WIRELESS COMMUNICATION IN THE PRESENCE OF ILLEGAL RECONFIGURABLE INTELLIGENT SURFACE: SIGNAL LEAKAGE AND INTERFERENCE ATTACK

Yazheng Wang, Hancheng Lu, Dan Zhao, Yansha Deng, and Arumugam Nallanathan

ABSTRACT

Reconfigurable intelligent surface (RIS) is considered as a promising technology to realize a smart wireless communication system. In detail, RIS is a man-made surface consisting of massive passive reflecting elements, where each element can reflect the incident signal with tunable phase shifts. To protect wireless communication from security breaches, physical layer security (PLS), which exploits the characteristics of wireless channels, has been widely studied to ensure secure transmission. Due to the reconfigurability of RIS, it has great potential to enhance PLS in wireless systems by enhancing the channel condition of legitimate user (LU) and impair that of eavesdropper (EAV). However, the low hardware cost and reconfigurability lead to non-negligible risk as the EAV and attacker can also apply RIS to promote the data rate at EAV or strengthen the interference signal transmitted to jam LU. In this article, we introduce a new concept, *illegal reconfigurable intelligent surface* (IRIS), which represents the illegal deployment and utilization of RIS. Two main security concerns in the presence of IRIS, namely, *signal leakage* and *interference attack* are investigated. The signal leakage is that IRIS can collect the information signal which could not be received before and interference attack is that it can deploy IRIS to enhance the interference signal power. We discuss several key challenges brought by IRIS, and an artificial noise (AN)-aided joint optimization-based solution to enhance PLS in the wireless communication system with both RIS and IRIS. Simulation results demonstrate the significant impact of IRIS on PLS and verify the effectiveness of the proposed AN-aided joint optimization-based solution.

INTRODUCTION

The future wireless communication system is supposed to serve massive devices and realize high spectrum and energy efficiency. To meet the demand, a variety of key technologies have been proposed, such as massive multiple-input multiple-output (MIMO), millimeter wave (mmWave), non-orthogonal multiple access (NOMA) and so on [1], [2]. However, these technologies incur high hardware cost, high computation complexity and huge energy consumption due to massive RF chains and complex signal processing. Moreover, they only focus on the transmitter and receiver sides to adapt the change of the wireless channels, while considering the wireless environment as an uncontrollable factor. It is imperative to develop innovative technologies to realize smart radio environment with affordable complexity and energy consumption.

To overcome these issues, reconfigurable intelligent surface (RIS), which smartly transforms the stochastic wireless channels into a software-defined environment, has been proposed as a promising new paradigm to achieve controllable wireless system [3], [4]. Specifically, RIS is a planar array consisting of a large number of low-cost reconfigurable reflecting elements, which are capable of independently changing the phase shifts of the incident signal. By smartly adjusting the elements, the signal reflected by RIS can be added coherently at the receiver to enhance the desired signal power without incurring huge energy consumption. Due to these appealing properties, the RIS-assisted communication system has attracted significant attention from researchers working on various aspects, e.g., system performance optimization [4]–[6], channel estimation [7] and so on.

Due to the broadcast and superposition properties of wireless medium, wireless systems are inherently vulnerable to eavesdropping. To address this, physical layer security (PLS), which is proposed to complement the existing encryption techniques by guaranteeing secure wireless communication from the perspective of information-theoretic, has been intensively studied to secure the information transmission [3]. PLS capitalizes on the intrinsic randomness of the noise and fading characteristics of the wireless channels to limit the amount of information that can be extracted by eavesdropper (EAV) [9]. Hence, the secure wireless transmission depends on the difference between the channel condition from access point (AP) to legitimate user (LU) and that from AP to EAV. A variety of techniques have been developed to enhance PLS, such as transmit beamforming based on degrees of freedom, cooperative jamming and relaying. However, employing massive active antennas and relays leads to unaffordable hardware cost and energy consumption [12]. Moreover, these techniques become less effective in PLS enhancement for unfavorable wireless propagation environment, and these traditional techniques is unable to control the undesirable and dynamic wireless channels. Therefore, RIS, which can reshape the wireless environment without incurring huge complexity and cost, is particularly compelling for exploiting in wireless

Yazheng Wang, Hancheng Lu, and Dan Zhao are with CAS Key Laboratory of Wireless-Optical Communications, University of Science and Technology of China; Hancheng Lu is also with Institute of Artificial Intelligence, Hefei Comprehensive National Science Center; Yansha Deng is with King's College London; Arumugam Nallanathan is with Queen Mary University of London.

systems to enhance PLS [8]–[12].

