Received 27 February 2024; revised 28 March 2024; accepted 12 April 2024. Date of publication 22 April 2024; date of current version 13 May 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3392359

Inspiring Physical Layer Security With RIS: Principles, Applications, and Challenges

MENGZHAO GUO[1], ZHI LIN[1,2], RUIQIAN MA[1], KANG AN[3], DONG LI[2] (Senior Member, IEEE), NAOFAL AL-DHAHIR[4] (Fellow, IEEE), AND JIANGZHOU WANG[5] (Fellow, IEEE)

[1]College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China

[2]School of Computer Science and Engineering, Macau University of Science and Technology, Macau, China

[3]Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China

[4]Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080, USA

[5]School of Engineering, University of Kent, CT2 7NZ Canterbury, U.K.

CORRESPONDING AUTHOR: Z. LIN (e-mail: linzhi945@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62201592; in part by the Research Plan Project of NUDT under Grant ZK21-33; in part by the Young Elite Scientist Sponsorship Program of CAST under Grant 2021-JCJQ-QT-048; in part by the Macau Young Scholars Program under Grant AM2022011; in part by the Science and Technology Development Fund, Macau, SAR, under Grant 0029/2021/AGJ; and in part by the Erik Jonsson Distinguished Professorship at UT-Dallas.

ABSTRACT With the commercialization of the fifth generation mobile networks, researchers are now focusing on discovering the potential key techniques of the next generation mobile networks, which are expected to provide more accurate perception, lower latency, and higher network capacity. As the communication equipments increase exponentially, wireless transmission environment becomes more complex, leveraging wireless security challenges more and more severe, such as computationally powerful interception, intelligent malicious jamming, communication behavior monitoring. The physical layer security (PLS) techniques have been widely explored as a complement to traditional encryption schemes by exploiting the randomness characteristics of wireless channels to achieve the security from the physical layer. Additionally, reconfigurable intelligent surface (RIS) is considered as a key enabling technology for the six generation (6G) mobile networks, due to its ability to achieve the reconstruction of wireless channel, which is also regarded as a good match with PLS techniques for improving communication security. This paper presents a comprehensive review of the latest research on the integration of RIS and PLS. First, we introduce the principles of PLS from the development of secure communications and the basics of RIS based on the generalized Snell's law. Then, we categorize RIS according to different hardware architectures, of which the corresponding scenarios are also presented. Subsequently, we review recent works on RIS-assisted PLS in different communication networks, and classify the security scenarios in which RIS is integrated with various advanced communication technologies. Finally, we discuss the potential future research directions and challenges of RIS-aided PLS communications.

INDEX TERMS Reconfigurable intelligent surfaces, physical layer security, secure communications, 6G.

I. INTRODUCTION

AS THE fifth generation mobile network has permeated into people to live aspect, supporting massive communication demand, substantial research works are devoted to promoting the development of the next generation mobile networks. The 6G networks aim to provide higher reliability, lower latency, higher data rates, and higher positioning accuracy to meet the needs of future large-scale Internet of Things (IoTs) applications [1], [2], [3]. In general, these applications pose higher requirements for real-time data transmission, and therefore, require more robust security mechanisms to protect users' data privacy. In this regard, 6G networks are facing more severe challenges in the field of wireless security and

requires more stringent measures to protect the information privacy.

The TCP/IP model consists of the application layer, transport layer, network layer, data link layer, and the physical layer. Current security measures include the use of key encryption, mainly ensuring communication security in the layers above the physical layer. Nevertheless, there are certain shortcomings of key encryption, like high computational complexity and key management costs, which lead to increased time and energy consumption. Another issue is that the security provided by encryption is not unbreakable. With the increasing computational capabilities of computers, particularly with the advent of quantum computers, the cost of cracking the encryption keys is gradually decreasing. This trend poses a potential threat for conventional password-based security mechanisms in specific scenarios. In addition, encryption methods have undergone considerable mature research, whereas there are still many urgent problems to be solved in the search of PLS.

Compared to the traditional encryption methods, PLS provides the ability to achieve "perfect secrecy" without the need for secret keys and codebooks. The core of PLS is to utilize the inherent randomness of the channel to increase the security of the system, which makes it more difficult for eavesdroppers to decrypt the private signals [4], [5]. Typically, conventional encryption methods require that the transmitter and receiver share a key in advance and use the key to encrypt and decrypt the data. However, if the key is leaked or cracked, the data would be exposed to the eavesdroppers. In contrast, PLS does not require key exchange to ensure the confidentiality of the system. For example, in PLS system, even if the received SINR of the eavesdropper is higher than that of the legitimate user, the fading characteristics of the wireless channel ensure the system's information security is achievable. Therefore, PLS is a good complement to traditional encryption methods. In detail, PLS is able to provide additional protection at the physical layer, reducing the likelihood that an eavesdropper gains access to information. By introducing interference or noise during transmission, PLS makes it difficult for unauthorized users to access the valid information. Furthermore, PLS typically has low computational and processing complexity. Last but not least, PLS has good compatibility with existing wireless communication systems, such as heterogeneous networks, visible light communication (VLC) systems, non-orthogonal multiple access (NOMA) networks, millimeter-wave networks, space-air-ground integrated network [6], and so on. In other words, PLS does not require large-scale modification or upgrading of existing systems, which means that PLS can be easily applied to a variety of communication scenarios and devices [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. However, the PLS techniques also have some shortcomings. According to the Maxwell equation, when the eavesdropper and the legitimate user are far from each other, the boundary conditions exhibit significant differences, resulting in a substantial distinction between the two channels. However, when the eavesdropper and the legitimate user are close to each other or in the same direction, the two channels are strongly correlated. Currently, the secrecy performance of the traditional PLS technique is very limited [22]. As a result, RIS, which allows for the reconfiguration of the electromagnetic environment, has attracted attention. The deployment of RIS in secure communication networks could reduce the channel correlation between legitimate users and eavesdroppers. For example, [23] considered the scenario where the strong channel correlation between the legitimate user and the eavesdropper where, a RIS was introduced to enhance the system's secrecy.

RIS is becoming increasingly popular as it can be used for boosting the received signal power, increasing cell-edge user rates, and green communication. RIS, which has led to a significant breakthrough in information transmission. Intuitively, RIS utilizes programmable sub-wavelength two-dimensional metamaterials to regulate electromagnetic waves intelligently through digital coding to achieve controllable amplitude, phase, polarization, and frequency of the electromagnetic field [24]. In other words, RIS is able to realize the adjustment of signal propagation direction, signal enhancement, or interference suppression by actively controlling the wireless propagation environment. In general, RIS builds intelligent programmable wireless environments and provides a new paradigm for wireless communication and transmission [25]. Due to the utilization of physical channel properties of PLS and dynamic reconfiguration of wireless channel of RIS, RIS and PLS can operate as a good match, complement each other and, in turn, will realize tremendous gains in communications security. Thus, RIS has been well exploited to various communication scenarios in recent networks [26], [27], [28], [29], [30], [31], [32], [33], [34], [35] to provide security guaranteeing ways with low cost and power consumption, strong anti-jamming ability, and ease of deployment [5], [23], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46].

For instance, in [47], [48], [49], [50], the RIS-assisted secure simultaneous wireless information and power transfer (SWIPT) system, boosted the received signal quality for the information user (IU), enhanced energy user (EU)'s energy efficiency, and protected against information theft from the EU. In addition, the use of RIS in cooperative networks can provide higher SR, SC, and secure energy efficiency (SEE). Thus, RIS is regarded as an effective way to support the wireless security of various networks, such as unmanned aerial vehicle (UAV) relay networks [38], [51], [52], [53], [54], [55], [56], [57], [58], satellite communication networks [59], [60], [61], NOMA networks [48], [55], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], cognitive radio networks [48], [57], [75], and cell-free networks [76], [77], which will be discussed in the main text.

Although there have been a number of surveys, introducing the applications of RIS in various networks, which has not considered the improvement of PLS with RIS [5], [78], [79], [80], [81], [82], [83], [84]. In particular, Chen et al. presented an overview of RIS applications for wireless positioning in the 6G IoTs, summarized the recent advances and the potential development directions in RIS-assisted positioning [78]. In [79] and [80], recent developments in the integration of RIS with NOMA schemes were presented. After that, in [5], authors discussed the integration of UAVs and RIS, such as UAVs carrying RIS, UAVs as base stations (BSs), and wall-mounted RIS in indoor and outdoor environments, to improve system performance. Besides, authors in [81] presented an overview of the downlink transmission performance as well as the energy efficiency of RIS-assisted cell-free massive multiple-input multiple-output (MIMO) networks. Authors in [82] provided an overview of state-of-the-art RIS technology from the RIS reflection and modulation perspective. Ahmed et al. reviewed the applications, recent advances, and future research challenges of simultaneously transmitting and reflecting RIS (STAR-RIS) in wireless networks and discussed its potential applications in 6G networks, such as wireless information and energy transfer, VLC and robotic communication [83]. Furthermore, authors in [84] introduced the application of machine learning methods to optimize the parameters of RIS, such as improving the accuracy of channel estimation by learning and modeling the received signal.

To the best of our knowledge, a detailed review of the application of RIS in PLS has not yet been reported. Additionally, some RIS aided communication networks with security demand have not been discussed, such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication networks. Besides, the existing surveys have not made a detailed distinction in terms of the hardware architectural aspects of RIS. Furthermore, there is a lack of discussion on the future challenges of applying RIS to PLS, for example, the deployment of RIS can lead to more complex channel estimation and pilot overloading problems. In light of the above, this paper overviews the use of RIS in different secure wireless communication networks and their integration with various advanced techniques.

This article is organized as follows. Section II is a description of the basics of RIS and PLS. Section III describes the hardware architecture of RIS and the application of RIS in different secure communication networks. In addition, Section IV studies the integration of RIS with state-of-the-art technologies. Finally, Section V investigates prospects for RIS-based PLS systems. The primary topics of this review are displayed in Fig. 1. The acronyms commonly used in this article are shown in Table 1.

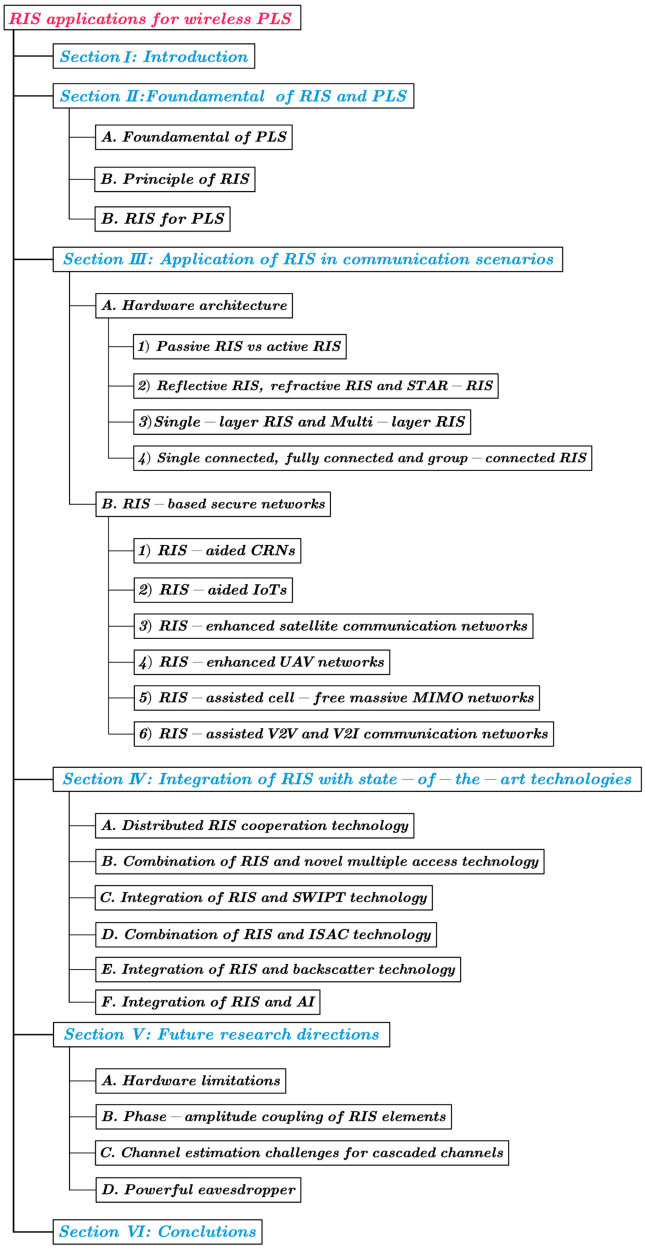


FIGURE 1. Outline and roadmap of this survey.

II. FUNDAMENTAL OF RIS AND PLS

The core concept of PLS relies on Shannon's information theory, leveraging the dynamic physical properties of the wireless transmission channel to accomplish "perfect secrecy" with low computational complexity [85]. Owing to the diverse advantages of PLS, numerous theoretical studies have been researched on various application scenarios of PLS. Besides, to show the advantages of integrating RIS with PLS, we will also introduce the operating principle of RIS in conjunction with the generalized Snell's law.

A. FUNDAMENTAL OF PLS

For the convenience of presentation, we denote Alice, Bob, and Eve as the transmitter, legitimate receiver, and eavesdropper, respectively. In 1949, Shannon developed a theoretical framework for cryptographic systems, applying concepts from information theory to address issues in

TABLE 1. List of abbreviations.

Abbreviation	Definition	Abbreviation	Definition
6G	Six Generation	MIMO	Multiple-Input Multiple-Output
AI	Artificial Intelligence	MISO	Multiple-Input Single-Output
AHB	Alternating Hybrid Beamforming	MS	Mode-Splitting
AWGN	Additive Complex White Gaussian Noise	MM	Majorization-Minimization
AN	Artificial Noise	NOMA	Non-Orthogonal Multiple Access
AO	Alternative Optimization	PLS	Physical Layer Security
AP	Access Point	QoS	Quality of Service
ADC	Analog-to-Digital Converter	RIS	Reconfigurable Intelligent Surface
BS	Base Station	RHI	Residual Hardware Impairment
BER	Bit Error Rate	RC	Reflection Coefficient
BD	Backscatter Device	RSMA	Rate-Splitting Multiple Access
CSI	Channel State Information	SWIPT	Simultaneous Wireless Information and Power Transfer
CSTN	Cognitive Satellite-Terrestrial Network	SR	Secrecy Rate
CRN	Cognitive Radio Network	SNR	Signal-to-Noise Ratio
CDMA	Code Division Multiple Access	SOP	Secrecy Outage Probability
DAC	Digital-to-Analog Converter	SDO	Secrecy Diversity Order
DDPG	Deep Deterministic Policy Gradient	SCG	Secrecy Coding Gain
DNN	Deep Neural Network	STAR-RIS	Simultaneously Transmitting and Reflecting RIS
DRL	Deep Reinforcement Learning	SCA	Successive Convex Approximation
ES	Energy Splitting	SEE	Secrecy Energy Efficiency
EU	Energy User	SIC	Successive Interference Cancellation
FP	Fractional Programming	SDR	Semi-Definite Relaxation
FDMA	Frequency Division Multiple Access	TDMA	Time Division Multiple Access
IU	Information User	TS	Time-Switching
IoTs	Internet of Things	VLC	Visible Light Communication
IWN	Industrial Wireless Network	V2V	Vehicle-to-Vehicle
ISAC	Integrated Sensing and Communication	V2I	Vehicle-to-Infrastructure
IRIS	Illegal Reconfigurable Intelligent Surface	WSSR	Weighted Sum Secrecy Rate
MRC	Maximal Ratio Combining		

cryptography and secure communication. At the theoretical level, Shannon delved into the mathematical structures and properties of secure systems. He introduced the concept of "perfect secrecy", which was regarded as the foundation of modern information security theory. "Perfect secrecy" refers to the condition wherein, upon interception of a confidential signal, the posterior probability of the information contained in the intercepted signal equals the prior probability of that information before interception, which can also be interpreted as the mutual information between the confidential message W and the intercepted message Z^n being zero for the eavesdropper.

