift coefficients at double RIS. Product Riemannian manifold based AO algorithm is applied to optimize phase shift coefficients at both RIS. Performance comparison with the SDR-based AO algorithm demonstrates that SR in both cases is nearly the same but with a faster speed of convergence in the case of the Product Riemannian manifold based AO algorithm.

Furthermore, the performance can be analyzed under the generalized Nakagami-m distribution for small-scale fading as opposed to the Rayleigh fading channel models considered in the aforementioned works [28], [38], [114], [178]. The Nakagami-m distribution reduces to Rayleigh for $m = 1$, unilateral Gauss distribution for $m = 0.5$, and for the channel without fading, $m \to \infty$ [191], where m is the diversity order. In another research work [30], the authors discussed the secrecy capacity of a RIS-assisted cooperative network consisting of a transmitter, receiver, and Eve. RIS is likely to be

aware of CSI of all channels. The authors in [30] formulated a generic multi-objective AO problem that focused on finding secrecy capacity by improving the receiver's channel and degrading the Eve's channel. The simulation results demonstrated that the average secrecy capacity improves irrespective of the system setup by deploying a RIS. To obtain optimal reflection coefficients for RIS elements, the authors in [192] use ML and deep learning (DL) techniques to reduce the computational complexity of the RIS-assisted wireless system. The system setup consists of a multi-antenna AP, a legitimate receiver, an Eve, and a RIS. All channels in the system experience quasi-static flat fading and AP and RIS controller are fully aware of CSI of all channels. The simulation results have shown that ML and DL approach provides a comparable SR performance with reduced time and computational complexity compared to the conventional learning approaches [28], [51].

The researchers also focus on enhancing the SR of wireless communication in the mm/terahertz (THz) band by applying powerful beamforming techniques [193], [194]. In [173], the authors investigated the performance of the RIS in providing security to wireless communication in the mm/THz band. The considered channel in [173] is a rank one channel model with a dominant LoS link for the BS-RIS case in the presence of passive Eve. This paper discussed the SR maximization assuming discrete phase shift by joint optimization of the transmit beamforming and reflecting matrix. SR performance in terms of simulation curves is reported, and it is shown that with the increase in the number of reflecting elements of RIS, there is a steady increase in SR. Also, the SR performance enhances appreciably by applying SDP-based and BCD methods. Authors in [174] maximized the SR of downlink THz communication in the MISO wiretap channel by designing the active beamformer at the BS and the passive reflecting phase shifters at the RIS. They use a clustered channel model based on the extended Saleh Valenzuela model. RIS operates in two modes, i.e., sensing mode (for channel estimation) and computing mode. To jointly optimize the phase shifters and beamformers, two high-quality suboptimal designs are discussed, i.e., the closed-form successive design (SD) and the iterative joint design (JD). It is shown that the proposed RIS-based SD and JD methods perform better than the traditional optimal secure beamforming without RIS in terms of achievable secrecy data rate.

In [175], the authors maximized the SR over the BS to the legitimate user by jointly optimizing the BS beamforming matrix and the RIS phase shift matrix. The system design consists of a single antenna receiver, a multiple antenna Eve, one RIS, and one BS equipped with a multi-antenna uniform linear array. CSI is available to the BS and the RIS. The difference between the works in [174] and [175] lies in the kind of applied optimization techniques and also in the chosen frequency band. In [175], the authors developed an efficient algorithm that is executed by optimizing the phase shift matrix at RIS and transmitting beamforming vectors alternately, keeping the other parameters fixed. They exploit Majorization-Minimization (MM) and manifold optimization (MO) techniques to obtain the solution. The proposed algorithm in [175] not only improves the SR but is also computationally more efficient than the existing Charnes-Cooper transform and semidefinite relaxation (CCT-SDR).

In this part, we have reviewed the performance of RIS in enhancing the SR of wireless communication in the mm/THz band considering a single Eve. Then the joint optimization of the transmitter's beamforming matrix and RIS phase shift matrix is done to maximize the SR. Further investigation can be done by considering multiple colluding as well as non-colluding Eves since we need to thoroughly study the more realistic scenario. Practical optimization techniques that are cost and energy-efficient need to be designed to accurately obtain the CSI of Eves.

3) MIMO

In Fig. 7, by considering n_t number of transmit antennas, n_r number of receive antennas, $t = 1$, $k = 1$, $n = 1$, and a RIS with multiple reflecting elements, a MIMO wireless network with a single transmitter, receiver and an Eve can be formulated. The representative work considering this setup is given in Table 3 and discussed here. Hong et al. in [176] aimed to enhance the SR in AN-assisted MIMO communication systems. The SR is improved by jointly optimizing the transmit precoding (TPC) matrix at the BS, the covariance matrix of AN, and phase shifts at the RIS. The proposed algorithm is BCD, assisted by the MM algorithm. The Rayleigh fading is considered for the direct links between the BSs to the Eve and the receiver while Rician fading is considered for RIS links [176]. It is shown that by increasing the number of RIS-reflecting elements, one can obtain a higher converged SR value at the cost of increased computational complexity. As inferred from the simulation results presented in [176], the proposed algorithm is found to be significantly superior to the existing algorithms, namely, no-RIS scenario, RandPhase, and block coordinate descent-quadratically constrained quadratic program-semidefinite relaxation in terms of SR.

