Received 27 August 2020; accepted 9 September 2020. Date of publication 16 September 2020; date of current version 9 October 2020.

Digital Object Identifier 10.1109/OJCOMS.2020.3023731

Smart and Secure Wireless Communications via Reflecting Intelligent Surfaces: A Short Survey

ABDULLATEEF ALMOHAMAD [1] (Member, IEEE), ANAS M. TAHIR[1] (Student Member, IEEE), AYMAN AL-KABABJI[1] (Student Member, IEEE), HAJI M. FURQAN[2], TAMER KHATTAB [1] (Senior Member, IEEE), MAZEN O. HASNA [1] (Senior Member, IEEE), AND HÜSEYIN ARSLAN[2,3] (Fellow, IEEE)

[1]Department of Electrical Engineering, Qatar University, Doha, Qatar

[2]Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey

[3]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA

CORRESPONDING AUTHOR: A. ALMOHAMAD (e-mail: abdullateef@ieee.org)

This publication was made possible by the grants NPRP12S-0225-190152 and GSRA6-2-0521-19034 from the Qatar National Research Fund (a member of The Qatar Foundation) and the publication of this article was funded by the Qatar National Library. The statements made herein are solely the responsibility of the author[s].

ABSTRACT With the emergence of the Internet of Things (IoT) technology, wireless connectivity should be more ubiquitous than ever. In fact, the availability of wireless connection everywhere comes with security threats that, unfortunately, cannot be handled by conventional cryptographic solutions alone, especially in heterogeneous and decentralized future wireless networks. In general, physical layer security (PLS) helps in bridging this gap by taking advantage of the fading propagation channel. Moreover, the adoption of reconfigurable intelligent surfaces (RIS) in wireless networks makes the PLS techniques more efficient by involving the channel into the design loop. In this article, we conduct a comprehensive literature review on the RIS-assisted PLS for future wireless communications. We start by introducing the basic concepts of RISs and their different applications in wireless communication networks and the most common PLS performance metrics. Then, we focus on the review and classification of RIS-assisted PLS applications, exhibiting multiple scenarios, system models, objectives, and methodologies. In fact, most of the works in this field formulate an optimization problem to maximize the secrecy rate (SR) or secrecy capacity (SC) at a legitimate user by jointly optimizing the beamformer at the transmitter and the RIS's coefficients, while the differences are in the adopted methodology to optimally/sub-optimally approach the solution. We finalize this survey by presenting some insightful recommendations and suggesting open problems for future research extensions.

INDEX TERMS Physical layer security (PLS), reconfigurable intelligent surface (RIS), secrecy outage probability, secrecy rate.

I. INTRODUCTION

DUE TO the considerable increase in the number of wirelessly communicating devices, different innovative technologies have been proposed in the literature to enhance the energy and spectrum efficiency along with the reliability and security of wireless communication systems. The future applications from 5G wireless communication's perspective include three use cases with diverse requirements such as ultra-reliable low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). The promising physical layer technologies to fulfill the requirements of the above-mentioned applications include cognitive radio (CR), cooperative communication, massive multiple-input multiple-output (ma-MIMO), millimeter-wave, orthogonal frequency division multiplexing (OFDM) numerologies, and so on [1].

The future wireless networks are expected to support highly (energy and spectral) efficient, secure, reliable, and flexible design for emerging applications of 6G and beyond [2]. In order to achieve this goal, rigorous efforts have been undertaken in the research and development of wireless communications. However, overall progress has been relatively slow. This is due to the fact that conventional wireless communication designers have focused only on transmitter and receiver ends while considering the wireless communication environment as an uncontrollable factor. Moreover, it is also presumed that this factor has usually a negative effect on communication efficiency and reliability, and consequently, needs to be compensated.

Recently, reconfigurable intelligent surfaces (RIS) received focused attention due to their significant capability in enabling a smart and controllable wireless propagation environment [3]. Specifically, an RIS is a uniform planar array that consists of low-cost passive reflecting elements. Each element in an RIS can be controlled to smartly adjust the amplitude and/or phase of incoming electromagnetic waves, thus, rendering the direction and strength of the wave highly controllable at the receivers. This feature can be exploited to add different signals constructively/destructively to enhance/weaken their overall strength at different receivers. Thus, RISs can be used to enhance the signal-to-noise ratio (SNR), data rate, security, and/or the coverage probability. In [4], the problem of minimizing the transmit power in the RIS-assisted MISO system under quality of service (QoS) constraints is investigated. Specifically, it is revealed that a squared power gain in terms of the number of reflecting elements can be achieved by applying active and passive beamforming. In addition, RIS-assisted systems offer significantly higher power-efficient alternatives to conventional multi-antenna amplify-and-forward relaying systems [5]. Moreover, the employment of real-time tunable RIS can be used to mitigate and/or eliminate the multipath and Doppler effects caused by the movement of the mobile receiver/transmitter [6].

Motivated by the appealing advantages, RIS-assisted networks have been investigated in many different contexts such as capacity and rate improvement analysis [7], [8], power efficiency optimization [5], [9], communication reliability [10], [11], physical layer security (PLS), and so on. PLS has emerged as a powerful complementary solution for enhancing the security of future wireless communication systems besides cryptographic algorithms. These approaches exploit the dynamic characteristics of the wireless channel such as channel randomness, interference, noise, fading, dispersion, diversity, separability, reciprocity, etc., to ensure secure communication [12], [13]. Due to RIS's capability in enabling a smart controllable wireless propagation, it is a promising solution to enhance the performance of PLS techniques, even for a challenging scenario when PLS techniques are ineffective. More specifically, when the legitimate node and illegitimate node are in the same direction, many PLS techniques including conventional beamforming, directional modulation, artificial noise (AN), etc., cannot fully ensure secure communication. However, this issue can be addressed with the employment of RIS near to legitimate/eavesdropping user along with the proper design of beamforming to enhance/weaken the signal strength at the legitimate/eavesdropping user, thus, significantly enhancing the overall security of the system. In fact, the efficiency of RISs in supporting a wireless communication system in terms of secrecy, for instance, is driven by some practical limitations. Ideally, an RIS can be seen as a continuous surface of reflecting elements (zero-spaced elements) with continuous induced phase shifts and reflection coefficients by each element. However, practically speaking, the controllable reflecting elements can be achieved using mechanical actuation, special materials (e.g., graphene), and electronic devices (e.g., positive-intrinsic-negative (PIN) diodes) [14]. Thus, it has a response switching time, frequency and angle-of-arrival (AoA) dependent response, and inter-element coupling effects. Furthermore, practically, the induced phase shift is nonlinearly coupled with the reflection coefficient [15], hence, optimizing the RIS beamforming/reflection should involve both the phase shifts and the reflection coefficients.

The major advantage of having an RIS in a communication system is the ability to perform passive beamforming, which is done at a middle point in the channel, unlike the traditional active beamforming at the base station (BS) side. This extra degree of freedom has been proved to enhance the system performance in terms of multiple metrics, especially in terms of PLS which is completely dependent on the system's ability to accurately direct the signal beam into a desired path (or exclude it). Moreover, with the aid of an RIS, the coverage area can be, more than ever, tailored as per the network designer requirements. Furthermore, with the passive intelligent reflection, the noise at the reflected signal is not amplified as with the conventional relays.

The adoption of RISs comes with an increased system complexity. For example, in a PLS application, conventionally the active beamforming is optimized to support the system secrecy, while with the presence of an RIS in the loop, joint optimization is required to take advantage of the passive beamforming which is highly dependent on the quality of the acquired CSI. This actually leads to another challenge, which is the acquisition of the CSI itself at the RIS's side, taking into account the high number of the RIS's reflecting elements and their passive nature. Moreover, the channel reciprocity assumption in time-division duplex (TDD) channels, which simplifies the channel estimation process, is no longer valid with the presence of an RIS in the system [14]. Additionally, under the far-field propagation assumption, the communication channel through an RIS suffers from double path loss, known as a product-distance path loss model, which needs to be compensated for either in the link budget or by increasing the number of reflecting elements [14].