In 1975, Wyner exploited the difference between the main channel and the wiretap channel to achieve "perfect secrecy" at the physical layer, thus initiated the research into PLS [86], where he first introduced the wiretap channel model by defining the main channel as a discrete memoryless channel, Eve obtained a degraded version of Bob's signal through eavesdropping on the main channel, as shown in Fig. 2.

Consequently, a variety of security methods for the physical layer have been developed. In MIMO systems, both secure beamforming schemes and secure precoding schemes can effectively exploit spatial degrees of freedom, thereby inducing significant discrepancies in signal quality between the legitimate node and eavesdropping node. Simultaneously, artificial noise (AN) can be employed to confuse the eavesdropping nodes, consequently diminishing the signal reception quality for the eavesdropper. For instance, to improve the PLS of the system, AN was utilized in heterogeneous cellular networks to disrupt signal reception by eavesdroppers [9]. Subsequently, to measure the safety of communication networks, several crucial performance metrics of PLS will be described below.

1) SECRECY RATE

The secrecy rate (SR) for confidential message can be expressed as

$$R_s = H(W)/n \tag{1}$$

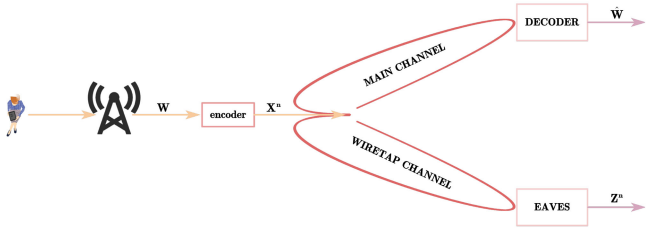


FIGURE 2. The wiretap channel of Wyner.

where W is the message sent by the transmitter, n is the communication block length, and $H(\cdot)$ is the entropy of the secret message. Equation (1) provides the definition of the SR. Alternatively, it can be defined as the difference in data rate between the legitimate user and the eavesdropper, which refers to the number of secret bits transmitted per second in a given channel. It can be represented as

$$R_s = [R_u - R_e]^+ \triangleq \max(R_u - R_e, 0), \tag{2}$$

where R_u denotes data rate between the transmitter and the legitimate user. R_e denotes data rate between the transmitter and eavesdropper. There are many optimization problems that use maximization of SR as a quantitative measure, for example in [87], [88], [89], [90], [91]. In some multi-user cellular or cell-free networks, the weighted sum secrecy rate (WSSR) is commonly used as a performance metric to express the total value of the secrecy rates of all users in the system, which can be expressed as [92]

$$R_s = \sum_{k=1}^{K} \eta_k \left[R_{u,k} - R_e\right]^+ \tag{3}$$

where $\eta_k > 0$ $(\forall k \in \mathcal{K})$ denotes the WSSR weight for the kth user with $\sum_{k=1}^{K} \eta_k = 1$.

2) SECRECY CAPACITY

The concept of secrecy capacity (SC) is closely related to channel capacity. Channel capacity describes the maximum information transmission rate of a system under ideal conditions without eavesdroppers. SC gives the maximum value of a practically achievable secure transmission rate, taking eavesdroppers into account. Mathematically, it can be expressed as

$$C_{sec} = \sup_{P_e < \epsilon} R_s \tag{4}$$

where P_e is the bit error rate (BER) at the legitimate user, which measures the reliability of information transmission in the legitimate channel and the pre-defined threshold $\epsilon > 0$. Accordingly, SC is the maximum secure transmission rate at which the transmitter's confidential message cannot be intercepted by eavesdroppers, ensuring that the confidential message can be received safely by the legitimate user. Besides, an auxiliary variable U was introduced to describe the SC in [93]. And the formulation could be represented as

$$C_{sec} = \max_{P(U,X)} I(U, Y) - I(U, Z) \tag{5}$$

For a given channel, the SC can be found by searching through all joint distributions $P(U, X)$ that satisfy the constraints necessary for the Markov chain $U \to X \to (Y, Z)$ to hold. In the commonly used Gaussian channel model, the channel capacity is also expressed as

$$C_{sec} = (C_u - C_e)^+ = \left(C\left(\frac{P_u}{\sigma_u^2}\right) - C\left(\frac{P_e}{\sigma_e^2}\right)\right)^+ \tag{6}$$

where C_u denotes the capacity of the transmitter to legitimate user link, C_e denotes the capacity of the transmitter to eavesdropper link, P_u and P_e represent the received signal power at the user and the eavesdropper, respectively. σ_u^2 and σ_e^2 represent the noise power at the user and the eavesdropper, respectively, and $C(x) = \log_2(1+x)$. To ensure a secure and reliable communication rate, it is necessary to guarantee that $\frac{P_u}{\sigma_u^2} > \frac{P_e}{\sigma_e^2}$, so that $C_u > C_e$. In addition, it is interesting to notice that the optimization problem considered in [94] introduces a weighted variable α, which can be expressed as follows

$$\max_{\phi_n} C(\gamma_u, \gamma_e) = \max_{\phi_n} \{log_2(1 + \gamma_u) - \alpha log_2(1 + \gamma_e)\} \tag{7}$$

where ϕ_n denotes the phase of RIS's nth reflective element, γ_u and γ_e stand for the signal-to-noise ratio (SNR) of the legitimate user and eavesdropper, respectively, and $0 \le \alpha \le 1$. Using the expression in (7), we can study the effect of the channel state information (CSI) of the eavesdropping channel on the user's SR and find the optimal value of α. It is worth noting that the SC introduced above assumes a constant channel during codeword transmission, i.e., slow fading conditions. To achieve a non-zero SR, the primary channel must be superior to the eavesdropping channel. However, wireless channel fading is a problem that must be considered in many communication scenarios. The channel coefficients may change rapidly in space, time, and frequency dimensions when the communication signals are being transmitted. The transmitter can achieve a positive SR by utilizing the dimension in which the legitimate channel outperform the eavesdropping channel, which is possible even if the eavesdropping channel outperform the primary channels on average. And the maximum achievable SR is referred to as the ergodic SC. Last but not least, the probability of strictly positive SC is defined as

$$P_{SPSC} = P_r(C_{sec} > 0) \tag{8}$$

which is used to express the probability that the SC is higher than zero.

3) SECRECY OUTAGE PROBABILITY

Coding all channels to achieve the ergodic SC mentioned above may be unsuitable for low-latency applications. In delay-constrained scenarios where confidential information is encoded in a single channel block, and the block is long enough such that the codeword rate is lower than the capacity of the eavesdropping channel, an eavesdropper can potentially decode the confidential information with a

very low BER. Researchers typically use the secrecy outage probability (SOP) as a performance metric at this stage. SOP refers to the likelihood that the target security rate cannot be achieved within the channel block, which is defined as the probability that the C_{sec} is lower than the target SR R_s^0. And it can be mathematically expressed as

$$P_{out}\left(R_s^0\right) = P_r\left(C_{sec} < R_s^0\right) \tag{9}$$

This outage event ($C_{sec} = C_u - C_e < R_s^0$) occurs when a legitimate user does not receive reliable confidential information or has confidential information leaked to an eavesdropper [95]. However, the above definition lacks rigour in describing secrecy performance. Therefore, [96] proposed a new definition of SOP, which was represented as

$$P_{out}\left(R_u^0, R_s^0\right) = 1 - Pr\left(C_u > R_u^0, C_{sec} > R_s^0\right) \tag{10}$$

where R_u^0 denotes the target transmission rate between the transmitter and the legitimate user. The probability of safe and reliable transmission is $1 - P_{out}(R_u^0, R_s^0)$. Clearly, the security of the system cannot be guaranteed when outage event ($C_{sec} < R_s$) occurs and the reliability of the system cannot be achieved when event ($C_u < R_u^0$) occurs. Beyond that, an alternative SOP formulation was given in [97], which could directly compute the probability that the system achieved "perfect secrecy" without considering reliability. The mathematical expression of alternative SOP can be written as

$$P_{out} = P(C_e > R_u - R_s | \text{message transmission}) \tag{11}$$

where $R_e \triangleq R_u - R_s$ denotes the eavesdropping data rate. When a signal is transmitted over a channel, and $C_u > R_u$, then a legitimate user can correctly decode the signal theoretically. Similarly, if $C_e > R_e$, an eavesdropper could succeed in stealing the confidential information, i.e., a secrecy outage event occurs. Using this formulation to evaluate system performance can describe security level more accurately and facilitate better system design. By properly designing the SR R_s and the transmission rate R_u of legitimate users, the SOP can be effectively reduced. Without loss of generality, the authors of [63] derived an exact expression of the SOP using a constant-rate coding strategy in the case of statistical eavesdropping CSI and developed an alternating hybrid beamforming (AHB) algorithm to minimize the maximum SOP among legitimate users. Numerical results also demonstrated the security superiority of the scheme. Besides, [75] investigated secrecy performance in cognitive radio networks (CRNs) with eavesdroppers. The study derived a closed-form solution for the SOP and verified the accuracy of the results by using Monte Carlo simulations. However, exact SOP calculations involve complex integral and probability density functions, making it difficult to obtain analytical expressions. Asymptotic SOP, on the other hand, is obtained through approximations and simplifications that can be computed and analyzed more easily. In most cases, the asymptotic SOP is sufficiently accurate and provides a helpful estimation of system performance. Therefore, asymptotic SOP is often used as a performance metric in research. As an example, [98] addressed the analysis of secrecy outage in a communication system assisted by RIS employing discrete phase-shift control. In this study, the authors refrained from deriving a closed-form expression for the SOP. Instead, they deduced a tight upper bound for SOP and conduct an asymptotic SOP analysis. The findings characterized the relationship between SOP and the number of antennas as well as the discrete phase selections. In a practical scenario, all nodes may have residual hardware impairments (RHIs). Considering this situation, a study in [99] derived an analytical expression for the SOP of a NOMA user on the Nakagami-m fading channel. The study also obtained an asymptotic expression for the SOP. Simulation results demonstrated that the asymptotic SOP fits well with the theoretical SOP under high SNR conditions.

B. PRINCIPLE OF RIS

RIS is a planar structure with programmable electromagnetic attributes due to metamaterial technologies. Metamaterials are artificially created materials with special structures and properties that allow precise control and manipulation of electromagnetic waves. Besides, metamaterials usually consist of tiny structural units whose diameters are much smaller than the wavelength of electromagnetic waves. Through meticulous engineering of the geometric configuration, spatial arrangement, and material characteristics of these constituent elements, metamaterials can attain precise manipulation of the refraction, reflection, and transmission of electromagnetic waves. Consequently, they manifest distinctive properties not inherent in natural materials, including negative refraction, perfect lensing effects, and cloaking capabilities [39].

The emergence of metasurface technology is intricately linked to the introduction of the generalized Snell's law, which allows for the tailored design of interface phase distributions to achieve highly customized control over electromagnetic waves. By leveraging the generalized Snell's law, metasurfaces with specific functionalities, such as focusing, polarization conversion, and absorption, can be systematically engineered. The generalized Snell's laws of refraction and reflection can be expressed as follows:

$$\begin{cases} \sin(\theta_t)n_t - \sin(\theta_i)n_i = \left(\frac{\lambda}{2\pi}\right)\left(\frac{\Delta\phi}{\Delta x}\right) \\ \sin(\theta_r) - \sin(\theta_i) = \left(\frac{\lambda}{2\pi n_i}\right)\left(\frac{\Delta\phi}{\Delta x}\right) \end{cases} \tag{12}$$

where the refractive indices of two media are denoted as n_i and n_t. θ_t, θ_r, and θ_i represent the angle of refraction, the angle of reflection, and the angle of incidence. ϕ and $\phi+\Delta\phi$ denote the phase-discontinuity points of the two paths at the interface of the bimedium in the Equation (12). The variable Δx denotes the distance between the intersecting points, and λ represents the wavelength of the electromagnetic wave in vacuum. As shown in Figs. 3 and 4, we can predict and design the reflection and refraction of electromagnetic

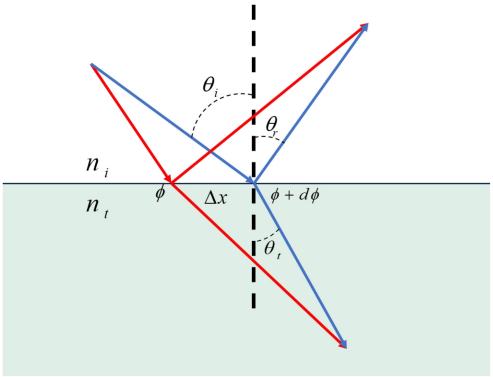


FIGURE 3. Generalized Snell's law (2D).

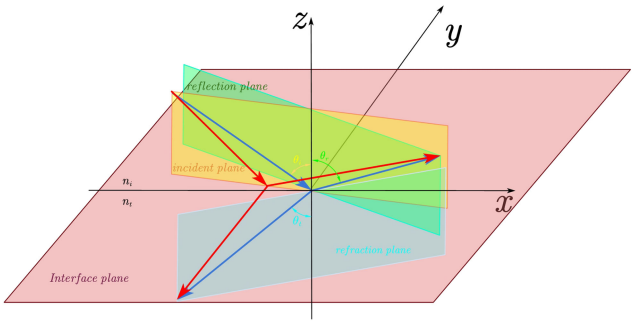


FIGURE 4. Generalized Snell's law (3D).

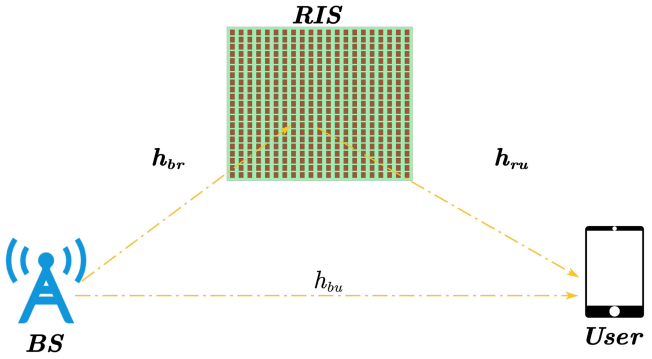


FIGURE 5. The three-node communication model of RIS.

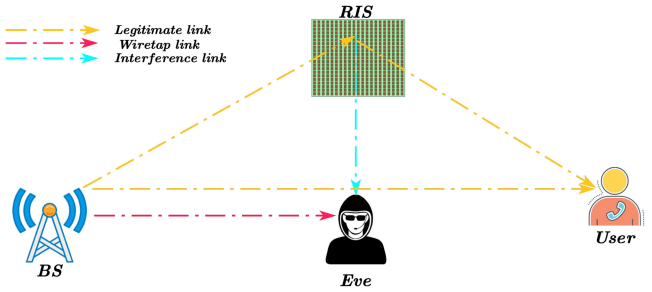


FIGURE 6. Application of RIS in scenarios where users and eavesdroppers have strong channel correlation.

waves on a metasurface by varying the parameter $\frac{\Delta\phi}{\Delta x}$ [100]. Likewise, equation (12) shows that n_i, n_t, λ are constants. The value of θ_t and θ_r can be controlled to determine the direction of the reflected and refracted waves by adjusting $\frac{\Delta\phi}{\Delta x}$. RIS operates by adjusting the phase shift matrix $\mathbf{\Theta}$, which controls the direction of refracted and reflected signal, thereby reconfiguring the electromagnetic environment. Building upon this theoretical foundation, we can manipulate the phase shift matrix $\mathbf{\Theta}$ of RIS to control the propagation direction of electromagnetic waves.

