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

Abdullateef Almohamad, Anas M. Tahir, Ayman Al-Kababji, Haji M. Furqan, Tamer Khattab, Mazen O. Hasna, Senior Member, IEEE, and Hseyin Arslan, Fellow, IEEE

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 the perspective of 5G (fifth generation) wireless communication 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, cooperative communication, massive multiple-input multiple-output, millimeter-wave, orthogonal frequency division multiplexing (OFDM) numerologies, and so on [1].

Although, rigorous efforts have been done in research and development of wireless communications to fulfill the requirements of diverse users and applications of future wireless communication generations, where we require extremely high energy and spectral efficiencies, ultra-security, ultra-reliability, and highly flexible design [2], overall progress has been relatively slow. This is due to the fact that the conventional wireless communication designers have been focusing only on transmitter and receiver ends while considering the wireless communication environment an uncontrollable factor that has usually a negative effect on communication efficiency and reliability, and needs to be compensated for.

Recently, reconfigurable intelligent surfaces (RIS) got much attention due to their capability to enable a smart and controllable wireless propagation environments [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 the incoming electromagnetic wave, thus making the direction and strength of the wave highly controllable at the receivers. This feature can be exploited to add different signals constructively or destructively to enhance or weaken, respectively, 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.

Motivated by the appealing advantages, RIS-assisted networks have been investigated in many different contexts such as capacity and rate improvement analysis [4], [5], power efficiency optimization [6], [7] and communication reliability [8], [9]. Few recent works have studied the RIS-assisted communications from a physical layer security (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 the secrecy rate 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 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 [10], [11]. 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 [11].

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 is shown in Fig. 1.

The remainder of this paper is organized as follows, the most common secrecy performance metrics are presented in Section II and the categorizing of the RIS-assisted PLS studies are 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

Secrecy rate (SR) is one of the fundamental metrics to measure the secrecy of a communication system. It represents the amount of information 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 secrecy rates can be achieved by active, at the transmitter, and/or passive, at the RIS, beamforming by degrading the eavesdropper channel while improving the legitimate one.

Similar to Shannon channel capacity, the secrecy capacity (SC) is defined as the upper bound of the SR \[12\]. The SC of the Wyner degraded wiretap channel is given as \[13\]

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

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 secrecy capacity, for a given channel realization, can be written in terms of Shannon’s channel capacities of the legitimate user and the eavesdropper as follows \[14\]

\[ C_s = \max \{ \log_2(1 + \gamma_D) - \log_2(1 + \gamma_E), 0 \}, \tag{3} \]

where \( \gamma_D \) and \( \gamma_E \) represent the instantaneous SNR at the legitimate user and the eavesdropper, respectively. The ergodic capacity is obtained by averaging \eqref{3} as per the available channel state information (CSI).

B. Secrecy Outage Probability/Capacity

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

\[ \text{SOP}(R_{th}) = \Pr \{ C_s < R_{th} \}. \tag{4} \]

In fact, the definition in \eqref{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 \[15\] as follows

\[ \text{SOP}(R_{\text{code}}, R_{th}) = 1 - \Pr \{ C_D \geq R_{\text{code}}, C_s \geq R_{th} \}, \tag{5} \]

where \( C_D \) is the instantaneous legitimate channel capacity, \( R_{\text{code}} \) is the coding rate of the transmitted message. It is clear, in this definition, that the secrecy outage event happens when the coding rate \( R_{\text{code}} \) 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, \( C_{\text{out}} \), that guarantees a SOP of less than \( \epsilon \) \[16\], which is expressed as follows

\[ \max \{ C_{\text{out}} \} \text{ with } \Pr \{ C_s < C_{\text{out}} \} = \epsilon \tag{6} \]
C. Average Secrecy Outage Rate/Duration

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 [17]. Namely, the average secrecy outage rate (ASOR) and the average secrecy outage duration (ASOD). The former, ASOR denoted by \( \mathcal{R}(R_{th}) \), measures the SC’s average rate of crossing a given threshold \( R_{th} \), 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

\[
\mathcal{T}(R_{th}) = \frac{\text{SOP}(R_{th})}{\mathcal{R}(R_{th})},
\]

(7)

D. Amount of Secrecy Loss

Recently, the authors in [18], 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

\[
\text{ASL} = \frac{\mathbb{E}\{C_s^2\}}{\mathbb{E}\{C_s\}^2} - 1,
\]

(8)

where \( \mathbb{E}\{\cdot\} \) 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 secrecy rate/capacity 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.