An increasing number of recent works have studied RIS-assisted communications from a PLS point of view. In general, there are two main research directions under the PLS concept, namely, information-theoretic secrecy and covert communications. The former focuses on improving

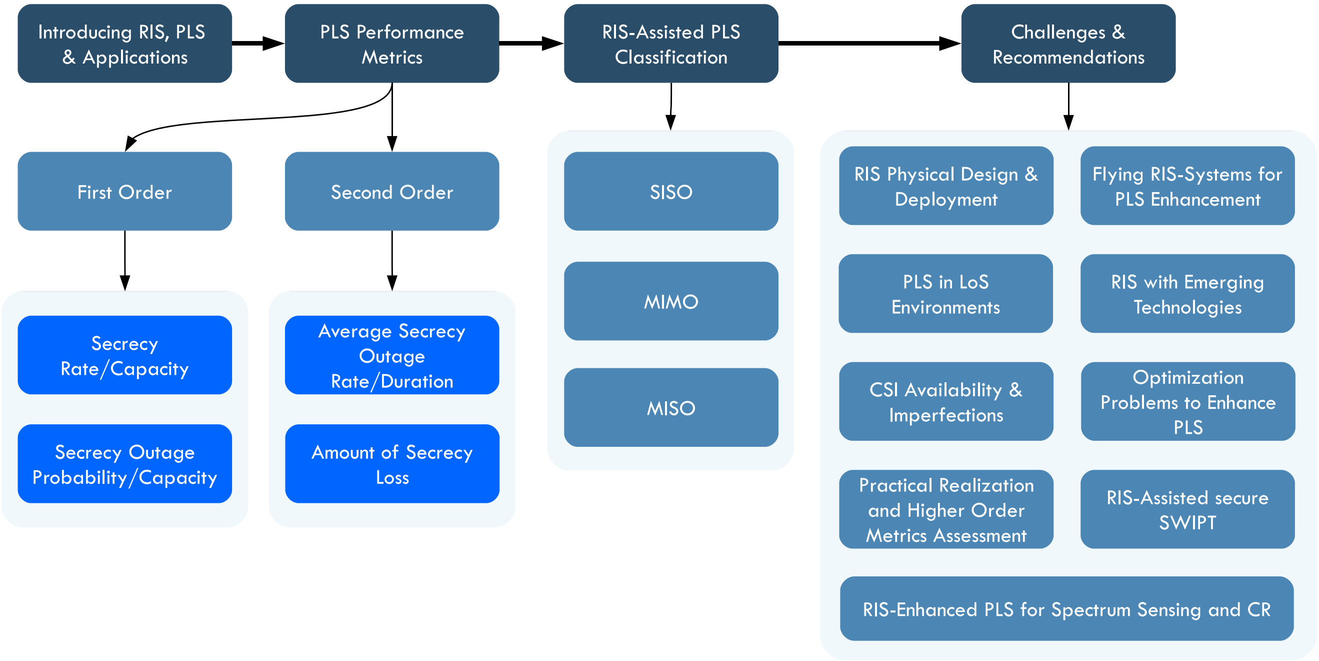

Introducing RIS, PLS & Applications
PLS Performance Metrics
RIS-Assisted PLS Classification
Challenges & Recommendations
First Order
Second Order
Secrecy Rate/Capacity
Secrecy Outage Probability/Capacity
Average Secrecy Outage Rate/Duration
Amount of Secrecy Loss
SISO
MIMO
MISO
RIS Physical Design & Deployment
Flying RIS-Systems for PLS Enhancement
PLS in LoS Environments
RIS with Emerging Technologies
CSI Availability & Imperfections
Optimization Problems to Enhance PLS
Practical Realization and Higher Order Metrics Assessment
RIS-Assisted secure SWIPT
RIS-Enhanced PLS for Spectrum Sensing and CR

FIGURE 1. A diagram to show the structure of the paper.

the secrecy rate (SR) of legitimate users by exploiting the dynamic features of wireless communications, for example, random channel, fading, interference, and noise, etc., to prevent the eavesdropper from decoding leaked data while ensuring that the legitimate user can decode it successfully. The covert communications direction, on the other hand, considers hiding the existence of communication from being detected by an enemy [12], [16]. In this survey, we will focus on the first direction, and for simplicity, it will be referred to as PLS. For more details on PLS in general, we refer the reader to our comprehensive survey in [12].

In this survey, and to the best of our knowledge, all related papers to the RIS-assisted PLS in wireless networks are systematically reviewed. Some common shortcomings in the current literature which lead to open extensions for research are highlighted. The outline and structure of this survey are shown in Fig. 1.

The remainder of this article is organized as follows, the most common secrecy performance metrics are presented in Section II. Then, categorization of the RIS-assisted PLS studies is included in Section III. Recommendations and open research directions are listed in Section IV. Finally, concluding remarks are drawn in Section V.

II. SECRECY PERFORMANCE METRICS

In this section, we present a brief but comprehensive review of the most commonly used metrics for assessing PLS. We include both first and second-order metrics.

A. SECRECY RATE/CAPACITY (SR/SC)

SR is one of the fundamental metrics to measure the secrecy of a communication system. It represents the amount of information in bits per second that can be securely delivered to the receiver over a given channel. Specifically, the achievable SR is the difference between the achievable data rate on the legitimate and the eavesdropper channels, respectively, which is given as

$$R_s = \max\{R_D - R_E, 0\}, \tag{1}$$

where R_D and R_E represent the achievable rates over the legitimate user and the eavesdropper channels, respectively. Practically, positive SR can be achieved by active, at the transmitter, and/or passive, at the RIS, beamforming by degrading the eavesdropper channel while improving the legitimate user one.

Similar to Shannon channel capacity, the SC is defined as the upper bound of the SR [17]. The SC of the Wyner degraded wiretap channel is given as [18]

$$C_s = \sup_{p(X)}\{I(X;Y) - I(X;Z)\}, \tag{2}$$

where $I(\cdot,\cdot)$ represents the mutual information, X and Y represent the input and the output of the legitimate user channel, respectively, Z denotes the output of the eavesdropper channel and $p(X)$ is the input probability distribution. The SC, for a given channel realization, can be written in terms of Shannon's channel capacities of the legitimate user and the eavesdropper as follows [19]

$$C_s = \max\left\{\log_2(1+\gamma_D) - \log_2(1+\gamma_E), 0\right\}, \tag{3}$$

where γ_D and γ_E represent the instantaneous SNR at the legitimate user and the eavesdropper, respectively. The ergodic capacity is obtained by averaging (3) as per the available channel state information (CSI).

B. SECRECY OUTAGE PROBABILITY/CAPACITY (SOP/SOC)

Similar to the known outage probability in communication systems, the secrecy outage probability (SOP) is defined as the probability of the event when the instantaneous SC falls below a given target SR, which is written as follows

$$\mathrm{SOP}(R_{\mathrm{th}}) = \Pr\{C_s < R_{\mathrm{th}}\}. \tag{4}$$

In fact, the definition in (4) does not differentiate between the outage due to non reliable legitimate channel and the outage due the leakage of information to the eavesdropper. Therefore, another more explicit definition is proposed in [20] as follows

$$\mathrm{SOP}(R_{\mathrm{code}}, R_{\mathrm{th}}) = 1 - \Pr\{C_D \geq R_{\mathrm{code}}, C_s \geq R_{\mathrm{th}}\}, \tag{5}$$

where C_D is the instantaneous legitimate channel capacity, R_{code} is the coding rate of the transmitted message. It is clear, in this definition, that the secrecy outage event happens when the coding rate R_{code} fails to satisfy Shannon's reliable transmission condition in addition to having the SC below a target SR threshold R_{th}.

A related and widely adopted metric is the secrecy outage capacity (SOC), which is defined as the maximum achievable SC, C_{out}, that guarantees an SOP of less than a threshold ϵ [21], which is expressed as follows

$$\max\{C_{\mathrm{out}}\} \text{ with } \Pr\{C_s < C_{\mathrm{out}}\} = \epsilon. \tag{6}$$

C. AVERAGE SECRECY OUTAGE RATE/DURATION (ASOR/ASOD)

The aforementioned performance metrics are based on the first-order statistics, however, incorporating the second-order statistics in the secrecy performance metrics offers a better understanding of the dynamics of the performance. Two secrecy performance metrics that fall under this category were proposed in [22]. Namely, the average secrecy outage rate (ASOR) and the average secrecy outage duration (ASOD). The former, ASOR denoted by $\mathcal{R}(R_{\mathrm{th}})$, measures the SC's average rate of crossing a given threshold level R_{th}, whereas the ASOD measures, in seconds, the average duration in which the system remains in a secrecy outage status. ASOD is expressed, at a given threshold R_{th}, in terms of the SOP and the ASOR as follows

$$\mathcal{T}(R_{\mathrm{th}}) = \frac{\mathrm{SOP}(R_{\mathrm{th}})}{\mathcal{R}(R_{\mathrm{th}})}. \tag{7}$$

D. AMOUNT OF SECRECY LOSS (ASL)

Recently, the authors in [23], proposed a new PLS performance metric, the amount of secrecy loss (ASL), based on the second order statistics of the SC. The ASL measures the amount of information leakage to the eavesdropper, which is expressed as

$$\mathrm{ASL} = \frac{\mathrm{E}\{C_s^2\}}{\mathrm{E}\{C_s\}^2} - 1, \tag{8}$$

where $\mathrm{E}\{\cdot\}$ is the statistical expectation operator.

III. CATEGORIZING RECENT STUDIES ON WIRELESS RIS-REINFORCED SECRECY

In this section, we classify the most recent works on RIS-reinforced PLS in wireless communications in terms of the considered system model. As we noted, most of the related works are aimed to maximize the SR/SC while the differences were found in the considered system model and the methodology to optimize the objective in hand. The classification is done based on the number of antennas at the transmitter and the receiver. In what follows, we interchangeably use the terms Alice/BS, Bob/legitimate and Eve/eavesdropper.

