Digital Communications and Networks 10 (2024) 1553–1565

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Overview of RIS-enabled secure transmission in 6G wireless networks

JungSook Bae [a,1], Waqas Khalid [b,1], Anseok Lee [a], Heesoo Lee [a], Song Noh [c,*], Heejung Yu [d,*]

[a] Terrestrial & Non-Terrestrial Integrated Telecommunications Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[b] Institute of Industrial Technology, Korea University, Sejong 30019, South Korea
[c] Department of Information and Telecommunication Engineering, Incheon National University, Incheon 22012, South Korea
[d] Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea

ARTICLE INFO

Keywords:
6G
Physical-layer security
Reconfigurable intelligent surface

ABSTRACT

As the 6th-Generation (6G) wireless communication networks evolve, privacy concerns are expected due to the transmission of vast amounts of security-sensitive private information. In this context, a Reconfigurable Intelligent Surface (RIS) emerges as a promising technology capable of enhancing transmission efficiency and strengthening information security. This study demonstrates how RISs can play a crucial role in making 6G networks more secure against eavesdropping attacks. We discuss the fundamentals and standardization aspects of RISs, along with an in-depth analysis of Physical-Layer Security (PLS). Our discussion centers on PLS design using RIS, highlighting aspects including beamforming, resource allocation, artificial noise, and cooperative communications. We also identify the research issues, propose potential solutions, and explore future perspectives. Finally, numerical results are provided to support our discussions and demonstrate the enhanced security enabled by RIS.

1. Introduction

The 6th-Generation (6G) wireless communication networks offer significantly higher transmission rates, reduced latency, and enhanced reliability. These enhancements can facilitate innovative applications, unprecedented services, and comprehensive solutions [1]. Nevertheless, 6G networks also introduce substantial security challenges attributed to the inherent broadcast nature of wireless channels, the voluminous influx of sensitive and confidential data (e.g., motion tracking, financial transactions, and cell phone information), and the exponential surge in potential attack vectors. Therefore, 6G networks must be hyper-secure, encompassing data security from the application to the physical layer. A Physical-Layer Security (PLS) approach based on information theory has attracted interest from industry and academia. Notably, PLS ensures data security by preventing unauthorized interception and malicious use of private information, without encryption methods [2].

In 6G networks, sub-terahertz (sub-THz) bands complement millimeter-wave (mmWave) bands that are adopted by 5th-Generation (5G) networks. Though high-frequency bands offer several advantages, they also pose unique propagation challenges that must be addressed. Notably, mmWave and sub-THz signals are susceptible to blockages and substantial penetration loss [3]. Therefore, algorithms and protocols for wireless transmission must be developed to mitigate the adverse effects of an uncontrolled radio environment. Conventional transmission strategies use multiple antennas, complex signal-processing algorithms, and advanced encoding-decoding procedures. However, the transceiver design cannot be overly complex in resource-constrained scenarios [4]. The true potential of 6G networks can be realized by deploying a radio environment that can be manipulated to optimize overall network performance. In this regard, seamless wireless connectivity in 6G networks requires novel physical-layer technologies, such as Reconfigurable Intelligent Surfaces (RISs), relays, Network-Controlled Repeaters (NCRs), and massive Multiple-Input Multiple-Output (mMIMO). Particularly, RIS is an emerging technology that provides a controllable and programmable radio environment [5]. Given the dependence of PLS on rich scattering environments, dynamically controlled channels enabled by RIS can significantly enhance security.

1.1. Motivation

A key aspect of PLS is the manipulation of the dynamic characteristics of wireless channels to enhance and/or limit the Signal-to-

* Corresponding authors.
E-mail addresses: jsbae@etri.re.kr (J. Bae), waqas283@korea.ac.kr (W. Khalid), alee@etri.re.kr (A. Lee), heelee@etri.re.kr (H. Lee), songnoh@inu.ac.kr (S. Noh), heejungyu@korea.ac.kr (H. Yu).
[1] Co-first authors with equal contribution.

https://doi.org/10.1016/j.dcan.2024.02.005
Received 25 April 2023; Received in revised form 6 February 2024; Accepted 27 February 2024
Available online 5 March 2024

Interference-plus-Noise Ratio (SINR) for legitimate users and/or eavesdroppers, respectively. Due to the dependency on wireless channels characterized by noise and fading, the effectiveness of PLS might diminish under challenging propagation conditions [6]. Considering this, the dynamic channel control offered by RIS provides an opportunity to fully harness the advantages of PLS pertaining to channel propagation, spatial diversity, beamforming, and cooperative communications. By enhancing the SINR at a legitimate receiver (e.g., by diminishing fading and stabilizing the channel) and/or degrading the eavesdropping link (e.g., by inducing additional signal attenuation), RIS hinders eavesdroppers from accessing the intended message. Due to its significant performance benefits and alignment with conventional PLS methods, RIS is a promising candidate to enhance PLS [7]. RIS-PLS strategies find applicability within both 5G and 6G domains. Nonetheless, safeguarding the receiver from eavesdropping attacks via RIS requires careful consideration of the strategic positioning of RIS, the optimal number of elements, and their precise configuration. Furthermore, the choice of RIS-enhanced PLS solutions depends on the specific design scenarios and communication objectives to balance security effectiveness and implementation complexity. In this study, therefore, we introduce various RIS-enabled PLS technologies and provide research issues and potential solutions.

1.2. Summary of goals

Based on the motivations above, this study demonstrates how RISs can play a crucial role in making 6G networks more secure against eavesdropping attacks. Specifically, the goals of the study can be summarized as follows:

- We explore RIS-enabled PLS design, focusing on beamforming, resource allocation, antenna/node selection, Artificial Noise (AN), and cooperative relaying and jamming communications.
- We identify the research issues and potential solutions in RIS-enabled PLS. In detail, channel estimation, beam configuration, resource management, strategic placement and passive information transfer for RIS, hardware/channel modeling, and optimization for RIS-enabled PLS are discussed.
- In addition, we outline future research directions, highlighting Machine Learning (ML)-based solutions, advances in RIS hardware (e.g., active RIS, and Simultaneous Transmitting And Reflecting-RIS (STAR-RIS)), and malicious RIS.
- Finally, numerical results are provided to support our discussion and demonstrate the enhanced security provided by RIS. In particular, we examine the impact of RIS modeling, the number of RIS elements, RIS beam design, placement of RIS, quantized RIS phases, and AN on security performance.

1.3. Organization

The remainder of this paper is organized as follows: Sections 2 and 3 provide foundational discussions on RIS and PLS, respectively. Section 4 discusses RIS-enabled PLS designs. In section 5, research issues and solutions are presented. In section 6, future directions are provided. Section 7 presents the simulation results to demonstrate the effectiveness of RIS in terms of PLS. Finally, section 8 presents the conclusions of this study.

2. Reconfigurable intelligent surface

RISs emerged as a promising hardware-based transmission technology to manipulate wireless propagation landscapes artificially. Incident electromagnetic (EM) waves are reflected by numerous flexible and discrete elements with each sub-wavelength dimension embedded on a planar surface. By tuning signal phases and/or amplitudes with a smart RIS controller, the RIS enhances the Degrees of Freedom (DoF) of wireless channels, improves signal transmission, and enables advanced wireless functionalities. For example, RISs can mitigate unfavorable propagation conditions, such as blockage and deep fading [8] as shown in Fig. 1. It is a novel approach to altering EM wave propagation, coupled with state-of-the-art signal processing at the transceiver, providing significant enhancements to wireless connectivity, including signal enhancement, interference suppression, reliable reception, and precise positioning [8,9].

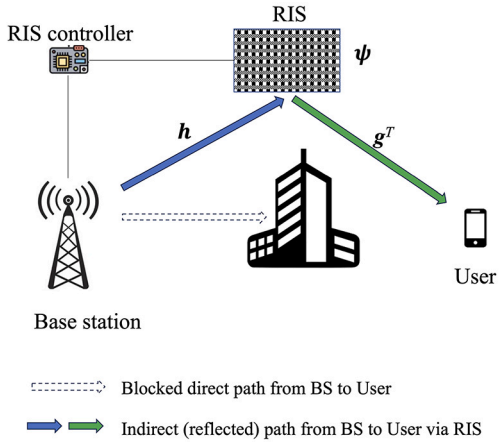

Fig. 1. An RIS-based wireless downlink transmission system.

2.1. Working principle of RIS

From a hardware perspective, RISs can be constructed using metamaterials and patch arrays. RISs can be designed to serve as reflective or refractive surfaces and strategically placed to enhance communications between a Base Station (BS) and users [10]. RISs can also be classified based on energy consumption into passive lossy, passive lossless, or active types. For operational analysis, reflected and refracted EM waves can be characterized using equivalent models of surface electric and magnetic currents. The interaction of EM waves with RISs can be analyzed using ray-optics or wave-optics methodologies. Despite being based on approximations, they provide valuable insights into how radio waves interact with materials and are widely used in the study of RISs [11].

For illustration, the reflection pattern of a patch-array RIS with N reflection elements can be expressed by a vector $\boldsymbol{\psi}$ whose ith element is given by

$$\psi_i = \beta_i e^{j\theta_i} \tag{1}$$

where β_i and θ_i denote the amplitude and phase responses, respectively. As shown in Fig. 1, where a single-antenna BS transmits a downlink signal to a single-antenna user through a RIS composed of N elements, the RIS can provide an indirect (reflected) path from the BS for the user. The effective channel gain of the reflected path via the RIS is expressed by

$$\mathbf{g}^T \mathbf{D}_{\boldsymbol{\psi}} \mathbf{h} = \sum_{i}^{N} h_i \psi_i g_i \tag{2}$$

where $\mathbf{g}^T$ and $\mathbf{h}$ denote the channels of the RIS-user and BS-RIS links, respectively, and $\mathbf{D}_{\boldsymbol{\psi}}$ is a diagonal matrix with the elements of $\boldsymbol{\psi}$ on the main diagonal. h_i and g_i denote the ith element of $\mathbf{h}$ and $\mathbf{g}$, respectively. Here, $(\cdot)^T$ denotes a transpose operation.