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. [19] studied the secrecy performance of an RIS-assisted SISO communication link in the presence of a direct link between the RIS and the eavesdropper and another direct link with the legitimate user. Single RIS was considered with \( N \) reflecting elements placed between the source and the legitimate user. The channel state information (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 received the SNR at the legitimate user. The analytical expression of the SOP was derived as an evaluation metric to assess the secrecy performance. The analytical and simulation results showed that the presence of an RIS significantly enhances the secrecy rate and the enhancement is driven by the number of RIS’s reflecting elements. However, the secrecy performance slightly drops when the eavesdropper enjoys the RIS as well. This is due to optimizing the RIS induced phases in order to maximize the SNR at the legitimate user and ignoring the effect it exercises on the eavesdropper received SNR. Hence, this shortcoming could be overcome by considering a joint optimization problem to maximize the SNR at the user while minimizing it at the eavesdropper at the same time. In [20], an unmanned aerial vehicle (UAV) equipped with an RIS is used as a mobile relay between a group of users and a base station (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) is used and successive convex approximation (SCA), where the objective is to attain fairness in secrecy rate among users and minimum energy.

A similar analytical approach is followed in [21], [22] to optimize the secrecy capacity in a vehicular Adhoc network (VANET), where the authors propose two setups to investigate
the PLS. The first setup assumes a source, a destination, and an eavesdropping vehicle are 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 [29]. Furthermore, the authors study the effect of the number of the RIS’s reflecting elements and the distance between the source and the RIS. Specifically, as the number of reflecting elements increases the secrecy rate (capacity) improves because better beamforming can be achieved, and the secrecy rate degrades while increasing the RIS-source distance which is due to the effect of the fading and the path loss.

A recent work conducted by the authors [23], investigated the effectiveness of RIS-assisted network by introducing a weighted variant of secrecy capacity definition. Simulation results showed that the existence of a reliable direct link dominates the systems secrecy capacity. However, it can be further enhanced by optimizing RIS-induced phase shifts. In addition, it was shown that the RIS-assisted system with blocked direct links achieves comparable secrecy capacity to that of dominant direct link systems with unknown RIS-Eve CSI.

B. MIMO System Model

Dong and Wang in [24] considered a MIMO system model, as shown in Fig. 2 (b), where the BS, the eavesdropper, and the legitimate user have multiple antennas. Noting that their system has a non-line-of-sight transmission (NLoS), the objective again is to maximize the secrecy rate at the legitimate user by jointly optimizing the transmit covariance matrix and the phase shift matrix of the RIS’s reflecting elements. Solving this non-convex problem is intractable, hence an AO algorithm was proposed assuming that the CSI of both the legitimate user, and the eavesdropper are available at the RIS and the transmitter. The convergence of the proposed solution is shown to monotonically converge within a number of iterations that is dependent on the number of antennas at the transmitter, legitimate user, and the eavesdropper. On the other hand, the authors in [25] opted for including the LoS transmission channel and the aid of artificial noise (AN) in their model, consequently, making the objective function much more challenging to solve. The optimization algorithm of choice was block coordinate descent (BCD) aided by the minimization maximization (MM) algorithm. The results show how increasing the number of RISs elements can increase the secrecy rate at the expense of burdening the optimization algorithm with a larger phase shift matrix to optimize. Similarly, the authors in [26] considered a LoS channel as in [25] where they provide a machine learning (ML) approach to tackle the problem. They utilized deep post-decision-state and prioritized-experience-replay schemes to enhance the learning performance and the secrecy rate in a dynamic RIS-aided communication system. Simulation results showed that the proposed algorithm outperforms conventional optimization approaches by achieving a higher average secrecy rate per user and higher quality of service (QoS) satisfaction probabilities.

A similar setup is considered in [27] with the same objective, but the authors considered 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, the successive convex approximation (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. The authors’ numerical simulations showed that a 3-bits quantized phase shifts yields an acceptable secrecy rate with negligible loss as compared to the continuous phase shifts case. Noting the large scale of this MIMO setup, it is clear that this AO of 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 [28], thus the AO gives a sub-optimal solution in the full rank channel case.