A. SISO SYSTEM MODEL

The simplest setup we encountered in the literature assumes a single-antenna transmitter, Alice, willing to securely deliver a message to a single-antenna legitimate user, Bob, in the presence of a single-antenna eavesdropper, Eve, as shown in Fig. 2-(a).

Yang *et al.* [24] studies the secrecy performance of an RIS-assisted SISO communication link in the presence of a line-of-sight (LoS) links between the RIS and the eavesdropper and the legitimate user. Single RIS is considered with N reflecting elements placed between the source and the legitimate user. The CSI of the legitimate user is assumed to be known at the RIS. Thus, the RIS can induce the required phase shifts on the reflected signal to maximize the received SNR at the legitimate user. The analytical expression of the SOP is derived as an evaluation metric to assess the secrecy performance. The analytical and simulation results show that the presence of an RIS significantly enhances the SR and the enhancement is driven by the number of RIS's reflecting elements. However, the secrecy performance slightly drops when the eavesdropper enjoys a LoS link with the RIS as well. This is due to optimizing the RIS's induced phases to maximize the SNR at the legitimate user but ignoring the effect it exercises on the eavesdropper's received SNR. In [25], an unmanned aerial vehicle (UAV) equipped with an RIS is used as a mobile relay between a group of users and a BS. The authors focus on the maximization of secrecy energy efficiency by joint optimization of the passive beamforming, the user-UAV association, the UAV trajectory, and the transmit power. Alternating optimization (AO) and successive convex approximation (SCA) algorithms are used, where the objective is to attain fairness in SR among users and minimum energy.

In vehicular ad hoc networks (VANET), PLS is a major concern, due to the broadcast nature of the wireless channels. Many papers, [26]–[28], have considered the analysis of PLS under such high mobility conditions and dynamic environments. In fact, RIS is proven to help compensating the multipath and Doppler effects in wireless propagation channels [6]. Capitalizing on this advantage, an analytical approach is followed in [29], [30] to optimize the SC in a VANET, where two setups are proposed to investigate the PLS. The first setup assumes a source, a destination, and an

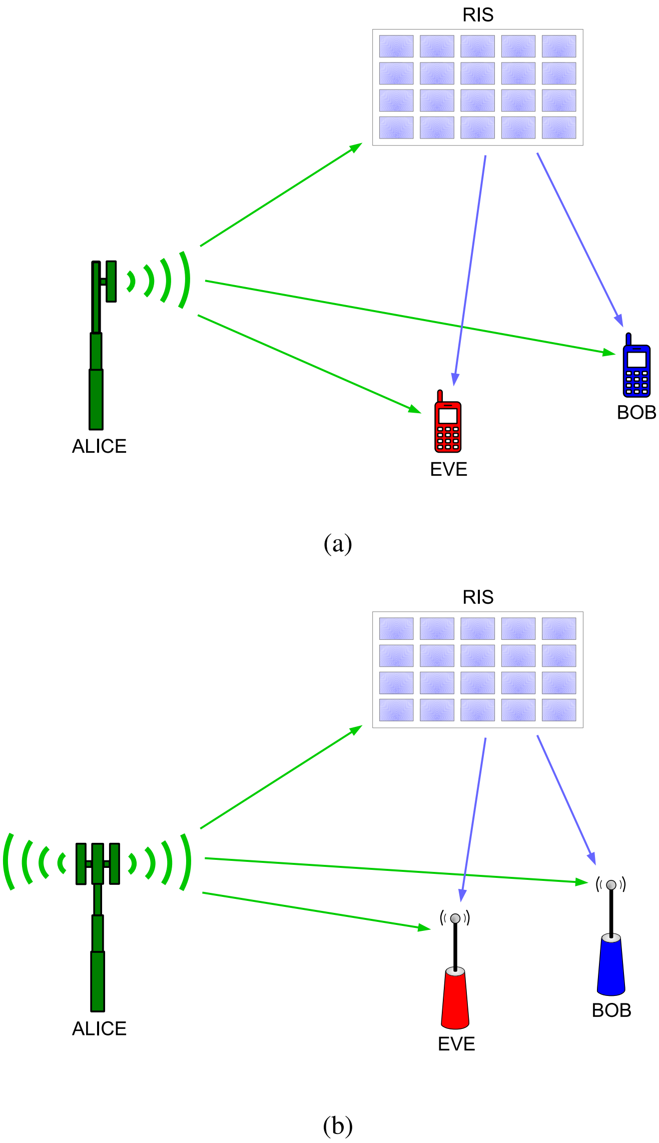


FIGURE 2. Most Common System Models in the Literature (a) SISO, (b) MIMO.

eavesdropping vehicle communicating with the support of an RIS mounted on a nearby building, while the second setup assumes that the source vehicle has an RIS coupled with its transmitter. A double Rayleigh distribution is assumed between the mobile ends, and the Meijer G-function is used to obtain the probability distribution function (PDF) of the received source, which slightly complicates the analysis. The reported results are similar to those in [24]. Furthermore, the authors study the effect of varying the number of RIS's reflecting elements and the distance between the source and the RIS. Specifically, as the number of reflecting elements increases, the SR/SC improves because better beamforming can be achieved, and the SR/SC degrades while increasing the source-RIS distance which is due to fading and path loss effects. A recent work, by the authors, [31], investigates the effectiveness of RIS-assisted network by introducing a weighted variant of the SC definition. Simulation results show that the existence of a reliable LoS link dominates the system's SC. However, it can be further enhanced by optimizing the RIS-induced phase shifts. In addition, it is shown that the RIS-assisted system with non-line-of-sight (NLoS) links achieves comparable SC to that of dominant LoS link systems with unknown RIS-Eve CSI.

A general indoor system model is considered in [32], where a SISO system with multiple Bobs and Eves is investigated. Analytical based genetic algorithm (GA) is utilized to find the optimal tile-allocation-and-phase-shift-adjustment (TAaPSA) strategy for the RIS to optimize the average SR. The obtained results show that the number of Eves in the system has a significant effect on optimal trend of TAaPSA strategy. For low number of Eves, the SR can be maximized by simultaneously enhancing average rate of Bobs and degrading the average rate of the Eves. In the contrary case, the RIS can be fully utilized to boost the average rate of Bob.

B. MIMO SYSTEM MODEL

Dong and Wang in [33] consider a MIMO system model, as shown in Fig. 2-(b), where the BS, the eavesdropper, and the legitimate user have multiple antennas. However, the system has NLoS transmission. The objective again is to maximize the SR at the legitimate user by jointly optimizing the transmit covariance matrix and the phase shift matrix of the RIS's reflecting elements. Solving this nonconvex problem is intractable, hence, an AO algorithm is proposed assuming complete knowledge of CSI of both the legitimate user, and the eavesdropper at the RIS and the BS. The proposed solution is shown to monotonically converge within a number of iterations that is dependent on the number of antennas at the BS, legitimate user, and eavesdropper. On the other hand, the authors in [34] opt for including the LoS transmission channel and using AN, consequently, rendering the objective function more challenging to solve. The proposed optimization algorithm is block coordinate descent (BCD) aided by the majorization minimization (MM) algorithm. The results show how increasing the number of RIS's elements can increase the SR at the expense of burdening the optimization algorithm with a larger phase shift matrix to optimize.

Similarly, the authors in [35] considered a LoS channel as in [34] with the same objective, but the authors consider the case of discrete phase shifts at the RIS after solving the optimization problem under the continuous phases assumption. As we know that the optimization problem under the continuous phases is non-convex, it can be solved using an AO method, where for a given RIS reflect coefficients, SCA is used to optimize the transmit covariance matrix. Next, for a given transmit covariance matrix, the AO method is used again to optimize the individual elements' phase shift of the RIS one by one, given the other elements' shifts at each step. Numerical simulations show that 3-bits quantized phase shifts yields an acceptable SR with negligible loss as compared to the continuous phase shifts case. Noting the large scale of this MIMO setup, it is clear that the adopted AO method in solving the optimization problem suffers from high computational complexity especially when we consider a large scale RIS and a high number of antennas at the BS, the legitimate user, and the eavesdropper. Furthermore, the optimization of the phases matrix and the covariance matrix are independent problems only if the BS-RIS channel is a rank-one matrix [36], thus, the AO gives a sub-optimal solution in the full rank channel case.

In order to highlight the benefits of having an RIS supporting the secure communications with an RIS-empowered eavesdropper, the authors in [37] consider an eavesdropper with a supporting passive eavesdropping RIS that competes against a legitimate RIS to impair the system's secrecy. As expected, it has been shown that a non-zero SR cannot be achieved with AN and preceding with the absence of the legitimate RIS. However, a legitimate RIS with L reflecting elements can safeguard secure communication against a larger than $3L$-elements eavesdropping RIS.

C. MISO SYSTEM MODEL

As most of the relevant works fall under this subsection, we further classify them based on the following: the number of users in the system, the CSI availability/acquiring assumptions, the pursued methodology, and practicality-related assumptions.