The authors in [177] investigated the secrecy performance of a RIS-assisted MIMO and multi-Eve system that aims to enhance the secured communication among the multi-antenna enabled mobile devices targeting the beyond fifth generation (5G) mobile communication networks. They presented a system where all entities, i.e., the transmitting AP, the legitimate receiving user, and the Eve, have multiple antennas. CSI for all channels are accurately known at AP. RIS composed of multiple passive elements dynamically adjusts the phase shift of each reflecting element based on the propagation environment learned through periodic sensing [195]. In order to enhance the SR, the transmit covariance matrix at the AP and the RIS reflection coefficients are optimized jointly for both discrete and continuous RIS coefficients. The transmit covariance matrix optimization problem is solved by

a successive convex approximation (SCA)-based algorithm to maximize the secrecy rate. This work can be extended to multiple legitimate users and multiple Eves. The authors of [32] investigated the impact of fading on the secrecy system performance and maximized the achievable secrecy rate with the required transmit power budget. The AN was introduced to bring in additional interference to degrade the reception of the Eve by exploiting the RIS-induced extra DoF. A generic MIMO system with a single BS, a legitimate receiver, a single Eve, and a RIS was considered. The work in [32] assumes that the CSI of the Eve is available at the BS. The BCD algorithm was applied to jointly optimize the secure precoder, the AN jamming precoder, and the phase shift matrix at the RIS. Using the weighted minimum mean square error (WMMSE) algorithm and the Karush-Kuhn-Tucker (KKT) conditions, the authors in [32] have derived the closed-form expressions for the secure precoder and the AN jamming precoder phase shift using the MM algorithm. The proposed algorithm proves to be superior over the baseline schemes in terms of SR. The authors in [196] have proposed RIS-assisted physical layer key generation (PLKG) strategy for TDD systems. The system model is a MIMO system composed of a transmitter, receiver, eavesdropper and RIS. The experimental results demonstrate that the proposed scheme achieves high KGR, low key error rate and randomness.

B. SECURED TRANSMISSION FOR A SINGLE USER WITH MULTIPLE EVES

In this Section, we classify the research works with a single receiver and multiple Eves based on number of antennas at the transmitter and receiver.

1) SISO

For this setup, we consider $n_t = 1$, $n_r = 1$, $t = 1$, $n = 1$, k number of Eves and an RIS. The related works are summarised in Table 3. The authors in [179] aimed to boost the average secrecy performance of a RIS-assisted indoor wireless communication system in which a legitimate transmitter wants to communicate with a legitimate receiver in the presence of potential Eves and a RIS. The channel fading follows the Rice distribution. Using an analytical genetic algorithm (GA), an optimal tile-allocation-and-phase-shift-adjustment (TAaPSA) strategy maximizes the achievable secrecy rate. The closed-form expressions for SOP and achievable secrecy rate are derived, and it shows that for low numbers of Eves, the achievable secrecy rate can be improved by increasing the achievable rate of legitimate users and simultaneously decreasing the overhearing rate of illegitimate users. Also, the location of the RIS proves to be a potential solution to further enhance the secrecy performance. Xu et al. in [67] studied the ESC of RIS-assisted communication systems considering discrete phase shifts and both colluding and non-colluding Eves. Assuming that RIS is fully aware of instantaneous legitimate CSI but completely unaware of the instantaneous eavesdropping CSI. The asymptotic analysis demonstrates that the ESC scales with the number of RIS reflecting elements for both kinds of Eves.

As discussed earlier, in [41], the authors adopted the secret key generation concept by utilizing RIS in order to enhance the secrecy key capacity. Multiple non-colluding Eves are considered and RIS's ability was utilized to modify reflection coefficients that helped in minimizing the secret key leakage to Eves. A closed-form expression for lower bound on RIS-assisted wireless networks' secret key capacity is derived along with the multiple elements reflecting coefficient matrix that helped to increase the minimum secret key capacity. Semidefinite relaxation-successive convex approximation (SDR-SCA) optimization technique was applied to obtain the desired solutions. The authors have shown that by increasing the size of RIS in the network and using SDR-SCA, the secret key capacity is improved compared to other benchmark systems, such as one without RIS and one with RIS. The authors presented another study in [164] to generate secret keys in a RIS-assisted wireless network. RIS was utilized to generate artificial randomness in the propagation channel to achieve fast phase switching and support one time password-encrypted data transmission. Secure transmission rate and key generation rate (KGR) are derived and based on this, an optimal time slot allocation algorithm is formulated that caters to two phases, one is for key generation, and the other corresponds to data transmission. Here, the authors considered multiple Eves with the non-availability of CSI, and the Poisson point process (PPP) is used to derive KGR. Simulation results demonstrated that this proposed scheme outperforms the other two schemes, i.e., random phase-shifted RIS and when there is no RIS.

2) MISO

Many research works in the literature deal with security enhancement in RIS-assisted MISO wireless networks with multiple Eves. Table 3 lists some notable works in this area. We consider a MISO wireless network consisting of a multi-antenna transmitter, receiver, multiple Eves, and a RIS with multiple reflecting elements by taking n_t number of transmit antennas, $n_r = 1$, $m = 1$, $k = 1$, n number of Eves and a RIS in Fig. 7. The authors in [181] have determined the viability of the introduction of AN to enhance the security of RIS-assisted communication systems under a Rayleigh faded scenario. The authors maximize the SR by joint transmit beamforming with AN and RIS reflect beamforming. They compared the performance of four scenarios, namely both AN and RIS networks, only AN networks, only RIS networks, and finally, no RIS networks. The numerical results presented in [181] indicate that the AN-assisted network delivers the best secrecy performance irrespective of the presence or absence of RIS. It was also demonstrated that with the increase in the number of eves, AN's presence proves to be more helpful than the RIS since it suppresses the information received by the Eve when the Eve and receiver are close to the RIS.

In [180], the authors considered two eavesdropping scenarios, i.e. colluding and non-colluding Eves and the transmitter is not completely aware about CSI of Eves' channels. The authors maximized the achievable secrecy rate in the presence of both the above eavesdropping scenarios. They distributed Eves randomly around the receiver, and the angle of arrival (AoA)-based CSI of the cascaded wiretap channel is imperfectly known. An efficient AO-based robust and secure beamforming (RSBF) scheme was presented that proved to perform better than the standard schemes. RIS can enhance spectrum as well as energy efficiency. So, there are a few papers that deal with improving energy efficiency besides providing security to the network [31], [197]. In [31], the authors investigated the secrecy performance of the RIS-assisted wireless network in the presence of cooperative jamming. The cooperative jamming concept involves transmitting the cooperative jamming signal that disturbs the Eve, and therefore, the signal helps in enhancing the SR. The work also aimed to maximize the energy efficiency of the network. The beamforming vector, jamming vector, and phase shift matrix were jointly optimized to maximize the energy efficiency and improve the SR over other benchmark schemes. In [197], the authors considered a RIS-assisted-secure-energy-efficient transmission that maximized the transmit power such that the SNR at legitimate user and Eve is under control. They optimized the beamforming weights at the transmitter and phase shift coefficients at RIS. All channels experience Rayleigh fading and perfect CSI is available at transmitter and receiver. It is shown that over the entire range of target SR, the transmit power of the proposed scheme remains almost constant, and noticeable improvement is seen compared to the other benchmark schemes.