C. MISO System Model

The most common scenario found in the literature is the MISO system, where a multiple-antennas BS is securely transmitting a message to a single-antenna legitimate user in the presence of a single-antenna eavesdropper(s), as shown in Fig. 3 (a) and (b).

In [29], the authors adopted the system model shown in Fig. 3 (a), where a multiple-antenna BS is securely communicating with a single-antenna legitimate user in the presence of a single-antenna eavesdropper. An optimization problem is proposed to maximize the secrecy rate at the legitimate user by jointly optimizing the beamforming at the BS and the discrete phase shifts at the RIS. Due to the intractability of this problem, an AO method is followed, 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. Simulation results show that the proposed setup outperforms the scenarios without RIS. However, the proposed solution is sub-optimal and was not compared with the continuous phase shift case.

In [28], the energy consumption was investigated considering the system model shown in Fig. 3 (a) assuming NLoS links between the BS and legitimate user/eavesdropper. Thus, the authors opted for reducing the consumed energy in BS-RIS link through beamforming at the transmitter and optimizing the phase shifts at the RIS, where they considered rank-one channel and full-rank channel scenarios for this link. As per the authors, the beamforming and the phase matrix optimization are independent and impose no cross-restrictions.
Fig. 3. Most Common System Models in the literature (a) MISO with single eavesdropper, (b) MISO with multiple eavesdroppers.

on each other in the rank-one channel case. However, in the full-rank channel case, they are inseparable. For both channel models, projected gradient descent (PGD) and semi-definite relaxation (SDR) are used to solve the joint optimization problem. The performance of both optimization algorithms was analyzed to find out that both of them yield similar results, however, the SDR algorithm converges faster than the PGD.

Wang et al. [30], considering the system model shown in Fig. 3(b), investigated the energy efficiency under the presence of multiple eavesdroppers. The energy efficiency is studied by considering the beamforming as in [28], [29] at the transmitter and the cooperative jamming with the support of the RISs phase shift matrix. An energy-efficiency maximization objective function was defined to optimize the consumed power at the transmitter, the cooperative jamming, and the RIS reflection coefficients. An SDR-based algorithm was proposed to optimize the objective function while achieving a given secrecy threshold. According to the authors, the proposed scheme is highly energy-efficient even with high jamming power, which implies the significance of the cooperative jammer that was introduced. Moreover, it also outperforms the other schemes they reported in maintaining a high secrecy rate along with energy efficiency. However, no reporting on the placement of the K eavesdroppers was mentioned in this work. In addition, the incorporation of the jammer increases the systems complexity and only sub-optimal solutions are available.

Guan et al. [31] investigated the RIS effectiveness in improving the secrecy rate. However, they used AN induced by the transmitter to jam the eavesdroppers instead of a cooperative jammer as in [30]. The objective is to maximize the secrecy rate at the legitimate user by jointly optimizing the transmitter beamforming, the AN (jamming), and the passive beamforming at the RIS. An AO method was used to optimize the three dependent elements in the objective function. In addition, they reported that the use of AN jamming requires fewer reflecting elements on the RIS in order to maintain a specific secrecy rate. Xu et al. in [32] investigated the PLS under a MISO model which has several legitimate users (L = 3), a single eavesdropper and a NLoS transmission channel. The CSI is assumed to be known at the BS so that the AN can be used to intentionally impair the eavesdroppers channel. The formulated optimization problem tune the phase shift matrix at the RIS, beamforming vector, and the ANs covariance matrix at the BS to maximize the average of secrecy rates sum among the legitimate users. The worst-case scenario assumes that the eavesdropper can cancel all multi-user interference before decoding the message. A sub-optimal solution is obtained for the non-convex problem where AO is used, and by applying several convex approximations, with the help of SDR and manifold optimization (MO) algorithms. Their results show an increase in the secrecy rate with the addition of tackling the PLS from a different angle. However, they limit their analysis to the case with NLoS which can simplify the issue in hand. The same authors in [32] extended their MISO model in [33] to include multiple legitimate users and multiple eavesdroppers with two RISs instead of one, rendering the problem to be much more challenging. Their objective remained the same, which is maximizing the secrecy rates average, but in their optimization process, they removed the MO algorithm step. In addition, the CSI of the link between the eavesdroppers and the BS is not known in advance but is approximated by deterministic models to characterize its uncertainty. They extended their work to also account for the SOP along with the average secrecy rates. Their significant contribution is in proposing to have 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 missing and that could prevent them from reaching the practical scenario.