2.2. Standardization of RIS

In the International Telecommunication Union Radiocommunication Sector (ITU-R) IMT-2030 framework document, released in 2023,

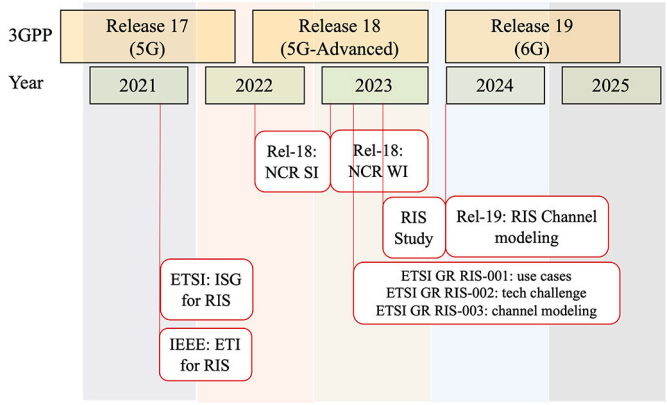

Fig. 2. Standardization and related timeline for RIS.

an RIS technology is discussed as one of the key enabling technologies for 6G wireless communications [12]. In 2021, an Industry Specification Group (ISG) for RIS was formed in European Telecommunications Standards Institute (ETSI) to study and standardize RIS. In 2023, the ISG provided three technical reports [13–15] as shown in Fig. 2. In the 3rd Generation Partnership Project (3GPP) Release 18, several companies proposed a study item for RIS. However, the majority of companies in 3GPP decided that it was too early to include RIS as a study item or working item because RIS is generally considered a candidate technology for 6G rather than 5G-Advanced. Then, it is expected to kick off a study item of RIS in 3GPP Release 19. The progression from NCR in Release 18 to RIS in Release 19 is analyzed by comparative studies in terms of architecture, operation, control signals, etc. [16–18]. For technical support of the standardization of RIS, an Emerging Technology Initiative (ETI) on RIS was formed by IEEE [19]. In the industry including NTT DOCOMO, preliminary field trials that demonstrate the potential of RIS in realistic environments have already been carried out [20]. The timeline of standardization events related to RIS is illustrated in Fig. 2.

3. Physical layer security

In this section, we examine PLS, highlighting its foundational principles, security designs, performance metrics, and optimization methods for secure 6G transmission.

3.1. Fundamental concept of PLS

Wyner investigated the concept of perfect secrecy for a wiretap channel at the physical layer by exploiting the capacity difference between legitimate and eavesdropping channels. With the rapid development of coding theories and the practical limitations of encryption-based security technologies, PLS has emerged as a leading method for secure communications [21]. Unlike cryptographic methods, PLS techniques do not require the design, storage, or distribution of keys, resulting in a more cost-effective electronic security solution. PLS schemes are intended to prevent eavesdropping by taking advantage of channel fading (despite its negative impact on reliability). By leveraging physical-layer characteristics, PLS methods refine transmission strategies and parameters, adapting to challenging channel conditions [22]. Additionally, PLS is distinguished by its reduced complexity and high resource efficiency. PLS categorizes eavesdropping scenarios into passive and active. Passive eavesdroppers intercept (decode/analyze) transmission from legitimate users without initiating active actions, such as transmitting signals. Conversely, active eavesdroppers engage in both interception and adversarial activities, such as generating AN or jamming attacks, disseminating deceptive information feedback, and exploiting pilot contamination. In Fig. 3, a classification structure for PLS solutions tailored for 6G wireless communications is illustrated, as well as representative examples and their merits and demerits. Each security strategy has its own unique strengths and limitations, making it particularly suitable for certain applications, systems, scenarios, and channel conditions. Therefore, a combination of these approaches is expected to provide superior security enhancements compared to an individual approach.

3.2. Performance metrics and optimization methods

From an information-theoretic viewpoint, PLS is often characterized by diverse security performance metrics and objective functions [21]. Table 1 provides a comprehensive breakdown of those employed for evaluating secure transmission. Furthermore, secure systems have been examined in terms of signal processing and optimization [22]. In the context of PLS, a variety of wiretap channel models have been described [23], as detailed below:

- MIMO wiretap channels: Encompassing a transmitter, a receiver, and an eavesdropper, all equipped with multiple antennas.
- Broadcast wiretap channels: Characterized by a single transmitter, multiple receivers, and several eavesdroppers.
- Relay wiretap channels: A cooperative framework featuring a transmitter, a relay, a receiver, and an eavesdropper.
- Multiple-access wiretap channels: Networks that include multiple transmitters, a single receiver, and an eavesdropper.
- Interference wiretap channels: Networks typified by multiple active communication links.

Based on the aforementioned security performance metrics, various optimization problems can be formulated [22,23]. For a typical example, we can consider the maximization of secrecy performance by controlling resources, such as transmit power, beamformers (or precoders), transmission duration, and bandwidth allocation. Heuristic algorithms, such as randomized algorithms, can solve non-convex optimization problems. A non-convex or intractable problem can be transformed into a tractable convex problem by approximation and relaxation methods and can be solved by convex optimization algorithms, such as interior point methods. Moreover, quadratic programming, mixed-integer programming (to solve problems with discrete and continuous variables), alternative optimization (an iterative method for solving convex sub-problems), fractional programming (to solve the ratio of nonlinear functions), and semidefinite programming have been employed to optimize PLS problems [24]. Furthermore, Deep Learning (DL) approaches can be adopted to address intricate network challenges, such as multi-cell and multi-user scenarios.

4. RIS-enabled PLS design

The risk of wiretapping is inherent in the vast and diverse ecosystem of 6G networks. Traditional PLS techniques (e.g., mMIMO and cooperative communications) are often challenged by unpredictable propagation conditions. Under such scenarios, RIS-aided PLS approaches outperform those without RIS integration [25]. Such scenarios could arise when the receiver requires a high level of secrecy, eavesdroppers are more numerous, equipped with superior antennas, control a dominant channel, exhibit a strong correlation with the receiver, or are located closer to the transmitter than the receiver [24,25]. In such circumstances, it may not be possible to exploit spatial DoF for secrecy enhancement through transmit beamforming with large-scale antenna arrays. In addition, hybrid techniques, such as transmit beamforming with AN or cooperative jamming, may not always prove effective in weakening the reception of an eavesdropper [23–25].

Using RIS to adjust the reflection of signals, coupled with signal processing optimization at both ends, offers distinct security benefits. Flexible signal adjustments via intelligent passive elements can address severe fading in traditional channels. An optimally configured RIS can

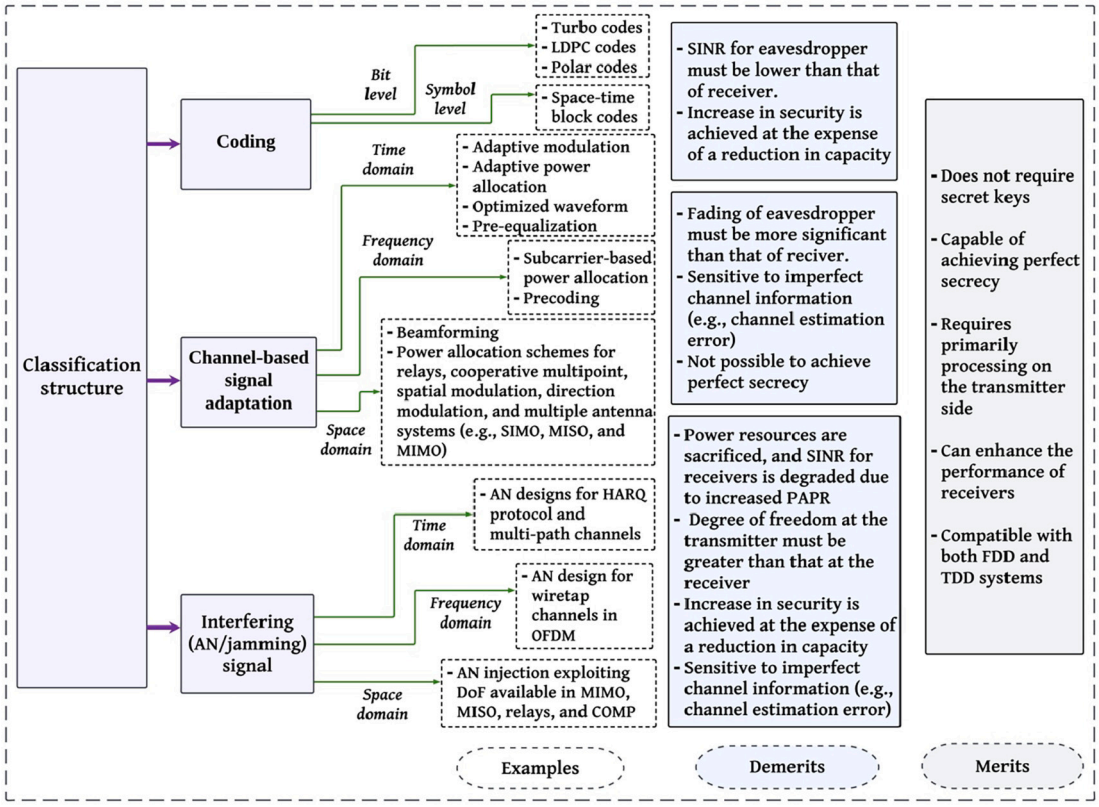

Fig. 3. Classification structures (including examples, merits, and demerits) for PLS solutions in the 6G wireless environment.

Table 1
Performance metrics for evaluating secure transmission in 6G networks.