C. SECURED TRANSMISSION FOR MULTIPLE USERS WITH ONE EVE

In this Section, the classification of research works consisting of multiple receivers with one Eve is done based on number of antennas at transmitter and receiver.

1) MISO

In [182], the authors proposed a multi-user two-way communication setup with RIS and evaluated its secrecy performance. The system setup comprises several pairs of end-users, a RIS, and an Eve. Due to the non-LoS scenario, the RIS establishes communication links between the end users. Channels experience quasi-static block fading. Due to passive Eve, the instantaneous CSI of the Eve is not known to the users. The proposed scheme in [182] utilizes the signal from one particular user as good jamming to disturb the reception of the signal at the Eve. A user scheduling scheme is also derived to enhance the ASR. It was shown that it improves with the number of reflecting elements. ASR scaling laws are also derived considering very large transmit power, RIS reflecting elements, and the number of end-user pairs.

D. SECURED TRANSMISSION FOR MULTIPLE USERS WITH MULTIPLE EVES

Here, we consider the case when multiple receivers with multiple eves are present.

1) MISO

This scenario considers a MISO wireless network consisting of a multi-antenna transmitter, multiple receivers, and Eves, and a RIS with multiple reflecting elements, by taking n_t number of transmit antennas, $n_r = 1$, $m = 1$, k number of receivers and n number of Eves in Fig. 7. In [183], the authors discussed the programmable wireless environment for PLS to achieve highly efficient secret communication. All receivers and Eves are in the same direction as the transmitter, due to which their channel responses are highly correlated. The conventional beamformers at transceivers are not guaranteed to deliver improved secrecy. The SNR needs to be increased at the desired receiver, thereby calling for RIS-based techniques. Hence, to improve the secrecy aspect of wireless communication between legitimate users, RIS is employed to create an extra link so that the SNR of legitimate links improves, whereas it suppresses at Eves. They jointly optimized the BS and beamformers and RIS reflection coefficients to maximize the minimum SR among all legitimate users. Since the problem is non-convex, AO based path-following algorithm is applied for a single transceiver and an Eve system. Heuristic closed-form solutions based on zero-forcing beamforming (ZFB) are formulated for multiple receivers and Eves.

In [184], the authors considered the worst-case assumption, i.e., Eves possess more hardware resources and computational capabilities than legitimate users. The perfect CSI of Eves is unknown at AP. The Rician fading model is employed. The system setup consists of multi-antenna AP, multiple single-antenna legitimate users, and multi-antenna potential Eves. Transmit beamformers, AN covariance matrix, and RIS phase shifts are jointly optimized, and a robust, secured system demonstrates the vast potential of RIS in enhancing the PLS of future wireless communication systems.

V. TECHNICAL CHALLENGES AND FUTURE DIRECTIONS

In this Section, we discuss the technical challenges and open research directions that are identified on the basis of the presented survey.

A. CSI ACQUISITION

Most of the research works in RIS-assisted wireless networks are based on the assumption of the availability of exact CSI at the transmitter and/or RIS since accurate CSI is critical in order to optimally adjust the RIS elements to achieve maximum performance gains [198]. By employing long-term CSI, we can reduce the computational complexity of the overall system [198]. Also, it plays a crucial role while choosing a suitable secrecy performance metric and accordingly the appropriate PLS technique that can be applied for secured

data transmission. However, in reality, knowledge of imperfect CSI can only be made available to the transmitter since the RIS is composed of a large number of passive reflecting elements, which makes it a very challenging task [45]. The conventional channel estimation schemes for RF are not suitable for RIS-assisted communication systems since the transceiver for RIS is entirely different from the conventional RF transceivers [198]. The authors in [114] assumed that the transmitter did not have complete knowledge of the CSI of the Eve, thereby necessitating more transmit power to achieve higher secrecy and reduce channel estimation inaccuracy. Hence, there is a need to design new channel estimation methods for RIS-assisted wireless communication links for different fading channel models.

B. COST AND ENERGY-EFFICIENT PRACTICAL PROTOCOLS

The practical protocols required to deploy RIS at different places, optimally design them, and facilitate information exchange between the RIS and the traditional transceivers need to be cost and energy-efficient. We can apply PLS techniques for secured data transmission in IoT-based networks, but these strategies should have cost and power efficiency besides being delay-sensitive [199]. In [200], the authors have proposed a dynamic spectrum learning-assisted RIS framework in which by intelligently controlling the ON-OFF status of RIS elements, the energy efficiency and hence, the received SINR can be improved. But from the PLS point of view, the design of cost and power-efficient techniques for RIS-assisted wireless communication systems is still an open research problem.

C. RIS-ASSISTED PLS OF LATEST 6G-BASED WIRELESS COMMUNICATION TECHNOLOGIES

6G networks focus on human-centric applications such as AI, virtual reality (VR), 3D media, blockchain technology, and the Internet of Everything (IoE) [201]. AI is the most crucial technology for 6G networks [202], [203], [204], [205], [206]. Tight integration of RIS with these latest wireless communication technologies such as mmWave communication, free-space optics, blockchain technology, mobile edge computing (MEC) architecture for space information networks (SIN) [207] etc., and its secrecy performance evaluation needs to be explored [208]. By optimally tuning the phase shifts of the scattering elements of RIS, the transmitted signals can be either reflected or refracted depending on the position of the legitimate receiver and Eve. With that adjustable reflected phase-shifted signal and the transmitted signal, one can improve the security and energy efficiency of the network.