1) SINGLE BOB AND EVE

Many works, [36], [38]–[44], considered a simplified system model as shown in Fig. 3-(a). Where a multiple antennas BS, is considered, communicating a secure messages to a single user (Bob) in the presence of a single Eve, both having a single antenna. In [38], [40]–[42], optimization problems are proposed to maximize the SR at the legitimate user by jointly optimizing the beamforming at the BS and the phase shifts at the RIS. Due to the intractability of this problem, different methodologies have been adopted. In [38], RIS discrete phase shifts is assumed and an AO method is followed, where for a given RIS phase shifts matrix, the optimal BS precoder is obtained using Rayleigh-Ritz theorem. On the other hand, for a given BS precoder matrix, a cross-entropy-based algorithm is adopted to optimize the RIS phase shifts matrix. In [40], two efficient joint optimization techniques are proposed, namely: AO-MM and BCD. It is revealed that the AO-MM algorithm is favorable for large-scale RIS-assisted systems, while the BCD is superior for wireless systems with small-scale RISs. In addition, the obtained results show that installing a large scale RIS yields better enhancement in terms of SR and is more energy-efficient as compared to enlarging the transmit antenna array size. However, continuous phase shifts is assumed at the RIS which serves as an upper bound on the practical performance. An AO-based algorithm is developed in [41] to solve the joint problem of optimizing the transmit covariance matrix of the BS and the RIS's phase shift matrix providing closed-form and semi-closed-form solutions, respectively. Moreover, the obtained AO-based solution, with the help of fractional optimization (FO), is extended to the case where the eavesdropper can have multiple antennas. It is shown that the SR degrades when the number of eavesdropper antennas increases, as it starts to achieve higher rates.

It is worth noting that the simulated distance-dependent scenarios conducted by different works considered one-dimensional (1D) movements only where the transmitter, the legitimate user, and the eavesdropper lie on a planar surface. However, no work addressed the two-dimensional (2D)/three-dimensional (3D) movements which are the case in many emerging scenarios. A more practical scenario is considered in [42], where the channels of the legitimate user and the eavesdropper are spatially correlated, and the latter has a stronger channel. An AO-SDR based method is adopted and similar results are achieved as in [41]. Similarly,

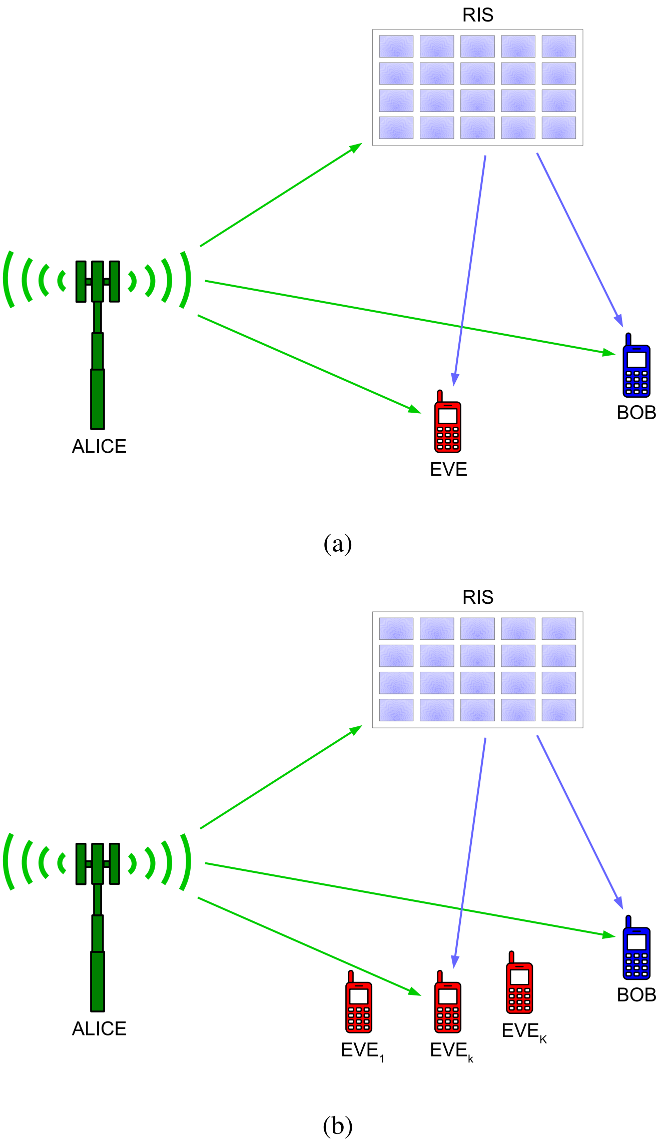


FIGURE 3. Most Common System Models in the literature (a) MISO with single eavesdropper, (b) MISO with multiple eavesdroppers.

the authors in [43] considered the joint optimization problem but for the Terahertz (THz) communications scenarios. An AO-based algorithm is developed, where for a given beamforming matrix, the optimal RIS's phase shifts is obtained by leveraging the characteristics of the THz channel. Then, given the obtained phase shifts, the optimal beamformer is derived by utilizing the Rayleigh-Ritz theorem [45]. It is worth mentioning here that the RIS in this work operates in two modes, namely: the sensing and reflection modes. In the former, the RIS reflecting elements turn into active antennas supported with RF chains. However, this assumption is not power efficient noting the high number of reflecting elements at the RIS.

Energy efficiency is another constraint that is incorporated in [36], [39]. In [36], the energy consumption is investigated assuming NLoS links between the BS and legitimate user/eavesdropper. Thus, the authors aimed for minimizing the consumed energy in BS-RIS link through beamforming at the transmitter and optimizing the phase shifts at the RIS. It is shown that the beamforming and the phase matrix optimization problems are independent in the rank-one channel case. However, in the full-rank channel case, they are inseparable. For both channel rank cases, projected gradient descent (PGD) and semidefinite relaxation (SDR) are used to solve the joint optimization problem. The performance of both optimization algorithms is analyzed to find out that both yield similar results, however, the SDR algorithm converges faster than the PGD. Within a related context, RIS-supported simultaneous wireless information and power transfer (SWIPT) is investigated in [39]. A MISO system supported by an RIS is considered to improve the delivered energy to an energy harvesting receiver (EHR) in addition to information transfer to a legitimate receiver with the presence of an eavesdropper. An AO method is adopted after relaxing the non-convex problem using the SDR technique. The resulting high complexity algorithm is further improved to reduce the complexity using the SCA approximation. The reported results reveal that, with the presence of an RIS, the harvested power can be doubled under SR constraint as compared to the traditional case with no RIS. A CR system is considered in [46], where the legitimate user, Bob, is considered as a secondary user that is trying to access a licensed band in the presence of an eavesdropper. A nearby RIS is installed to support a secure communication for Bob while maintaining an upper bound on the interference level at the primary user. An AO algorithm is proposed to maximize the SR of Bob subject to total power constrain at Alice, and inference power constrain at the primary Bob in the presence of Eve. Simulation results show that SR can be significantly enhanced compared with no RIS case. In addition, even with the constraint on the interference, the SR keeps increasing with transmit power unlike the case with no RIS which shows a saturation in the SR at higher transmit power levels.

Different from the ideal assumption in existing literature that full Eve' CSI is available, Wang *et al.* [47] consider a more practical scenario where Eve's CSI is not available. To enhance the system security given a total transmit power at Alice, two joint beamforming and jamming optimization algorithms are proposed based on OM and MM methods. The transmit power is firstly optimized at Alice to meet the QoS at Bob, while AN is emitted to jam Eve by using the residual power at Alice. The AN is projected onto the null space of Bob's channel to ensure that only Eve is jammed. As compared to the ideal case of full CSI, security could still be guaranteed by relaxing the QoS threshold at Bob as well as increasing the number of RIS reflecting elements. Unlike the current research trend on utilizing RIS to enhance the system secrecy, Lyu *et al.* [48] propose the use of an RIS as a passive jammer to attack legitimate communication between BS and Bob. BCD, SDR, and Gaussian randomization techniques are utilized to jointly optimize reflection coefficient magnitudes and discrete phase shifts at the RIS to diminish the signal-to-interference-plus-noise ratio (SINR) at Bob. Obtained results show that the performance of the proposed RIS-based jammer outperforms that of conventional active jamming attacks in some scenarios, especially when the distance between RIS and Bob is small (less than 10m). Noting the high computational complexity of solving the joint optimization problem, discussed so far, the authors in [44] introduce a machine learning (ML) model by utilizing deep neural network (DNN) to maximize the system's SR in real time. Simulation results show that the DNN can achieve comparable results to the conventional optimization methods with simpler and faster implementation.