Performance metric	Description	Mathematical representation
Secrecy rate	• Defined as the difference between the achievable rate of a legitimate link (C_l) and that of an eavesdropping link (C_e)	$C_s = \max(C_l - C_e, 0)$
Secrecy outage probability	• Probability that the secrecy rate (C_s) falls below a predefined target (C_{target})	$P_{out} = \Pr(C_s < C_{target})$
Intercept probability	• It is defined with a target secrecy rate of zero offering a worst-case evaluation of system security • It quantifies the likelihood of observing a negative secrecy rate, implying that C_s consistently falls below zero	$P_{intercept} = \Pr(C_s \leq 0)$
Strictly positive secrecy capacity	• Another special case of P_{out} and is defined as the probability that a non-zero C_s exists	$P_{positive} = \Pr(C_s > 0)$
Secrecy coverage probability	• It measures the success of the secure delivery process and has an opposite definition to P_{out} • It is defined as the probability that C_s exceeds C_{target}	$P_{coverage} = \Pr(C_s > C_{target}) = 1 - P_{out}$
Secure energy efficiency	• The number of secured bits transferred (B) per unit of energy or the total energy (E) required for sending a bit with secrecy	$SEE = \frac{B}{E}$
Secure power consumption	• The minimum amount of power required to achieve a specified C_{target} and E_{secure} is the corresponding energy consumed over the transmission time (t)	$P_{secure} = \frac{E_{secure}}{t}$ subject to $C_s \geq C_{target}$

enhance wireless channel efficiency for secure communications, regardless of the number, position, and channel state of transmitters, receivers, and potential eavesdroppers [26]. In typical RIS-aided PLS systems, a transmitter can send a message to a receiver via an RIS in the event of an eavesdropping attack. When an RIS is positioned closer to a transmitter or receiver, PLS performance can be enhanced, which is primarily influenced by the number of reflecting elements. Several studies have demonstrated that increasing the number of reflecting elements within an RIS is more effective than expanding the antenna array at a transmitter in ensuring transmission security [25,26]. The PLS performance may deteriorate due to the fact that eavesdroppers may receive multiple copies of the intended signals through the RIS, resulting in a severe leak of information. In these scenarios, however, relying solely on a secure technique may not provide adequate protection against eavesdropping. The implementation of a synergistic strategy for reducing the quality of the signal for the eavesdropper while enhancing the quality

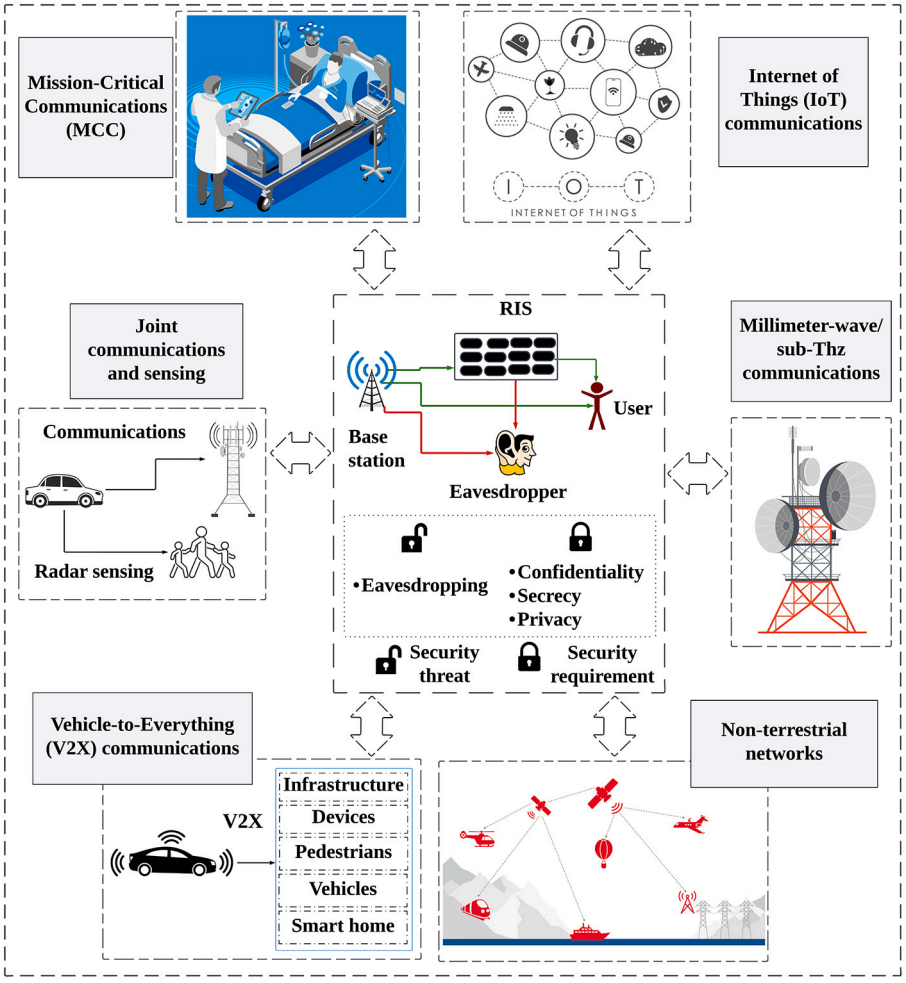

Fig. 4. Illustration of 6G wireless paradigm where RIS-PLS can play a crucial role.

of the signal for the receiver can yield significant security improvements.

In terms of secure transmission, RIS systems offer compelling advantages [25,26]. As illustrated in Fig. 4, PLS designs based on RIS can be integrated into key 6G technologies, such as mission-critical communications, non-terrestrial networks, vehicle-to-everything, joint communications and sensing, mmWave/sub-THz communications, and Internet of Things communications. However, research on RIS-aided PLS solutions within 6G networks remains in its infancy [27]. Further investigation is essential to understand the strengths and limitations of solutions across diverse network topologies and application scenarios, focusing on their implementation efficacy, inherent complexity, and control variables. Based on this, we present RIS-enhanced PLS designs in terms of resource allocation, beamforming, antenna/node selection, AN generation, and cooperative methods.

4.1. Resource allocation in RIS-enabled PLS

Secure resource allocation involves the use of network resources, including frequency bandwidths, time slots, and power levels, to ensure secure transmission [28]. PLS provisioning can be achieved by using subcarrier allocation, adaptive power allocation, or a combined approach of subcarrier and power allocation. By adapting the link between the transmitter and receiver via RIS by adjusting transmission parameters, a secure communication link can be established. RIS can direct signals to the receiver and/or degrade the eavesdropper's Signal to Noise Ratio (SNR). In particular, RIS-based link adaptation and channel-dependent resource allocation can be designed to provide flexible and scenario-specific secure transmission. In this context, parameter adjustments based on channel characteristics include the transmit power, number of RIS elements, reflection coefficients, subcarriers, and channel bandwidth [29].

4.2. Beamforming in RIS-enabled PLS

The spatial DoF offered by multiple antennas in MIMO systems enhances both the reliability and security of data transmission. Utilizing beamforming and precoding techniques, spatially focused signals can be strategically transmitted to realize diversity and array gains. Specifically, beamforming applies to rank-one transmission, where a single data stream is transmitted via a multi-antenna array. Conversely, precoding involves multi-rank transmission, signifying the concurrent transmission of multiple data streams [30,31]. A robust security strategy entails the mathematical optimization of beamforming and precoding vectors to fulfill predefined PLS design criteria.

The passive beamforming capabilities of RIS can synergistically complement the active beamforming techniques employed by the transmitter to enhance PLS performance metrics. For instance, through the joint optimization of the transmit beamforming vectors and the phase shift design of RIS elements, it is possible to strategically degrade the eavesdropping channel relative to a legitimate channel, while concurrently enhancing the decoding signal strength at the receiver. Secure transmission efficiency can be improved by increasing the number of RIS elements, rather than by enlarging the transmitter's antenna array. Hence, when complemented by RIS deployments, a reduced antenna count at the transmitter will result in significant secrecy gains [32].

Table 2
Comparison of RIS vs. DF and AF relays.

Attributes	RIS	DF relay	AF relay
Hardware cost	Low	High	Intermediate
Duplex	Full	Half	Full/Half
Power consumption	Low	High	Intermediate
Noise amplification	No	No	Yes
Complicated signal processing	No	Yes	No
RF chain	No	Yes	Yes

Enhanced secure beamforming via RIS integration can improve PLS in various setups, such as multiple data streams, multiple users, or wide frequency bands. The optimal approach, however, is determined by the rank of the transmitted data and the level of security requirements.

4.3. Antenna/node selection in RIS-enabled PLS

The selection of antennas or nodes in MIMO systems plays a critical role in optimizing system performance, including aspects such as spectral efficiency and SNR [33,34]. With RIS-enabled PLS, antenna/node selection can provide a complementary advantage. Specifically, while RIS elements manipulate the wireless propagation environment to secure the channel against eavesdroppers, an optimized antenna/node selection in the MIMO system can further enhance this security paradigm by adaptively choosing the best set of antennas and nodes to transmit. Combining these strategies allows for the sophisticated manipulation of channel states between receivers and eavesdroppers. Therefore, the combination creates a multi-layered security approach that not only meets predefined PLS design criteria but also optimizes the tradeoff between security and system performance. Thus, integrating antenna/node selection with RIS-enabled PLS is essential to achieve a comprehensive and robust secure communication system.

4.4. AN generation in RIS-enabled PLS

AN can be generated by either the transmitter or the receiver to mitigate eavesdropping attacks [35]. Specifically, the transmitter can send AN within the same frequency band as the legitimate signal by leveraging the null space in the channel. Alternatively, the receiver can generate AN via in-band full-duplex communications. RIS serves as a promising countermeasure by reflecting AN, thereby intensifying interference experienced by eavesdroppers. An RIS-aided AN design can achieve an equivalent secrecy level with fewer elements and reduced computational complexity compared to a design without AN [36]. However, AN methods are power-intensive, requiring a delicate balance of transmit power for both secure and reliable communications. By utilizing RIS, power constraints may be alleviated while maintaining higher communication performance. Optimizing RIS-based AN generally involves selecting optimal AN power using real-time Channel State Information (CSI) and determining the phase shifts for RIS.

4.5. Cooperative relaying and jamming in RIS-enabled PLS

Spatial diversity in cooperative relaying and jamming enhances efficient security measures. In cooperative relaying, trusted relays provide the diversity benefits of MIMO to improve PLS. As outlined in Table 2, Amplify-and-Forward (AF) and Decode-and-Forward (DF) are commonly employed relaying protocols. Cooperative jamming strategically employs relays to send disruptive signals to interfere with eavesdroppers' interceptions [37]. Nevertheless, cooperative relaying raises unresolved challenges, such as relay selection, reliability, power management, positioning, and computational burden. Cooperative jamming challenges include incentive policy, power allocation under imperfect CSI, and jamming signal design against multiple eavesdroppers [38].