D. RIS-ASSISTED MIMO SYSTEM WITH MULTIPLE EVES AND USERS

The researchers need to address yet another challenge based on this literature survey. They need to consider a more practical scenario with multiple Eves, and receivers [17] and improve the secrecy performance of the system. In [209], the authors investigated the secrecy performance of the system composed of multiple Eves and receivers. The authors in [210] investigated the secrecy performance of the massive MIMO system composed of a BS, multiple users, and an Eve. In another research, [211], the system setup consists of a downlink Rician MIMO channel, a multi-antenna BS, multi-antenna user, multi-antenna Eve, and a RIS, and they generate ergodic SRs. So, a more practical scenario with a better practical PLS improvement strategy and less signaling overhead needs to be designed [157].

VI. CONCLUSION

The RIS is found to be a promising technology for enhancing the PLS of wireless networks and facilitating 6G wireless communication. Their ability to smartly control the propagation environment helps in improving the SR of wireless communication. This paper presents a detailed literature survey on the PLS of RIS-assisted wireless communication links for different systems and channel models. First, a brief discussion on the RIS and its applications in the 6G scenario is presented in this survey article. We discuss the various performance metrics used to evaluate the secrecy performance of wireless networks. Next, we present a detailed literature review on the RIS-assisted PLS of different wireless systems, including SISO, MISO and MIMO categorized based on the number of Eves. Finally, this survey presents the technical challenges and a few possible future research directions.

The research topics are related to RIS usage in 6G networks due to its diversified applications, and practical limitations such as the availability of complete CSI and hardware impairments. The performance of RIS-assisted wireless networks can be further analyzed whilst considering the mobility and orientation of RIS in combination with the MIMO system comprising multiple Eves and receivers. The performance gain in terms of secrecy rate due to RIS can be further studied by considering information encoding and QoS provisioning as well. Also, practical optimization strategies that can provide maximum performance gains from channel and RIS physical characteristics can be explored. Apart from security, the critical concern that one should consider while designing the PLS techniques for RIS-assisted links is the satisfaction of QoS requirements like reliability, power efficiency, spectral efficiency, and delay conditions.

REFERENCES

[1] 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, Secondquarter 2019.

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

[3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.

[6] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017, doi: 10.1073/pnas.1618130114.

[7] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[8] J. Yuan, Y. Yang, and N. Zhou, *SPECIAL TOPIC: Physical Layer Security for Wireless and Quantum Communications*, vol. 11, no. 3, P. R. China: ZTE Commun., 2013.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[10] R. T. Yazicigil et al., "Beyond crypto: Physical-layer security for Internet of Things devices," *IEEE Solid-State Circuits Mag.*, vol. 12, no. 4, pp. 66–78, Fall 2020.

[11] J. Xu et al., "Reconfiguring wireless environments via intelligent surfaces for 6G: Reflection, modulation, and security," *Sci. China Inf. Sci.*, vol. 66, Mar. 2023, Art. no. 130304.

[12] I. Union, "IMT traffic estimates for the years 2020 to 2030," *Rep. ITU*, 2015.

[13] W. Long, R. Chen, M. Moretti, W. Zhang, and J. Li, "A promising technology for 6G wireless networks: Intelligent reflecting surface," *J. Commun. Inf. Netw.*, vol. 6, no. 1, pp. 1–16, Mar. 2021.

[14] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019.

[15] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G," *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018.

[16] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[17] 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.

[18] Q. Gu, D. Wu, X. Su, J. Jin, Y. Yuan, and J. Wang, "Performance comparisons between reconfigurable intelligent surface and full/half-duplex relays," in *Proc. IEEE 94th Veh. Technol. Conf.*, 2021, pp. 01–06.

[19] 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.

[20] B. Yang et al., "Federated spectrum learning for reconfigurable intelligent surfaces-aided wireless edge networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9610–9626, Nov. 2022.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

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

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

[28] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[29] 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.

[30] A. Almohamad, A. Al-Kababji, A. Tahir, T. Khattab, and M. Hasna, "On optimizing the secrecy performance of RIS-assisted cooperative networks," in *Proc. IEEE 92nd Veh. Technol. Conf.*, 2020, pp. 1–5.

[31] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy-efficient beamforming and cooperative jamming in IRS-assisted MISO networks," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–7.

[32] Z. Chu et al., "Secrecy rate optimization for intelligent reflecting surface assisted MIMO system," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1655–1669, 2020.

[33] L. Subrt and P. Pechac, "Controlling propagation environments using intelligent walls," in *Proc. 6th Eur. Conf. Antennas Propag.*, 2012, pp. 1–5.

[34] T. Cui, M. Q. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light: Sci. Appl.*, vol. 3, 2014, Art. no. 218.

[35] 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.

[36] 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.

[37] X. Cao et al., "AI-assisted MAC for reconfigurable intelligent-surface-aided wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 21–27, Jun. 2021.

[38] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300–1304, 2020.

[39] L. Dong and H.-M. Wang, "Enhancing secure MIMO transmission via intelligent reflecting surface," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7543–7556, Nov. 2020.

[40] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[41] Z. Jiet al., "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030–1034, Jan. 2021.

[42] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1867–1870, Sep. 2021.

[43] C. Pan et al., "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, 2021.

[44] L. Dong, H.-M. Wang, and J. Bai, "Active reconfigurable intelligent surface aided secure transmission," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2181–2186, Feb. 2022.

[45] 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.

[46] L. Mucchi et al., "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[47] W. U. Khan et al., "Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 22–28, Dec. 2022.

[48] M. S. Kumar, R. Ramanathan, and M. Jayakumar, "Key less physical layer security for wireless networks: A survey," *Eng. Sci. Technol., Int. J.*, vol. 35, Art. no. 101260, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098622001690

[49] 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.

[50] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1196–1217, 2023.

[51] 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.

[52] 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*, 2021, pp. 1–6.

[53] 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.

[54] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[55] S. Majhi, "Intelligent and secure transceiver design and implementation for future wireless communication," *CSI Trans. ICT*, vol. 8, pp. 157–164, 2020.

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

[57] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 1, pp. 196–248, Firstquarter 2020.

[58] E. Yaacoub and M. Al-Husseini, "Achieving physical layer security with massive MIMO beamforming," in *Proc. 11th Eur. Conf. Antennas Propag.*, 2017, pp. 1753–1757.