In Table 1, we list some existing research on PLS enhancement in RIS-assisted legitimate wireless systems, with an emphasis on their key features, solutions, advantages and disadvantages. These work focuses on regarding RIS as a beneficial factor and designing judicious algorithm to improve various PLS metrics. It can be seen that proper use of RIS can reap significant PLS enhancement. However, the low cost and reconfigurability of RIS can cause the following serious potential risks. Different from adopting RIS to boost PLS, the EAVs or attackers can utilize RIS to enhance the eavesdropping links or deteriorate the performance of legitimate links, which strongly threatens the overall security of wireless communication system. In a sharp contrast to the existing work on RIS-assisted PLS enhancement, we raise the security concerns from the perspective of illegal deployment and exploitation of RIS. We name the RIS deployed by EAVs or attackers as *illegal reconfigurable intelligent surface* (IRIS). On one hand, a passive EAV is able to collect the transmission signal which cannot be received before, by properly deploying its own IRIS next to the transmitter or itself. In this way, the phase shifts of IRIS can be optimized to improve the received eavesdropping signal power, and the secrecy rate (SR) will be severely reduced. This concern is named as *signal leakage*. On the other hand, an active EAV or attacker is able to transmit interference signal with the aid of IRIS, which can create additional reflecting links to jam the LU. By carefully designing the phase shifts of IRIS, the power of interference signal received at LU can be substantially improved, which leads to serious performance degradation. We name this critical concern as *interference attack*.

In the case of IRIS deployment, wireless systems become more prone to security threats. In this article, two main security concerns in the presence of IRIS, i.e., signal leakage and interference attack, are considered and investigated. To safeguard wireless communication against IRIS as well as enhance security at the physical layer, the following challenges should be considered. First, the passive IRIS is usually covert and the channel state information (CSI) of illegitimate links is hard to be acquired. The second challenge is the degradation of legitimate links CSI accuracy since the channel estimation procedure is prone to attack. Due to these dilemmas, another challenge follows that joint optimization should be redesigned based on imperfect CSI to ensure the secure communication. Meanwhile, IRIS can swiftly reshape the illegitimate communication links, which makes the optimization based on instantaneous CSI insufficient and outdated. To overcome these challenges, the artificial noise (AN) technology, which can boost PLS without relying on the CSI of illegitimate communication links, has been adopted. In this article, we propose an AN-aided joint optimization-based solution to improve the SR of the wireless system in the presence of both RIS and IRIS. The simulation results are provided to show the non-negligible impact brought by IRIS and verify the effectiveness of the proposed solution.

Wireless Communication with Illegal Reconfigurable Intelligent Surface

In this section, we introduce two main security concerns in the presence of IRIS.

As a new promising paradigm, RIS is supposed to be widely applied in future wireless systems to boost the system performance. However, both legitimate users (LUs) and eavesdroppers (EAVs) can exploit RIS. That is to say, there exists not only RIS but also IRIS in the wireless communication system. In the RIS-assisted system, legitimate communication links are enhanced by RIS, where the transmit beamforming at AP and the phase shifts of RIS elements are jointly optimized to increase the data rate at LU. Meanwhile, the EAV deploys IRIS to promote its communication quality, while the attacker intends to impair LU's channel condition. Both of them can cause serious PLS performance degradation and we specifically discuss these two typical types of IRIS utilization in the following. It is worth mentioning that the scenarios in Fig. 1 are specific examples to show the ability of IRIS, while the application of IRIS about threatening PLS is really broad and the actual wireless network can be more complex, e.g., hybrid signal leakage/interference attack secure threat, distributed network and so on.

Signal Leakage

We call the utilization of IRIS for improving eavesdropping data rate as signal leakage, since IRIS is used for receiving more EAV's signal and enhancing the information leakage at the EAV. In a conventional wireless communication system, an EAV can use IRIS to reflect the signal from the environment and collects the transmission signal which cannot be received before, as shown in Fig. 1(a). Another typical scenario of signal leakage in RIS-assisted wireless system is illustrated in Fig. 1(b). Multiple RISs are deployed to assist the communication while the beamforming vector at AP and the phase shifts of RISs are carefully designed to improve the SR, by taking the RIS-EAV links into consideration. However, the EAV deploys IRIS close to AP and the phase shifts of IRIS are further optimized to improve the received signal power at EAV, which efficiently limits the improvement brought by RIS and seriously reduces the SR of the system. Knowing that the AP is unaware of the existence of IRIS, it is impossible to perform a global design of the whole system and the optimization of RIS-assisted legitimate wireless system is insufficient to guarantee the secure transmission. This type of IRIS passively enhances the communication quality of illegitimate links and degrades PLS performance without creating additional radio frequency signal. Hence signal leakage is especially hard to be detected and prevented. The concept of signal leakage concentrates on collecting more legitimate signal leakaged from AP to improve the EAV's wiretapping capability. This is different from the RIS-based jammer in [14], which minimizes the received signal power at LU by destructively adding the signal from AP and RIS.