Yu et al. [34] investigated the PLS of RIS-assisted wireless systems in the presence of an eavesdropper using two efficient joint optimization techniques, for the system model presented in Fig. 3(a). BCD and AO with minorization maximization (MM) methods were considered for the non-convex optimization of the beamformer at the transmitter and the phase shifts at the RIS to maximize the system secrecy rate. Simulation results showed 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, obtained
results showed that installing a large scale RIS yields better enhancement of the secrecy rate and is more energy-efficient compared to enlarging the transmit antenna array size.

Chu et al. [35] presented a power-efficient scheme for the model presented in Fig. 3-(a) that minimizes the transmitted power while maintaining a secure channel to the legitimate user. Considering the non-convex nature of the problem, they proposed an AO algorithm and an SDR method to optimize the secure and power-efficient transmission. Few simulation scenarios were presented that illustrate 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. Even though different scenarios were mimicked considering secure transmission cases, no study was done to investigate different spatial scenarios that lead to insecure communication.

Shen et al. [36] developed an AO algorithm, for the model presented in Fig. 3-(a), to optimize the transmit covariance matrix of the source and the RIS phase shifts matrix providing closed-form and semi-closed-form solution respectively. The obtained AO-based solution, with the help of fractional programming (FP), is extended to RIS-assisted MIMO systems where the eavesdropper can have multiple antennas. The secrecy rate degrades when the number of eavesdropper antennas increases, as it starts to achieve higher rates. 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 the same line. However, no work addressed the two-dimensional (2D)/three-dimensional (3D) movements which are usually the case in real-life scenarios.

Cui et al. [37] investigated a similar system to the one in Fig. 3-(a), where more critical setups were investigated as the channels of the legitimate user and the eavesdropper are spatially correlated, and the latter has a stronger channel. The active and passive beamforming at the transmitter and the phase shifts at the RIS were jointly optimized to maximize the secrecy rate under similar constraints to those in [36]. Again, noting the intractability of this optimization problem, a sub-optimal solution was obtained by adopting an AO and SDR methods.

The authors in [38] tackle the model in Fig. 3-(a) where they proposed a low-complexity successive design that tackles the secure optimization problem for Terahertz (THz) communication utilizing the Rayleigh-Ritz Theorem explained in [39]. The proposed low complexity design helps in cases where centralized controllers with low computational capacities are used. However, they exhibit low performance with strong NLoS components. Therefore, similar to previous studies, the authors proposed an alternating joint optimization that iteratively optimizes the phase shifts at the RIS and the beamformer at the transmitter. The simulation results in [39] show significant improvement compared to two previous RIS studies. However, a fair comparison would need a complete benchmarking with all similar studies or at least the state-of-the-art in the field. In a new approach, authors in [40] introduced an ML approach to tune the RIS reflections in real-time to maximize the secrecy rate of the model in Fig. 3-(a). Simulation results showed that the ML approach can achieve comparable results to conventional optimization methods with simpler and faster implementation. To the best of the authors’ knowledge, [40] and [26] are the only studies that use an ML approach to tackle the PLS problem in RIS-aided communication systems, which opens the door for a new area to exploit.

As a generalization of the above-mentioned works, the authors in [41] considered a MISO system with multiple single-antenna legitimate users and eavesdroppers. An optimization problem has been formulated to maximize the minimum secrecy rate 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, i.e., it allows for discrete phase shifts only, and a spatial channel correlation between the legitimate users and the eavesdropper is considered 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. In fact, this work provides solid contributions under a general and practical setup, but it still relies on heuristic and numerical solutions to approach the complex problem-solving. Furthermore, the fairness between users in terms of secrecy rate is ignored, as, under this setup, the solution might end up with a high variance in the secrecy rates among users. Finally, as a shared drawback of most of the studied works, the CSIs of all users are assumed to be perfectly known at the BS.

Based on the conducted survey, we assemble the reviewed works in Table I which classify them in terms of the system model (SISO, MISO, and MIMO) and the adopted methodology to approach the considered objective. Moreover, Fig. 4 summarizes the different assumptions and system models with methodologies and performance metrics in the conducted literature review.