We establish a three-node communication model that comprises a BS with an antenna, a user with an antenna, and a RIS with L-reflecting elements, as illustrated in Fig. 5. It is noted that the signal reflected by an individual RIS element can be represented as the product of the incident signal and the reflection coefficient (RC) of that particular RIS unit. Accordingly, the received signal at the user can be given by

$$y = (h_{bu} + \mathbf{h}_{ru}\mathbf{\Theta}\mathbf{h}_{br})s + n \tag{13}$$

where n represents additive complex white Gaussian noise (AWGN) with zero mean and variance δ^2 received by the user, s represents the signal transmitted by BS, h_{bu} denotes the line-of-sight channel from the BS to the user, $\mathbf{\Theta}$ denotes the RC matrix, $\mathbf{h}_{ru}\mathbf{\Theta}\mathbf{h}_{br}$ denotes the equivalent channel from the BS to the user through the RIS. Since the RIS has L reflection elements, the channel vector $\mathbf{h}_{ru}, \mathbf{h}_{br} \in \mathcal{C}^{L\times 1}$. Therefore, by designing the RC matrix of RIS to ensure coherent superposition of the reflected signals at the user end, the SNR at the user terminal is optimized, consequently improving the system's transmission rate.

C. RIS FOR PLS

Information theory security and covert communications are two of PLS's most popular research directions. Information theory security involves exploiting the random nature of the wireless channel and using signal processing methods to increase the difference in transmission rates between legitimate users and eavesdroppers, thereby enhancing the system security performance. Covert communication aims to meet the user's communication needs without being detected by the warden [101], [102]. In this paper, We discuss PLS mainly from an information-theoretic perspective.

However, PLS technology inevitably has some limitations. As shown in Fig. 6, if the eavesdropper and the user are nearby, their channel correlation is strong. At this time, a high secure transmission rate cannot be achieved. Thus, new techniques are required to overcome this challenge. The field of PLS heavily utilizes a two-dimensional thin surface composed of numerous low-cost passive components known as RIS. Each component of RIS can independently alter the amplitude and phase of the incident signal, allowing for the reconfiguration of the electromagnetic environment. RIS is able to enhance the channel differentiation between the user and the eavesdropper, significantly improving system security performance. For example, the authors in [23] deployed

active RIS in communication scenarios under strong channel correlation, which not only improved the overall security performance of the system but also mitigated the double fading effect caused by passive RIS. To further enhance the user's communication experience and restrain eavesdroppers from stealing signals, the research [29] virtually divided the reflective elements of RIS into two components, wherein one was dedicated to enhancing the expected signal for legitimate users, while the other was employed in conjunction with AN to prevent unauthorized access. Simulation results validated the significantly improved SC of the proposed RIS partitioning method. Many previous research studies have been conducted based on perfect CSI, but the generality and practicality of such models are not strong. In [103], a novel and effective twin-deep deterministic policy gradient (DDPG) deep reinforcement learning algorithm was proposed by utilizing a DDPG framework, which considered the imperfect CSI and CSI obsolescence problem due to the mobility of UAVs, and the final simulation results proved that the overall secrecy rate of the proposed scheme outperforms all the benchmark schemes. Similarly, [104] derived an expression for the SOP based on the statistical CSI of the eavesdropper as a metric for PLS and achieved SOP minimization by alternately optimizing the beamforming vectors and phase shift matrices. High performance and security are paramount in the production processes of industrial wireless network (IWN) systems. Authors in [105] introduced RIS to aid IWN in thwarting eavesdropping attacks, thereby enhancing PLS. Moreover, satellite communication, as an essential part of next-generation communication networks, has also received a great deal of attention in terms of its security. In [51], the multiple vehicular eavesdroppers was considered in a RIS-assisted satellite UAV relay system, and the eavesdroppers adopted a maximal ratio combining (MRC) eavesdropping scheme to eavesdrop on legitimate users. In addition, an approximate analysis of the SOP was carried out by combining the secrecy diversity order (SDO) and secrecy coding gain (SCG), and the theoretical analysis matched with typical Monte Carlo results.

III. APPLICATION OF RIS IN WIRELESS COMMUNICATION

A. HARDWARE ARCHITECTURE

Classifying RIS into multiple categories facilitates a more precise and effective selection tailored to diverse communication requirements and scenarios. Such categorization not only aids in customized applications for optimizing system performance but also enables a better balance between cost-effectiveness and resource utilization. This subsection will embark on a hardware architecture perspective, providing a comprehensive overview of various characteristics and performance comparisons of RIS.

1) PASSIVE RIS VS ACTIVE RIS

Passive RIS consists of electromagnetic metamaterials, artificially manufactured materials with unique structures and properties. These metamaterials allow for the precise control and manipulation of electromagnetic waves and usually consists of tiny structural units with diameters much smaller than the wavelength of electromagnetic waves. By precisely designing the shape, arrangement, and material parameters of these structural units, metamaterials can achieve exceptional control over the refraction, reflection, and transmission of electromagnetic waves. Thus, it exhibits some unique properties that are not available in natural materials, such as negative refraction, perfect lens effect and invisibility [39]. Passive RIS exhibits greater environmental sustainability compared to traditional communication relay systems, as it solely leverages each reflective element to modify the input signal without the use of power amplifiers. On top of that, passive RIS is exclusively employed for signal reflection, endowing it with the characteristics of full-duplex and full-bandwidth transmission. Despite providing an additional communication link, passive RIS exhibits limited capacity gains due to the impact of double fading or multiplicative fading effects.

To overcome the bottleneck associated with the passive RIS, scholars have proposed the concept of active RIS as a solution to address multiplicative fading effects. Regarding the hardware structure, the passive RIS element only has a phase-shift circuit, which does not consume direct-current power. In contrast, the active RIS integrates an amplifier circuit, which consumes additional power [106]. The difference in hardware structure between the two is demonstrated in Fig. 7. Active RIS can amplify the strength of the incident signal for each reflection element, thereby enhancing the SNR at the receiver. Compared to the passive RIS, active RIS incurs higher system power consumption and a more intricate hardware structure attributed to the integration of power amplification components. Despite the drawbacks of active RIS, its application prospects remain promising. In recent researches on RIS, more attention has been directed towards active RIS. For instance, considering the high correlation in the channel between legitimate users and eavesdroppers, Sun et al. conducted a comparative analysis of the security performance of systems employing passive RIS versus active RIS [23]. Simulation results demonstrated that deploying active RIS leads to a higher SR. In recent years, integrated sensing and communication (ISAC) systems have undergone extensive research and development. However, these systems are also confronted with inevitable challenges, such as spectrum congestion. When radar and communication coexist in the same spectrum, the mutual interference between them can have a detrimental impact on the system's performance. In [107], incorporating an active RIS in the multi-user multiple-input single-output (MISO) ISAC system had not only mitigated interference between radar and communication and expanded the system's coverage area. Besides, it also resulted in an enhancement of the system's average SR. Cognitive satellite-terrestrial network (CSTN) is a spectrum-sharing network capable of facilitating reliable communication in

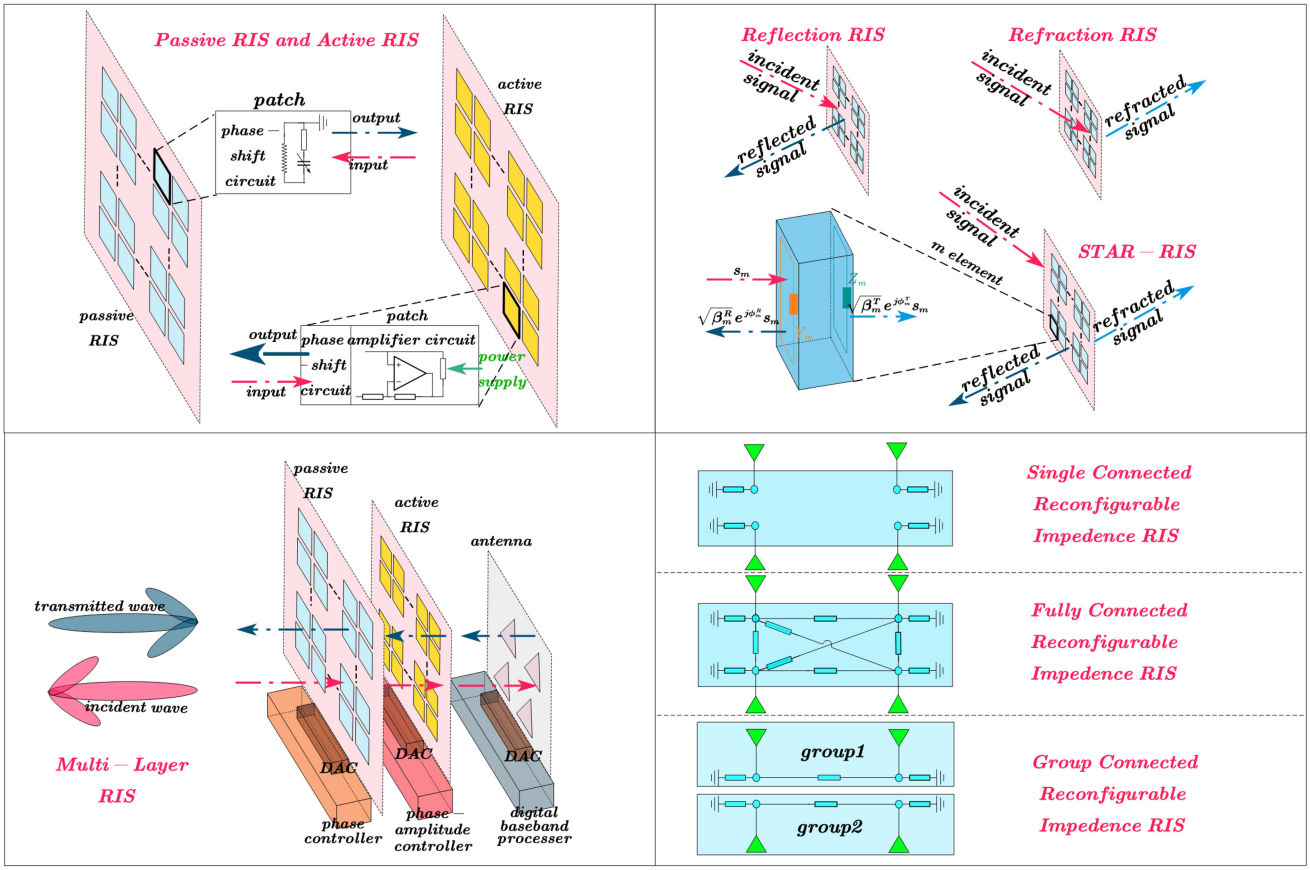


FIGURE 7. Schematic diagrams of the different hardware architectures of the RIS.

both densely populated and remote areas. However, CSTN encounters challenges such as limited spectrum resources and constraints on transmission power. To address this issue, a PLS solution employing an active RIS was proposed in [108], which achieved superior system performance compared to scenarios without RIS or with passive RIS. Simultaneously, to address the prominent drawback of single-faced passive RIS, Guo et al. proposed a dual-faced active RIS, which not only alleviated the multiplicative fading effects but also achieved full-space operability [87].

2) REFLECTION RIS, REFRACTION RIS AND STAR-RIS

To adapt RIS to various wireless communication systems and requirements, three operating modes of RIS have been widely studied: refraction RIS, reflection RIS, and STAR-RIS. The following section will compare and analyze the performance of RIS in these three operating modes and discuss the advantages and limitations of each.

The reflection RIS is the most extensively researched of the three. Deploying reflection RIS at a reasonable location, we can establish an additional line-of-sight link, which can intelligently reconfigure the electromagnetic environment, improve signal quality, increase system capacity, and save energy consumption. Furthermore, the reflection RIS can enlarge the channel difference between legitimate users and eavesdroppers, thus improving the system's security performance. However, the reflection RIS can only function when the BS and the user are located on the same side, meaning that the reflection RIS's working range angle is limited to 180 degrees.

When the communication link between the BS and the user is blocked, such as an outdoor to indoor communication environment. In cases where high-frequency signals penetrate obstacles, their attenuation is significant. Under such conditions, using reflection RIS alone cannot provide a good communication environment.

In order to break through this limitation, the concept of refraction RIS, has been proposed and gained much attention. Taking the example of outdoor-to-indoor communication scenarios in the millimeter-wave frequency band, signal attenuation through walls is significant, and the use of reflection RIS is insufficient to redirect signals around obstacles. The active refraction RIS proposed in [109] effectively addressed this issue, ensuring system performance while simultaneously reducing the number of transmissive-type elements. Before the concept of refraction RIS was introduced, there was a lack of research addressing the challenges in the blocked satellite communication scenario. In [110], Lin et al. pioneered the application of refraction RIS in a hybrid satellite-terrestrial relay network. The

proposed alternative optimization (AO) scheme significantly optimized the quality of service (QoS) for satellite communication.

In practical communication scenarios, users are often situated on both sides of the RIS. In such cases, the sole utilization of reflection RIS or refraction RIS proves insufficient. Consequently, researchers have introduced the concept of STAR-RIS to address this limitation. The unique characteristics inherent to STAR-RIS afford it a 360-degree coverage range, providing additional degrees of freedom compared to conventional RIS for reconfiguring the electromagnetic environment. STAR-RIS operates in three distinct modes: mode-switching (MS), energy-splitting (ES), and time-switching (TS). In the MS protocol, STAR-RIS is categorized into transmission mode and reception mode. The MS protocol can be regarded as a combination of standard RISs that perform either reflection or transmission exclusively. This protocol achieves its functionality through the element-wise optimization of mode selection and phase shift coefficients for both transmission and reflection. However, MS mode utilizes only a subset of elements for transmission and reflection, so it cannot achieve the same gain level as ES. In the ES mode, all elements of STAR-RIS are assumed to operate concurrently in transmission and reflection modes, affording considerable design flexibility with adjustable coefficients for each element. However, the multitude of elements in this configuration results in increased costs. In contrast to ES and MS, the TS mode involves the alternating transition of all elements between transmission and reflection modes. This approach simplifies coefficient adjustments, as temporal intervals determine reflection and transmission coefficients. Nevertheless, the high frequency of mode transitions places stringent demands on hardware capabilities [83]. Due to the comprehensive spatial coverage capability of STAR-RIS, there is a natural trend to integrate it with NOMA technology, which inherently possesses the capability to achieve large-scale connectivity. This integration aims to enhance system security performance while facilitating flexible deployment and improving QoS. It is shown in [64], Pin Xu et al. employed the STAR-RIS to assist the downlink NOMA system, optimizing power allocation and phase adjustment coefficients to achieve the maximization of the system's SR.

Furthermore, Zhang et al. investigated a STAR-RIS-assisted uplink NOMA system [63]. They proposed an AHB algorithm and its extended version in two scenarios where the eavesdropper's CSI is known either completely or statistically. These contributions were shown to enhance the system's security performance. It is noteworthy that unless STAR-RIS operates exclusively in the transmission mode or solely in the reflection mode, its transmission and reflection phase shift coefficients are coupled. Furthermore, the absolute difference between the two is either $\pi/2$ or $3\pi/2$. The performance degradation caused by the coupled phase shift model for both symmetric and asymmetric users is analyzed in detail in [111].

Furthermore, Fig. 7 illustrates the working principles of reflection RIS, refraction RIS, and STAR-RIS. The focus of this explanation is on the working principle of STAR-RIS. According to [112], if we assume that $\boldsymbol{s_m}$ is the mth incident signal from STAR-RIS, then the reflected signal and refracted signal are $\boldsymbol{s_m^R}$ and $\boldsymbol{s_m^T}$:

$$\boldsymbol{s_m^R} = \sqrt{\beta_m^R} e^{j\phi_m^R} \boldsymbol{s_m}, \ \boldsymbol{s_m^T} = \sqrt{\beta_m^T} e^{j\phi_m^T} \boldsymbol{s_m} \tag{14}$$

where $\beta_m^R \in [0, 1]$, $\beta_m^T \in [0, 1]$ denote the real coefficients and $\beta_m^R + \beta_m^T < 1$. And $\phi_m^R, \phi_m^T \in [0, 2\pi]$ represent the phase shift coefficients of STAR-RIS, respectively.