Table 1. Some research on PLS enhancement in RIS-assisted legitimate wireless systems.

Refs.	Key Features	Solutions	Advantages	Disadvantages
[8]	RIS-assisted MISO system with one LU and one EAV.	SR maximization based on fractional programming and manifold optimization.	Low-complexity algorithm with closed-form beamforming solution.	Ideal continue phase shifts and simple scenario.
[9]	RIS-assisted MISO system with multiple LUs and multiple EAVs.	Minimum-SR maximization based on path-following algorithm and zero-forcing beamforming.	More general scenario and different types of RIS reflecting coefficients.	Perfect CSI assumption of complicated system.
[10]	RIS-assisted one LU and one EAV MIMO system.	SR maximization based on minorization-maximization algorithm.	Multiple-antenna transmitter and receiver.	Ideal continue phase shifts and too specific scenario.
[11]	RIS-assisted one LU and one EAV MISO system.	Transmit power minimization based on semidefinite relaxation (SDR) algorithm.	Different CSI assumptions and channel cases.	Ideal continue phase shifts, simple and too specific scenario.
[12]	RIS-assisted one LU and multiple EAVs MISO system with a friendly jammer.	Energy efficiency maximization based on $\mathcal{S}$-procedure and SDR methods.	Bounded CSI error model and independently cooperative jamming.	Ideal continue phase shifts.

Interference Attack

The adoption of IRIS for interference signal transmission is named as interference attack. A typical scenario with IRIS is shown in Fig. 1(c), where IRIS is deployed in the vicinity of an attacker. Similar to the typical use of RIS in wireless system [4], [5], where RIS creates additional reflection links and the signal power is improved at receiver, the attacker can also deploy IRIS to reflect more interference signal to jam the LU. Moreover, with the help of IRIS, the coverage of the interference signal is extended while more LUs will be influenced. This operation of IRIS seriously degrades the signal-to-interference-plus-noise ratio (SINR) at LU and impairs the receive quality. As shown in Fig. 1(d), when the direct links between the attacker and LU are blocked, IRIS can be employed to bypass the obstacles and the interference signal can be transmitted to LU. Although RIS is utilized to improve PLS, it is hard to reap a satisfying system performance since the legitimate system is unable to control the IRIS-assisted interference links and the interference signal from IRIS is almost impossible to be cancelled. The scenarios in Fig. 1(c) and Fig. 1(d) are examples to reveal the strong ability of IRIS, while the concept of interference attack can be extended to more general scenarios, e.g., distributed IRIS network. It is worth noting that not only the data transmission procedure but also the channel estimation procedure can be rigorously hindered. Specifically, during the channel estimation procedure, the AP sends a pilot symbol to LU while the attacker is able to send another pilot symbol with the help of IRIS. If the attacker uses high transmit power and optimizes the IRIS reasonably, it might dominate the training phase and degrades the channel estimation accuracy.

Enhance PLS in the Presence of IRIS Based on Artificial Noise

In this section, several imperative challenges in the wireless communication system with RIS and IRIS are discussed. Then we propose a solution based on AN-aided joint optimization to promote PLS in the cases of signal leakage and interference attack. To be specific, a portion of the transmit power is used to generate AN signal and the beamforming vector at AP as well as the phase shifts of RIS are jointly optimized with maximum data transmission power and quality of service (QoS) threshold.

Challenges

The first challenge brought by IRIS is the acquisition of the illegitimate links CSI. The direct CSI of an illegitimate node is available only if it is active or it is a licensed user that has legal access to the legitimate communication system [3]. Meanwhile, the advantageous feature of RIS, passive reflection, makes IRIS extremely hard to be detected for the reason that IRIS can almost imperceptibly deteriorate the PLS performance of the system. Hence, the deployment of IRIS is usually covert and the legitimate system is probably unaware of the existence of IRIS. Therefore, the acquisition of the illegitimate links CSI (i.e., the CSI of both the direct AP-EAV links and the cascaded AP-IRIS-EAV links) and the phase shifts configuration of IRIS are highly impracticable.