Distinct from cooperative relaying and jamming approaches, an RIS-enabled architecture boasts enhanced spectral and energy efficiencies, facilitated by full-duplex operations. Moreover, RIS passive attributes obviate the need for additional phase or interference cancellation techniques, resulting in a significant advancement over conventional cooperative approaches. In the domain of PLS enhancement methodologies, RIS can also operate in an integrated manner with cooperative relaying and jamming techniques [39]. Specifically, RIS can tailor the propagation environment to improve the SNR at the receiver or degrade it at an eavesdropper, while cooperative relays can forward the intended signals over multiple paths, adding an extra layer of security through spatial diversity. Alternatively, cooperative jamming can disrupt eavesdropper reception selectively, without compromising legitimate communications. Through leveraging cooperative diversity benefits and RIS reconfigurability, the system can adaptively modify its transmission and jamming strategies to meet the dynamic security requirements of 6G networks.

5. Research issues and potential solutions in RIS-enabled PLS

In this section, we discuss the research issues and potential solutions related to the design and implementation of secure 6G wireless networks using RIS.

5.1. Estimation of channels involving RIS

Research issues: In RIS-enabled frameworks, PLS enhancement depends on the precise reconfiguration of the RIS elements, which requires accurate, timely, and low-complex channel estimation. While the theoretical upper bound of performance can be obtained with the assumption of perfect CSI for both the receiver and eavesdropper, obtaining such perfect CSI presents formidable challenges [40]. The challenges include hardware limitations, non-linear characteristics of RIS elements, lack of information for passive eavesdroppers, and channel estimation errors [41].

Potential solutions: Under varying system architectures and channel conditions, channel estimation problems have been studied in RIS-enhanced secure systems [42]. By employing training signals, low-power receiving RF chains at the RIS can be used to estimate individual channels between the transmitter and the RIS, as well as between the RIS and receiver. Extrapolation-based methods offer enhanced accuracy in spatially sparse channels, especially in mmWave and sub-THz bands, although the development of reliable hardware and channel modeling remains a priority. Using ML and sparsity-aware algorithms can reduce pilot overheads. For example, the transmitter-RIS channel has more unknown coefficients due to the greater number of antennas at the transmitter and can be estimated less frequently than the more dynamic RIS-receiver channel. In setups where RIS lacks receiving RF chains, another method is to estimate the concatenated transmitter-receiver channel via RIS, taking advantage of assumed uniform configurations among nearby reflective elements to minimize computational complexity, but at the expense of degraded estimation accuracy [43]. In future 6G networks, a complex network topology, the dense deployment of multiple RISs, and the unique propagation characteristics of mmWave/sub-THz bands will make real-time estimation of RIS channels challenging.

5.2. Beam configuration in RIS-enabled PLS

Research issues: In RIS-enabled PLS systems, beam configuration is implemented to optimize signal propagation and enhance security [44]. Nevertheless, it presents a number of challenges. Advanced algorithms are necessary for optimizing RIS orientations when dealing with highly directional beams. Coherent signal processing requires synchronization between RIS elements and existing transceivers. Dynamic changes in the environment require quick reconfiguration algorithms and robust channel estimation methods. Finally, beamforming efficacy is constrained by hardware limitations, such as phase quantization errors and spatial correlations [45].

Potential solutions: For adaptive beamforming under time-varying channels, ML algorithms are emerging as viable solutions. Time and phase coordination can be developed with advanced clock synchronization methods. The use of robust optimization techniques is promising for adapting to environmental changes and hybrid channel estimation methods can be developed to improve CSI accuracy. Overall, ML methods, optimization algorithms, and synchronization techniques offer increasingly effective solutions for beam configuration in RIS-enabled PLS systems.

5.3. Resource management in RIS-enabled PLS

Research issues: Future 6G networks may have complex scenarios due to the large-scale and random deployment of RIS, transmitters, receivers, and eavesdroppers with large antenna arrays [46]. In such scenarios, centralized transmission is not recommended due to the high feedback overheads, computational complexity, and energy consumption.

Potential solutions: The development of distributed algorithms is becoming increasingly important in managing complex scenarios. These can be tailored to optimize various network functionalities, such as active beamforming at the transmitter, passive beamforming at the RIS, and relay selection/scheduling in cooperative PLS methods. Due to the massive scale and complexity of future 6G networks, the design, configuration, and operation of distributed architectures will remain a formidable challenge.

5.4. Placement of the RIS for enhanced PLS

Research issues: Despite their shorter coverage range compared to active relays, RISs pose unique PLS challenges for hybrid 6G networks (having both passive RISs and active transmitters). In particular, passive eavesdroppers may exploit spatial correlations or beamforming errors to intercept confidential communications. RIS placement can mitigate this issue by increasing the SNR at the receiver while minimizing the SNR at the eavesdropper [45,46].

Potential solutions: Optimal RIS placement in the context of PLS can be achieved by utilizing optimization algorithms that take into account the geometrical relationship between the RIS, transmitter, receiver, and eavesdropper. When full CSI is available, exhaustive search methods can be used. A heuristic approach can be used for simple configurations (e.g., single-cell scenarios) [47]. ML approaches enable the deployment of RIS in complicated network topologies and the adaptive configuration of RIS elements in real-time, providing the network with greater protection against eavesdropping threats. Due to the complexity involved in estimating CSI involving RISs in future 6G networks, especially in scenarios involving multiple transmitters and RISs, ML approaches are becoming increasingly relevant.

5.5. Passive information transfer for RIS

Research issues: An RIS has information about its control signals (to coordinate with a transceiver), maintenance signals (to ensure correct operation), and feedback signals (to transmit the estimated CSI). To develop an RIS setup for PLS enhancement, this information must be passively transmitted.

Potential solutions: In [48], the authors proposed a joint Passive Beamforming and Information Transfer (PBIT) approach to transmit RIS information without consuming additional resources. However, there has been no investigation of the inherent tradeoff between passive information transfer and passive beamforming designs for secure transmission in PBIT. Furthermore, PBIT is characterized by stochastic optimization problems that are difficult to resolve.

5.6. Hardware and channel modeling for RIS-enabled PLS

Research issues: The development of unified and physics-compliant hardware models for RIS-enabled PLS constitutes a dynamic research frontier. It involves evaluating RIS functionality across hardware architectures and investigating its interactions with arbitrary EM fields. RIS models must rigorously consider element coupling, impedance matching, hardware imperfections, and scattering properties. Additionally, channel models serve as a bridge between hardware specifications and communication theory, providing mathematical formulations of the complex interaction between wireless signals and radio environments. For large-scale and small-scale channel characteristics, conventional channel models utilize path loss and multi-path fading, respectively. However, 6G ecosystems require rigorously validated channel models that are specifically tailored to RIS-enabled PLS.

Potential solutions: Phase shift, load impedance, and generalized sheet transition condition models can characterize RIS reconfigurability and define RIS-EM field boundary conditions. Innovative hardware designs and manufacturing solutions are essential to increase the scalability and cost-effectiveness of RISs while maintaining their tunability and real-time control [49]. Both amplitude-phase and phase-only control methods can use quasi-continuous quantization, with a trade-off between implementation complexity and performance. Furthermore, a unified channel modeling framework is imperative for diverse application scenarios, including mMIMO, underwater communications, and satellite networks. Path loss models must incorporate design-specific scaling variables, such as RIS size, element arrangement, and transmission distance. As 6G RIS systems move toward higher frequencies and enlarged apertures, indoor wireless and near-field propagation will become more critical. There is a noticeable absence of empirically and mathematically robust channel models suitable for evaluating physical-layer performance under diverse deployment scenarios, architecture paradigms, and system parameters. Generally, channel models can be categorized into deterministic and stochastic types. Mathematical approximations are also necessary for complicated fading distributions.

5.7. Optimization for RIS-enabled PLS

Research issues: Due to the multiple and coupled variables (related to transmit beamforming, passive beamforming, and relays/jammers in cooperative scenarios), RIS-aided PLS designs present an intricate mathematical challenge. Joint optimization of these variables is typically intractable. Additionally, non-convex constraints, such as the source power constraint, unit-modulus constraint, and discrete phase adjustment constraint, complicate the optimization process. Security is generally improved by large-scale RISs. However, it increases the dimensions of phase-shift matrices, adding a computational burden. Multi-user and multi-element RIS configurations require a large channel space, which makes fading channel conditions difficult to describe mathematically. In addition, 6G systems have complex topologies and nonlinear components. Thus, advanced optimization techniques are required to design algorithms that manage non-convexity with minimal signaling overheads [50,51].

Potential solutions: RIS-enabled 6G systems present a diverse and complex optimization landscape, rendering traditional convex methods like linear programming or dynamic programming ineffective. To address high-dimensional or multi-objective optimization problems, robust strategies are needed. Hardware limitations and channel imperfections such as the phase-dependent amplitude of RIS, transceiver distortion, and CSI error can be ignored for simplification. Through relaxation techniques, intractable non-convex problems can be approximated analytically. Using iterative or heuristic algorithms, non-convex objectives can be approximated more accurately into convex ones.