2) MULTIPLE BOBS OR EVES

Fewer works, [49]–[51], considered the case when multiple eavesdroppers are attacking a single legitimate user as shown in Fig. 3-(b). Jamming is a common technique to deny the eavesdropper from receiving any useful signal, which can be done even actively as in [47], [49], [50] or passively with the aid of an illegitimate RIS as in [48]. Wang *et al.* [49], considered the energy efficiency by optimizing the beamforming at the transmitter, as in [36], [38], [47], aided by a cooperative jamming with the support of an optimized RIS phase shifts. An SDR-based energy-efficiency maximization problem is defined to optimize the transmit power, the independent cooperative jamming, and the RIS reflection coefficients under a constraint on the SR. The proposed scheme is highly energy-efficient even with high jamming power, which implies the significance of the cooperative jammer that is introduced. Moreover, it also outperforms the other reported schemes in maintaining a high SR along with being energy efficient. On the other hand, Guan *et al.* [50] investigate the RIS's effectiveness in improving the SR, with an AN induced by the transmitter to jam the eavesdroppers instead of the cooperative jammer in [49]. The objective is to maximize the SR at the legitimate user by jointly optimizing the transmitter beamforming, the AN (jamming), and the passive beamforming at the RIS. An AO-based method is used to optimize the three dependent elements in the objective function. It is shown that the use of AN jamming requires fewer reflecting elements on the RIS in order to maintain a specific SR threshold. In a related context, where the power efficiency is considered, the authors in [51], study the role of RIS in minimizing the transmitted power while maintaining a secrecy level. Considering the non-convex nature of the problem, an AO algorithm and an SDR method to optimize the secure and power-efficient transmission are proposed. Few simulation scenarios are presented illustrating the distance effect on the transmitted power showing that as the legitimate user moves away from the BS and getting closer to the RIS, the overall system energy efficiency increases as less power needs to be transmitted. In addition, in scenarios where the eavesdropper is close to BS/RIS, higher transmitted power is needed to keep a secure communication. Unlike the above mentioned works, multiple legitimate users in the presence of a single eavesdropper is considered in [52], where the beamformer, the AN's covariance matrix at the BS and the RIS's phase shifts are optimized to maximize the average sum of the legitimate users' SRs. A sub-optimal solution is obtained for the non-convex problem using AO method, and applying SCA, SDR and manifold optimization (MO) approaches. Results show an increase in the average SR with the support of the RIS and the AN generated at the BS. However, the analysis is limited to the case with NLoS which simplifies the problem in hand.

3) MULTIPLE BOBS AND EVES

On the other hand, as a more realistic scenario, multiple legitimate users are assumed to be attacked by multiple eavesdroppers in [53]–[56]. Considering the high computational complexity of the involved optimization problem for this generalized scenario, ML-based algorithms would provide a fast and flexible solutions. For instance, Yang *et al.* [54] consider a novel deep reinforcement learning (RL) approach to achieve optimal beamforming policy in a dynamic environment. In addition, post-decision state (PDS) and prioritized experience replay (PER) schemes are employed to enhance the secrecy performance and learning efficiency. Simulation results show that the proposed algorithm outperforms conventional optimization approaches by achieving a higher average SR per user and higher QoS satisfaction probabilities. Another critical security challenge against legitimate transmission is malicious jamming launched by smart jammers. Authors in [55] consider the use of RIS to mitigate the jamming interference and enhance the communication performance by proposing joint optimization approach using fuzzy win or learn fast-policy hill-climbing method. The fuzzy model helps to estimate the dynamic jamming model, where uncertain environments states are represented as aggregate of fuzzy states. Simulation results show that the proposed approach can improve both transmission protection level and RIS-assisted system rate compared with existing solutions.

An extension to the work in [52] is made in [53] to include multiple legitimate users and multiple eavesdroppers with two RISs instead of one, rendering the problem to be much more challenging. Moreover, the potential eavesdroppers are roaming users within another BS, where their feedback leaked signal to their corresponding BS can be utilized for coarse CSI estimation at the BS. To improve the estimation, a deterministic model is adopted to characterize the CSI's uncertainty. The work is extended to account for the SOP along with the average SR. The significant contribution is in incorporating several RISs with a uniform number of elements instead of having a single RIS with a huge number of elements. However, the LoS analysis is not included, which is an important aspect in practical scenarios. The authors in [56] propose an optimization problem to maximize the minimum SR at the legitimate users by jointly optimizing the BS beamforming and the RIS's phase shifts. Furthermore, the reflecting elements of the RIS are assumed to be discrete, and a spatial channel correlation between the legitimate users and the eavesdropper is assumed as well. Again, due to the non-convexity of the problem, and hence the non-tractability, an AO method and a path-following algorithm are proposed to maximize the objective function.

Based on the conducted survey, we assemble the reviewed works in Table 1 which summarizes the different assumptions and system models with methodologies and performance metrics in the conducted literature review. Moreover, Table 2 classifies them in terms of the system model (SISO, MISO, and MIMO) and the adopted methodology to approach the considered objective.

IV. CHALLENGES, RECOMMENDATIONS, AND FUTURE RESEARCH DIRECTIONS

This section presents the challenges, recommendations, and future research directions for designing practical, efficient, and secure RIS-assisted future wireless communication systems, as summarized in Fig. 4. The conducted survey reveals that the simultaneous control of transmission from the BS and the reflections at the RISs can be an efficient solution to ensure confidentiality in wireless communication. Several simulation results verify the enhancement of the overall SR in such systems compared to the conventional ones. However, we stumbled upon several challenges and open directions for further investigation which we discuss along with recommendations, and future directions as follows.

A. EFFECT OF RIS PHYSICAL DESIGN AND DEPLOYMENT

The effect of the physical design and deployment of RISs on PLS can be an interesting research direction, yet, it is not explored well in the literature. The physical design includes the number of RISs, their distribution, orientation, size, and geometrical shape. Moreover, the effect of varying the RIS's number of elements and their distribution on PLS needs further exploration. The effect of mobility and trajectory design in the case of mobile/flying RISs is yet to be studied, and the feasibility of using them in such scenarios is still an open problem.

TABLE 1. Summary of the different assumptions, system models, methodologies, and performance metrics. Where N_a, N_b, N_e and N_r denote the number of antennas at Alice, Bob, Eve and RIS, respectively, K, L and M denote the number of Eves, Bobs and RISs, respectively, I_i denotes the number of iterations of the i^{th} loop, and I_ϵ denotes the total number of iterations to achieve the target accuracy ϵ.

Ref.	System Model	Methodology	Assumptions	Complexity	Metric
[24]	SISO	Analytical	Quasi-static flat fading	–	SOP
[25]	SISO, Bob=L	Approximation (AO-SCA)	Rayleigh/Rician fading	–	Secrecy Energy Efficiency
[26], [30]	SISO	Analytical	Double Rayleigh fading	–	Average SC & SOP
[31]	SISO	Analytical	Rayleigh flat fading	–	SC
[32]	SISO, Eve=K, Bob=L	Analytical (GA)	Ray model, Rice distribution	–	SOP
[33]	MIMO	Approximation (AO-MM)	Gaussian wiretap	–	SR
[34]	MIMO	Approximation (BCD-MM)	Narrow-band & non-dispersive channel	–	SR
[35]	MIMO, Eve=K	Approximation (AO-SCA)	Discrete phase shifts	$O(I_3(I_1(N_e^3+N_a^6)+ I_2N_r(N_b^3+N_e^3-\log_2\epsilon)))$	SR
[36]	MISO	Approximation (PGD-SDR)	Multiple channel models	–	Average SR
[38]	MISO	Approximation (AO)	Discrete phase shifts	–	SR
[39]	MISO	Approximation (AO-SDR-SCA)	Rayleigh fading, EHR	$O(N_a^8+N_r^8)$ & $O(N_a^3+N_r^3)$ AO-SDR & AO-SCA	SR & Harvested Power
[40]	MISO	Approximation (AO-MM-BCD)	Rayleigh fading	–	Average SR
[41]	MISO	Approximation (AO-FO)	Rayleigh fading	–	SR
[42]	MISO	Approximation (AO-SDR)	Bob & Eve channels are correlated	$O(I_1(N_a^3+(N_r+1)^{3.5}))$	Average SR
[43]	MISO	Approximation (AO-FO)	Saleh Valenzuela model	–	SR
[44]	MISO	Approximation (DNN)	Quasi-static flat-fading	–	Average SR
[46]	MISO, Primary Receiver=1	Approximation (AO)	RIS-assisted Gaussian CR wiretap channel	O(N_a^3+N_a^2) or O($N_a^3+I_\epsilon N_a^2$)	SR
[47]	MISO	Approximation (OM and MM)	Quasi-static flat-fading, Unknown Eve's CSI	O($I_1N_a^2$)	SR
[49]	MISO, Eve=K	Approximation (AO-SDR-FO)	Quasi-static flat fading	–	SR
[50]	MISO, Eve=K	Approximation (AO)	Quasi-static flat-fading	$O(I_3(I_1\max\{N_r,K\}^4N_r^{0.5} + I_2\max\{N_a,K\}^4N_a^{0.5}))$	SR
[51]	MISO, Eve=K	Approximation (AO-SDR)	Rayleigh flat fading	$O(N_r^2\sqrt{N_r}\log(1/\epsilon) (N_r^3+1+N_r)+ N_r^2(N_r^2+1+N_r)+N_r^4)$	SR

Generally speaking, the deployment of RISs at different locations is a different problem compared to BSs/relays deployment because of the passive nature of RISs. Moreover, RISs are easier to deploy practically without interfering with each other due to their much shorter range when compared with active BSs/relays. However, how to optimally

TABLE 1. *(Continued.)* Summary of the different assumptions, system models, methodologies, and performance metrics. Where N_a, N_b, N_e and N_r denote the number of antennas at Alice, Bob, Eve and RIS, respectively, K, L and M denote the number of Eves, Bobs and RISs, respectively, I_i denotes the number of iterations of the i^{th} loop, and I_ϵ denotes the total number of iterations to achieve the target accuracy ϵ.