3) SINGLE-LAYER RIS AND MULTI-LAYER RIS

Single-layer RIS has been extensively studied because of its ability to reshape the electromagnetic environment. However, the single-layer RIS has only one component layer, so it can only adjust the phase but not the signal amplitude, e.g., [113] and [114]. Motivated by this, researchers have turned their attention to multi-layer RIS in the quest for better system performance. Multi-layer RIS refers to the stacking multiple RIS on top of each other. Moreover, each layer of the multi-layer RIS can adjust the surface elements independently. Thus, the multi-layer RIS can adjust the phase of the incident signal and partially adjust the amplitude of the incident signal. To our knowledge, multi-layer RIS is usually used to support a transmitter or receiver and is generally not employed as a relay. In particular, [115] used a multi-layer RIS on the user side, which added a new degree of freedom to the beamforming design. In addition, in [116], the authors demonstrated a multi-layer RIS-supported integrated terrestrial-aerial network to defend against eavesdroppers with both eavesdropping and jamming capabilities. Moreover, it is important to mention that in [117], an active-passive cascaded multi-layer RIS architecture is proposed, whose hardware architecture is shown in Fig. 7, and the architecture's performance is analyzed to demonstrate the superiority of the framework.

4) SINGLE CONNECTED, FULLY CONNECTED AND GROUP-CONNECTED RIS

Within the existing literature, the most extensively explored application of RIS involves the utilization of a diagonal phase-shift matrix in a singly connected impedance network with N ports. In this configuration, each network port is isolated from others, allowing adjustment solely of the phase of the incident waves through its diagonal scattering matrix. To enhance the received signal power, Shen et al. [118] proposed a more efficient RIS architecture, namely, fully connected and group-connected reconfigurable impedance networks. In the fully connected reconfigurable impedance network, each port is interconnected with others to improve RIS performance. The phase shift matrix $\boldsymbol{\Theta}$ of the RIS in this hardware architecture is a symmetric unitary matrix. By adjusting the phase shift matrix $\boldsymbol{\Theta}$, the channel vector $\boldsymbol{h_{\{IT\}}}$ from the transmitter to the RIS and the channel vector

TABLE 2. Characteristics of different types of communication networks and their approaches to security issues.

RIS-aided secuere networks	characteristics	References	Main contributions
Cognitive radio networks	Spectrum utilization enhancement	[26]	Powerful eavesdroppers using two combining techniques for eavesdropping are considered.
		[75]	Demonstrating the accuracy of the derived SOP through Monte Carlo simulation.
		[119]	Converting interference from secondary networks into green interference.
		[120]	Using multiple RIS to secure the CRN system.
Internet of Things	Real-time and efficient interactive connectivity	[57]	Gamma distributions are used to model RIS-assisted ground-to-air and air-to-ground links.
		[67]	The investigation examines the effect of RHI on system security performance.
		[121]	A proposal for an IoTs encryption scheme based on secret key generation is presented.
Satellite communication networks	Wide coverage	[51]	The case of multiple users with MRC eavesdropping schemes is considered.
		[108]	Joint design of RIS RCs, AN, and beamforming at the BS.
		[122]	Optimizing UAV trajectories using deep learning.
UAV networks	High flexibility and communication range extension	[52]	Use DRL to make real-time decisions.
		[55]	The BS uses DNN to make adaptive parameter adjustments based on environmental changes.
		[56]	A fractional programming and relaxation method based on the AO algorithm is presented.
		[58]	Approximating the trajectory optimization sub-problem using an SCA algorithm
Cell-free massive MIMO networks	Enhancing user fairness	[77]	An active eavesdropper using a pilot spoofing attack is considered.
		[123]	The impact of DAV/ADC resolution on system performance was evaluated.
V2V and V2I communication networks	High timeliness and low latency	[60]	Using multiple RIS to act as passive relays at the top of the building.
		[61]	Two scenarios where the RIS acts as a relay and a receiver are considered.

$\boldsymbol{h}_{\{IR\}}$ from the RIS to the receiver can be aligned in the same direction, similar to a maximum ratio combining. RIS can alter the incident signal's amplitude with a fully connected architecture. However, as N increases, the number of reconfigurable impedance components between different ports also increases, resulting in a highly complex circuit that is challenging to implement in engineering. To address this issue, the concept of group-connected reconfigurable impedance networks is proposed, dividing N ports into m groups, where each group employs a fully connected architecture. Hence, the phase shift matrix $\boldsymbol{\Theta}$ of the group connected RIS is the block unitary matrix. This effectively reduces the number of reconfigurable impedance components and enables the adjustment of both the phase and magnitude of incident waves. To better illustrate this architecture, the single connected, fully connected, and group-connected impedance architecture networks for 4-element RIS are shown in Fig. 7. It can be inferred that a single-connected RIS with N elements has N reconfigurable impedance elements. In contrast, a fully connected RIS has $N(N+1)/2$ reconfigurable impedance elements, and a group-connected RIS with m groups has $N(N/m+1)/2$ impedance components [118]. The system's performance improves with an increase in reconfigurable impedance components, but this also leads to higher system complexity, so it is essential to weigh up performance and complexity when designing the system to choose the organizational structure of the RIS. In summary, the introduction of fully connected and group-connected non-diagonal RIS structures provides new insights for the further development of RIS technology. This innovation holds significant theoretical and practical implications.

B. RIS-BASED SECURE NETWORKS

This subsection aims to explore the applications of RIS in several crucial secure communication networks, encompassing RIS-aided CRNs, RIS-aided IoTs, RIS-enhanced satellite communication networks, RIS-enhanced UAV networks, RIS-assisted cell-free massive MIMO networks, as well as RIS-assisted V2V and V2I communication networks. The details are listed in Table 2. Note that typical scenarios of these communication networks are shown in Fig. 8. Through an in-depth investigation of the role and advantages of RIS in each scenario, we aim to elucidate its significant contributions to enhancing secrecy performance.

1) RIS-AIDED CRNS

Cognitive radio, as a crucial technology addressing spectrum scarcity, fundamentally aims at achieving spectrum sharing. In CRNs, users with authorized spectrum access are designated as primary users, while users possessing cognitive capabilities are termed as secondary users. This entails the cognitive BS selectively accessing the idle spectrum within the working frequency bands of primary users, ensuring the undisturbed communication service quality for primary users. Through the adoption of dynamic spectrum allocation, the coexistence of primary and cognitive networks is facilitated, thereby enhancing overall spectrum efficiency. However, the secondary network will inevitably cause some interference to the primary network. Incorporating RIS technology into CRNs can eliminate the interference and improve the system security due to its reconfigurable nature to the electromagnetic environment. For example, the authors of [119] employed RIS to convert interference from secondary networks to the primary network into factors that were favorable to the system and utilized this green interference to enhance the secure performance of the primary user. The deployment of RIS in an underlay CRN was considered in [75], and the correctness of the derived exact SOPs was verified by using Monte Carlo methods. Besides, multiple RIS-assisted millimeter-wave CRN was considered in [120] to resist the effects of eavesdropping and jamming. It is worth mentioning that authors in [26] considered the case where an eavesdropper used the MRC method and the selective combining method to enhance their

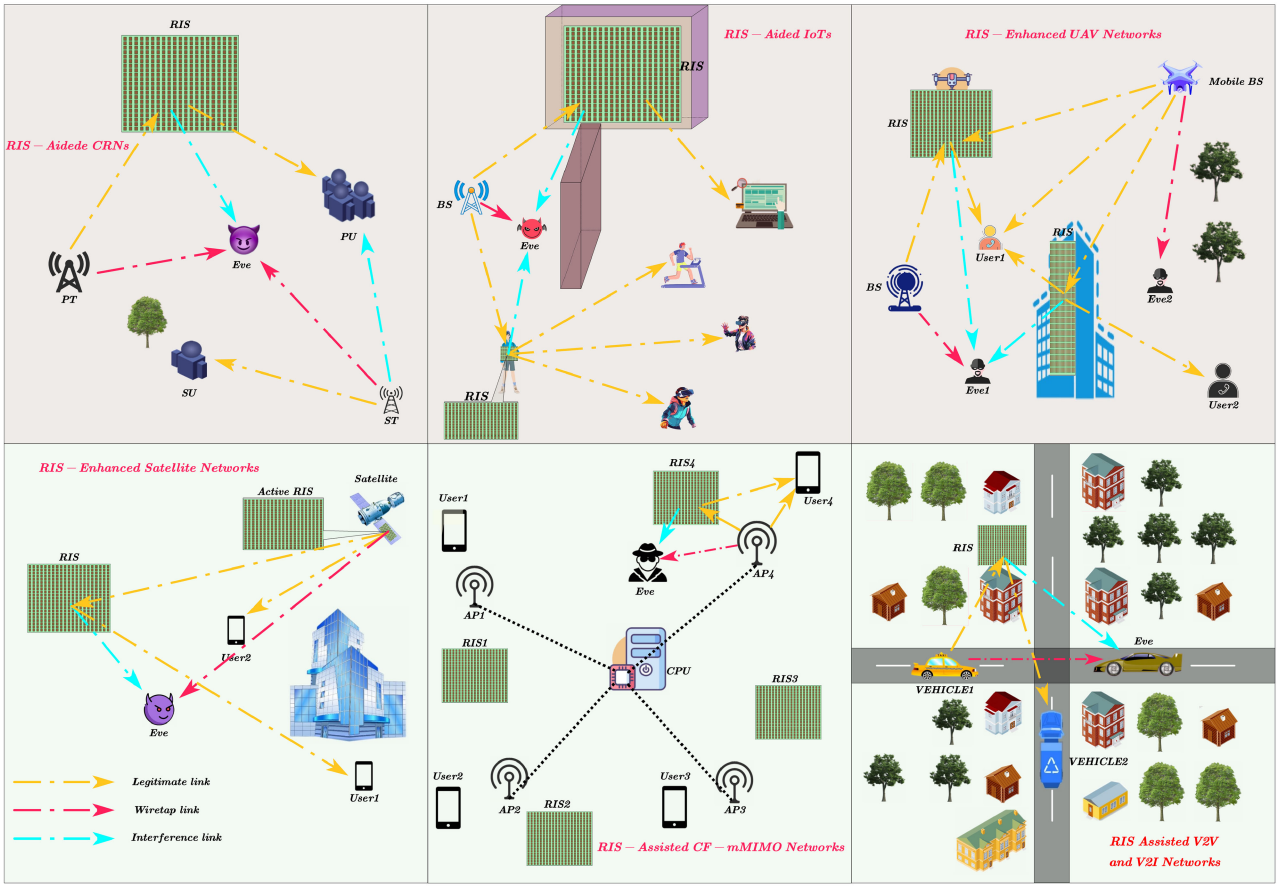


FIGURE 8. Typical application scenarios of six communication networks.

interception of the primary user's signals, proving that the introduction of RIS improved the security of the system. All of these studies demonstrate that implementing RIS can significantly improve safety in CRNs.

2) RIS-AIDED IOTS

IoT devices lack resources for local data processing, so data is sent to cloud servers. But cloud servers are far from IoT devices, causing latency issues. Edge computing moves computing and storage resources closer to end devices, reducing latency and improving data processing speed [121]. IoT communication security is crucial for efficient communication and coordination between devices, edge nodes, and cloud servers. Naturally, researchers focus on developing low-power and portable RIS technology to ensure security without compromising system performance. For instance, a scenario combining RIS-assisted NOMA technology with IoTs was considered in [67], and the impact of transceiver devices' RHI characteristics on the system's security performance was taken into account. The main factors affecting the SOP were described with simulation results. In addition, UAV-RIS was used in [57] to help the IoTs CRN communicate with multiple IoTs users, and it was demonstrated through numerical results that as the number of RIS increases, the confidentiality performance of the secondary network improves.

3) RIS-ENHANCED SATELLITE COMMUNICATION NETWORKS

Satellite communication, as an emerging choice for the future 6G communication system, is garnering considerable attention in military and civilian domains due to its extensive coverage and long-distance transmission. However, the QoS in satellite communication is prone to decline due to the deterioration of line-of-sight channel links, particularly in urban environments. To address this challenge, BSs are employed to relay and strengthen satellite signals, extending communication coverage to both densely populated and remote areas. In the intriguing study detailed in [108], the authors devised a PLS scheme within the context of a CSTN. In this scenario, satellites and BSs operate within the same frequency band, while multiple eavesdroppers attempt signal interception during the transmission process from BSs to mobile users. To maximize the SC, the authors employed active RIS and jointly designed BS beamforming, AN, and RIS RCs. They introduced a novel AO algorithm, which transformed each subproblem of the non-convex issue into a convex one, and simulation results confirmed the superiority

of the proposed scheme over the benchmark scheme. Further, in [51], the authors employed RIS and UAV as relays in a satellite communication network. They investigated the SOP under the condition of multiple eavesdroppers employing MRC eavesdropping schemes to intercept private signals, considering the scenario of a whole SNR. Their analysis used a combination of SDO and SCG to provide a comprehensive assessment of SOP and validate the results. Optimizing the trajectory of a UAV in a UAV-RIS-enhanced satellite communication network is very challenging. In [122], a deep learning method was used to optimize the trajectory of the UAV, and a double cascade correlation network was proposed to optimize the RC of the RIS. The results proved that the SR of the proposed scheme was improved compared to other benchmark schemes.

4) RIS-ENHANCED UAV NETWORKS

The application of UAV in communication networks demonstrates a diverse range of prospects, including communication relays, network expansion, mobile BSs, support for the IoTs, emergency response, and rapid deployment. It provides innovative solutions for various scenarios. Furthermore, the synergistic integration of the high maneuverability of UAV and the channel adaptability of RIS significantly enhances system security and energy efficiency. In [58], UAVs were employed to fly at a constant altitude, transmitting confidential information to users, while RIS were deployed on the facades of buildings to thwart eavesdroppers. The authors initially derived a closed-form expression for phase alignment to meet the specified phase shift. Under the condition of fixed phase shift, the authors employed the successive convex approximation (SCA) method to solve the trajectory optimization sub-problem approximately. Finally, this design was extended to a multi-user, multi-eavesdropper system. Furthermore, [56] addressed the security communication concerns within a UAV MISO network aided by RIS. By introducing fractional programming and relaxation techniques, a method based on AO was proposed to enhance the SR maximally. To analyze the security performance of aerial RIS NOMA-Aided systems more effectively, [55] introduced a deep neural network (DNN) approach. Through the acquisition of system variables and computation of security metrics, DNN enabled BSs to dynamically adapt parameters in varying environments, ultimately enhancing their ability to efficiently cater to the needs of mobile users. Moreover, DNNs exceled not only in the precise prediction of security performance metrics, including secure output power and energy efficiency, but also presented heightened computational efficiency in their execution. The study of [52] presented the joint optimization of flight trajectories, proactive UAV beamforming, and passive beamforming of RIS, aimed at maximizing SEE under worst-case scenarios. Real-time decision-making for each time slot was facilitated through the application of deep reinforcement learning (DRL). In the effort to decouple continuous optimization variables, they presented a twin-delayed deep deterministic policy gradient for the purpose of maximizing the anticipated cumulative reward intricately linked to the enhancement of SEE. Simulation results indicated that, when contrasted with conventional twin-deep deterministic policy gradient DRL-based methodologies, this approach manifested more notable impacts in the realms of confidentiality and energy preservation.