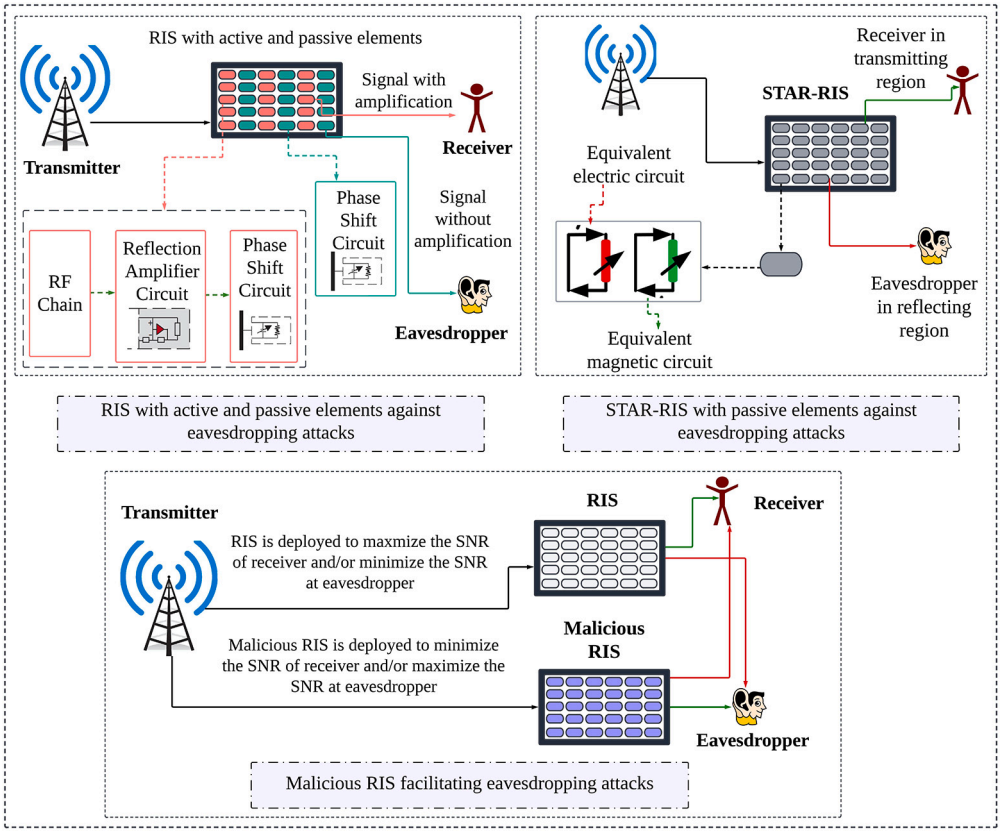

Fig. 5. Active RIS, STAR-RIS, and malicious RIS in the context of RIS-enabled PLS.

6. Future perspectives and research avenues for RIS-enabled PLS

This section outlines future research avenues, focusing on ML-based solutions, advanced RIS types, and malicious RISs. These topics are clarified in the context of RIS-enabled PLS illustrated in Fig. 5.

6.1. ML-based solutions

Analytical approaches in RIS-aided PLS often employ complex mathematical models that are limited in applicability and adaptability due to their rigid assumptions. Conventional methods often fail in cases involving variable RIS configurations, dynamic channel states, and adversarial user behaviors. RIS configurations can be optimized for security through ML algorithms, particularly DL and Deep Reinforcement Learning (DRL) [52]. These algorithms learn network environments and dynamically adapt RIS settings to create secure communication links. This makes eavesdropping significantly more challenging because it introduces high dimensionality and randomness into the channel response. DL- and DRL-based approaches offer robust solutions to various aspects of RIS-PLS in 6G systems, including transmitter-side beamforming, receiver-side optimization, and RIS-side passive beamforming. With DL, channel estimation and tracking are improved regardless of imperfect conditions by leveraging model-free mappings and learnable parameters. DRL has the advantage of large search spaces and the ability to optimize multi-objective problems, such as coverage and secrecy. However, RIS-aided secure 6G systems have expansive channel spaces, which impose computational demands on DRL algorithms. Therefore, further research is necessary to create learning algorithms that reduce computational overheads, ensure real-time adaptability, and maintain accuracy and stability. In this context, the future direction may lie in a holistic approach to RIS-enabled PLS in 6G networks, necessitating the co-design of ML algorithms and cryptographic measures.

6.2. Advances in RIS hardware

Active RIS: To mitigate double-fading attenuation, active RIS was proposed [53]. Unlike passive RISs, active RISs reflect incident signals with adjustable phase shifts as well as amplify them. In active RISs, phase shift circuits and reflection-type amplifiers are embedded in the architecture to convert multiplicative channel loss into an additive form and augment it with an amplification gain. It is possible to achieve optimal system performance through the combination of active and passive RIS elements, although power consumption must be considered. Active RISs have lower hardware overheads than traditional relays, which require components such as digital-to-analog converters, mixers, and power amplifiers. Under equivalent conditions, active RISs offer better performance-to-overhead ratios since they use only power amplifiers and diodes. While RIS-aided secure communications have been studied, the impacts of the deployment and use of active RISs on the secrecy rate are unknown. Hence, future work should address these challenges and investigate the efficiency and cost-effectiveness of active RISs.

STAR-RIS: The transmitter and receiver must be on the same side of a reflecting-only RIS system, limiting receiver coverage behind the RIS. STAR-RISs can provide additional DoF by modifying signals simultaneously in full space [54]. In [55], STAR-RIS is categorized as a special case of beyond diagonal RIS [55]. STAR-RISs support both transmission and reflection functionalities. In its hardware design, STAR-RIS uses electric and magnetic currents to generate simultaneous or sequential transmission and reflection signals. To enable independent or coupled communications, STAR-RIS uses 3 operating protocols, namely energy splitting, mode selection, and time splitting. Adapting RIS-based PLS strategies to a STAR-RIS-based framework remains challenging. This is primarily due to the performance analysis incorporating newly introduced tunable parameters for both transmission and reflection links, hardware tuning mechanisms for transmission and reflection elements, and comprehensive channel modeling in full space. In particular, de-

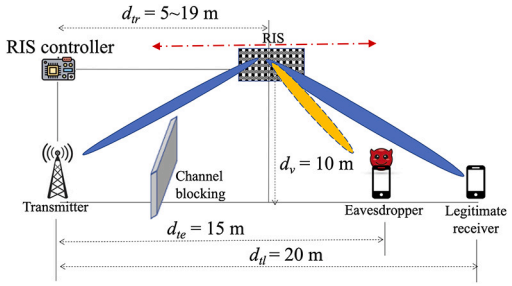

Fig. 6. Network topology for simulations.

ployment strategies for STAR-RIS and multi-user beamforming should be further investigated. It is essential to select an optimal STAR-RIS protocol that balances complexity and performance. Furthermore, intrinsic theoretical constraints, such as coupled phase and unit modulus constraints complicate PLS optimization. To address these issues, it is necessary to design ML algorithms and optimal convex algorithms that can handle hybrid control schemes incorporating both continuous and discrete variables.

6.3. Malicious RISs

Legitimate and malicious RISs can coexist in the emerging 6G landscape. By maximizing information leakage, malicious RISs compromise security, increasing the eavesdropper's SNR rather than the receiver's. PLS challenges are complicated by illicit data transmission and pilot contamination. Due to the malicious RIS's passive nature and lack of CSI, legitimate RISs cannot nullify their signal impacts, reducing the accuracy of channel estimation for legitimate links and undermining pilot-based CSI techniques. Therefore, existing optimization strategies based on instantaneous CSI become outdated and ineffective [56]. In the presence of malicious RISs, comprehensive analyses, and countermeasures are needed for secure RIS-aided 6G networks. In future research, optimization frameworks can be developed to counter eavesdropping even without perfect CSI. Furthermore, empirical case studies and performance evaluations are essential to validate PLS solutions against malicious RISs.

7. Numerical results

In this section, simulation results are presented to demonstrate the effectiveness of RISs in terms of PLS, particularly through the enhancement of the secrecy rate which is one of the critical and widely used measures of secure communication performance. We examine the effects of a practical RIS model, number of RIS elements, RIS beam design strategy, placement of RIS, quantized RIS phases, and AN generation on the secrecy rate under the network topology depicted in Fig. 6. Because the focus of simulations is to examine the secrecy rate improvement owing to RISs, a single-antenna scenario is considered as in [57]. To facilitate communications between the transmitter and receiver, an RIS with N reflecting elements is deployed between them; its location may vary in the horizontal direction. Depending on the distance, the path loss model can be expressed as follows:

$$L(d) = C_o \left(\frac{d}{d_o}\right)^{-\gamma} \tag{3}$$

where C_o represents the path loss at reference distance d_o, d is the distance between the transmitter and the destination of a given link, and γ is the path loss exponent. It is assumed that all the channel links follow a Rayleigh distribution [58]. In the simulation setup, we set C_o = -30 dB, d_o = 1 m, and γ = 3.0 or 3.5. There is a noise variance of -100 dBm on the receiving end and a transmit power of 20 dBm on the transmitting end.

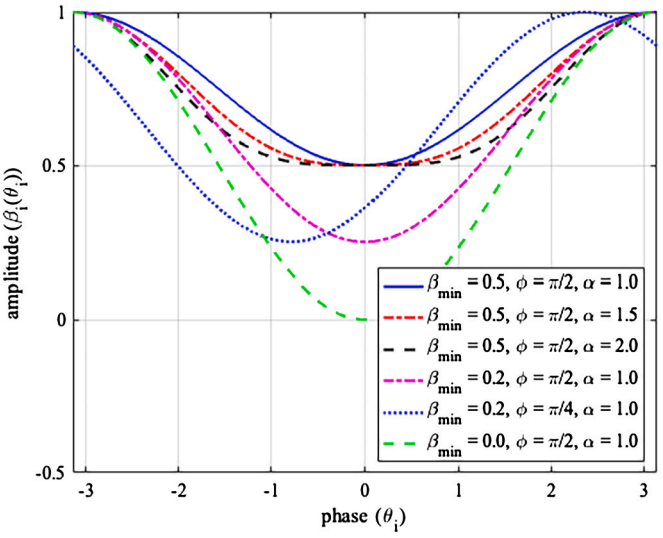

Fig. 7. Practical RIS model with different parameters: β_{min}, ϕ, and α.

In an ideal RIS phase model, the amplitude is constant regardless of the phase, i.e., $\psi_i = e^{j\theta_i}$ for $i \in \{1, \cdots, N\}$. However, practical implementation and measurement results indicate that the amplitude of the RIS reflection coefficient varies with its phase. Specifically, the amplitude of the reflection coefficient of an RIS, $|\psi_i| = \beta_i(\theta_i)$, is a function of θ as follows [59].

$$\begin{aligned}\psi_i &= \beta_i(\theta_i)e^{j\theta_i} \\ &= \left[(1-\beta_{min})\left(\frac{\sin(\theta_i-\phi)+1}{2}\right)^{\alpha} + \beta_{min}\right] e^{j\theta_i}\end{aligned} \tag{4}$$

where β_{min} is the amplitude level with maximal attenuation, that is, the minimum amplitude, ϕ is the phase difference between the phases at β_{min} and $-\frac{\pi}{2}$, and α is the rate of amplitude attenuation. Fig. 7 illustrates several typical examples of phase-dependent amplitude responses. When $\beta_{min} = 1$ or $\alpha = 0$, the amplitude becomes 1, regardless of θ_i, i.e., $\beta_i(\theta_i) = 1$. Consequently, the phase-dependent amplitude model is transformed into an ideal RIS model. As the amplitude of an RIS is attenuated, that is, $\beta_i(\theta_i) \leq 1$, the quality of the RIS-reflected signal deteriorates.