The second challenge caused by IRIS is the degradation of channel estimation accuracy, i.e., the accuracy of the legitimate links CSI can be critically degraded. Several approaches for channel estimation in RIS-assisted system are proposed, including least-square estimation and deep learning based methods [7]. However, these methods depend on the pilot transmission, which is prone to the utilization of IRIS. During the pilot transmission procedure, an attacker can simultaneously transmit pilot symbol and enhance the interference power by IRIS, while a passive EAV can deploy IRIS to reflect the pilot symbol transmitted by LU to BS (or BS to LU) and the IRIS is designed to decrease the channel estimation accuracy [15].

The above difficulties lead to another challenge, joint optimization of the beamforming vector at AP and the phase

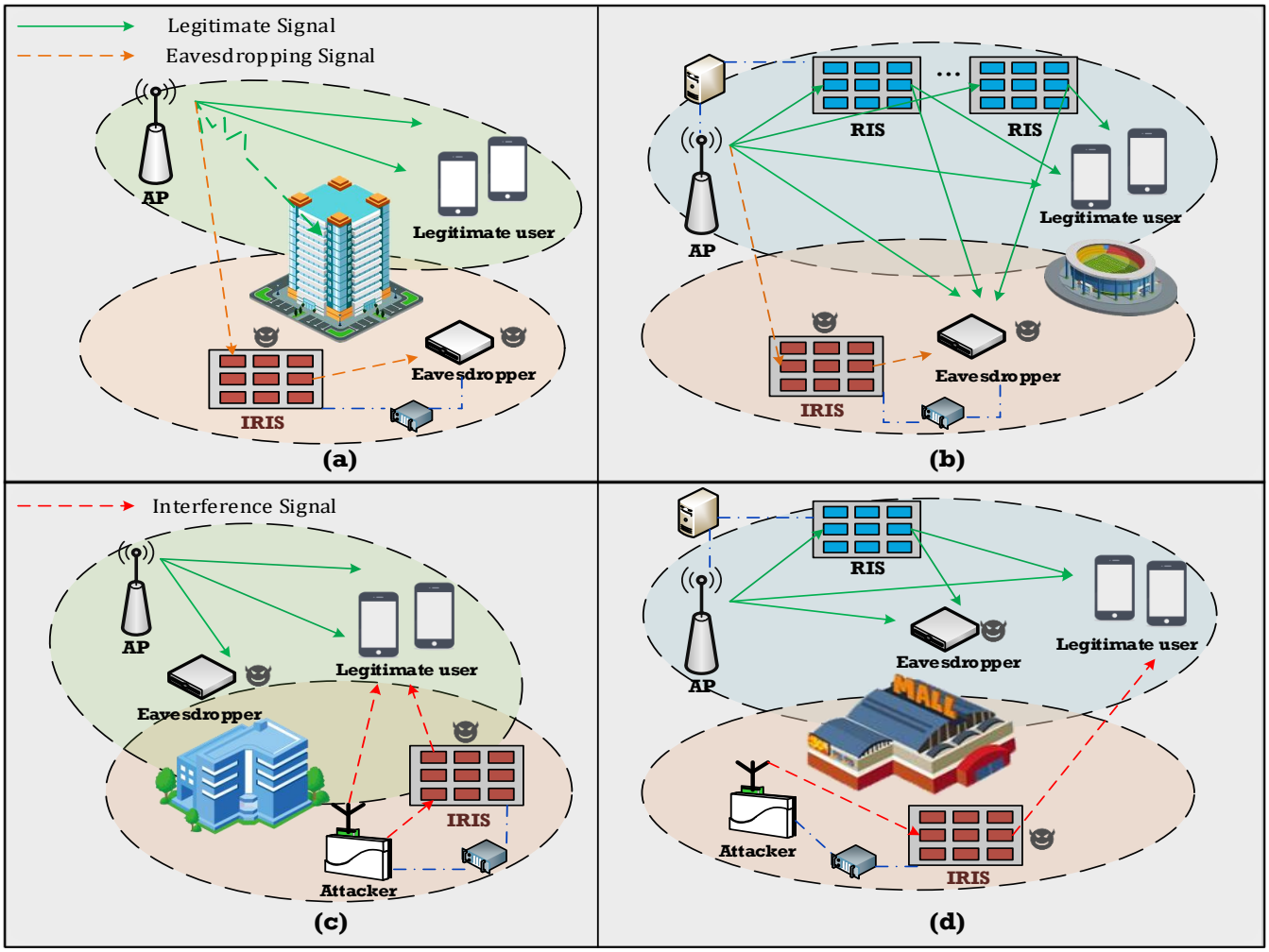

Figure 1. Conventional and RIS-assisted wireless systems in the presence of IRIS.