Ref.	System Model	Methodology	Assumptions	Complexity	Metric
[52]	MISO, Bob=L	Approximation (AO-SDR-MO)	Interference cancellation at Eve	–	Average Sum SR
[53]	MISO, Eve=K, Bob=L	Approximation (AO-SCA-SDR)	Interference cancellation at Eve & Multiple RISs	$O(\log(1/\epsilon)((\sqrt{N_a}+\sqrt{N_e})K^3L^3$ $+(N_a^{5/2}+N_r^{5/2})K^2L^2)$	Average Sum SR & SOP
[54]	MISO, Eve=K, Bob=L	Approximation (Deep RL PDS-PER)	Outdated/real-time CSI, Rayleigh flat fading	–	SR
[56]	MISO, Eve=K, Bob=L	Approximation (AO)	Discrete/continuous phases & active Eves	$O((LK+1)K^2N_a^2)$ $O((LK+N_r+1)(N_r+1)^2)$	Max min SR

TABLE 2. Summary of methodologies and key assumptions in the literature.

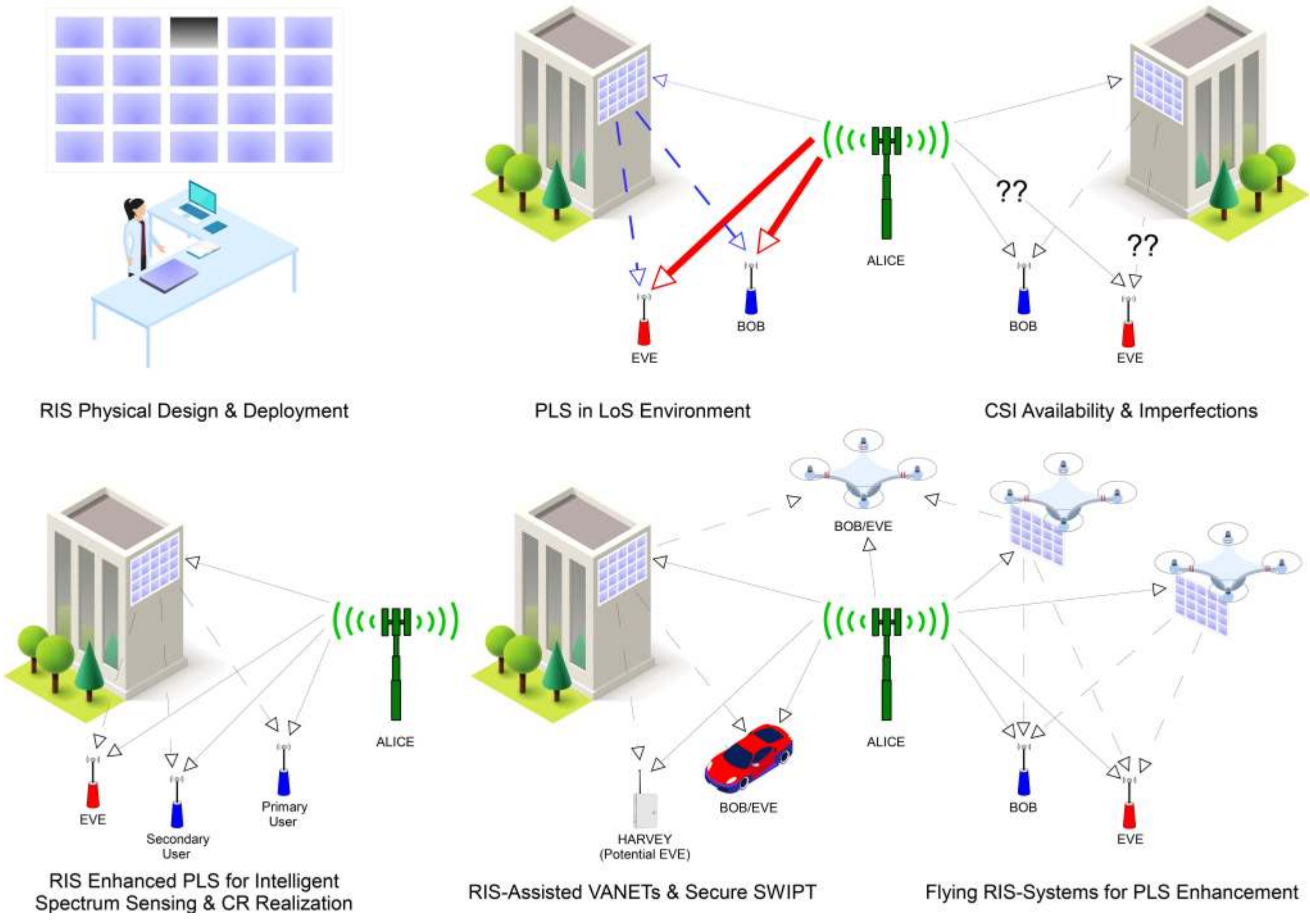
Methodology/System Model	SISO	MISO	MIMO
Machine learning (DNN, Deep RL)		[44], [54]	
Jamming (Artificial Noise)		[49], [50], [52]	[34]
Analytical	[24], [26], [30], [32]		
Alternating Optimization (AO)	[25]	[38]–[43], [46], [49]–[53], [56]	[33], [35], [37]
Minorization Maximization/Majorization Minorization (MM)		[39], [40]	[34]
Path-Following		[56]	
Semidefinite Relaxation (SDR)		[36], [39], [42], [49], [51]–[53]	
Successive Convex Approximation (SCA)	[25]	[39], [53]	[35]
Projected Gradient Descent/Ascent (PGD/PGA)		[36]	[37]
Block Coordinate Descent (BCD)		[40]	[34]
RIS Quantized Phase Shifts		[38], [56]	[35]
RIS Continuous Phase Shifts	[24]–[26], [30]	[36], [39]–[44], [49]–[54]	[33]–[35], [37]
Manifold Optimization (MO)		[47], [52]	
Fractional Optimization (FO)		[41], [43], [49]	

adjust the physical design, deployment, collaboration, and association to enhance RIS-assisted PLS is still an open challenge. ML and stochastic geometry-based solutions can be good options for efficient deployment of RIS assisted systems.

Furthermore, RIS-reinforced secrecy with imperfect RIS reflecting elements, i.e., discrete phase shifts and non-unit modulus (attenuating reflecting elements) also need to be considered while designing RIS-assisted PLS techniques.

B. PLS IN LOS ENVIRONMENTS

Ensuring confidential communication in the case of LoS transmission scenarios, where the eavesdropper is located within the same direction as that of the legitimate user, is quite challenging. Under these cases, several PLS techniques, including conventional beamforming, AN-based MIMO techniques, etc., [12] will fail to provide secure communication. RIS can ensure secure communication even in such scenarios by providing additional channel paths between the



RIS Physical Design & Deployment
ALICE
BOB
EVE
PLS in LoS Environment
??
??
BOB
EVE
CSI Availability & Imperfections
ALICE
EVE
Secondary User
Primary User
RIS Enhanced PLS for Intelligent Spectrum Sensing & CR Realization
BOB/EVE
ALICE
HARVEY (Potential EVE)
BOB/EVE
RIS-Assisted VANETs & Secure SWIPT
BOB
EVE
Flying RIS-Systems for PLS Enhancement

FIGURE 4. Challenges and Future Directions.

legitimate nodes. There are few works reported in this direction [42], but further investigation is required, especially, when combining those scenarios with the imperfect or partially available CSI practical assumption.

C. EFFECT OF CSI AVAILABILITY AND IMPERFECT CSI

Based on the conducted survey, it is observed that the majority of the RIS-assisted PLS techniques in the literature assume the availability of perfect CSI at the transmitter and/or the RIS. However, channel estimation for the RIS assisted system is a challenging task due to a large number of passive reflecting elements. Moreover, these elements are passive in nature without signal processing capabilities and active transmitting/receiving abilities. Thus, in practice, only imperfect CSI can be accessed by the transmitter. Another issue that needs to be considered is that the CSI of an illegitimate node is available only if it is active or it is a licensed user that has legal access to the network. However, in the case of a passive eavesdropper, the CSI of the eavesdropper is not available. Moreover, in PLS literature, channel reciprocity property in TDD is assumed. However, with the involvement of RIS, this assumption may no longer be valid, which further complicates the problem [14]. A practical approach for acquiring the CSI at the RIS is proposed in [57], [58], where some of the reflecting elements are assumed to be active and can estimate the CSI, then, using compressive sensing or deep learning techniques, the CSI at all reflecting elements can be recovered/estimated. However, the channel is assumed to be sparse in the compressive sensing technique and requires a higher number of active elements as compared to the deep learning approach. Consequently, this calls for taking into account the effect of imperfect/incomplete CSI and its availability at transmitter while designing RIS-assisted security techniques for different channel models [59] to ensure that these techniques are robust to these imperfections [14].