The received signal at the receiver and eavesdropper can be derived [60],

$$y_l = \sum_{i=1}^{N} h_i e^{j\theta_i} g_i s + z_l \tag{5}$$

$$y_e = \sum_{i=1}^{N} h_i e^{j\theta_i} k_i s + z_e \tag{6}$$

where h_i is a channel gain between the transmitter and the ith RIS element, and g_i and k_i are channel coefficients from the ith RIS element to the receiver and eavesdropper, respectively. z_l and z_e are additive white Gaussian noise with a variance σ^2 at the receiver and eavesdropper, respectively. As a measure of secrecy performance, the achievable secrecy rate can be expressed as follows:

$$\begin{aligned}C_s = \max\Bigg\{&\log_2\left(1+\frac{\left\|\sum_{i=1}^{N} h_i g_i e^{j\theta_i}\right\|^2}{\sigma^2}\right) \\ &-\log_2\left(1+\frac{\left|\sum_{i=1}^{N} h_i k_i e^{j\theta_i}\right|^2}{\sigma^2}\right), 0\Bigg\}\end{aligned} \tag{7}$$

Assuming that the transmitter has the channel information from the transmitter to the receiver via RIS, i.e., h_i and g_i for all $i \in \{1, \cdots, N\}$, but no information on the eavesdropping link, the optimal phase to maximize the capacity of the legitimate link and the secrecy rate is given by

$$\theta_i = -\arg(h_i g_i) \tag{8}$$

Consequently, all the RIS signals at the receiver have the same phase, and the received signal power is maximized. In this scenario, the eavesdropper is assumed to be an out-of-network malicious device.

On the other hand, if the channel information on the eavesdropping link is available, the transmitter can take a pre-nulling policy to eliminate the transmit signal leakage to the eavesdropper and the whole information can be securely sent to the receiver. In this case, the transmitter is a BS, and the receiver and eavesdropper are User Equipments (UEs). The BS sends downlink data to UEs in a Time Division Multiple Access (TDMA) manner. The receiver is the UE served in the current time slot while the eavesdropper was served in the previous time slot. The eavesdropper tries to overhear the UE in the current time slot, which is called an in-network eavesdropper. When the channel information of the eavesdropping link is perfectly known at the transmitter, the RIS coefficient design for pre-nulling can be expressed as

$$\boldsymbol{\xi}^T \boldsymbol{\psi} = 0 \tag{9}$$

where $\boldsymbol{\xi} = [h_1 k_1, h_2 k_2, \cdots, h_N k_N]^T$. If both the amplitude and phase are controllable, the solution to (9) is a vector in the null space of $\boldsymbol{\xi}^T$. When the elements of $\boldsymbol{\psi}$ have a unit amplitude, the solution to (9) cannot obtained simply. An iterative algorithm in which an orthogonal projection and normalization processes are alternatively repeated can be used to obtain the solution to (9) [61]. In practice, the channel information of the eavesdropping link may be outdated and then the perfect pre-nulling of information leakage cannot be achieved.

As shown in Fig. 6, the transmitter, eavesdropper, and receiver are arranged in a line, and the RIS is located along a parallel line at a vertical distance of d_v (= 10 m). The distance between the transmitter and receiver is d_{tl} (= 20 m), and the distance between the transmitter and eavesdropper is d_{te} (= 15 m). The horizontal distance between the transmitter and RIS is d_{tr}, which can vary from 5 to 19 m. As the eavesdropper is closer to the transmitter than to the receiver, the eavesdropping link has a higher capacity than the legitimate link. Thus, a positive secrecy rate cannot be achieved without the RIS when the eavesdropping channel is not available at the transmitter.

Fig. 8 illustrates the secrecy rate under ideal and non-ideal RIS models with $d_{tr} = 10$ m and $\gamma = 3.0$ depending on the availability of eavesdropping channel information. In the non-ideal RIS model, we set $\beta_{min} = 0.5$, $\phi = \pi/2$, and $\alpha = 2.0$. Because of the obstruction located between the legitimate and eavesdropping links, the direct path from the transmitter is not considered when evaluating the secrecy rate. To reduce the overheads of the control link between the transmitter and RIS, the optimal phases are quantized as follows:

$$\hat{\theta}_i = Q_b(\theta_i) \tag{10}$$

where $Q_b(\cdot)$ denotes the quantization of b bits. For example, $Q_1(\cdot)$ selects the phase closest to $\{\pi/2, -\pi/2\}$.

Fig. 8 shows that the secrecy rate increases with the number of RIS elements, and the 3-bit quantization can accurately represent the performance achieved by the RIS under a given simulation environment. In addition, performance degradation is observed in the non-ideal RIS model. When N is large, the enhancement of the legitimate link quality with the RIS array gain is more effective in terms of the secrecy rate than the pre-nulling of signal leakage in the eavesdropping link. Therefore, the secrecy rates in Fig. 8 (a) are much higher than those in Fig. 8 (b). In this study, a uniform RIS codebook is assumed in both ideal and non-ideal RIS models. By designing the codebook and determining RIS phases under a non-ideal RIS model, the loss of the secrecy rate can be mitigated. However, this issue needs to be addressed in future studies.

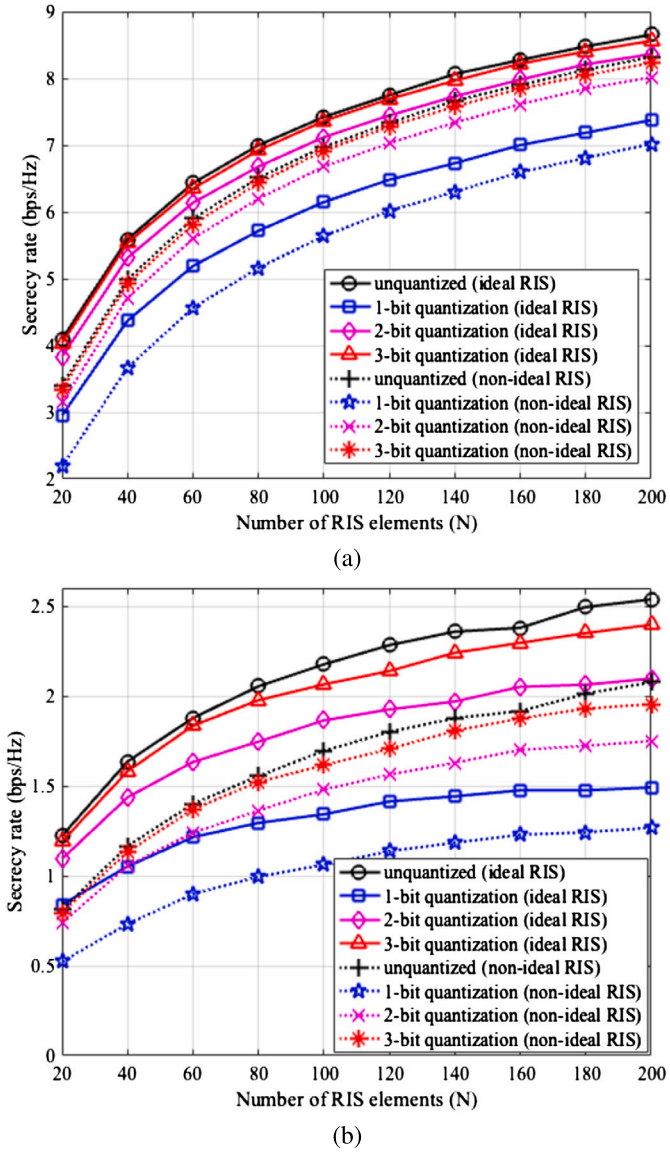

Fig. 8. The secrecy rate versus number of RIS elements (N) with different quantization levels of RIS reflection angles under ideal and non-ideal RIS models: (a) when the channel information of the eavesdropping link is unknown, (b) when the channel information of the eavesdropping link is known at the transmitter.

Fig. 9 shows the secrecy rate with respect to the RIS location, i.e., $d_{tr} \in [5, 19]$ m, depending on the eavesdropping scenario when the path loss exponents (γ) are 3.0 and 3.5. Fig. 9 (a) shows the secrecy rate with the out-of-network eavesdropper and Fig. 9 (b) shows the secrecy rate with the eavesdropping channel information. For this simulation, the number of RIS elements is $N = 50$. When $\gamma = 3$, the secrecy rate increases with d_{tr}. This is because the distance between the receiver and RIS becomes shorter and the quality of the legitimate link becomes better than that of the eavesdropping link. In contrast, when $\gamma = 3.5$, the secrecy rate decreases slightly with d_{tr} because the effect of the link distance is more dominant than that of the RIS array gain. These results suggest that the path loss exponent has a greater impact on the secrecy performance than the location of the eavesdropper. Therefore, the RIS location can be optimized based on channel conditions, such as path loss exponents, to maximize the PLS performance.