shifts of RIS based on imperfect CSI. Since most existing studies of RIS-assisted PLS optimization assume that the CSI of both legitimate and illegitimate communication links are perfectly known [8]–[10], the joint optimization for wireless systems with RIS and IRIS should be redesigned without the illegitimate links CSI and under imperfect legitimate links CSI, which complicates the optimization problem and harshly limits the performance improvement brought by joint optimization. Meanwhile, the deployment of IRIS effectively enhances the communication quality of illegitimate wireless system and further causes PLS performance degradation. Therefore, simple joint optimization of beamforming vector at AP and IRS phase shifts is insufficient to relieve the significant impact brought by IRIS and it is imperative to explore new solutions to safeguard the secure transmission.

AN-aided Joint Optimization-Based Solution

The main idea of AN technology is to combine the information signal with a noise signal. The noise signal is designed to be orthogonal to the legitimate channel so that the LU will not be affected while the EAVs will be influenced [13]. As a result, the data rate at EAVs will be effectively reduced and the SR of wireless system will be improved. The AN signal is able to interfere with all the potential EAVs, without relying on the location detection of EAVs and IRIS. Therefore, the AN can efficiently improve the SR and secure the transmission against EAVs and IRIS.

The generation of AN requires only the CSI of legitimate communication links but not that of illegitimate communication links, since the AN is effective as long as it is orthogonal to the legitimate channel. This property makes it attractive in wireless system with IRIS. Therefore, we utilize AN to decrease the data rate at the EAV. Specifically, the transmit signal $\boldsymbol{x}$ is the sum of information signal $\boldsymbol{\omega}s$ and AN signal $\boldsymbol{n_a}$, where $\boldsymbol{\omega}$ is the beamforming vector at AP. The total transmit power p at AP is divided into data transmission power p_t and AN signal transmission power p_{an}. As shown in Fig. 2, the equivalent channel matrix of the AP-UE links is the sum of the direct AP-UE channel matrix and the cascaded AP-RIS-UE channel matrix (i.e., the multiplication of AP-RIS channel matrix, the RIS phase shifts matrix and the RIS-user channel matrix). Hence, the AN signal is projected onto the null space of the equivalent channel matrix, i.e., the AN signal is orthogonal to the legitimate channel. Then it has no effect

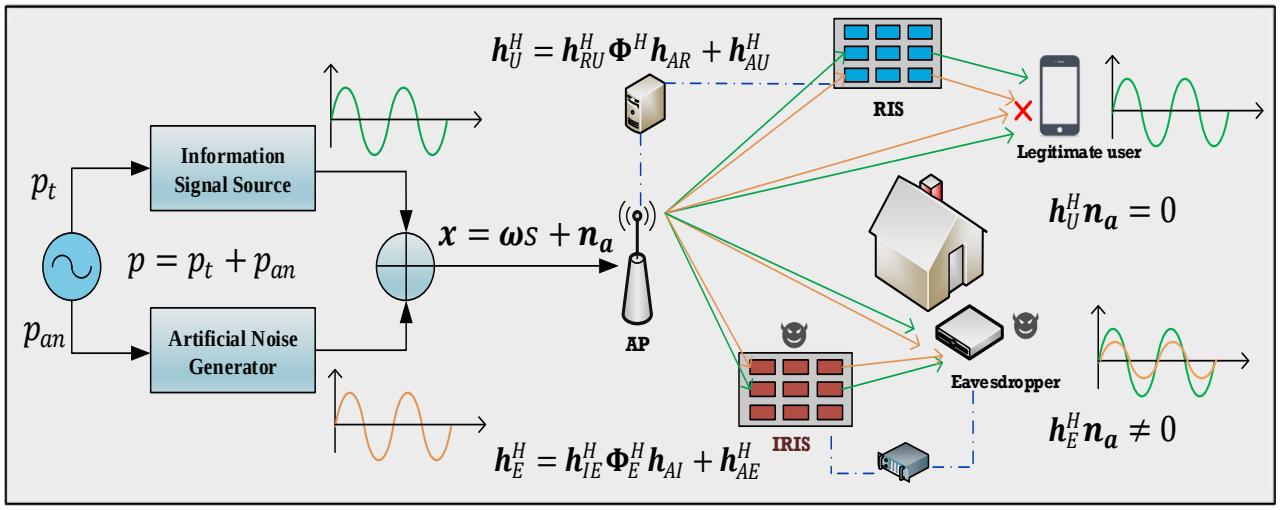

Figure 2. AN-aided joint optimization-based solution.

on the LU, yet is able to jam the EAV and reduce the data rate at EAV.