[59] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic distributed space-time coding for decode-and-forward cooperation systems," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1766–1781, Apr. 2012.

[60] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, pp. 311–335, 1998.

[61] W. Fang et al., "Information security of PHY layer in wireless networks," *J. Sensors*, vol. 2016, 2016, Art. no. 1230387.

[62] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[63] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 356–360.

[64] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[65] Y. Liu, L. Li, H. Zhang, A. Gao, and X. Li, "Optimal secrecy throughput and efficient energy harvesting for SWIPT system," in *Proc. 13th IEEE Conf. Ind. Electron. Appl.*, 2018, pp. 111–116.

[66] 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*.

[67] P. Xu, G. Chen, G. Pan, and M. D. Renzo, "Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[68] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[69] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.

[70] Y. Zou, J. Zhu, and X. Wang, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2014.

[71] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[72] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 2052–2057.

[73] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3480–3495, 2021.

[74] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[75] H. Zhang, Y. Huang, S. Li, and L. Yang, "Energy-efficient precoder design for MIMO wiretap channels," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1559–1562, Sep. 2014.

[76] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[77] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on OFDM physical layer security," *Phys. Commun.*, vol. 32, pp. 1–30, 2019.

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

[79] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Thirdquarter 2014.

[80] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1878–1911, Secondquarter 2019.

[81] M. A. Arfaoui et al., "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, thirdquarter 2020.

[82] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

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

[84] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[85] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[86] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84–104, 2016.

[87] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[88] D. H. Tashman and W. Hamouda, "An overview and future directions on physical-layer security for cognitive radio networks," *IEEE Netw.*, vol. 35, no. 3, pp. 205–211, May/Jun. 2021.

[89] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[90] P. Yadav, S. Kumar, and R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, 2021, Art. no. e4270.

[91] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, "An overview of physical layer security with finite-alphabet signaling," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1829–1850, Secondquarter 2019.

[92] A. K. Kamboj, P. Jindal, and P. Verma, "Machine learning-based physical layer security: Techniques, open challenges, and applications," *Wireless Netw.*, vol. 27, no. 8, pp. 5351–5383, Nov. 2021.

[93] K. W. Choi et al., "Simultaneous wireless information and power transfer (SWIPT) for Internet of Things: Novel receiver design and experimental validation," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2996–3012, Apr. 2020.

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

[95] C. You, Z. Kang, Y. Zeng, and R. Zhang, "Enabling smart reflection in integrated air-ground wireless network: IRS meets UAV," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 138–144, Dec. 2021.

[96] E. C. Strinati et al., "Reconfigurable, intelligent, and sustainable wireless environments for 6G smart connectivity," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 99–105, Oct. 2021.

[97] X. Cao, B. Yang, H. Zhang, C. Huang, C. Yuen, and Z. Han, "Reconfigurable-intelligent-surface-assisted MAC for wireless networks: Protocol design, analysis, and optimization," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14171–14186, Sep. 2021.

[98] M. D. 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.
[99] E. C. Strinati et al., "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–50, Sep. 2019.
[100] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.
[101] S. Kisseleff, W. A. Martins, H. Al-Hraishawi, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1781–1797, 2020.
[102] Z. Wan, Z. Gao, F. Gao, M. D. Renzo, and M.-S. Alouini, "Terahertz massive MIMO with holographic reconfigurable intelligent surfaces," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4732–4750, Jul. 2021.
[103] W. Xu, J. An, C. Huang, L. Gan, and C. Yuen, "Deep reinforcement learning based on location-aware imitation environment for RIS-aided mmwave mimo systems," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1493–1497, Jul. 2022.
[104] S. Zhang et al., "Intelligent Omni-surfaces: Ubiquitous wireless transmission by reflective-refractive metasurfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 219–233, Jan. 2022.
[105] N. Mensi, D. B. Rawat, and E. Balti, "Physical layer security for V2I communications: Reflecting surfaces vs. relaying," in *Proc. IEEE Glob. Commun. Conf.*, 2021, pp. 01–06.
[106] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf.*, 2020, pp. 1–6.
[107] Y. Ai, F. A. P. deFigueiredo, L. Kong, M. Cheffena, S. Chatzinotas, and B. Ottersten, "Secure vehicular communications through reconfigurable intelligent surfaces," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7272–7276, Jul. 2021.
[108] L. Qian, X. Chi, L. Zhao, and A. Chaaban, "Secure visible light communications via intelligent reflecting surfaces," in *Proc. IEEE Int. Conf. Commun.*, 2021, pp. 1–6.
[109] 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.
[110] W. Zhang, X. Zhao, and G. Jiang, "Physical layer security for intelligent reflecting surface-assisted VLC/RF hybrid network," in *Proc. 14th Int. Conf. Commun. Softw. Netw.*, 2022, pp. 23–27.
[111] 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.
[112] 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.
[113] H. Long et al., "Joint trajectory and passive beamforming design for secure UAV networks with RIS," in *Proc. IEEE Globecom Workshops*, 2020, pp. 1–6.
[114] Z. Zhang, L. Lv, Q. Wu, H. Deng, and J. Chen, "Robust and secure communications in intelligent reflecting surface assisted NOMA networks," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 739–743, Mar. 2021.
[115] N. Li, M. Li, Y. Liu, C. Yuan, and X. Tao, "Intelligent reflecting surface assisted NOMA with heterogeneous internal secrecy requirements," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 1103–1107, May 2021.
[116] W. Wang et al., "Beamforming and jamming optimization for irs-aided secure noma networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.
[117] 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.
[118] N. Nandan, S. Majhi, and H.-C. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5327–5337, Aug. 2018.
[119] H. Xiao, L. Dong, and W. Wang, "Intelligent reflecting surface-assisted secure multi-input single-output cognitive radio transmission," *Sensors*, vol. 20, no. 12, 2020, Art. no. 3480.
[120] L. Dong, H.-M. Wang, H. Xiao, and J. Bai, "Secure intelligent reflecting surface assisted MIMO cognitive radio transmission," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2021, pp. 1–6.
[121] L. Dong, H.-M. Wang, and H. Xiao, "Secure cognitive radio communication via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4678–4690, Jul. 2021.
[122] X. Wu, J. Ma, Z. Xing, C. Gu, X. Xue, and X. Zeng, "Secure and energy efficient transmission for IRS-assisted cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 1, pp. 170–185, Mar. 2022.
[123] M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, and M. S. Hossain, "The shift to 6G communications: Vision and requirements," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–27, 2020.
[124] 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.
[125] X. Li, H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Comput. Standards Interfaces*, vol. 78, 2021, Art. no. 103540.
[126] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.
[127] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, 2018, Art. no. 730.
[128] M. B. Janjua, A. E. Duranay, and H. Arslan, "Role of wireless communication in healthcare system to cater disaster situations under 6G vision," *Front. Commun. Netw.*, vol. 1, 2020, Art. no. 6.
[129] Z. E. Ankaralı et al., "Physical layer security for wireless implantable medical devices," in *Proc. IEEE 20th Int. Workshop Comput. Aided Modelling Des. Commun. Links Netw.*, 2015, pp. 144–147.
[130] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334–366, 2021.
[131] H. Zhang, B. Di, K. Bian, Z. Han, H. V. Poor, and L. Song, "Toward ubiquitous sensing and localization with reconfigurable intelligent surfaces," *Proc. IEEE*, vol. 110, no. 9, pp. 1401–1422, Sep. 2022.
[132] C. D. Alwis et al., "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.
[133] P. Saarika, K. Sandhya, and T. Sudha, "Smart transportation system using IoT," in *Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon)*, 2017, pp. 1104–1107.
[134] S. Jaffry, "Intelligent reflecting surface aided wireless energy transfer and mobile edge computing for public transport vehicles," 2021, *arXiv:2102.08672*.
[135] M. Noor-A-Rahim et al., "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022.
[136] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.
[137] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, and G. Nauryzbayev, "Physical layer security in vehicular communication networks in the presence of interference," in *Proc. IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.
[138] A. Pandey and S. Yadav, "Physical layer security in cooperative AF relaying networks with direct links over mixed rayleigh and double-Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10615–10630, Nov. 2018.
[139] L. Xu et al., "Physical layer security performance of mobile vehicular networks," *Mobile Netw. Appl.*, vol. 25, no. 2, pp. 643–649, 2020.
[140] A. Pandey and S. Yadav, "Performance evaluation of amplify-and-forward relaying cooperative vehicular networks under physical layer security," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 12, 2018, Art. no. e3534.