5) RIS-ASSISTED CELL-FREE MASSIVE MIMO NETWORKS

In many scenarios, traditional cellular communication networks face numerous challenges, such as cell-edge effects, spectrum resource sparsity, and system capacity limitations. Researchers have proposed a cell-free massive MIMO communication network to improve communication systems. The network includes multiple access points (APs) spread across an area, serving multiple users simultaneously to enhance efficiency. These APs coordinate through a backhaul link to a central processing unit, eliminating the need for mutual CSI exchange and thereby reducing signaling overhead. In cell-free massive MIMO systems, active eavesdroppers often pose a significant threat, as they can intercept higher information rates. The authors in [77] deliberated on the system security in cell-free massive MIMO networks under the scenario of active eavesdroppers conducting pilot spoofing attacks. They proposed a downlink transmission scheme based on RIS to jointly optimize the downlink power coefficient at the APs and the phase shift of the RIS. Experimental results showed the substantial potential of RIS in enhancing the robustness of cell-free massive MIMO systems against pilot spoofing attacks, with only a minimal number of RIS panels requiring activation to prevent information leakage. Similarly, [123] discussed secure communication in a cell-free massive MIMO network attacked by active eavesdroppers. This system was equipped with RIS, while the APs were furnished with low-resolution analog-to-digital/digital-to-analog converters (ADC/DAC). Through the utilization of an additive quantization noise model to capture the effects of coarse ADCs/DACs and employing a minimum mean square error channel estimator, the authors estimated the combined channel, which encompassed both the direct and indirect channels, thereby reducing the computational expenses associated with channel estimation. Furthermore, they derived a closed-form expression for the achievable ergodic SR which served as a tool to assess the influence of the number of APs, the quantity of RISs, and the resolution of ADCs/DACs on the system's performance. The integration of RIS into a cell-free massive MIMO network can further elevate system security and mitigate energy consumption. This strategic incorporation not only addresses the challenges inherent in traditional cellular networks but also aligns with the broader goal of optimizing communication systems for increased efficiency and reliability.

TABLE 3. Characteristics and researches on the integration of RIS with different advanced technologies.

Techniques	characteristics	References	Main contributions
Distributed RIS cooperation technology	Wide coverage and high performance gain.	[68]	Two practical communication scenarios are studied.
		[126]	The switching state of each RIS is jointly optimized with the phase shift of the RIS to maximize the SR.
		[127]	SR balancing for systems with multiple RISs supporting multiple users is investigated.
		[128]	Deploy multiple RIS to defend against jamming and eavesdropping.
Novel multiple access technology	Spectrum efficiency enhancement	[63]	Two eavesdropping channel scenarios in the STAR-RIS assisted uplink NOMA system are considered.
		[64]	Joint optimization of the power allocation factor and the ES factor of STAR-RIS to reduce the SOP of the NOMA system.
		[125]	The impact of transceiver RHI and imperfect SIC techniques on noma system security performance is considered.
		[130]	Designing three types of network interference to prevent information leakage.
		[131]	The security performance gain of active RIS with AN to the system is investigated.
		[132]	Deploying two RISs improves the security of the V2V NOMA system.
		[134]	STAR-RIS assisted downlink RSMA scenarios are considered.
SWIPT	High energy efficiency	[47]	A dual time scale beamforming scheme is proposed.
		[135]	A heterogeneous network of RIS-assisted SWIPT is considered.
		[136]	A two-stage communication process in the presence of a passive eavesdropper is considered.
ISAC	Alleviate spectrum congestion	[107]	Deploying active RIS against malicious UAV eavesdropping.
		[137]	Joint optimization of active beamforming, passive beamforming and AN to maximize SR.
		[138]	Optimization of radar receiver filters to increase the received SNR.
Backscatter	energy conservation	[139]	Proposing a constrained concave convex procedure ϵ-outage SR optimization algorithm.
		[140]	Secure communications for RIS-assisted millimeter-wave symbiotic radios are investigated.
		[141]	Maximizing SNR for secondary users.
		[142]	The CSI error model in the presence of an eavesdropper in a symbiotic radio system is considered.
AI	High adaptability and efficiency	[55]	Predicting accurate SOPs in a short period of time using a DNN framework.
		[143]	Use DRL to intelligently adjust beamforming strategies.
		[144]	Using DNN to enhance the effectiveness of RIS-assisted SWIPT systems.

6) RIS-ASSISTED V2V AND V2I COMMUNICATION NETWORKS

The establishment of a secure and reliable V2V and V2I communication network is pivotal for the future realization of autonomous driving and intelligent vehicles. Traditional encryption algorithms is proven to be unsuitable in V2V and V2I communication networks due to the limited computational capabilities of onboard systems and the high mobility of vehicles. Moreover, if vehicles take longer to process information, they may be unable to adapt to rapidly changing traffic environments. Therefore, the integration of PLS technology in vehicular systems is highly promising. The high level of compatibility between PLS and RIS makes RIS a natural fit for vehicle communication systems. The deployment of RIS serves to enhance the expected signal power for legitimate users while concurrently attenuating the signal power for eavesdropping nodes, thereby elevating the level of PLS. Specifically, [60] considered a V2I network model where multiple RISs are deployed on building tops as passive relays, with the presence of multiple eavesdroppers near the destination. It introduced a keyless PLS scheme utilizing RIS for beamforming. The study demonstrated that as the number of reflection elements in RIS increases, the achievable SC significantly improves while the SOP markedly decreases. In addition, [61] presented both V2V and V2I communication scenarios, each involving a passive eavesdropper attempting to obtain information illegally. The authors derived closed-form expressions for the SOP, providing evidence that RIS can effectively enhance the confidentiality of both V2V and V2I systems.

IV. INTEGRATION OF RIS WITH STATE-OF-THE-ART TECHNOLOGIES

This section focuses on the integration of RIS technology with several other novel technologies, including distributed RIS cooperation, new multiple access, SWIPT, ISAC, backscatter technology, and artificial intelligence (AI). By integrating these technologies, the communication secrecy performance can be further enhanced to meet more complex communication needs. We will discuss the integration of these technologies in detail and analyze their applications and advantages in communication systems to provide new ideas and directions for the future development of communication technologies. Table 3 summarizes relevant researches on the integration of RIS with these advanced technologies. Meanwhile, the principles and typical application scenarios about these technologies are shown in Fig. 9.

A. DISTRIBUTED RIS COOPERATION TECHNOLOGY

Previous literature has primarily focused on the communication scenarios assisted by single RIS due to its low complexity and ease of study [47], [94], [124], [125]. However, single RIS does not meet the performance requirements of real-life complex communication scenarios. Thus researchers have started to investigate distributed and collaborative ways of working with multiple RISs to improve the security of the system. Specifically, in [126], it was pointed out that the coverage of a single RIS was insufficient and could not reach the user's QoS. Hence, the authors investigated a multiple reflection RIS-assisted millimeter-wave communication system with switches to optimize the phase shift and switching state of the reflection RIS, and demonstrated numerically that the SR of deploying multiple RISs is significantly higher than that of the conventional single RIS based on the proposed AO algorithm. Compared to the single RIS, multiple RISs can provide more freedom and the ability to work together by adjusting the transmission direction of the signal to achieve flexible focusing of the beams, thus enhancing the secrecy rate of the system.

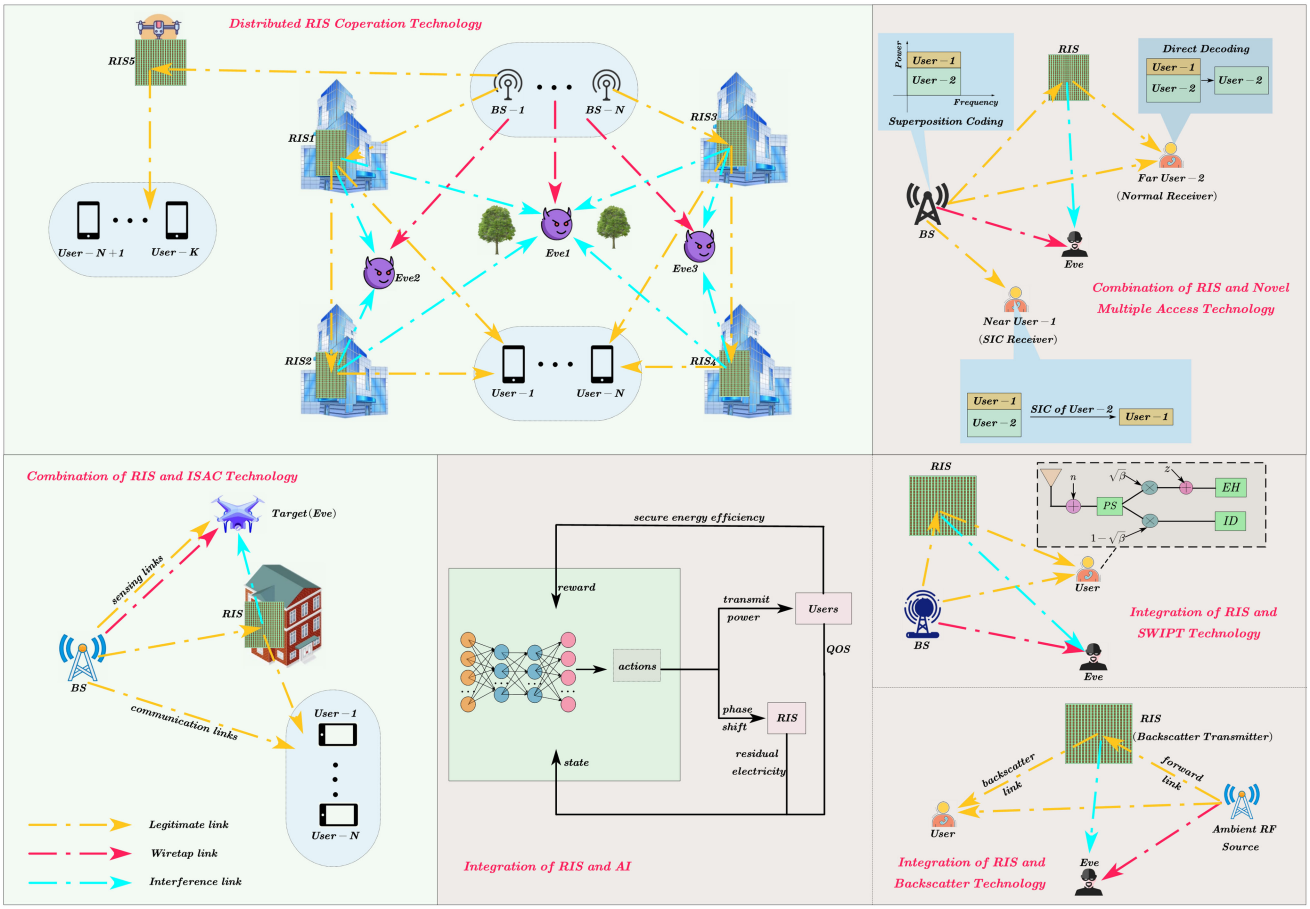


FIGURE 9. Principles and classic scenarios of RIS integration with different advanced technologies.

An optimal design of a collaborative beamforming-based transmission strategy in a multi-user MISO interference channel was considered in [127], and the experimental results also demonstrated the superiority of using multiple RISs. Distributed RISs can work together to resist interference signals from interference sources. By adjusting the RIS phase matrix, the impact of interference signals on legitimate users can be attenuated, improving the anti-interference capability of the communication system. It can also provide redundant paths so that when some RISs are attacked or fail, other RISs can continue to work, thus improving the reliability and robustness of the system. Take the example of intelligent transport systems, which will flourish in the future. Intelligent transport systems will rely on connected vehicle technologies to manage functions such as road safety, traffic flow, information, and entertainment. However, like conventional communication systems, vehicular communication systems can be subject to misuse or attack, which in turn threatens the entire transport system and the safety of drivers and vehicles. In [128], the authors were motivated in this background to create multiple transmission links between the user and multiple BS antennas to protect the communication network in the presence of single eavesdropper and interferers using multiple reflection RISs. In addition, two cases with different pairs of communication links over Nakagami-m fading channels were investigated in [68] to derive an expression for the average SC and to evaluate the impact of the relevant parameters of the system.

B. COMBINATION OF RIS AND NOVEL MULTIPLE ACCESS TECHNOLOGY

Conventional orthogonal multiple access requires each user to occupy a certain amount of spectrum resources exclusively for communication. This leads to the waste of spectrum resources and limits the system capacity. In future 6G communication scenarios, the number of users will increase significantly, and spectrum resources are far from enough. The traditional Time Division Multiple Access (TDMA) [129], Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA) technologies are not able to meet people's communication requirements because it is challenging to use orthogonal resource allocation to serve the ever-expanding IoTs. The NOMA technique has been proposed as a solution to break the constraints of resource orthogonality allocation. It allows for multiple users to be served on the same time-frequency resource and achieve large-scale connectivity through the utilization of superposition coding technology and successive interference

cancellation (SIC) technology at the transmitter and the receiver. Besides, NOMA has better user fairness and lower latency compared to OMA. In summary, NOMA is a highly promising multi-access technology.

However, NOMA technology also inevitably poses some confidentiality threats; every user can use SIC technology to decode other users' messages, i.e., every user can be a potential eavesdropper. To tackle this issue, [130] deployed RIS in NOMA system to constructively design inter-user interference at the legitimate receiver and destructively at the eavesdrover to reduce the eavesdropping capability. To improve the coverage and to increase the confidentiality performance of the system, [64] investigated a STAR-RIS-supported NOMA user communication operating under the ES protocol, aiming at optimizing the power allocation coefficients and the ES coefficients in order to reduce the SOP of the system. Similarly, a study of a STAR-RIS-assisted uplink NOMA transmission system was presented in [63]. The study considered two eavesdropping channel scenarios, full CSI and statistical CSI of the eavesdropper. It has to be mentioned that the study provides valuable guidance for STAR-RIS deployment. The previous researches were studied under ideal hardware conditions. However, in practical communication scenarios, imperfect hardware can produce distortion noise, which can make the user's communication experience worse and reduce the overall performance of the system. To deal with the degradation of the RIS-assisted NOMA system's performance caused by the RHI of the transceiver, [125] analyzed the influence of the transceiver RHI on the system. The study also developed a mathematical formula for the power of the distortion noise resulting from these impairments. The authors also considered the case that the user's SIC technique is imperfect, aiming to shape a more robust system. The total SR was maximized under the influence of distortion noise. As the optimization problem was non-convex, the multi-dimensional quadratic transform method, semi-definite relaxation (SDR) technique, and SCA algorithm were employed to convert the original problem into a convex one. Finally, an AO algorithm was utilized to solve it. In addition, active RIS was introduced in [131] to assist the NOMA system, and the superiority of the proposed scheme was demonstrated. In [132], the authors presented a dual RIS secure communication scenario in a V2V NOMA system. One RIS was deployed near the transmitting vehicle, and the other was deployed near the receiving vehicle. The authors employed the Gauss-Laguerre quadrature to derive ASC, SOP, and SEE. They used numerical results to verify that incorporating a dual RIS into a refraction RIS will result in a significant improvement in system safety.

On the other hand, Mao et al. introduced Rate-Splitting Multiple Access (RSMA) in [133]. RSMA combines the features of Spatial Division Multiple Access (SDMA), which treats residual multi-user interference as noise, and the use of the SIC technique in NOMA to eliminate interference from other users. In other words, RSMA is a more general downlink multi-antenna system access technology, and SDMA and NOMA are special cases of RSMA. After combining the advantages of NOMA and SDMA, RSMA has higher transmission rates, throughput, and lower computational complexity. Similarly, the system security of RSMA has also received the attention of researchers. For example, the authors of [134] investigated the STAR-RIS assisted downlink RSMA network, where the BS split the transmitted message into two parts, a public part that all users can decode and a private part that can only be decoded by the respective users. Finally, a suboptimal two-step iterative algorithm based on the sequential parametric convex approximation method is proposed to maximize total SR of the system.