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. The conducted survey revealed that the simultaneous control of transmission from the base station and the reflections at the RISs can be an efficient solution to ensure confidentiality in wireless communication. Several simulations results verify the enhancement of the overall secrecy rate in such systems compared to conventional systems. However, there are some challenges and open directions for further investigation which are discussed 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
TABLE I
SUMMARY OF METHODOLOGIES AND KEY ASSUMPTIONS IN THE LITERATURE

| Methodology/System Model                  | SISO | MISO | MIMO |
|------------------------------------------|------|------|------|
| Machine learning (ML)                    | 40   |      | 26   |
| Jamming (Artificial Noise)               | 30–32|      |      |
| Analytical                               | 19, 21, 22 |      |      |
| Alternating Optimization (AO)            | 31   |      |      |
| Minorization Maximization (MM)           | 20   |      |      |
| Path-Following                           | 29, 31, 38, 41 |      |      |
| Semidefinite Relaxation (SDR)            | 20   |      |      |
| Successive Convex Approximation (SCA)    | 28, 30, 32, 33, 35, 37 |      |      |
| Projected Gradient Descent (PGD)         | 29   |      |      |
| Block Coordinate Descent (BCD)           | 34   |      |      |
| RIS Quantized Phase Shifts               | 34   |      |      |
| RIS Continuous Phase Shifts              | 32   |      |      |
| Manifold Optimization                    | 36, 38, 40 |      |      |
| Fractional Optimization                  |      |      |      |

the number of RISs, their distribution, orientation, size, and geometrical shape. Moreover, the effect of the number of elements and their distribution in an RIS on PLS needs also to be explored. 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.

Generally speaking, the deployment of RISs at different locations is a different problem compared to base stations/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 compared to active base stations/relays. However, how to optimally adjust the physical design, deployment, and association to enhance RIS-assisted PLS is still an open challenge. 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 PLS techniques.

B. 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, in practice, only imperfect CSI can be accessed by the transmitter. The imperfect channel can be categorized into four types: 1) Imperfect CSI due to imperfect channel estimation, 2) statistical CSI, which is based on statistical information such as mean and variance, 3) outdated CSI due to the highly dynamic propagation channel, and 4) imperfect CSI with limited feedback, where the receiver can only send a limited number of bits for channel estimation. Statistical CSI and imperfect CSI with limited feedback can reduce the amount of overhead needed for channel estimation at the expense of system performance degradation.

Another issue that needs to be considered is that the CSI is available only if the illegitimate node is active or it is a licensed user that has legal access to the network but had a bad intention to other users. However, in the case of a passive eavesdropper, the CSI of Eve is not available. Thus, the effect of imperfect CSI and its availability should be taken into account while designing different RIS-assisted security techniques to ensure that these techniques are robust to these imperfections.

C. 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 [42] [43] [44] 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 focuses on first-order metrics for PLS assessment. Evaluation of higher-order metrics may result in new insights that can reflect on the realization of practical RISs.

D. Flying RIS-Systems for PLS Enhancement

Recently, flying RISs (UAV equipped with an RIS) assisted communications have received much attention. Some key features of flying RISs include three-dimensional mobility, changeable direction and location, easy deployment, adaptive altitude, and power-efficient beamforming. The trajectory of a flying RIS can be optimized along with the phase shifts adjustment at the RIS elements for enhancing PLS. More specifically, the positioning/trajectory of UAVs
(equipped with RIS) 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 receiver. Besides, flying RISs can also be used as mobile cooperative jammers jointly with active UAV 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.

**E. PLS in LoS Environments**

Ensuring confidential communication in case of the LoS 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, artificial noise-based MIMO techniques, etc. [11] will fail to provide secure communication. RIS can ensure secure communication even in such scenarios by providing additional channel paths between the legitimate nodes. There are few works reported in this direction [37], but further investigation is still required, especially, when combining those scenarios with the imperfect or partially available CSI practical assumption.

**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 such as millimeter-wave communications, massive MIMO, visible light communications, drones-aided communications, internet of things (IoT), terahertz communication, free-space optics, full-duplex communication, non-orthogonal multiple access (NOMA) [47], vehicular ad-hoc network, and so on [1] are promising research directions.

Moreover, designing effective, adaptive, and intelligent [48] RIS-assisted PLS techniques under joint consideration of security, reliability, latency, complexity, and throughput based on quality of service (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 security of the system, it results in high complexity in terms of design and analysis as compared to conventional wireless systems [50]. The use of data-driven tools such as ML, deep learning, and reinforcement learning, is a promising solution to support the flexibility and the self-optimizability of such networks. Only a few works, [26], [40], have been reported employing ML-based approaches to solve the PLS problem in RIS-assisted networks.