With given total transmit power, we minimize the data transmission power to meet a required QoS threshold γ at LU and then the residual power for AN signal transmission to jam the eavasdropper can be larger [13]. Therefore, the target of joint optimization is to minimum the data transmission power with required QoS threshold, by optimizing the beamforming vector at AP and the phase shifts of RIS. This problem is non-convex since the available phase shifts are discrete values and the QoS constraint is not jointly convex with respect to the beamforming vector and phase shifts. Generally, it is difficult to efficiently solve such a non-convex problem optimally. We solve this problem based on the alternating optimization method, where the beamforming vector and phase shifts are alternatively optimized with the other one fixed. This method can obtain a satisfying solution with low complexity and is widely adopted in RIS-assisted systems [4], [5], [8]–[12]. Specifically, the optimal beamforming vector at AP can be obtained by the maximum-ratio transmission (MRT) with given RIS phase shifts [4]. On the other hand, with given beamforming vector, the problem is equivalent to maximize the channel power gain, and this subproblem is still non-convex. However, the objective function of this subproblem, i.e., the channel power gain, is linear with respect to one of the phase shifts. Therefore, the optimal value of one phase shift can be obtained in a closed-form expression. According to this closed-form expression, we repeatedly optimize one of the RIS phase shifts and keep the other RIS phase shifts fixed, by selecting the optimal phase shift from the available discrete phase set. As a result, the subproblem is efficiently solved with complexity of $\mathcal{O}(N^2)$, where N is the number of RIS reflecting elements.

The AN singal can be transmitted to jam all the potential EAVs whether they are covert or not. It is especially suitable for signal leakage, since the EAVs receive more AN signal reflected by IRIS. Meanwhile, the joint optimization for data transmission power minimization can be extended to diverse cases, e.g., RIS with hardware impairment, statistic CSI of legitimate links, mmWave communication and so on. For example, our proposed solution can be implemented in distributed network with multiple RISs. Specifically, multiple RISs are regarded as a super-RIS and controlled by a central RIS controller. All the reflecting elements of RISs are successively optimized by our proposed solution and the phase shifts configuration are exchanged via controller [5]. Therefore, this AN-aided joint optimization-based solution can be regraded as a general solution.

Case Studies

We assume that the legitimate system exploits channel reciprocity in time division duplexing system to obtain CSI. The channel coherence period is divided into an uplink channel estimation stage and a downlink information transmission stage. The CSI of legitimate links can be efficiently acquired in uplink stage by some powerful channel estimation methods, such as the method in [7] with low complexity and overhead. Then we enhance PLS in downlink transmission stage by our proposed AN-aided joint optimization-based solution.

We consider the more practical cases where the RIS-assisted legitimate wireless system can only acquire the CSI of the legitimate wireless links (i.e., the CSI of AP-RIS, AP-LU and RIS-LU communication links), while the CSI of illegitimate wireless links are completely unknown at AP. Hence, the SR can not be maximized globally by taking illegitimate wireless links into consideration. Meanwhile, the IRIS-assisted illegitimate wireless system only knows its own CSI (i.e., the CSI of the AP-IRIS-EAV/Attacker-IRIS-LU links) and the phase shifts of IRIS are optimized to maximize the channel gain of the cascaded illegitimate communication links to improve/decrease the data rate at EAV/LU. To show the strong impact on PLS brought by IRIS, we study cases about signal leakage and interference attack. We compare the SR with the schemes that did not exploit IRIS to show the severe performance degradation caused by IRIS. Furthermore, we compare the AN-aided joint optimization with the distributed

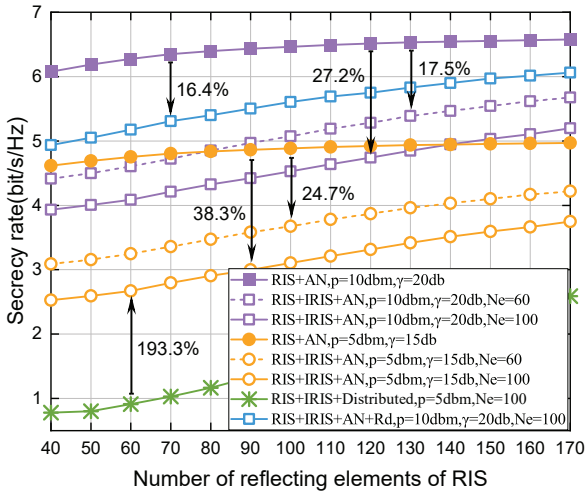

Figure 3. Secrecy rate vs. the number of reflecting elements of RIS.