[141] N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6G: Advances, challenges, and prospects," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 93–102, Dec. 2020.

[142] S. Aboagye, T. M. N. Ngatched, O. A. Dobre, and A. R. Ndjiongue, "Intelligent reflecting surface-aided indoor visible light communication systems," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 3913–3917, Dec. 2021.

[143] A. M. Abdelhady, A. K. S. Salem, O. Amin, B. Shihada, and M.-S. Alouini, "Visible light communications via intelligent reflecting surfaces: Metasurfaces vs mirror arrays," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1–20, 2021.

[144] D. Ma, M. Ding, and M. Hassan, "Enhancing cellular communications for UAVs via intelligent reflective surface," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2020, pp. 1–6.

[145] S. Li, B. Duo, X. Yuan, Y.-C. Liang, and M. D. Renzo, "Reconfigurable intelligent surface assisted UAV communication: Joint trajectory design and passive beamforming," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 716–720, May 2020.

[146] L. Ge, P. Dong, H. Zhang, J.-B. Wang, and X. You, "Joint beamforming and trajectory optimization for intelligent reflecting surfaces-assisted UAV communications," *IEEE Access*, vol. 8, pp. 78702–78712, 2020.

[147] H. Lu, Y. Zeng, S. Jin, and R. Zhang, "Enabling panoramic full-angle reflection via aerial intelligent reflecting surface," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2020, pp. 1–6.

[148] X. Liu, Y. Liu, and Y. Chen, "Machine learning empowered trajectory and passive beamforming design in UAV-RIS wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 2042–2055, Jul. 2021.

[149] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[150] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, Secondquarter 2016.

[151] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.

[152] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[153] Y. Cheng, W. Peng, C. Huang, G. C. Alexandropoulos, C. Yuen, and M. Debbah, "RIS-aided wireless communications: Extra degrees of freedom via rotation and location optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 6656–6671, Aug. 2022.

[154] A. C. Pogaku, D.-T. Do, B. M. Lee, and N. D. Nguyen, "UAV-assisted RIS for future wireless communications: A survey on optimization and performance analysis," *IEEE Access*, vol. 10, pp. 16320–16336, 2022.

[155] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Phys. Commun.*, vol. 12, pp. 16–32, 2014.

[156] K. Tekbıyık, A. R. Ekti, G. K. Kurt, and A. Görçin, "Terahertz band communication systems: Challenges, novelties and standardization efforts," *Phys. Commun.*, vol. 35, 2019, Art. no. 100700.

[157] J. Youn, W. Son, and B. C. Jung, "Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems," *Sensors*, vol. 21, no. 4, 2021, Art. no. 1439.

[158] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 3, pp. 2294–2323, Thirdquarter 2018.

[159] N. Nandan, S. Majhi, and H.-C. wu, "Beamforming and power optimization for physical layer security of MIMO-NOMA based CRN over imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5990–6001, Jun. 2021.

[160] N. Nandan, S. Majhi, and H.-C. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, Aug. 2018.

[161] H. M. Furqanet al., "Physical layer security for NOMA: Requirements, merits, challenges, and recommendations," 2019, *arXiv:1905.05064*.

[162] J. D. V. Sánchez, P. Ramírez-Espinosa, and F. J. López-Martínez, "Physical layer security of large reflecting surface aided communications with phase errors," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 325–329, Feb. 2021.

[163] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1036–1040, 2021.

[164] Z. Ji et al., "Random shifting intelligent reflecting surface for OTP encrypted data transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1192–1196, 2021.

[165] T. Lu, L. Chen, J. Zhang, K. Cao, and A. Hu, "Reconfigurable intelligent surface assisted secret key generation in quasi-static environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244–248, Feb. 2022.