**H. RIS Enhanced PLS for Intelligent Spectrum Sensing and Cognitive Radio Realization**

Intelligent spectrum sensing involves user detection, interference identification, and resource prediction, and 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 cognitive radio (CR) systems if primary/secondary users can be treated as eavesdroppers and where RISs are used to ensure secured communication in a targeted network (primary or secondary).

**V. CONCLUSIONS**

Physical layer security does support 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 with 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 is identified as a promising research direction, as it adds more flexibility in the network by optimizing the RIS’s 3D location, orientation and trajectory to boost the system secrecy as well as to improve the overall energy efficiency.

**REFERENCES**

[1] E. Basar et al., “Wireless Communications Through Reconfigurable Intelligent Surfaces,” IEEE Access, vol. 7, pp. 116 753–116 773, 2019.

[2] P. Yang et al., “6G Wireless Communications: Vision and Potential Techniques,” IEEE Network, vol. 33, no. 4, pp. 70–75, 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, 2020.

[4] S. Hu et al., “Capacity Degradation with Modeling Hardware Impairment in Large Intelligent Surface,” in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.

[5] M. Jung et al., “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, 2020.

[6] C. Huang et al., “Reconfigurable intelligent surfaces for energy efficiency in wireless communication,” IEEE Trans. Wireless Commun., vol. 18, no. 8, pp. 4157–4170, 2019.

[7] M. Fu et al., “Intelligent Reflecting Surface for Downlink Non-Orthogonal Multiple Access Networks,” in 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–6.
[8] M. Jung et al., “Reliability analysis of large intelligent surfaces (LISs): Rate distribution and outage probability,” IEEE Wireless Commun. Lett., vol. 8, no. 6, pp. 1662–1666, 2019.

[9] M. Chaffai et al., “A necessary condition for waveforms with better PAPR than OFDM,” IEEE Trans. Commun., vol. 64, no. 8, pp. 3395–3405, 2016.

[10] X. Lu et al., “Intelligent reflecting surface (IRS)-enabled covert communications in wireless networks,” arXiv preprint arXiv:1911.00986, 2019.

[11] J. M. Hamamreh et al., “Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1773–1829, 2018.

[12] Y. Liang et al., “Information theoretic security,” Foundations and Trends in communications and Information Theory, vol. 5, no. 4–5, pp. 355–580, 2009.

[13] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, 1978.

[15] B. Bai et al., “Outage optimal subcarrier allocation for downlink secure OFDMA systems,” in 2014 IEEE Globecom Workshops (GC Wkshps), 2014, pp. 1322–1327.

[16] O. Gungor et al., “Secrecy outage capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5379–5397, 2013.

[17] 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, 2018.

[18] S. Li et al., “Amount of Secrecy Loss: A Novel Metric for Physical Layer Security Analysis,” IEEE Commun. Lett., 2020.

[19] L. Yang et al., “Intelligent Reflecting Surface-Aided Secure Wireless Communications,” IEEE Wireless Commun. Lett., 2020.

[20] H. Long et al., “Reflections in the Sky: Joint Trajectory and Passive Beamforming Design for Secure UAV Networks with Reconfigurable Intelligent Surfaces,” arXiv preprint arXiv:2005.10559, 2020.

[21] A. U. Makkar et al., “Physical Layer Security in Vehicular Networks: A Perspective with Reconfigurable Intelligent Surfaces,” arXiv preprint arXiv:1912.12783, 2019.

[22] ——, “Reconfigurable Intelligent Surfaces-Enabled Vehicular Networks: A Physical Layer Security Perspective,” arXiv preprint arXiv:2004.11288, 2020.

[23] A. Alimohamad et al., “On Optimizing the Secrecy Performance of RIS-Assisted Cooperative Networks,” in IEEE VTC2020 Fall (Submitted), 2020.

[24] L. Dong and H. Wang, “Secure MIMO Transmission via Intelligent Reflecting Surface,” IEEE Wireless Commun. Lett., vol. 9, no. 6, pp. 787–790, 2020.