Fig. 10 shows the secrecy rate achieved by utilizing AN and the corresponding RIS reflection design strategy. To incorporate AN, it is

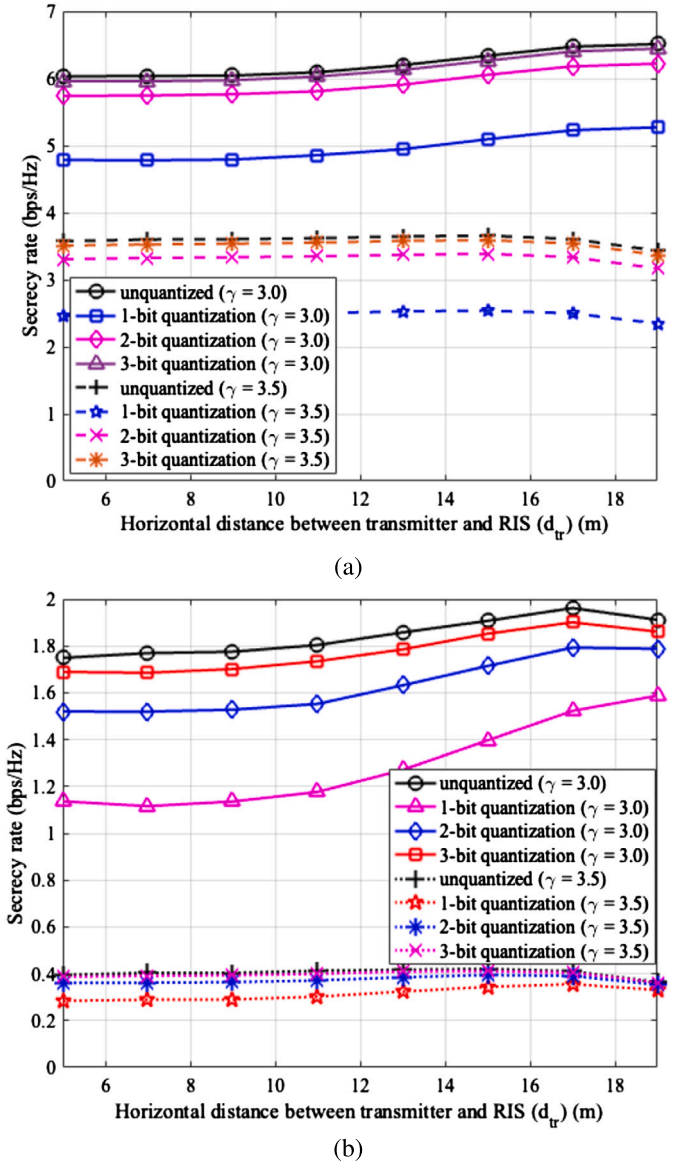

Fig. 9. Secrecy rates versus RIS locations, i.e., the horizontal distance between the transmitter and RIS (d_{tr}), with different quantization levels of RIS reflection angles and path loss exponents $\gamma \in \{3.0, 3.5\}$: (a) when the channel information of the eavesdropping link is unknown, (b) known at the transmitter.

assumed that one more antenna to transmit an AN signal is added to a transmitter. Therefore, an information signal and AN are separately transmitted by two transmit antennas with a power allocation ratio μ. For example, when $\mu = 0.3$ and the total transmit power is 100 mW (i.e., 20 dBm), the transmit power of an information signal is 30 mW and that of an AN signal is 70 mW. The RIS elements are partitioned into two groups with a ratio ρ: the reflection angles of the first group with ρN RIS elements are determined to maximize the AN signal power to the eavesdropper while those of the second group with $(1-\rho)N$ RIS elements are determined to maximize the information signal power to the legitimate receiver [62]

$$\theta_i = \begin{cases} -\arg\{h_i k_i\}, & \text{for } i \in \{1, \cdots, \rho N\} \\ -\arg\{h_i g_i\}, & \text{for } i \in \{\rho N + 1, \cdots, N\} \end{cases} \tag{11}$$

It is noteworthy that different RIS reflection design strategies for information and AN signals can be employed depending on the network condition. Fig. 10 demonstrates the secrecy rate depending on the ratio of RIS elements used for AN reflection with the different power allocation factors for information and AN signals when $\gamma = 3.0$ and $N = 100$. It is shown that the optimal ratio of RIS elements for AN reflection (ρ) maximizing the secrecy rate increases when the power allocation ratio to the information signal (μ) increases. It means that more RIS elements should be used for AN reflection rather than information signal reflection when the higher power is allocated to the information signal to achieve the balance between information and AN signals. Such an optimal ratio under the unquantized RIS phase is also optimal in the quantized RIS phases.

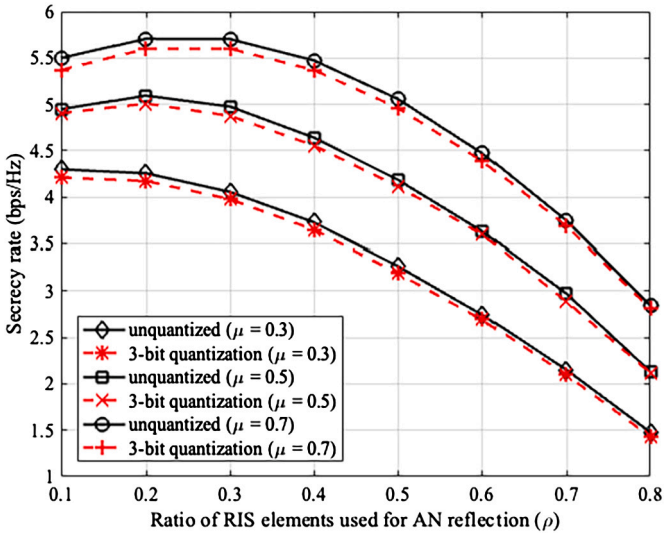

Fig. 10. Secrecy rate versus the ratio of RIS elements used for AN reflection (ρ) with different power allocation factors to information signal $\mu \in \{0.3, 0.5, 0.7\}$ when $\gamma = 3.0$ and $N = 100$.

In this section, we perform various simulations to investigate the impact of ideal/non-ideal RIS models, number of RIS elements, RIS reflection pattern design depending on available CSI, RIS placement, unquantized/quantized RIS reflection phase, and AN power allocation/reflection on the secrecy rate. Based on the results, we can conclude that RISs can provide an effective solution to PLS by optimizing various RIS design parameters in unfavorable channel conditions.

8. Conclusions

In this study, we investigated RIS in the context of PLS, offering valuable insights into secure transmission design in the 6G era. First, we presented a comprehensive discussion of RIS and PLS. We examined RIS-enabled PLS designs, including beamforming, resource allocation, antenna/node selection, AN, and cooperative communications. Furthermore, we clarified key research issues and their prospective solutions in the domain of RIS-enabled PLS, addressing channel estimation, beam configuration, resource management, strategic placement, and passive information transfer for RIS, hardware and channel modeling, and optimization techniques. Additionally, we identified future research avenues highlighting ML-based solutions, advancements in RIS hardware, such as active RIS, and STAR-RIS, and security threats exploited by malicious RIS. Finally, numerical results were presented to demonstrate the effectiveness of RIS in improving PLS. Future research will focus on developing PLS solutions based on active RIS, STAR-RIS, and malicious RIS.

CRediT authorship contribution statement

JungSook Bae: Writing – original draft, Investigation, Conceptualization. **Waqas Khalid:** Writing – original draft, Visualization, Methodology, Investigation, Formal analysis. **Anseok Lee:** Project administration, Investigation, Conceptualization. **Heesoo Lee:** Supervision,

Project administration, Funding acquisition, Conceptualization. **Song Noh:** Writing – review & editing, Supervision, Conceptualization. **Heejung Yu:** Writing – review & editing, Writing – original draft, Supervision, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2020-0-00045, Development of movable high-capacity mobile communication infrastructure for telecommunication disaster and rescue) and by IITP grant funded by the Korea government (MSIT) (No. 2021-0-00972, Development of intelligent wireless access technology).

References

[1] M. Shahjalal, W. Kim, W. Khalid, S. Moon, M. Khan, S. Liu, S. Lim, E. Kim, D.-W. Yun, J. Lee, W.-C. Lee, S.-H. Hwang, D. Kim, J.-W. Lee, H. Yu, Y. Sung, Y.M. Jang, Enabling technologies for AI empowered 6G massive radio access networks, ICT Express 9 (3) (2023) 341–355.

[2] W. Khalid, H. Yu, Security improvement with QoS provisioning using service priority and power allocation for NOMA-IoT networks, IEEE Access 9 (2021) 2169–3536.

[3] C.-X. Wang, J. Huang, H. Wang, X. Gao, X. You, Y. Hao, 6G wireless channel measurements and models: trends and challenges, IEEE Veh. Technol. Mag. 15 (4) (2020) 22–32.

[4] W. Khalid, M. Rehman, T. Chien, Z. Kaleem, H. Lee, H. Yu, Reconfigurable intelligent surface for physical layer security in 6G-IoT: designs, issues, and advances, IEEE Int. Things J. 11 (2) (2024) 3599–3613.

[5] C. Molero, A. Palomares-Caballero, A. Alex-Amor, I. Parellada-Serrano, F. Gamiz, P. Padilla, J.F. Valenzuela-Valdés, Metamaterial-based reconfigurable intelligent surface: 3D meta-atoms controlled by graphene structures, IEEE Commun. Mag. 59 (6) (2021) 42–48.

[6] V.L. Nguyen, P.C. Lin, B.C. Cheng, R.H. Hwang, Y.D. Lin, Security and privacy for 6G: a survey on prospective technologies and challenges, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2384–2428.

[7] W. Xu, J. Zhang, S. Cai, J. Wang, Y. Wu, RIS-assisted MIMO secure communications with Bob's statistical CSI and without Eve's CSI, Digit. Commun. Netw. 9 (3) (2023) 638–644.

[8] A.S.d. Sena, D. Carrillo, F. Fang, P.H.J. Nardelli, D.B. d. Costa, U.S. Dias, Z. Ding, C.B. Papadias, W. Saad, What role do intelligent reflecting surfaces play in multi-antenna non-orthogonal multiple access?, IEEE Wirel. Commun. 27 (5) (2020) 24–31.

[9] W. Khalid, H. Yu, J. Cho, Z. Kaleem, S. Ahmad, Rate-energy tradeoff analysis in RIS-SWIPT systems with hardware impairments and phase-based amplitude response, IEEE Access 10 (2022) 31821–31835.

[10] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M.D. Renzo, N. Al-Dhahir, Reconfigurable intelligent surfaces: principles and opportunities, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1546–1577.

[11] C. Pan, H. Ren, K. Wang, J.F. Kolb, M. Elkashlan, M. Chen, M.D. Renzo, Y. Hao, J. Wang, A.L. Swindlehurst, X. You, L. Hanzo, Reconfigurable intelligent surfaces for 6G systems: principles, applications, and research directions, IEEE Commun. Mag. 59 (6) (2021) 14–20.

[12] ITU-R WP 5D, Framework and overall objectives of the future development of IMT for 2030 and beyond, Tech. Rep., International Telecommunication Union Radiocommunication Sector (ITU-R), Jun. 2023.

[13] ETSI, Reconfigurable intelligent surfaces (RIS); use cases, deployment scenarios and requirements, Tech. Rep. GR RIS-001, European Telecommunications Standards Institute (ETSI), Apr. 2023.