[166] Y. Liu, M. Wang, J. Xu, S. Gong, D. T. Hoang, and D. Niyato, "Boosting secret key generation for IRS-assisted symbiotic radio communications," in *Proc. IEEE 93rd Veh. Technol. Conf.*, 2021, pp. 1–6.

[167] G. Li et al., "Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive ?," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 146–153, Aug. 2022.

[168] 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," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2022, pp. 208–221, doi: 10.1145/3488932.3497767.

[169] P. Staat et al., "IRShield: A countermeasure against adversarial physical-layer wireless sensing," in *Proc. IEEE Symp. Secur. Privacy*, 2022, pp. 1705–1721.

[170] I.-M. Kim, B.-H. Kim, and J. K. Ahn, "BER-based physical layer security with finite codelength: Combining strong converse and error amplification," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3844–3857, Sep. 2016.

[171] K. Yu, J. Yu, and A. Dong, "Cooperative communication and mobility for securing URLLC of future wireless networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5331–5342, May 2022.

[172] Y. Wu, K. Mu, K. Duan, S. Yin, and H. Yang, "On the secure performance of intelligent reflecting surface-assisted HARQ systems," *Entropy*, vol. 25, no. 3, 2023, Art. no. 519.

[173] 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.

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

[175] 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.

[176] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851–7866, Dec. 2020.

[177] W. Jiang, Y. Zhang, J. Wu, W. Feng, and Y. Jin, "Intelligent reflecting surface assisted secure wireless communications with multiple-transmit and multiple-receive antennas," *IEEE Access*, vol. 8, pp. 86659–86673, 2020.

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

[179] I. P. Honget al., "Secrecy performance analysis and optimization of intelligent reflecting surface-aided indoor wireless communications," *IEEE Access*, vol. 8, pp. 109440–109452, 2020.

[180] X. Lu, W. Yang, X. Guan, Q. Wu, and Y. Cai, "Robust and secure beamforming for intelligent reflecting surface aided mmWave MISO systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2068–2072, Dec. 2020.

[181] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not ?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[182] L. Lv, Q. Wu, Z. Li, N. Al-Dhahir, and J. Chen, "Secure two-way communications via intelligent reflecting surfaces," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 744–748, Mar. 2021.

[183] 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.

[184] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[185] 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.
[186] Y. Xiu and Z. Zhang, "Wireless secure signal transmission for distributed intelligent surface-aided millimeter wave systems," *IEEE Access*, vol. 8, pp. 193478–193491, 2020.
[187] G. C. Alexandropoulos, K. Katsanos, M. Wen, and D. B. D. Costa, "Safeguarding MIMO communications with reconfigurable metasurfaces and artificial noise," in *Proc. IEEE Int. Conf. Commun.*, 2021, pp. 1–6.
[188] A. Rafieifar and S. M. Razavizadeh, "Secrecy rate maximization in multi-IRS mmWave networks," *Phys. Commun.*, vol. 48, 2021, Art. no. 101436.
[189] L. Dong, H.-M. Wang, J. Bai, and H. Xiao, "Double intelligent reflecting surface for secure transmission with inter-surface signal reflection," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2912–2916, Mar. 2021.
[190] G. C. Alexandropoulos, K. Stylianopoulos, C. Huang, C. Yuen, M. Bennis, and M. Debbah, "Pervasive machine learning for smart radio environments enabled by reconfigurable intelligent surfaces," *Proc. IEEE*, vol. 110, no. 9, pp. 1494–1525, Sep. 2022.
[191] H. Popovic, D. Stefanovic, A. Mitic, I. Stefanovic, and D. Stefanovic, "Some statistical characteristics of Nakagami-m distribution," in *Proc. 8th Int. Conf. Telecommun. Modern Satell., Cable Broadcast. Serv.*, 2007, pp. 509–512.
[192] Y. Song, M. R. Khandaker, F. Tariq, K.-K. Wong, and A. Toding, "Truly intelligent reflecting surface-aided secure communication using deep learning," in *Proc. IEEE 93rd Veh. Technol. Conf.*, 2021, pp. 1–6.
[193] V. Degli-Esposti et al., "IEEE access special section editorial: Millimeter-wave and terahertz propagation, channel modeling, and applications," *IEEE Access*, vol. 9, pp. 67660–67666, 2021.
[194] Z. Haque, V. S. Kumar, and S. Majhi, "A closed-form secrecy outage probability for mmWave communication by ordered transmit beamforming," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 721–725, Mar. 2021.
[195] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," in *Proc. IEEE Glob. Commun. Conf.*, 2018, pp. 1–6.
[196] S. Liu et al., "Intelligent reflecting surface-assisted physical layer key generation with deep learning in MIMO systems," *Sensors*, vol. 23, no. 1, 2022, Art. no. 55.
[197] Y. Kawai and S. Sugiura, "QoS-constrained optimization of intelligent reflecting surface aided secure energy-efficient transmission," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 5137–5142, May 2021.
[198] C. Panet al., "Reconfigurable intelligent surfaces for 6G and beyond: Principles, applications, and research directions," 2020, *arXiv:2011.04300*.
[199] V. M. Rohokale, N. R. Prasad, and R. Prasad, "Cooperative wireless communications and physical layer security: State-of-the-art," *J. Cyber Secur. Mobility*, vol. 1, pp. 226–249, 2012.
[200] B. Yang et al., "Spectrum-learning-aided reconfigurable intelligent surfaces for "green" 6G networks," *IEEE Netw.*, vol. 35, no. 6, pp. 20–26, Nov./Dec. 2021.
[201] 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.
[202] R.-A. Stoica and G. T. F. de Abreu, "6G: The wireless communications network for collaborative and AI applications," 2019, *arXiv:1904.03413*.
[203] L. Lovén et al., "EdgeAI: A vision for distributed, edge-native artificial intelligence in future 6G networks," in *Proc. 1st 6G Wireless Summit*, 2019, pp. 1–2.
[204] F. Clazzer, A. Munari, G. Liva, F. Lazaro, C. Stefanovic, and P. Popovski, "From 5G to 6G: Has the time for modern random access come ?," 2019, *arXiv:1903.03063*.
[205] N. H. Mahmood, H. Alves, O. A. López, M. Shehab, D. P. M. Osorio, and M. Latva-Aho, "Six key features of machine type communication in 6G," in *Proc. 2nd 6G Wireless Summit*, 2020, pp. 1–5.
[206] J. Zhao, "A survey of intelligent reflecting surfaces (IRSs): Towards 6G wireless communication networks," 2019, *arXiv:1907.04789*.
[207] X. Cao et al., "Converged reconfigurable intelligent surface and mobile edge computing for space information networks," *IEEE Netw.*, vol. 35, no. 4, pp. 42–48, Jul./Aug. 2021.
[208] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 3, pp. 2794–2830, thirdquarter 2019.
[209] S. Majhi and N. Nandan, "Secrecy capacity analysis of MIMO system over multiple destinations and multiple eavesdroppers," *Wireless Pers. Commun.*, vol. 100, no. 3, pp. 1009–1022, 2018.
[210] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical layer security in massive MIMO systems," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput*., 2017, pp. 3–8.
[211] J. Liu, J. Zhang, Q. Zhang, J. Wang, and X. Sun, "Secrecy rate analysis for reconfigurable intelligent surface-assisted MIMO communications with statistical CSI," *China Commun.*, vol. 18, no. 3, pp. 52–62, 2021.