D. PRACTICAL REALIZATION AND HIGHER-ORDER METRICS ASSESSMENT

To show the effect of RIS-assisted secure communication in real environments, experimental work needs to be done. Although some promising experimental works have been reported in [60]–[62] to verify the gains offered by the RIS system, there is still a paucity of practical work for RIS-assisted secure communication. Moreover, the current practical work on RIS is not enough to decide the actual potential of RISs in practical conditions.

On the other hand, most of the current work focus on first-order metrics for PLS assessment such as SR/SC and SOP. In this review, we highlighted new emerging higher-order metrics, which can add more insights to enable the actual realization of practical RISs. When security is a concern in adaptive transmission schemes and dynamic deployment of systems, ASOR and ASOD metrics can help in both their design and deployment. ASOR helps in quantifying the average secrecy level crossing rate at a specific secrecy threshold level predefined in the system, which in a sense shows "how many times" the communication system was vulnerable. On the other hand, ASOD specifies for "how long" this vulnerability was attained. Moreover, ASL, which is based on SR statistics, is also highlighted to quantify the amount of information that was lost in vulnerability durations [23].

E. FLYING RIS-SYSTEMS FOR PLS ENHANCEMENT

Recently, flying RISs-assisted communications (UAVs equipped with an RIS) have received much attention. Some key features of flying RISs include 3D mobility, changeable direction and location, easy deployment, adaptive altitude, and power-efficient beamforming [63], [64]. The trajectory of a flying RIS can be optimized along with the phase shifts adjustment at the RIS elements for enhancing PLS [25]. More specifically, the positioning/trajectory of the UAVs can be adjusted more flexibly in 3D space compared to terrestrial RISs. This feature can be used to improve the overall security by adapting the transmission based on the requirements, location, and channel conditions of the legitimate user. Besides, flying RISs can also be used as mobile cooperative jammers jointly with active UAVs or ground BSs to improve the secrecy performance. Moreover, in practice, a single flying RIS has limited capabilities in terms of communication and maneuvering. Hence, in some challenging scenarios, it may not achieve the desired secure communication performance, which motivates the investigations on multiple flying RISs along with active UAVs.

F. INTEGRATION OF RISS WITH EMERGING TECHNOLOGIES AND FUTURE APPLICATIONS

RIS-assisted PLS solutions against passive and active eavesdropping for emerging and state-of-the-art technologies comes naturally. Promising research directions are, but not limited to, millimeter-wave communications, ma-MIMO, visible light communications, drones-aided communications, Internet of Things (IoT), THz communication, free-space optics, full-duplex communication, non-orthogonal multiple access (NOMA) [65] and VANET [1].

Moreover, designing effective, adaptive, and intelligent [66], [67] RIS-assisted PLS techniques under joint consideration of security, reliability, latency, complexity, and throughput based on QoS requirements of future applications to support URLLC, eMBB, and mMTC is also an interesting area of research. Furthermore, RIS-assisted cross-layer security design including the interaction of different layers, such as the physical layer, media access control (MAC) layer, network layer, and application layer, is not yet studied in the literature from the physical layer perspective.

G. OPTIMIZATION PROBLEMS TO ENHANCE PLS

Although the adoption of RISs in communication systems can enhance the overall systems' security, it results in higher complexity systems in terms of design and analysis as compared to conventional wireless systems [68]. The use of data-driven tools such as ML, deep learning, and RL, is a promising solution to support the flexibility and the self-optimizability of such networks. Only a few works, [44], [54], have reported employing ML-based approaches to solve the PLS problem in RIS-assisted networks.

H. RIS-ASSISTED SECURE SWIPT

SWIPT is a promising technology to power massive low-power devices in the IoT for future wireless networks. The employment of RIS can enhance the performance of both the received information as well as the received energy in SWIPT systems [14]. In [39], a system with an access point, information eavesdropper, legitimate information receiver, and a separated legitimate energy harvesting receiver, is investigated. It is reported that with the support of an RIS, the harvested power can be significantly improved under secrecy constraints. However, an untrusted energy harvesting receiver (HARVEY) can also eavesdrop the information intended for legitimate receivers. Designing efficient RIS-assisted secure SWIPT to prevent the untrusted energy harvesting receiver from eavesdropping the information is an interesting area for future research consideration. Obviously, this problem should be investigated under practical assumptions such as discrete phase shifts at the RIS, the coupling between the RIS elements' phase and the reflection gain, and the imperfect/unavailable eavesdropper's CSI.

I. RIS ENHANCED PLS FOR INTELLIGENT SPECTRUM SENSING AND CR REALIZATION

Intelligent spectrum sensing involves user detection, interference identification, and resource prediction, where those processes are often needed to be done in a secure manner. RISs can be utilized to create a secure environment against eavesdroppers in which spectrum sensing can be conducted reliably and securely. Moreover, RISs can be enablers for realizing secure CR systems, where RISs are used to ensure secured communication in a targeted network (primary or secondary).

V. CONCLUSION

PLS supports the transmission secrecy when the conventional cryptographic methods fail due to the limited computational capacity at the legitimate communicating pairs or due to computationally over-powered eavesdropper. Yet, the efficiency of PLS is limited in some scenarios, for instance in the case of highly correlated legitimate and eavesdropping channels. RISs can be looked at as a promising solution in such scenarios, not to mention others, in the sense of adding more degrees of freedom by involving the propagation channel manipulation into the design problem. The most common, in addition to the recently proposed, performance metrics in PLS analysis were discussed. Furthermore, the PLS related works under the RIS-assisted networks have been reported and classified based on the adopted system model and the adopted methodologies.

Insightful recommendations are revealed upon this survey regarding the availability of the CSI, RIS design and deployment challenges, and the ML-based approaches to tackle the computational complexity encountered in all surveyed works. The deployment and orientation of RISs are key factors in reaping their full benefits in terms of system secrecy level. Hence, flying RISs are identified as a promising research direction, as they add more flexibility in the network by optimizing the RISs' 3D location, orientation, and trajectory to boost the system secrecy as well as to improve the overall energy efficiency.

REFERENCES

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

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

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

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

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

[6] E. Basar and I. F. Akyildiz, "Reconfigurable intelligent surfaces for Doppler effect and multipath fading mitigation," 2019. [Online]. Available: arXiv:1912.04080.

[7] S. Hu, F. Rusek, and O. Edfors, "Capacity degradation with modeling hardware impairment in large intelligent surface," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.

[8] M. Jung, W. Saad, Y. R. Jang, G. Kong, and S. Choi, "Performance analysis of large intelligent surfaces (LISs): Asymptotic data rate and channel hardening effects," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2052–2065, Mar. 2020.

[9] M. Fu, Y. Zhou, and Y. Shi, "Intelligent reflecting surface for downlink non-orthogonal multiple access networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[10] M. Jung, W. Saad, Y. R. Jang, G. Kong, and S. Choi, "Reliability analysis of large intelligent surfaces (LISs): Rate distribution and outage probability," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1662–1666, Mar. 2019.

[11] M. Chafii, J. Palicot, R. Gribonval, and F. Bader, "A necessary condition for waveforms with better PAPR than OFDM," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3395–3405, Mar. 2016.

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

[13] S. Naderi, D. B. da Costa, and H. Arslan, "Joint random subcarrier selection and channel-based artificial signal design aided PLS," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 976–980, Feb. 2020.

[14] Q. Wu *et al.*, "Intelligent reflecting surface aided wireless communications: A tutorial," 2020. [Online]. Available: arXiv:2007.02759.

[15] S. Abeywickrama *et al.*, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," 2020. [Online]. Available: arXiv:2002.10112.

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

[17] Y. Liang *et al.*, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

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

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

[20] B. Bai *et al.*, "Outage optimal subcarrier allocation for downlink secure OFDMA systems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 1320–1325.

[21] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[22] A. Omri and M. O. Hasna, "Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3822–3833, Apr. 2018.

[23] S. Li, L. Yang, M. O. Hasna, M.-S. Alouini, and J. Zhang, "Amount of secrecy loss: A novel metric for physical layer security analysis," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1626–1630, Aug. 2020.

[24] L. Yang *et al.*, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, early access, Jul. 7, 2020, doi: 10.1109/TVT.2020.3007521.

[25] H. Long *et al.*, "Reflections in the sky: Joint trajectory and passive beamforming design for secure UAV networks with reconfigurable intelligent surface," 2020. [Online]. Available: arXiv:2005.10559.