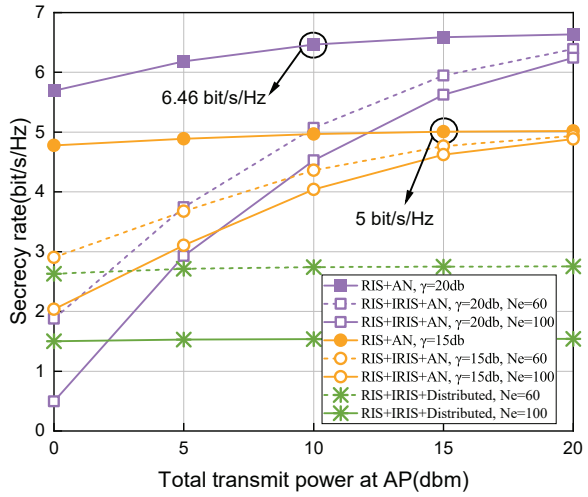

Figure 4. Secrecy rate vs. the total transmit power at AP with N=100.

algorithm in [4], which only maximizes the received signal power (RSP) at LU, to show the superiority of the AN-aided joint optimization in PLS enhancement.

Signal Leakage

In the first case with signal leakage, we consider an AP with $M = 16$ antennas, a RIS with N reflecting elements, an IRIS with N_e reflecting elements, a single-antenna LU and a single-antenna EAV. The RIS is utilized to assist the data transmission and the IRIS is deployed to enhance the eavesdropping links. We assume that there are obstacles between the LU and the EAV so that the signal from RIS to the EAV and that from IRIS to the LU are blocked. Due to the deployment of IRIS, the EAV can receive the signal directly leaked from AP and reflected by IRIS. The AP-RIS and AP-IRIS channels, the RIS-LU and IRIS-EAV channels are assumed to follow Rician fading with factor $K_{AR} = K_{AI} = K_{RU} = K_{IE} = 5$ and path loss $\beta_{AR} = \beta_{AI} = 2, \beta_{RU} = \beta_{IE} = 2.5$. The direct channels of AP-LU and AP-EAV follow Rayleigh fading with path loss $\beta_{AU} = \beta_{AE} = 3.5$. The phase resolution bit of RIS and IRIS are set as 2. The illegitimate system optimizes the IRIS phase shifts to maximize the channel gain of the cascaded AP-IRIS-EAV links and we utilize the above AN-aided joint optimization-based solution to jointly obtain the beamforming vector at AP and the phase shifts of RIS, under different setting of total transmit power p and required QoS threshold of LU γ, i.e, the SNR at LU should be larger than γ.

In Fig 3, we investigate the impact of the reflecting elements number of RIS N on the SR, which is defined as the data rate difference between the legitimate and eavesdropper links. As can be seen, the AN-aided joint optimization achieves higher SR for various N. Specifically, when $N = 60$, the SR improves about 193.3% compared with the distributed algorithm in [4]. This is because that the presence of IRIS helps the EAV to collect more information signal and the distributed algorithm also increases the data rate at the EAV, which has slight contribution to SR improvement. However, the AN-aided joint optimization guarantees the required threshold γ and allocates part of the total transmit power p to transmit the AN signal to jam the EAV and efficiently decrease the data rate at EAV, which significantly improves the SR. With increasing N, the SR of AN-aided joint optimization also increases due to that less power is allocated to reach γ while more power is left to send AN signal. On the other hand, it can be seen that with the assistance of IRIS, the SR severely goes down, e.g., about 38.3%/24.7% SR degradation is brought by IRIS when $Ne = 100/60$, $p = 5$dbm and $\gamma = 15$db, which shows the great impact of IRIS on signal leakage. Moreover, we investigate the PLS degradation brought by IRIS without any knowledge of CSI, i.e., random phase shifts. When N is insufficient, IRIS still results in more than 15% SR decrease. Furthermore, when only imperfect CSI can be obtained at illegitimate system, phase shifts configuration based on CSI error model can be implemented [12].

As can be seen in Fig. 4, with larger total transmit power p, the AN-aided joint optimization-based solution can achieve better performance since more power is used to transmit AN signal and the data rate at EAV gradually decreases to zero. However, when p is small, more power is used to reach the required threshold and the AN signal is insufficient to jam the EAV due to the efficient utilization of IRIS. Meanwhile, the distributed algorithm has no improvement on SR, because IRIS can also receive more signal.