C. INTEGRATION OF RIS AND SWIPT TECHNOLOGY

In recent years, the issue of energy conservation has become critical as the growth in the number of users and the expansion of network infrastructure, such as transmission links, terminals, and BSs, has led to a significant increase in power consumption. Therefore, the SWIPT transmission technology has emerged to meet these pressing needs. In SWIPT systems, the received signals can be used for both energy harvesting and information decoding, making full use of radio frequency (RF) signals. The bottleneck is typically the wireless transmission efficiency of EUs in SWIPT systems. As a result, the distance from EUs to the BS is usually shorter than that from IUs to the BS.

Consequently, security concerns in SWIPT systems are significant. The signal strength received by EUs is greater than that of IUs, making it easier for EUs to intercept and eavesdrop on information signals. In [47], to ensure system security, the authors investigated the RIS-assisted SWIPT system scenario, which included an IU and multiple EUs. Utilizing dual-timescale transmission, they aimed to minimize system complexity and overheads, ultimately optimizing the average worst-case SR for IUs, considering energy harvesting constraints for EUs and power constraints for BSs. Then, a stochastic SCA algorithm was proposed to solve this optimization problem.

Furthermore, [135] considered a RIS-assisted SWIPT system within a heterogeneous network framework. The BS's beamforming vector and the RIS's phase shift matrix were jointly optimized to minimize total power consumption while satisfying safety and energy condition constraints. In [136], a RIS-assisted SWIPT system was studied with a passive eavesdropper located in the path from the BS to the users intercepting one of them. To meet the confidentiality requirements, the authors divided the transmission into two phases. In the first phase, the BS refrained from transmitting the signal to the eavesdropped user. In the second phase, it permitted other users to forward the signal to the attacked user through the RIS. The authors then solved the problem of maximizing the average SR using a majorization-minimization (MM)-based AO framework.

D. COMBINATION OF RIS AND ISAC TECHNOLOGY

The Internet of Everything has created an urgent need for new solutions to address spectrum congestion. ISAC is a solution that can allocate spectrum resources to improve spectrum utilization. However, security issues arise when ISAC focuses on radar tracking, making it challenging to ensure system security if the target intends to eavesdrop. Deploying RIS in an ISAC system can enhance overall system performance. Without loss of generality, the deployment of RIS in ISAC systems to enhance PLS was considered in [137]. Specifically, the authors performed a joint optimization of the active beamforming vector and RIS phase-shift matrices and introduced AN to maximize SR. Furthermore, [138] researched the RIS-supported multi-user MISO ISAC system to resist the detection of malicious radar targets. The authors proposed a research scheme that optimized the active transmit beamforming vector, passive beamforming of RIS, and radar receive filter to improve the SNR of the radar while satisfying communication requirements, power constraints, and secure transmission requirements. However, the use of passive RIS does not provide a significant performance gain to the system due to the presence of multiplicative fading effects.

Therefore, in [107], active RIS was incorporated to maximize the achievable SR in a MISO ISAC system in the presence of a malicious UAV for eavesdropping. To solve this optimization problem, the authors divided it into three sub-problems, and then formulated a closed-form expression for the radar receive beamforming formation, optimized the dual transmit beamformer, and designed the phase shift matrix for the active RIS in three sub-problems. They proposed an iterative optimization algorithm based on fractional programming (FP) and MM to solve these problems. Simulation results demonstrated that the proposed active RIS-assisted ISAC system outperformed the benchmark scheme.

E. INTEGRATION OF RIS AND BACKSCATTER TECHNOLOGY

Backscatter technology reflects signals from a transmitter to a receiver using a passive reflective device called backscatter device (BD), significantly reducing energy consumption. Secondary transmissions do not affect primary transmissions, and the primary transmission enhances the performance of the secondary transmission. However, we still need some security measures to ensure the confidential performance of the system. For instance, [139] considered backscatter-assisted communication that apply NOMA techniques. The paper solved the secure beamforming problem using a constrained concave-convex procedure ϵ-outage SR optimization algorithm. However, backscatter links in backscatter communication are subject to high path loss due to double fading. The integration of RIS and the backscatter technique could increase the SR and received SNR of the secondary user. Specifically, a millimeter-wave backscatter communication using an reflection RIS as a BD was investigated in [140], where the reflection RIS enhanced the security of the BS for information transmission by adjusting the passive beamforming. The SNR for secondary users was maximized in [141] by jointly optimizing the active beamforming of the primary transmitter, the amplitude RCs and phase-shift matrix of the RIS. The performance gain that passive RIS can bring to a system is ultimately limited because the double fading effect also hampers passive RIS. In [142], an active RIS was used to support the backscatter communication. At the same time, the CSI error model in the presence of an eavesdropper was considered for the first time. Robust and secure transmission schemes were designed for the bounded CSI error model and the statistical CSI error model, respectively. The experimental results showed that the scheme considering the statistical CSI error model is more energy efficient than the scheme considering the bounded CSI.

F. INTEGRATION OF RIS AND AI

In modern wireless systems, many factors affect the security, and the complexity of the optimization problem is such that it cannot be solved using traditional optimization methods alone. Traditional methods for real-time channel estimation, beamforming, and power allocation often suffer from high overhead and inefficiency. In this way, the BS is unable to obtain the eavesdropper's instantaneous CSI. As a result, the BS's transmitting beamforming and the RIS's passive beamforming cannot be adjusted in time, which compromises the system's security performance.

AI has been utilized to enhance control of the signal transmission environment to address the issues mentioned above. Specifically, [143] considered a dynamic communication environment where the channel coefficients were time-varying, using a DRL approach to jointly optimize the beamforming matrix at the BS and the passive beamforming matrix at the reflection RIS. The authors integrated the SR and the user's QoS requirements into the reinforcement learning framework to create the reward function. A central controller was responsible for monitoring changes in the dynamic environment and using a Markov decision process to adjust the beamforming strategy intelligently. Furthermore, the authors suggested implementing a post-decision state to monitor the channel's dynamic changes. They also recommended using prioritized experience replay schemes to enhance learning efficiency. The results of the simulation showed that the proposed deep learning approach improved both SR and QoS satisfaction when compared to the benchmark method.

Not coincidentally, to enhance security for mobile users, [55] proposed a DNN approach to assist BS in adjusting their parameters to protect against eavesdropping. The authors also utilized a DNN framework to accurately predict SOPs in a short amount of time. Simulation results showed that the prediction curves of SOPs were consistent with mathematical curves, demonstrating the validity of the DNN model. Finally, the effectiveness of the DNN

framework was also verified using mean square error verification. In the past, when dealing with optimization problems in RIS-assisted secure communication systems, AO algorithms were commonly used to solve both convex and non-convex problems. However, this approach required a high number of iterations, resulting in significant time and complexity costs. Furthermore, [144] investigated the utilization of DNNs to enhance the efficiency of reflection RIS-assisted SWIPT systems. A comparison showed that the DNN-based method significantly reduced computational time compared to the traditional approach.

V. FUTURE RESEARCH DIRECTIONS

A. HARDWARE LIMITATIONS

Most of existing literature focused on RIS with single-connected architectures, i.e., the case where the scattering matrix of the RIS is diagonal. However, although the single-connected architecture is easy to implement, its performance gain may be not insufficient. Moreover, the diagonal structure of RIS is not universal, it is just a special case. As far as we know, the fully connected and group-connected RIS with a more flexible structure was only studied in [118], [145], [146]. The beyond diagonal structure of RIS was first proposed in [118]. After that, in [145], three working modes of beyond-diagonal RIS were introduced, and nine models of beyond-diagonal RIS were summarized. The authors in [146] studied the discrete-valued group-connected RIS, and analyzed its performance. Numerical results demonstrated that the system performance of fully connected and group-connected RIS were better than that of single connected RIS. In the future system design, the researcher should focus on the trade-off between system performance and complexity for fully connected and group-connected RIS, which can satisfy the users' needs and make the system more feasible.

B. PHASE-AMPLITUDE COUPLING OF RIS ELEMENTS

In practical RIS-based communication systems, the phase of each element on the RIS is coupled to its amplitude. However, many previous studies [58], [94], [147] assumed that the RIS has a uniform linear array, i.e., its amplitude response was the same for different phases of the elements, which was an ideal phase-shifting model. These non-ideal elements can lead to threats to the security of the physical layer of the system. We believe that in the future, it is needed to focus on the coupling relationship between the phase and amplitude of RIS elements and precisely control the amplitude and phase to improve the robustness and security of the system. AI techniques should also be utilized to adaptively adjust the phase and amplitude of RIS according to changes in the dynamic communication environment.

C. CHANNEL ESTIMATION CHALLENGES FOR CASCADED CHANNELS

RIS can not be only used to improve the QoS for users of communications systems but also to improve the confidentiality of the systems. However, RIS inevitably brings some new problems. The primary issue is estimation of the cascade channel. It is widely acknowledged that the RIS is composed of passive components, making direct estimation of the cascaded channel's CSI impossible from the RIS side. Therefore, indirect estimation of the cascaded channel is required through an active device located elsewhere.

Additionally, many channel coefficients need to be estimated due to the large number of scattering elements in the RIS. To address this issue, [148] suggested exploiting the scaling property among multiple users. This involved estimating the channel of a typical user first, followed by estimating the scaling factor among the users, thereby reducing system complexity and cost overhead. However, the accuracy of this method was naturally low. Furthermore, [149] proposed an algorithm consisting of three stages: sparse matrix factorization, probabilistic ambiguity elimination, and matrix completion to solve the cascaded channel estimation problem. Additionally, [150] proposed a method for placing active sensors in a passive array of RIS for cascaded channel estimation. Although there have been many solutions to the cascade channel estimation problem of RIS, these methods are still in their early stages and require further development. Researchers still have a lot of work to do when it comes to estimating cascade channels in the future.

D. POWERFUL EAVESDROPPER

The use of RIS can enhance the PLS of communication systems by intelligently reconfiguring the channel environment. However, RIS can also be exploited by illegal eavesdroppers, known as powerful eavesdroppers. On the one hand, illegal RIS can allow eavesdroppers to remain undetected while increasing the received SNR of eavesdroppers. On the other hand, IRIS is able to interfere with legitimate communication networks. The literature [91], [97], [151] has studied the illegal deployment of IRIS and has shown that it can cause significant damage to the system. In [97], a performance analysis of a system in the presence of IRIS was performed, and the numerical results showed that IRIS can cause a greater performance loss than traditional eavesdropping attacks. Both [91] and [151] proposed AN-based schemes to defend against IRIS, which could only partially mitigate the deterioration of security performance caused by IRIS. In summary, there is still a lack of research on illegal RIS. Designing more effective security policies to protect the system from IRIS attacks is an important research direction for the future.

VI. CONCLUSION

This paper presented a comprehensive review of the use of RIS in PLS systems. First, we introduced the principles of RIS and PLS, explaining how they can be integrated to enhance the confidentiality performance of the system. Then, we categorized RIS according to its different hardware architectures and described the advantages, disadvantages, and application scenarios of each type of RIS. In addition, we introduced the application of RIS in several kinds of typical

secure communication networks and the integration of RIS with some state-of-the-art technologies. Finally, the need for additional research on RIS-assisted secure communication systems was highlighted, along with the suggestion of promising research directions for the future. In general, the majority of the PLS works in the literature considered cooperative methods, which need additional power budget to generate artificial noise or use a relay to make the spectral efficiency halved. Thus, RIS indeed opens up many interesting secure transmission problems for both industry and academia, and offers the prospect of boosting wireless communication security. Therefore, this survey highlights various applications of RIS for improving PLS in multifarious scenarios and presents novel combination of RIS and PLS techniques in the literature. It is hoped that the RIS in PLS field discussed here will inspire further treatment from the research community and this survey can behave as a contribution to this exciting area.

REFERENCES

[1] 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.

[2] Q. Xue et al., "Beam management in ultra-dense mmWave network via federated reinforcement learning: An intelligent and secure approach," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 1, pp. 185–197, Feb. 2023.

[3] Q. Xue et al., "A survey of beam management for mmWave and THz communications towards 6G," *IEEE Commun. Surveys Tuts.*, early access, Mar. 12, 2024, doi: 10.1109/COMST.2024.3361991.

[4] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[5] 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, Feb. 2022.

[6] Z. Yin, N. Cheng, T. H. Luan, Y. Song, and W. Wang, "DT-assisted multi-point symbiotic security in space-air-ground integrated networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5721–5734, 2023.

[7] N. Yang and A. Shafie, "Terahertz communications for massive connectivity and security in 6G and beyond era," *IEEE Commun. Mag.*, vol. 62, no. 2, pp. 72–78, Feb. 2024.

[8] I. Ajayi, Y. Medjahdi, L. Mroueh, O. Okubadejo, and F. Kaddour, "Low-complexity neural networks for denoising imperfect CSI in physical layer security," in *Proc. IEEE Eur. Conf. Netw. Commun. (EUCNC) 6G Summit (EuCNC/6G Summit)*, 2023, pp. 48–53.

[9] S. Kavaiya and D. K. Patel, "Restricting passive attacks in 6G vehicular networks: A physical layer security perspective," *Wireless Netw.*, vol. 29, pp. 1355–1365, Dec. 2022.

[10] C. Amini, P. Azmi, and S. S. Kashef, "Relay-aided based physical layer security in VLC system with improved noise model," *IEEE Trans. Commun.*, vol. 71, no. 7, pp. 4193–4203, Jul. 2023.

[11] J. Ahmed, T. N. Nguyen, B. Ali, M. A. Javed, and J. Mirza, "On the physical layer security of federated learning based IoMT networks," *IEEE J. Biomed. Health*, vol. 27, no. 2, pp. 691–697, Feb. 2023.

[12] G. J. Anaya-López, J. P. Gonzàlez-Coma, and F. J. López-Martínez, "Leakage subspace precoding and scheduling for physical layer security in multi-user XL-MIMO systems," *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 467–471, Feb. 2023.

[13] M. A. Al-Atta, K. A. Said, M. A. Mohamed, and W. A. Raslan, "Physical-layer security in power-domain NOMA based on different chaotic maps," *Entropy*, vol. 25, no. 1, p. 140, Jan. 2023.

[14] A. Cenk, C. Sinasi, T. Kadir and A. Huseyin, "Physical layer security for visible light communication in reflected indoor environments with inter-symbol interference," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2709–2722, 2023.

[15] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[16] A. Zhang, P. Zhang, H. Wang, and X. Lin, "Application-oriented block generation for consortium blockchain-based IoT systems With dynamic device management," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7874–7888, May 2021.

[17] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017.

[18] Y. Feng, S. Yan, N. Yang, Z. Yang, and J. Yuan, "Safeguarding non-orthogonal multiple access with physical layer techniques," *IEEE Netw.*, vol. 36, no. 3, pp. 145–151, May/Jun. 2022.

[19] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, May 2019.

[20] Z. Yin et al., "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transport. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2021.

[21] X. Li et al., "Physical layer security for wireless-powered ambient backscatter cooperative communication networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 9, no. 4, pp. 927–939, Aug. 2023.

[22] L. Jin et al., "Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions," *China Commun.*, vol. 18, no. 9, pp. 88–99, Sep. 2021.

[23] J. Sun, J. Li, W. Hao, X. Mu, Z. Chu, and P. Xiao, "Secure transmission design with strong channel correlation for passive/active RIS communications," *IEEE Wireless Commun. Lett.*, vol. 12, no. 8, pp. 1394–1398, Aug. 2023.

[24] D. Li, "Ergodic capacity of intelligent reflecting surface-assisted communication systems with phase errors," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1646–1650, Aug. 2020.

[25] D. Li, "How many reflecting elements are needed for energy- and spectral-efficient intelligent reflecting surface-assisted communication," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1320–1331, Feb. 2022.

[26] M. H. Khoshafa, T. M. N. Ngatchede, M. H. Ahmed, "RIS-aided physical layer security improvement in underlay cognitive radio networks," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6437–6448, Dec. 2023.