[25] S. Hong et al., “Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface,” arXiv preprint arXiv:2002.07063, pp. 1–30, 2020. [Online]. Available: http://arxiv.org/pdf/2002.07063

[26] H. Yang et al., “Deep Reinforcement Learning Based Intelligent Reflecting Surface for Secure Wireless Communications,” arXiv preprint arXiv:2002.12271, 2020

[27] W. Jiang et al., “Intelligent Reflecting Surface Assisted Secure Wireless Communications With Multiple-Transmit and Multiple-Receive Antennas,” IEEE Access, vol. 8, pp. 86 659–86 673, 2020.

[28] B. Feng et al., “Secure Transmission Strategy for Intelligent Reflecting Surface Enhanced Wireless System,” in 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), 2019, pp. 1–6.

[29] 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.33273

[30] Q. Yang et al., “Energy-Efficient Beamforming and Cooperative Jamming in IRS-Assisted MISO Networks,” arXiv preprint arXiv:1911.05133, 2019.

[31] X. Guan et al., “Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?” IEEE Wireless Commun. Lett., vol. 9, no. 6, pp. 778–782, 2020.

[32] D. Xu et al., “Resource Allocation for Secure IRS-Assisted Multiuser MISO Systems,” in 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–6.

[33] X. Yu et al., “Robust and secure wireless communications via intelligent reflecting surfaces,” arXiv preprint arXiv:1912.01497, 2019.
## Overall System Model & Assumptions

| Ref. | System Model | CSI Availability | Others | Methodology | Metric |
|------|--------------|------------------|--------|-------------|--------|
| [19] | SISO, Eve = 1 @ BS & RIS | Quasi-static flat fading | Analytical | SOP |
| [20] | SISO, Eve = 1, Bob=K @ BS & RIS | Rayleigh/Rician fading | Approximation (AO-SCA) | Secrecy Energy Efficiency |
| [21], [22] | SISO, Eve = 1 @ BS & RIS | Double Rayleigh fading | Analytical | SC & SOP |
| [23] | SISO, Eve = 1 @ BS & RIS | Rayleigh flat fading | Analytical | SC |
| [24] | MIMO, Eve = 1 @ BS & RIS | Gaussian wiretap | Approximation (AO-MM) | SR |
| [25] | MIMO, Eve = 1 @ BS & RIS | Narrow-band & non-dispersive channel | Approximation (BCD-MM) | SR |
| [26] | MIMO, Eve = K @ BS & RIS | Outdated/real-time CSI | Approximation (ML) | SR |
| [27] | MIMO, Eve = K @ BS & RIS | Discrete phase shifts | Approximation (AU, SCA) | SR |
| [28] | MISO, Eve = 1 Multiple scenarios | Multiple channel models | Approximation (PGD-SDR) | SR |
| [29] | MISO, Eve = 1 @ BS & RIS | Discrete phase shifts | Approximation (AO) | SR |
| [30] | MISO, Eve = M @ BS & RIS | Quasi-static flat fading | Approximation (AO-SDR-FP) | SR |
| [31] | MISO, Eve = M @ BS & RIS | Quasi-static flat-fading | Approximation (AO) | SR |
| [32] | MISO, Eve = 1, Bob = L @ BS & RIS | Interference cancellation at Eve | Approximation (AO-SDR-MO) | Sum SR |
| [33] | MISO, Eve = K, Bob = L @ BS & RIS | Interference cancellation at Eve & Multiple RIS | Approximation (AO-SDR) | Average SR & SOP |
| [34] | MISO, Eve = 1 @ BS & RIS | Rayleigh fading | Approximation (AO-MM-BCD) | SR |
| [35] | MISO, Eve = K @ BS & RIS | Rayleigh flat fading | Approximation (AO-SDR) | SR |
| [36] | MISO, Eve = 1 @ BS & RIS | Rayleigh fading | Approximation (AO-FP) | SR |
| [37] | MISO, Eve = 1 @ BS & RIS | Bob & Eve channels are correlated | Approximation (AO-SDR) | SR |
| [38] | MISO, Eve = 1 @ BS & RIS | Saleh Valenzuela model | Approximation (AO-FP) | SR |
| [40] | MISO, Eve = 1 @ BS & RIS | Quasi-static flat-fading | Approximation (ANN with FP) | SR |
| [41] | MISO, Eve = K, Bob = L @ BS & RIS | Discrete and continuous phases | Approximation (AO) | Max min SR |

Fig. 4. Summary of the different assumptions, system models, methodologies, and performance metrics.