RAVNEET KAUR received the M.Tech. degree in digital communication from the Department of Electronics and Communication Engineering, Guru Gobind Singh Indraprastha University, New Delhi, India, in 2014. Her research interests include passive optical networks, wireless communication, physical layer security, and RIS-assisted communication.

BAJRANG BANSAL (Member, IEEE) received the B.E. degree in electronics and communication engineering from Institute of Technology and Management, Gurgaon, India, in 2005, the M.Tech. degree in VLSI Design and CAD from the Thapar University, Punjab, India, in 2008, and the Ph.D. degree in wireless communication from Delhi Technological University, New Delhi, India, in 2017. He is currently an Assistant Professor with Jaypee Institute of Information Technology, Noida, India. His research interests include wireless channel modeling for UWB propagation, performance analysis of fading channels, physical layer security, RIS-assisted communication, and analysis of mm-wave propagation for 5G cellular networks.

SUDHAN MAJHI (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2004, and the Ph.D. degree from Nanyang Technological University (NTU), Singapore, in 2008. He was a Posdoctoral Researcher with the University of Michigan-Dearborn, Dearborn, MI, USA, the Institute of Electronics and Telecommunications, Rennes, France, and NTU. He is currently an Associate Professor with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, Bengaluru, India. His research focuses on signal processing for wireless communication.

SANDESH JAIN (Member, IEEE) received the Ph.D. degree from Indian Institute of Technology (IIT) Indore, Indore, India, in 2022. He has been working in the field of Wireless Communication for more than 7 years. He was with the Department of Electrical Communication Engineering, Indian Institute of Science (IISc) Bangalore, Bengaluru, India, as a Postdoctoral Fellow. He is currently an Assistant Professor with the Department of Electrical and Electronics Engineering, Atal Bihari Vajpayee-Indian Institute of Information Technology and Management, Gwalior, India. His research interests include design of adaptive signal processing and machine learning algorithms for emerging wireless communication technology. In recent years, his work has centered on developing sparse channel estimation algorithms for millimeter wave and terahertz communication systems.

CHONGWEN HUANG (Member, IEEE) received the B.Sc. degree from Nankai University, Tianjin, China, in 2010, the M.Sc. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2013, and the Ph.D. degree from the Singapore University of Technology and Design (SUTD), Singapore, in 2019. From 2019 to 2020, he was a Postdoc with SUTD. In September 2020, he joined Zhejiang University, Hangzhou, China, as a tenure-track young Professor. His main research interests include holographic MIMO surface/reconfigurable intelligent surface, B5G/6G wireless communications, mmWave/THz communications, deep learning technologies for wireless communications. Dr. Huang was the recipient of 2021 IEEE Marconi Prize Paper Award, 2023 IEEE Fred W. Ellersick Prize Paper Award and 2021 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award. He has been the Editor of IEEE COMMUNICATIONS LETTER, *Elsevier Signal Processing*, *EURASIP Journal on Wireless Communications and Networking and Physical Communication* since 2021.

CHAU YUEN (Fellow, IEEE) received the B.Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 2000 and 2004, respectively. He was a Postdoctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, NJ, USA, in 2005, and a Visiting Assistant Professor with The Hong Kong Polytechnic University, Hong Kong, in 2008. From 2006 to 2010, he was with the Institute for Infocomm Research (I2R), Singapore, where he was involved in an industrial project on developing an 802.11n Wireless LAN system and participated actively in 3Gpp long-term evolution (LTE) and LTE-Advanced (LTE-A) standardization. From 2010 to 2023, he was with the Engineering Product Development Pillar, Singapore University of Technology and Design, Singapore. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. He has three U.S. patents and authored or coauthored more than 500 research papers at international journals or conferences. Dr. Yuen was the recipient of the IEEE Communications Society Fred W. Ellersick Prize in 2023, IEEE Marconi Prize Paper Award in Wireless Communications in 2021, IEEE APB Outstanding Paper Award in 2023, IEEE ICC and ICCT Best Paper Award in 2023, and EURASIP Best Paper Award for *Journal on Wireless Communications and Networking* in 2021. He was the 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 the recipient of the Hewlett Packard Prize, IEEE Asia Pacific Outstanding Young Researcher Award in 2012 and IEEE VTS Singapore Chapter Outstanding Service Award on 2019. Dr Yuen is currently the Editor-in-Chief for *Springer Nature Computer Science*, Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE SYSTEM JOURNAL, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, where he was awarded as IEEE Transactions on Network Science and Engineering Excellent Editor Award and Top Associate Editor for Transactions on Vehicular Technology from 2009 to 2015. He also was 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 *Elsevier Applied Energy*. He is a Distinguished Lecturer of IEEE Vehicular Technology Society, Top 2% Scientists by Stanford University, and also a Highly Cited Researcher by Clarivate Web of Science.