[27] T. Hossain, S. Shabab, A. S. M. Badrudduza, M. K. Kundu, and I. S. Ansari, "On the physical layer security performance over RIS-aided dual-hop RF-UOWC mixed network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2246–2257, Feb. 2023.

[28] X. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, and P.-H. Ho, "Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions," *IEEE Syst. J.*, vol. 17, no. 1, pp. 848–859, Mar. 2023.

[29] S. Arzykulov, A. Celik, G. Nauryzbayev, and A. M. Eltawil, "Artificial noise and RIS-aided physical layer security: Optimal RIS partitioning and power control," *IEEE Wireless Commun. Lett.*, vol. 12, no. 6, pp. 992–996, Jun. 2023.

[30] Y. Zhang, G. Zhang, S. Chen, J. Choi, and P. Han Ho, "Optimal element allocation for RIS-aided physical layer security," *Wireless Commun. Mobile Comput.*, vol. 2022, Sep. 2022, Art. no. 4617366.

[31] S. Yadav, A. K. Yadav, D. S. Gurjar, and A. Pandey, "Physical layer security performance analysis of RIS-assisted wireless communication systems," in *Proc. IEEE Veh. Tech. Conf. (VTC)*, 2022, pp. 1–7.

[32] J. D. V. Sánchez, G. Kaddoum, and F. J. López-Martínez, "Physical layer security of RIS-assisted communications under electromagnetic interference," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2870–2874, Dec. 2022.

[33] S. Soderi, A. Brighente, F. Turrin, and M. Conti, "VLC physical layer security through RIS-aided jamming receiver for 6G wireless networks," in *Proc. 19th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, 2022, pp. 370–378.

[34] Z. Tang, T. Hou, Y. Liu, J. Zhang, and C. Zhong, "A novel design of RIS for enhancing the physical layer security for RIS-aided NOMA networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2398–2401, Nov. 2021.

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

[36] M. Katwe, K. Singh, B. Clerckx, and C.-P. Li, "Improved spectral efficiency in STAR-RIS aided uplink communication using rate splitting multiple access," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5365–5382, Aug. 2023.

[37] Z. Li, S. Wang, M. Wen, and Y.-C. Wu, "Secure multicast energy-efficiency maximization with massive RISs and uncertain CSI: First-order algorithms and convergence analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 6818–6833, Sep. 2022.

[38] X. Tang, H. He, L. Dong, L. Li, Q. Du, and Z. Han, "Robust secrecy via aerial reflection and jamming: Joint optimization of deployment and transmission," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12562–12576, Jul. 2023.

[39] T. jun Cui, M. Q. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light, Sci. Appl.*, vol. 3, pp. e218–e218, Oct. 2014.

[40] Z. Zhu et al., "Intelligent reflecting surface-assisted wireless powered heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 12, pp. 9881–9892, Dec. 2023.

[41] Z. Zhu et al., "Active reconfigurable intelligent surface enhanced Internet of Medical Things," *IEEE J. Biomed. Health Inform.*, early access, Dec. 21, 2023, doi: 10.1109/JBHI.2023.3343497.

[42] W. Hao et al., "Robust design for intelligent reflecting surface-assisted MIMO-OFDMA terahertz IoT networks," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 13052–13064, Aug. 2021.

[43] W. Yan et al., "Beamforming analysis and design for wideband THz reconfigurable intelligent surface communications," *IEEE J. Sel. Area Commun.*, vol. 41, no. 8, pp. 2306–2320, Aug. 2023.

[44] C. Zhou et al., "Energy-efficient maximization for RIS-aided MISO symbiotic radio systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13689–13694, Oct. 2023.

[45] Y. Xu, H. Xie, Q. Wu, C. Huang, and C. Yuen, "Robust max-min energy efficiency for RIS-aided HetNets with distortion noises," *IEEE Trans. Wireless Commun.*, vol. 70, no. 2, pp. 1457–1471, Feb. 2022.

[46] H. Niu, Z. Chu, F. Zhou, C. Pan, D. W. K. Ng, and H. X. Nguyen, "Double intelligent reflecting surface-assisted multi-user MIMO mmWave systems with hybrid precoding," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1575–1587, Feb. 2022.

[47] M.-M. Zhao, K. Xu, Y. Cai, Y. Niu, and L. H. Hanzo, "Secrecy rate maximization of RIS-assisted SWIPT systems: A two-timescale beamforming design approach," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4489–4504, Jul. 2022.

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

[49] Y. Xu, B. Gu, Z. Gao, D. Li, Q. Wu, and C. Yuen, "Applying RIS in multi-user SWIPT-WPCN systems: A robust and environmentally-friendly design," *IEEE Trans. Cogn. Commun. Netw.* , vol. 10, no. 1, pp. 209–222, Feb. 2024.

[50] H. Niu, Z. Chu, F. Zhou, Z. Zhu, L. Zhen, and K.-K. Wong, "Robust design for intelligent reflecting surface-assisted secrecy SWIPT network," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4133–4149, Jun. 2022.

[51] F. Zhou, X. Li, M. Alazab, R. H. Jhaveri, and K. Guo, "Secrecy performance for RIS-based integrated satellite vehicle networks with a UAV relay and MRC eavesdropping," *IEEE Trans. Intell. Veh.*, vol. 8, no. 2, pp. 1676–1685, Feb. 2023.

[52] M.-L. Tham, Y. J. Wong, A. Iqbal, N. B. Ramli, Y. Zhu, and T. Dagiuklas, "Deep reinforcement learning for secrecy energy- efficient UAV communication with reconfigurable intelligent surface," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2023, pp. 1–6.

[53] K. Guo, M. Wu, X. Li, H. Song, and N. Kumar, "Deep reinforcement learning and NOMA-based multi-objective RIS-assisted IS-UAV-TNs: Trajectory optimization and beamforming design," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 10197–10210, Sep. 2023.

[54] K. Guo, R. Liu, M. Alazab, R. H. Jhaveri, X. Li, and M. Zhu, "STAR-RIS-empowered cognitive non-terrestrial vehicle network with NOMA," *IEEE Trans. Intell. Veh.*, vol. 8, no. 6, pp. 3735–3749, Jun. 2023.

[55] H. P. Dang, M.-S. V. Nguyen, D.-T. Do, M.-H. Nguyen, M.-T. Pham, and A.-T. Kim, "Secure performance analysis of aerial RIS-NOMA-aided systems: Deep neural network approach," *Electronics*, vol. 11, no. 16, p. 2588, Aug. 2022.

[56] W. Wang, H. Tian, W. Ni, and M. Hua, "Reconfigurable intelligent surface aided secure UAV communications," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2021, pp. 818–823.

[57] V. N. Vo, N. Q. Long, V.-H. Dang, C. So-In, A.-N. Nguyen, and H. Tran, "Physical layer security in cognitive radio networks for IoT using UAV with reconfigurable intelligent surfaces," in *Proc. 18th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, 2021, pp. 1–5.

[58] J. Li, S. Xu, J. Liu, Y. Cao, and W. Gao, "Reconfigurable intelligent surface enhanced secure aerial-ground communication," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6185–6197, Sep. 2021.

[59] H. Ayaz, M. Waqas, G. Abbas, Z. H. Abbas, M. Bilal, and K. S. Kwak, "Improved rate of secret key generation using passive re-configurable intelligent surfaces for vehicular networks," *Sustainability*, vol. 15, no. 1, p. 342, Jan. 2022.

[60] H. Ayaz, M. Waqas, G. Abbas, Z. H. Abbas, and M. Bilal, "Multiple re-configurable intelligent surfaces based physical layer eavesdropper detection for V2I communications," *Phys. Commun.*, vol. 58, Apr. 2023, Art. no. 102074.

[61] Y. Ai, F. A. P. deFigueiredo, L. Kong, M. Cheffena, S. Chatzinotas, and B. E. Ottersten, "Secure vehicular communications through reconfigurable intelligent surfaces," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7272–7276, Jul. 2020.

[62] X. Zhao and J. Sun, "Secure reconfigurable intelligent surface aided heterogeneous VLC–RF cooperative NOMA networks," *Opt. Commun.*, vol. 511, Jan. 2022, Art. no. 127983.

[63] Z. Zhang, J. Chen, Y. Liu, Q. Wu, B. He, and L. Yang, "On the secrecy design of STAR-RIS assisted uplink NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 12, pp. 11207–11221, Dec. 2021.

[64] S. P. Xu, C. Liu, H. Wang, M. Qian, and J. Li, "On secrecy performance analysis of multi-antenna STAR-RIS-assisted downlink NOMA systems," *EURASIP J. Adv. Sig. Pr.*, vol. 2022, pp. 1–31, Dec. 2022.

[65] N. D. Nguyen, M.-S. V. Nguyen, and M. Munochiveyi, "Empowering reconfigurable intelligent surfaces for security of downlink NOMA," *Wireless Commun. Mobile Comput.*, vol. 2022, May 2022, Art. no. 1498918.

[66] C. Jiang, C. Zhang, P. Hao, Z. Zhang, and J. Hua Ge, "Robust secure design for RIS-aided NOMA network against internal near-end eavesdropping," *IEEE Access*, vol. 9, pp. 142105–142113, 2021.

[67] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks," *IEEE Access*, vol. 9, pp. 42583–42592, 2021.

[68] B. C. Nguyen, Q.-N. Van, L. T. Dung, T. M. Hoang, N. V. Vinh, and G. T. Luu, "Secrecy performance of multi-RIS-assisted wireless systems," *Mobile Netw. Appl.*, pp. 1–14, Jun. 2023, doi: 10.1007/s11036-023-02125-7.

[69] J. Xu, Z. Zhu, Z. Chu, H. Niu, P. Xiao, and I. Lee, "Sum secrecy rate maximization for IRS-aided multi-cluster MIMO-NOMA terahertz systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4463–4474, 2023.

[70] X. Li et al., "Reliability and security of CR-STAR-RIS-NOMA assisted IoT networks," *IEEE Internet Things J.*, early access, Dec. 7, 2023, doi: 10.1109/JIOT.2023.3340371.

[71] H. Liu, G. Li, X. Li, Y. Liu, G. Huang, and Z. Ding, "Effective capacity analysis of STAR-RIS-assisted NOMA networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 9, pp. 1930–1934, Jul. 2022.

[72] X. Yue, J. Xie, C. Ouyang, Y. Liu, X. Shen, and Z. Ding, "Active simultaneously transmitting and reflecting surface assisted NOMA networks," *IEEE Trans. Wireless Commun.*, early access, Feb. 28, 2024, doi: 10.1109/TWC.2024.3367302.

[73] X. Yue, M. Song, C. Ouyang, Y. Liu, T. Li, and T. Hou, "Exploiting active RIS in NOMA networks with hardware impairments," *IEEE Trans. Veh. Technol.*, early access, Jan. 15, 2024, doi: 10.1109/TVT.2024.3352813.

[74] Y. Pei, X. Yue, W. Yi, Y. Liu, X. Li, and Z. Ding, "Secrecy outage probability analysis for downlink RIS-NOMA networks with on-off control," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, pp. 11772–11786, Sep. 2023.

[75] N. D. Nguyen, A.-T. Le, and M. Munochiveyi, "Secrecy outage probability of reconfigurable intelligent surface-aided cooperative underlay cognitive radio network communications," in *Proc. 22nd Asia-Pac. Netw. Oper. Manag. Symp. (APNOMS)*, 2021, pp. 73–77.

[76] W. Hao, J. Li, G. Sun, M. Zeng, and O. A. Dobre, "Securing reconfigurable intelligent surface-aided cell-free networks," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3720–3733, 2022.

[77] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Exploiting RIS for limiting information leakage to active eavesdropper in cell-free massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 443–447, Mar. 2022.

[78] R. Chen, M. Liu, Y. Hui, N. Cheng, and J. Li, "Reconfigurable intelligent surfaces for 6G IoT wireless positioning: A contemporary survey," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23570–23582, Dec. 2022.

[79] Z. Ding et al., "A state-of-the-art survey on reconfigurable intelligent surface-assisted non-orthogonal multiple access networks," *Proc. IEEE*, vol. 110, no. 9, pp. 1358–1379, Sep. 2022.

[80] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. D. Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, May 2020.

[81] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive MIMO: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no.1 pp. 492–523, 1st Quat., 2022.

[82] J. Xu et al., "Reconfiguring wireless environment via intelligent surfaces for 6G: Reflection, modulation, and security," 2022, *arXiv:2208.10931*.

[83] M. Ahmed et al., "A survey on STAR-RIS: Use cases, recent advances, and future research challenges," *IEEE Internet Things J.*, vol. 10, no. 16 pp. 14689–14711, Aug. 2023.

[84] K. M. Faisal and W. Choi, "Machine learning approaches for reconfigurable intelligent surfaces: A survey," *IEEE Access*, vol. 10, pp. 27343–27367, 2022.

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

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

[87] Y. Guo, Y. Liu, Q.-H. Wu, Q. Shi, and Y. Zhao, "Enhanced secure communication via novel double-faced active RIS," *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3497–3512, Jun. 2023.

[88] L. Gong, W. Xu, X. Ding, N. Zhou, and Q. Zhu, "Joint optimization scheme for the reconfigurable intelligent surface-assisted untrusted relay networks," *China Commun.*, vol. 20, pp. 19–29, Dec. 2023.

[89] E. O. Frimpong, B.-H. Oh, T. Kim, and I. Bang, "Physical-layer security with irregular reconfigurable intelligent surfaces for 6G networks," *Sensors*, vol. 23, no. 4, p. 1881, Feb. 2023.

[90] Z. Cheng, N. Li, J. Zhu, X. She, C. Ouyang, and P. Chen, "RIS-assisted secure communications: Low-complexity beamforming design," *IEEE Wireless Commun. Lett.*, vol. 12, no. 6, pp. 1012–1016, Jun. 2023.

[91] F. Chen, H. Lu, Y. Wang, and C. Zhang, "Secure mmWave MIMO communication against signal leakage when meeting illegal reconfigurable intelligent surface," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2023, pp. 1–6.

[92] H. Niu, Z. Chu, F. Zhou, Z. Zhu, M. Zhang, and K.-K. Wong, "Weighted sum secrecy rate maximization using intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6170–6184, Sep. 2021.

[93] 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.

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

[95] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[96] B. Bai, W. Chen, and Z. Cao, "Outage optimal subcarrier allocation for downlink secure OFDMA systems," in *in Proc. IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 1320–1325.

[97] H. Alakoca et al., "Metasurface manipulation attacks: potential security threats of RIS-aided 6G communications," *IEEE Commun. Mag.*, vol. 61, pp. 24–30, Jan. 2023.

[98] W. Shi, J. Xu, W.-Q. Xu, M. D. Renzo, and C. Zhao, "Secure outage analysis of RIS-assisted communications with discrete phase control," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5435–5440, Apr. 2022.

[99] X. Li, Y. Zheng, M. Zeng, Y. Liu, and O. A. Dobre, "Enhancing secrecy performance for STAR-RIS NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684–2688, Feb. 2023.

[100] N. Yu et al., "Light propagation with phase discontinuities: Generalized laws of reflection and refraction," *Science*, vol. 334, pp. 333–337, Sep. 2011.

[101] R. Ma, W. Yang, X. Guan, X. Lu, Y. Song, and D. Chen, "Covert mmWave communications with finite blocklength against spatially random wardens," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3402–3416, Jan. 2024.

[102] R. Ma, W. Yang, H. Shi, X. Lu, and J. Liu, "Covert communication with a spectrum sharing relay in the finite blocklength regime," *China Commun.*, vol. 20, no. 4, pp. 195–211, Apr. 2023.

[103] X. Guo, Y. Chen, and Y. Wang, "Learning-based robust and secure transmission for reconfigurable intelligent surface aided millimeter wave UAV communications," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8 pp. 1795–1799, Aug. 2021.