[26] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, and G. Nauryzbayev, "Physical layer security in vehicular communication networks in the presence of interference," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[27] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Jul. 2018.

[28] L. Xu *et al.*, "Physical layer security performance of mobile vehicular networks," *Mobile Netw. Appl.*, vol. 25, pp. 1–7, Apr. 2019.

[29] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, 2020, pp. 1–6.

[30] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," 2020. [Online]. Available: arXiv:2004.11288.

[31] A. Almohamad *et al.*, "On optimizing the secrecy performance of RIS-assisted cooperative networks," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Spring)*, 2020, pp. 45913–45923.

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

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

[34] S. Hong *et al.* (2020). *Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface*. [Online]. Available: http://arxiv.org/abs/2002.07063

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

[36] B. Feng, Y. Wu, and M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2019, pp. 1–6.

[37] G. C. Alexandropoulos *et al.*, "Safeguarding MIMO communications with reconfigurable metasurfaces and artificial noise," 2020. [Online]. Available: arXiv:2005.10062.

[38] W. Chen *et al.*, "Secrecy rate optimization for intelligent reflecting surface aided multi-input–single-output terahertz communication," *Microw. Opt. Technol. Lett.*, vol. 62, no. 8, pp. 2760–2765, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/mop.32373

[39] W. Shi *et al.*, "Enhanced secure wireless information and power transfer via intelligent reflecting surface," 2019. [Online]. Available: arXiv:1911.01001.

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

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

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

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

[44] Y. Song *et al.*, "Truly intelligent reflecting surface-aided secure communication using deep learning," 2020. [Online]. Available: arXiv:2004.03056.

[45] G. H. Golub and C. F. Van Loan, *Matrix Computations*, vol. 3. New York, NY, USA: JHU Press, 2012.

[46] H. Xiao, L. Dong, and W. Wang, "Intelligent reflecting surface-assisted secure multi-input single-output cognitive radio transmission," *Sensors*, vol. 20, no. 12, p. 3480, 2020.

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

[48] B. Lyu *et al.*, "IRS-based wireless jamming attacks: When jammers can attack without power," 2020. [Online]. Available: arXiv:2001.01887.

[49] Q. Wang *et al.*, "Energy-efficient beamforming and cooperative jamming in IRS-assisted MISO networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–7.

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

[51] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Sep. 2019.

[52] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.

[53] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, early access.

[54] H. Yang *et al.*, "Deep reinforcement learning based intelligent reflecting surface for secure wireless communications," 2020. [Online]. Available: arXiv:2002.12271.

[55] H. Yang *et al.*, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," 2020. [Online]. Available: arXiv:2004.12539.

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

[57] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Deep learning for large intelligent surfaces in millimeter wave and massive MIMO systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[58] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," 2019. [Online]. Available: arXiv:1904.10136.

[59] E. Basar *et al.*, "Indoor and outdoor physical channel modeling and efficient positioning for reconfigurable intelligent surfaces in mmWave bands," 2020. [Online]. Available: arXiv:2006.02240.

[60] V. Arun and H. Balakrishnan, "RFocus: Practical beamforming for small devices," 2019. [Online]. Available: arXiv:1905.05130.

[61] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. F. Akyildiz, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Netw.*, vol. 87, pp. 1–16, May 2019.

[62] N. Kaina *et al.*, "Shaping complex microwave fields in reverberating media with binary tunable metasurfaces," *Sci. Rep.*, vol. 4, no. 1, pp. 1–8, 2014.

[63] Q. Zhang, W. Saad, and M. Bennis, "Reflections in the sky: Millimeter wave communication with UAV-carried intelligent reflectors," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[64] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[65] H. M. Furqan *et al.*, "Physical layer security for NOMA: Requirements, merits, challenges, and recommendations," 2019. [Online]. Available: arXiv:1905.05064.

[66] M. H. Yılmaz *et al.*, "Cognitive security of wireless communication systems in the physical layer," *Wireless Commun. Mobile Commun.*, vol. 2017, Dec. 2017, Art. no. 3592792.

[67] H. M. Furqan *et al.*, "Intelligent physical layer security approach for V2X communication," May 2019. [Online]. Available: arXiv:1905.05075.

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

ABDULLATEEF ALMOHAMAD (Member, IEEE) received the B.Sc. degree in communication engineering from the Higher Institute for Applied Sciences and Technology, Syria, in Fall 2015. He is currently pursuing the M.Sc. degree in electrical engineering with Qatar university, where he worked as a Research Assistant from 2018 to 2020. From 2015 to 2017, he was with the Core Network Department, MTN Syria, as an IP-Backbone Network Engineer. His research interests, under the wireless communication theory, lie in the area of UAV-based communications, multiple access techniques, and physical layer security.

ANAS M. TAHIR (Student Member, IEEE) received the B.S. degree in electrical engineering from Qatar University, Qatar, in 2018. He is currently pursuing the M.S. degree in electrical engineering with Qatar University, where he is currently working as a Research Assistant. His current research interests are machine learning and artificial intelligence application in biomedical engineering research field.

AYMAN AL-KABABJI (Student Member, IEEE) received the B.Sc. degree in electrical engineering from Qatar University in Spring 2019. He is currently pursuing the M.Sc. degree in electrical engineering with Qatar University, where he is awarded GSRA from QNRF. His current research interests revolve around machine learning and artificial intelligence in energy efficiency and biomedical engineering.

HAJI M. FURQAN received the B.S. degree in electrical engineering (telecommunication) and the M.S. degree in electrical engineering (wireless communication) from the COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan, in 2013 and 2014, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with Istanbul Medipol University, where he is a Researcher. In 2014, he joined the Department of Electrical, CIIT, as a Trainee Researcher and a Teacher Assistant. His current research interests include physical layer security, cooperative communication, adaptive index modulation, cryptography, 5G systems, RIS, and wireless channel modeling and characterization.

TAMER KHATTAB (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics and communications engineering from Cairo University, Giza, Egypt, and the Ph.D. degree in electrical and computer engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 2007. He joined electrical engineering with Qatar University (QU) in 2007. He is currently a Full Professor and an affiliated Senior Member of the Technical Staff with Qatar Mobility Innovation Center, an Research and Development Center owned by QU and funded by Qatar Science and Technology Park. From 2006 to 2007, he was a Postdoctoral Fellow in Electrical and Computer Engineering with UBC working on prototyping advanced Gigabit/sec wireless LAN baseband transceivers. From 2000 to 2003, he was with the Network and Service Management Research and Development, Nokia Siemens Networks Canada, Inc., Vancouver, as a Member of the Technical Staff working on development of core components for network and service management platforms. He has more than 200 published refereed journal and conference papers and holds several U.S. and European patents. He serves as the Founding Chair of the Joint IEEE ComSoc and ITSoc Chapter in Qatar. He is an Associate Editor for the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY and the IEEE COMMUNICATIONS LETTERS.

MAZEN O. HASNA (Senior Member, IEEE) received the B.S. degree in electrical engineering from Qatar University, Doha, Qatar, in 1994, the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1998, and the Ph.D. degree in electrical engineering from the University of Minnesota Twin Cities, Minneapolis, MN, USA, in 2003. In 2003, he joined the Department of Electrical Engineering, Qatar University, where he is currently a Professor. He has served in several administrative capacities with Qatar University from 2005 to 2017, including the Head of the EE Department, the Dean of the College of Engineering, the Vice President, and the Chief Academic Officer. His research interests include the general area of digital communication theory and its application to the performance evaluation of wireless communication systems over fading channels. His current specific research interests include cooperative communications, UAV-based networks, physical layer security, and FSO/RF hybrid networks. He appears in the 2015 highly cited researchers list of Clarivate Analytics. He is a Founding Member of the IEEE Qatar section and served as its founding VP, and currently serves on the Joint Management Committee of Qatar Mobility Innovation Center.

HÜSEYIN ARSLAN (Fellow, IEEE) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the Research Group, Ericsson Inc., Charlotte, NC, USA, where he was involved with several projects related to 2G and 3G wireless communication systems. Since 2002, he has been with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. He has also been the Dean of the College of Engineering and Natural Sciences, Istanbul Medipol University, since 2014. He was a part-time Consultant for various companies and institutions, including Anritsu Company, Morgan Hill, CA, USA, and the Scientific and Technological Research Council of Turkey (TÜBITAK). His research interests are in physical layer security, mmWave communications, small cells, multicarrier wireless technologies, co-existence issues on heterogeneous networks, aeronautical (high-altitude platform) communications, in vivo channel modeling, and system design. He has served as a technical program committee chair, a technical program committee member, a session and symposium organizer, and a workshop chair in several IEEE conferences. He is currently a member of the editorial board for the IEEE SURVEYS AND TUTORIALS and the *Sensors Journal*. He has also served as a member of the editorial board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, the *Physical Communication Journal* (Elsevier), the *Journal of Electrical and Computer Engineering* (Hindawi), and *Wireless Communication and Mobile Computing Journal* (Wiley).