[14] ETSI, Reconfigurable intelligent surfaces (RIS); technological challenges, architecture and impact on standardization, Tech. Rep. GR RIS-002, European Telecommunications Standards Institute (ETSI), Aug. 2023.

[15] ETSI, Reconfigurable intelligent surfaces (RIS); communication models, channel models, channel estimation and evaluation methodology, Tech. Rep. GR RIS-003, European Telecommunications Standards Institute (ETSI), Jun. 2023.

[16] 3GPP, Study on NR network-controlled repeaters, Tech. Rep. TR 38.867, 3rd Generation Partnership Project, Oct. 2022.

[17] R.A. Ayoubi, M. Mizmizi, D. Tagliaferri, D.D. Donno, U. Spagnolini, Network-controlled repeaters vs. reconfigurable intelligent surfaces for 6G mmW coverage extension: a simulative comparison, in: Proceedings of the 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), 2023, pp. 196–202.

[18] N. Li, J. Zhu, P. Li, B. Wang, X. She, P. Chen, Considerations on potential standardization work for reconfigurable intelligent surface, in: Proceedings of the 2022 IEEE 8th International Conference on Computer and Communications (ICCC), 2022, pp. 320–324.

[19] IEEE, Emerging technology initiative of RIS, IEEE Communication Society, https://riseti.committees.comsoc.org.

[20] D. Kitayama, Y. Hama, K. Miyachi, K. Kishiyama, Research of transparent RIS technology toward 5G evolution & 6G, NTT Tech. Rev. 19 (11) (2021) 26–34.

[21] D. Fang, Y. Qian, 5G wireless security and privacy: architecture and flexible mechanisms, IEEE Veh. Technol. Mag. 15 (2) (2020) 58–64.

[22] H. Yu, J. Joung, Secure IoT communications using HARQ-based beamforming for MISOSE channels, IEEE Int. Things J. 8 (23) (2021) 17211–17226.

[23] M. Rice, B. Clark, D. Flanary, B. Jensen, N. Nelson, K. Norman, E. Perrins, W.K. Harrison, Physical-layer security for vehicle-to-everything networks: increasing security while maintaining reliable communications, IEEE Veh. Technol. Mag. 15 (3) (2020) 68–76.

[24] R. Khan, P. Kumar, D.N.K. Jayakody, M. Liyanage, A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions, IEEE Commun. Surv. Tutor. 22 (1) (2020) 196–248.

[25] H. Shen, W. Xu, S. Gong, Z. He, C. Zhao, Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications, IEEE Commun. Lett. 23 (9) (2019) 1488–1492.

[26] L. Dong, H.-M. Wang, Secure MIMO transmission via intelligent reflecting surface, IEEE Wirel. Commun. Lett. 9 (6) (2020) 787–790.

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

[28] W. Khalid, H. Yu, S. Noh, Residual energy analysis in cognitive radios with energy harvesting UAV under reliability and secrecy constraints, Sensors 20 (10) (2020) 2998.

[29] W. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, P.H. Ho, Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions, IEEE Syst. J. 17 (1) (2023) 848–859.

[30] W. Khalid, H. Yu, R. Ali, R. Ullah, Advanced physical-layer technologies for beyond 5G wireless communication networks, Sensors 21 (9) (2021) 3197.

[31] H. Yu, T. Kim, H. Jafarkhani, Wireless secure communication with beamforming and jamming in time-varying wiretap channels, IEEE Trans. Inf. Forensics Secur. 13 (8) (2018) 2087–2100.

[32] M. Dajer, Z. Ma, L. Piazzi, P. Narayan, X.-F. Qi, B. Sheen, J. Yang, G. Yue, Reconfigurable intelligent surface: design the channel – a new opportunity for future wireless networks, Digit. Commun. Netw. 8 (2) (2022) 87–104.

[33] H.B. Chikha, A. Almadhor, W. Khalid, Machine learning for 5G MIMO modulation detection, Sensors 21 (5) (2021) 1556.

[34] P. Gu, C. Hua, W. Xu, R. Khatoun, Y. Wu, A. Serhrouchni, Control channel anti-jamming in vehicular networks via cooperative relay beamforming, IEEE Int. Things J. 7 (6) (2020) 5064–5077.

[35] H. Yu, J. Joung, Design of the power and dimension of artificial noise for secure communication systems, IEEE Trans. Commun. 69 (6) (2021) 4001–4010.

[36] X. Guan, Q. Wu, R. Zhang, Intelligent reflecting surface assisted secrecy communication: is artificial noise helpful or not?, IEEE Wirel. Commun. Lett. 9 (6) (2020) 778–782.

[37] Z. Abdullah, G. Chen, M.A.M. Abdullah, J.A. Chambers, Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming, IEEE Trans. Inf. Forensics Secur. 16 (2021) 161–172.

[38] F. Jameel, S. Wyne, G. Kaddoum, T.Q. Duong, A comprehensive survey on cooperative relaying and jamming strategies for physical layer security, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2734–2771.

[39] W. Khalid, M. Shahjalal, H. Yu, Outage performance analysis of hybrid relay-reconfigurable intelligent surface networks, in: Proceedings of the 2022 27th Asia Pacific Conference on Communications (APCC), 2022, pp. 253–254.

[40] H. Yu, T. Kim, Training and data structures for AN-aided secure communication, IEEE Syst. J. 13 (3) (2019) 2869–2872.

[41] H. Yu, I.-G. Lee, Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay, Future Gener. Comput. Syst. 102 (2020) 611–618.

[42] S. Noh, K. Seo, Y. Sung, J.D. Love, J. Lee, H. Yu, Joint direct and indirect channel estimation for RIS-assisted millimeter-wave systems based on array signal processing, IEEE Trans. Wirel. Commun. 22 (11) (2023) 8378–8391.

[43] S. Noh, J. Lee, H. Yu, J. Song, Design of channel estimation for hybrid beamforming millimeter-wave systems in the presence of beam squint, IEEE Syst. J. 16 (2) (2022) 2834–2843.

[44] M. Misbah, Z. Kaleem, W. Khalid, C. Yuen, A. Jamalipour, Phase and 3D placement optimization for rate enhancement in RIS-assisted UAV networks, IEEE Wirel. Commun. Lett. 12 (7) (2023) 1135–1138.

[45] W. Khalid, M.A. Rehman, T.V. Chien, H. Yu, Simultaneously transmitting and reflecting-reconfigurable intelligent surfaces with hardware impairment and phase error, in: Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2023, pp. 654–656.

[46] Q. Wu, R. Zhang, Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network, IEEE Commun. Mag. 58 (1) (2020) 106–112.

[47] Z. Kaleem, W. Khalid, A.A. Muqaibel, A. Nasir, C. Yuen, G.K. Karagiannidis, Learning-aided UAV 3D placement and power allocation for sum-capacity enhancement under varying altitudes, IEEE Commun. Lett. 26 (7) (2022) 1633–1637.
[48] W. Yan, X. Yuan, X. Kuai, Passive beamforming and information transfer via large intelligent surface, IEEE Wirel. Commun. Lett. 9 (4) (2020) 533–537.
[49] C. Huang, S. Hu, G.C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M.D. Renzo, M. Debbah, Holographic MIMO surfaces for 6G wireless networks: opportunities, challenges, and trends, IEEE Wirel. Commun. 27 (5) (2020) 118–125.
[50] W. Khalid, H. Yu, Optimal sensing performance for cooperative and non-cooperative cognitive radio networks, Int. J. Distrib. Sens. Netw. 13 (11) (2017) 1–16.
[51] C.B. Le, D.T. Do, A. Silva, W.U. Khan, W. Khalid, H. Yu, N.D. Nguyen, Joint design of improved spectrum and energy efficiency with backscatter NOMA for IoT, IEEE Access 10 (2021) 7504–7519.
[52] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, Q. Wu, Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications, IEEE Trans. Wirel. Commun. 20 (1) (2021) 375–388.
[53] S. Zhang, H. Gao, Y. Su, J. Cheng, M. Jo, Intelligent mixed reflecting/relaying surface-aided secure wireless communications, IEEE Trans. Veh. Technol. 73 (1) (2023) 532–543.
[54] W. Khalid, Z. Kaleem, R. Ullah, T.V. Chien, S. Noh, H. Yu, Simultaneous transmitting and reflecting-reconfigurable intelligent surface in 6G: design guidelines and future perspectives, IEEE Netw. (Early Access) (2022) 1–9, https://doi.org/10.1109/MNET.129.2200389.
[55] H. Li, S. Shen, B. Clerckx, Beyond diagonal reconfigurable intelligent surfaces: from transmitting and reflecting modes to single-, group-, and fully-connected architectures, IEEE Trans. Wirel. Commun. 22 (4) (2023) 2311–2324.
[56] Y. Wang, H. Lu, D.Z. Zhao, Y. Deng, A. Nallanathan, Wireless communication in the presence of illegal reconfigurable intelligent surface: signal leakage and interference attack, IEEE Wirel. Commun. 29 (3) (2022) 131–138.
[57] W. Khalid, H. Yu, Spatial-temporal sensing and utilization in full duplex spectrum-heterogeneous cognitive radio networks for the Internet of things, Sensors 19 (6) (2019) 1441.
[58] W. Khalid, H. Yu, Sum utilization of spectrum with spectrum handoff and imperfect sensing in interweave multi-channel cognitive radio networks, Sustainability 10 (6) (2018) 1764.
[59] Y. Zhang, J. Zhang, M.D. Renzo, H. Xiao, Performance analysis of RIS-aided systems with practical phase shift and amplitude response, IEEE Trans. Veh. Technol. 70 (5) (2021) 4501–4511.
[60] Z. Kaleem, M.A. Ali, I. Ahmad, W. Khalid, A. Alkhayyat, A. Jamalipour, Artificial intelligence-driven real-time automatic modulation classification scheme for next-generation cellular networks, IEEE Access 9 (2021) 155584–155597.
[61] T. Jiang, W. Yu, Interference nulling using reconfigurable intelligent surface, IEEE J. Sel. Areas Commun. 40 (5) (2022) 1392–1406.
[62] S. Arzykulov, A. Celik, G. Nauryzbayev, A.M. Eltawil, Artificial noise and RIS-aided physical layer security: optimal RIS partitioning and power control, IEEE Wirel. Commun. Lett. 12 (6) (2023) 992–996.