[104] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted MIMOME system," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1374–1387, Feb. 2023.

[105] T. Zhang, H. Wen, Z. Pang, and H. H. Song, "CSI-free physical layer security against eavesdropping attack based on intelligent surface for industrial wireless," in *Proc. 17th IEEE Int. Conf. Fact. Commun. Syst. (WFCS)*, 2021, pp. 175–182.

[106] Z. Zhang et al., "Active RIS vs. passive RIS: Which will prevail in 6G?" *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1707–1725, Mar. 2023.

[107] A. A. Salem, M. H. Ismail, and A. S. Ibrahim, "Active reconfigurable intelligent surface-assisted MISO integrated sensing and communication systems for secure operation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4 pp. 4919–4931, Apr. 2023.

[108] H. Niu et al., "Active RIS-assisted secure transmission for cognitive satellite terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2 pp. 2609–2614, Feb. 2023.

[109] X. Xie, C. He, X. Ma, F. Gao, Z. Han, and Z. J. Wang, "Joint precoding for active intelligent transmitting surface empowered outdoor-to-indoor communication in mmWave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 10, pp. 7072–7086, Oct. 2023.

[110] Z. Lin et al., "Refracting RIS-aided hybrid satellite-terrestrial relay networks: Joint beamforming design and optimization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 4, pp. 3717–3724, Aug. 2022.

[111] Y. Liu, X. Mu, R. Schober, and H. V. Poor, "Simultaneously transmitting and reflecting (STAR)-RISs: A coupled phase-shift model," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2021, pp. 2840–2845.

[112] J. Xu, Y. Liu, X. Mu, and O. A. Dobre, "STAR-RISs: Simultaneous transmitting and reflecting reconfigurable intelligent surfaces," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 3134–3138, Sep. 2021.

[113] Z. Yang, W. Xu, C. Huang, J. Shi, and M. R. Shikh-Bahaei, "Beamforming design for multiuser transmission through reconfigurable intelligent surface," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 589–601, Jan. 2020.

[114] V. Jamali, A. M. Tulino, G. Fischer, R. R. Müller, and R. Schober, "Intelligent surface-aided transmitter architectures for millimeter-wave ultra massive MIMO systems," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 144–167, 2020.

[115] K. Liu, Z. Zhang, L. Dai, and L. H. Hanzo, "Compact user-specific reconfigurable intelligent surfaces for uplink transmission," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 680–692, Jan. 2021.

[116] Y. Sun et al., "Energy-efficient hybrid beamforming for multilayer RIS-assisted secure integrated terrestrial-aerial networks," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4189–4210, Jun. 2022.

[117] Y. Sun et al., "Active-passive cascaded RIS-aided receiver design for jamming nulling and signal enhancing," *IEEE Trans. Wireless Commun.*, early access, Oct. 25, 2023, doi: 10.1109/TWC.2023.3325813.

[118] S. Shen, B. Clerckx, and R. D. Murch, "Modeling and architecture design of reconfigurable intelligent surfaces using scattering parameter network analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 1229–1243, Feb. 2022.

[119] X. Wu, J. Ma, and X. Xue, "Joint beamforming for secure communication in RIS-assisted cognitive radio networks," *J. Commun. Netw.*, vol. 24, no. 5, pp. 518–529, Oct. 2022.

[120] R. Alsabet and D. B. Rawat, "Securing communications for IRSs-assisted mmWave cognitive radio networks," in *Proc. IEEE 14th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, 2023, pp. 0595–0600.

[121] L. Chen, K. Cao, T. Lu, Y. Lu, and A. Hu, "A one-time pad encryption scheme based on efficient physical-layer secret key generation for intelligent IoT system," *China Commun.*, vol. 19, pp. 185–196, Jul. 2022.

[122] Y. Liu, C. Huang, G. Chen, R. Song, S. Song, and P. Xiao, "Deep learning empowered trajectory and passive beamforming design in UAV-RIS enabled secure cognitive non-terrestrial networks," *IEEE Wireless Commun. Lett.*, vol. 13, no. 1, pp. 188–192, Jan. 2024.

[123] X. Zhang, T. Liang, K. An, H. Yang, and C. Niu, "Secure transmission in RIS-assisted cell-free massive MIMO system with low resolution ADCs/DACs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 339–344.

[124] Z. Zheng, W. lin, L. wei, He, tao, L. Lu, and C. Jian, "Security enhancement for coupled phase-shift STAR-RIS networks," *IEEE Netw.*, vol. 72, no. 6 pp. 278–285, Jun. 2023.

[125] Q. Zhang et al., "Robust beamforming design for RIS-aided NOMA secure networks with transceiver hardware impairments," *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3637–3649, Jun. 2023.

[126] Y. Xiu, J. Zhao, C. Yuen, Z. pei Zhang, and G. Gui, "Secure beamforming for multiple intelligent reflecting surfaces aided mmWave systems," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 417–421, Feb. 2021.

[127] Y. L. Liu, J. Yang, K. Huang, X. Sun, and Y. Wang, "Secure wireless communications in the multi-user MISO interference channel assisted by multiple reconfigurable intelligent surfaces," *J. Commun. Networks*, vol. 24, no. 5, pp. 530–540, Oct. 2022.

[128] R. Alsabet and D. B. Rawat, "Securing multi-IRS aided mmWave communications against eavesdropping and jamming in vehicular cyber physical systems," in *Proc. IEEE/ACM 23rd Int. Symp. Clust., Cloud Internet Comput. Workshops (CCGridW)*, 2023, pp. 26–32.

[129] Y. He, Y. Liu, C. Jiang, and X. Zhong, "Multiobjective anti-collision for massive access ranging in MF-TDMA satellite communication system," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14655–14666, Aug. 2022.

[130] L. Lv, H. Jiang, Z. Ding, Q. Ye, N. Al-Dhahir, and J. Chen, "Secure non-orthogonal multiple access: An interference engineering perspective," *IEEE Netw.*, vol. 35, no. 4, pp. 278–285, Jul./Aug. 2021.

[131] F.-C. Yang, W. Guo, and J. Dai, "Artificial noise aided secure transmission for active RIS-aided NOMA networks," *IEEE Access*, vol. 11, pp. 78111–78118, Jul. 2023.

[132] F. R. Ghadi, M. Kaveh, K.-K. Wong, and D. Martín, "Physical layer security performance of dual RIS-aided V2V NOMA communications," 2024, *arXiv:2401.04059*.

[133] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-splitting multiple access for downlink communication systems: Bridging, generalizing, and outperforming SDMA and NOMA," *EURASIP J. Wireless Comm.*, vol. 2018, p. 133, May 2018.

[134] H. R. Hashempour, H. Bastami, M. Moradikia, S. A.Zekavat, H. Behroozi, and A. L. Swindlehurst, "Secure SWIPT in STAR-RIS aided downlink MISO rate-splitting multiple access networks," 2022, *arXiv:2211.09081*.

[135] W. Jiang, J. Yang, X. Ji, K. Huang, and J.-M. Yang, "Robust security transmission scheme for SWIPT-enable heterogeneous networks with RIS," *IEEE Syst. J.*, vol. 17, no. 4, pp. 5417–5428, Dec. 2023.

[136] G. Zhou, C. Pan, H. Ren, K. Zhi, S. Hong, and K. K. Chai, "User cooperation for RIS-aided secure SWIPT MIMO systems under the passive eavesdropping," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, 2021, pp. 171–176.

[137] C. Jiang, C. Zhang, C. Huang, J. Ge, J. He, and C. Yuen, "Secure beamforming design for RIS-assisted integrated sensing and communication systems," *IEEE Wireless Commun. Lett.*, vol. 13, no. 2, pp. 520–524, Feb. 2024.

[138] J. Chu, Z. Lu, R. Liu, M. Li, and Q. Liu, "Joint beamforming and reflection design for secure RIS-ISAC systems," *IEEE Trans. Veh. Technol.*, vol. 73, no. 3, pp. 4471–4475, Mar. 2024.

[139] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Secure beamforming in MISO NOMA backscatter device aided symbiotic radio networks," 2019, *arXiv:1906.03410*.

[140] C. Wang, Z. Li, T. Zheng, D. W. K. Ng, and N. Al-Dhahir, "Intelligent reflecting surface-aided secure broadcasting in millimeter wave symbiotic radio networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 11050–11055, Oct. 2021.

[141] C. Zhou, B. Lyu, D. T. Hoang, and S. Gong, "Reconfigurable intelligent surface assisted secure symbiotic radio multicast communications," in *Proc. IEEE 96th Veh. Technol. Conf. (VTC)*, 2022, pp. 1–6.

[142] B. Lyu, C. Zhou, S. Gong, D. T. Hoang, Y.-C. Liang , "Robust secure transmission for active RIS enabled symbiotic radio multicast communications," *IEEE Trans. Wireless Commun.*, vol. 22, no. 12, pp. 8766–8780, Dec. 2023.

[143] H. Yang, Z. Xiong, J. Zhao, D. T. 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. 2020.

[144] H. T. Thien, P. V. Tuan, and I. Koo, "A secure-transmission maximization scheme for SWIPT systems assisted by an intelligent reflecting surface and deep learning," *IEEE Access*, vol. 10, pp. 31851–31867, 2022.

[145] H. Li, S. Shen, and B. Clerckx, "Beyond diagonal reconfigurable intelligent surfaces: From transmitting and reflecting modes to single-, group-, and fully-connected architectures," *IEEE Trans. Wireless Commun.*, vol. 22, no. 4, pp. 2311–2324, Apr. 2022.

[146] M. Nerini, S. Shen, and B. Clerckx, "Discrete-value group and fully connected architectures for beyond diagonal reconfigurable intelligent surfaces," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16354–16368, Dec. 2021.

[147] H. Luo, G. Li, and L. Hu, "On the security of RIS-assisted manipulating attack in MISO systems," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC)*, 2021, pp. 1–5.

[148] Y. Han, S. Jin, C.-K. Wen, and T. Q. S. Quek, "Localization and channel reconstruction for extra large RIS-assisted massive MIMO systems," *IEEE J. Sel. Top. Signal Process.*, vol. 16, no. 5, pp. 1011–1025, Aug. 2022.

[149] Z.-Q. He and X. Yuan, "Cascaded channel estimation for large intelligent metasurface assisted massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 210–214, Feb. 2019.

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

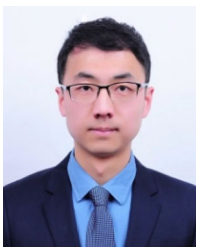
[151] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, Jun. 2022.

MENGZHAO GUO received the B.E. degree in radar engineering from the College of Electronic Engineering, National University of Defence Technology, Hefei, China, in 2023, where he is currently pursuing the M.E. degree in information and communication engineering with the College of Electronic Engineering.

ZHI LIN received the B.E. and M.E. degrees in information and communication engineering from the PLA University of Science and Technology in 2013 and 2016, respectively, and the Ph.D. degree in electronic science and technology from the Army Engineering University of PLA, Nanjing, China, in 2020.

From March 2019 to June 2020, he was a visiting Ph.D. student with the Department of Electrical and Computer Engineering, McGill University, Montréal, Canada. Since February 2023, he has been a Postdoctoral Fellow with the School of Computer Science and Engineering, Macau University of Science and Technology, Macau, China. Since January 2021, he has been with the College of Electronic Engineering, National University of Defense Technology, Hefei, China, where he is currently an Associate Professor. His research interests include array signal processing, physical layer security, reconfigurable intelligent surface, and satellite-aerial-terrestrial integrated networks. He was the recipient of the Outstanding Ph.D. Thesis Award of Chinese Institute of Electronics in 2022, the Macao Young Scholars Fellowship in 2022, and the Best Paper Awards from IEEE IWCMC 2023 and IEEE ICCT 2023 Conferences. He was listed in the World's Top 2% Scientists identified by Stanford University in 2022 and 2023. He has been serving as an Area Editor for the *Physical Communication* since 2024. He was also a Lead Guest Editor of the *IET Communications* Special Issues on Reconfigurable Intelligent Surfaces Aided Physical Layer Security in 6G Wireless Networks. He was the Symposium Co-Chair of IEEE WCSP'22 and a TPC member of IEEE flagship conferences, including IEEE ICC, Globecom, Infocom, and VTC.

RUIQIAN MA received the B.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2017, and the M.S. and Ph.D. degrees from the Army Engineering University of PLA, Nanjing, China, in 2019, and 2022, respectively. He is currently a Lecturer with the College of Electronic Engineering, National University of Defense Technology, Hefei, China. His research interests include physical layer security, cooperative communication, and covert communication.



KANG AN received the B.E. degree in electronic engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011, the M.E. degree in communication engineering from the PLA University of Science and Technology, Nanjing, in 2014, and the Ph.D. degree in communication engineering from Army Engineering University, Nanjing, in 2017. Since January 2018, he has been with the National University of Defense Technology, Nanjing, where he is currently an Associate Professor. His current research interests include satellite communication, reconfigurable intelligent surface, anti-jamming communications, cooperative and cognitive communications, physical-layer security, and signal processing for wireless communications.

DONG LI (Senior Member, IEEE) received the Ph.D. degree in electronics and communication engineering from Sun Yat-sen University, Guangzhou, China, in 2010. Since 2010, he has been with the School of Computer Science and Engineering (formally, Faculty of Information Technology), Macau University of Science and Technology (MUST), Macau, China, where he is currently an Associate Professor. He held a visiting position with the Institute for Infocomm Research, Singapore, in 2012. His current research interests focus on 6G wireless communications, battery-free Internet of Things, and wireless AI. He was a recipient of the MUST Best Research Output Award in 2022, and the MUST Bank of China Excellent Research Award in 2011, 2016, 2019, and 2021. He was a co-recipient of the Best Paper Awards of IEEE ICCT 2023 and IEEE HealthCom 2023, and the Distinguished Paper Award of IEEE GreenCom 2023. He has been listed among World's Top 2% Scientists recognized by Stanford University since 2020. He is currently an Editor for the IEEE MMTC Review, an Executive Board Member of the IEEE Macau Section, and a member of the Association for Promotion of Science and Technology of Macau.

NAOFAL AL-DHAHIR (Fellow, IEEE) received the Ph.D. degree from Stanford University. He is an Erik Jonsson Distinguished Professor and the ECE Associate Head of UT-Dallas. He was a Principal Member of Technical Staff with GE Research Center and AT & T Shannon Laboratory from 1994 to 2003. He is a co-inventor of 43 issued patents and a coauthor of over 600 papers. He is co-recipient of eight IEEE best paper awards. He received the 2019 IEEE COMSOC SPCC Technical Recognition Award, the 2021 Qualcomm Faculty Award, and the 2022 IEEE COMSOC RCC Technical Recognition Award. He served as the Editor-in-Chief of IEEE TRANSACTIONS ON COMMUNICATIONS from January 2016 to December 2019. He is a Fellow of the U.S. National Academy of Inventors and a member of the European Academy of Sciences and Arts. He is an AAIA Fellow.

JIANGZHOU WANG (Fellow, IEEE) is a Professor with the University of Kent, U.K. He has published more than 400 papers and four books. His research focuses on mobile communications. He was a recipient of the 2022 IEEE Communications Society Leonard G. Abraham Prize and the IEEE Globecom2012 Best Paper Award. He was the Technical Program Chair of the 2019 IEEE International Conference on Communications, Shanghai, the Executive Chair of the IEEE ICC2015, London, and the Technical Program Chair of the IEEE WCNC2013. He is/was an Editor of a number of international journals, including IEEE TRANSACTIONS ON COMMUNICATIONS from 1998 to 2013. He is a Foreign Fellow of the Chinese Academy of Engineering, and a Fellow of the Royal Academy of Engineering, U.K. and of IET.