Interference Attack

In the second case with interference attack, we consider an AP with $M = 16$ antennas, a single-antenna LU, EAV and attacker. The IRIS with N_a reflecting elements is properly deployed by the attacker to transmit interference signal with transmit power p_a to jam the LU only. We assume that the signal reflected by RIS can be received by both LU and EAV. The Attacker-IRIS and IRIS-LU channels are assumed to follow Rician fading with factor $K_{A_tI} = K_{IU} = 5$ and path loss $\beta_{A_tI} = \beta_{IU} = 2.5$ while the other channels are the same as the former case.

Fig. 5 depicts the impact of the reflecting elements of IRIS N_a on SR. With increasing N_a or p_a, the interference

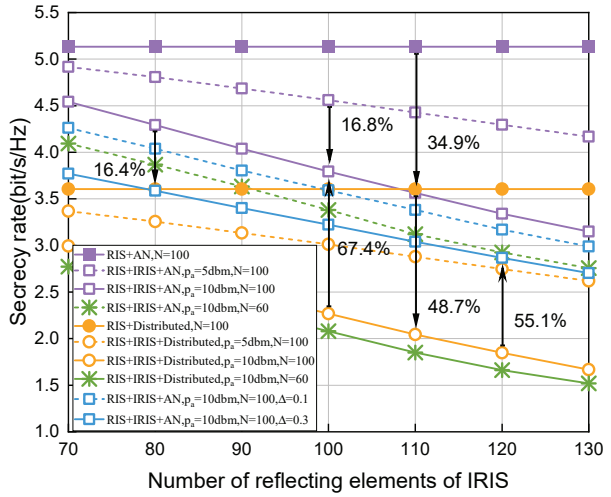

Figure 5. Secrecy rate versus the number of reflecting elements of IRIS with $p = 10$dbm and $\gamma = 20$db.

signal power improves and the SR decreases. It can be seen that 48.7% SR degradation is brought by IRIS under the distributed algorithm while that of the AN-aided solution is 34.9%, which shows that the AN-aided solution is more powerful to relieve the performance degradation caused by IRIS. Meanwhile, the SR of AN-aided solution improves about 67.4% compared with the distributed algorithm with $N_a = N = 100, p_a = 10$dbm. Furthermore, we study the performance of the AN-aided solution under imperfect CSI, e.g., existence of IRIS-assisted pilot attack or inaccurate channel estimation. Specifically, the AN-aided solution is implemented under channel uncertainty model, where the entries of error matrix are i.i.d. complex Gaussian distributed variables with zero mean and variance Δ. Δ is set to be 10%/30% of the average channel gain. When $\Delta = 0.3$, the SR reduces about 16.4% compared to the result under perfect CSI, while it still achieves about 55.1% SR improvement compared to the distributed algorithm under perferc CSI.

Conclusions and Future Research

In this article, we raise the non-negligible risk of illegal utilization of RIS and this concept is introduced as IRIS. Two main security concerns in the presence of IRIS, namely, signal leakage and interference attack, are investigated. Specifically, we discuss how the IRIS is exploited to efficiently enhance the illegitimate links or weaken the legitimate links, which leads to severe PLS performance degradation. Challenges in the wireless communication systems with IRIS are presented and an AN-aided joint optimization-based solution is proposed to relieve PLS degradation brought by IRIS. Finally, case studies validate the effectiveness of the proposed solution.

We hope that this article raises the concerns about IRIS, while the application of IRIS is not just confined to these two secure threats, which aim at strengthening eavesdropping/interference signal via IRIS. To safeguard the secure transmission, more elaborate solutions should be developed.

Future Discussions about IRIS

Passive Jammer: Apart from being adopted by EAVs to facilitate eavesdropping and jamming, IRIS can be directly used in legitimate systems to stealthily affect PLS, which acts as a passive jammer to disturb the communication without leaving any energy footprint [14]. Specifically, IRIS is deployed between AP and LU to reflect the existing confidential signal in the victim wireless systems. By changing the IRIS phase shifts, the direct signal will be destructively suppressed by the reflected signal. This adverse application can be applied in both data transmission attack and pilot contamination attack [15].

Hybrid Leakage/Attack: It is possible that signal leakage and interference attack exist at the same time. Meanwhile, fake pilots might be transmitted to jam LU with the aid of IRIS. Such a complicated hybrid leakage/attack wireless environment is volatile, and can cause catastrophic PLS threats. Conventional channel estimation and beamforming schemes become disabled. Therefore, it is more challenging and requires further investigation.

Strategic Game: In some cases, the legitimate system is able to discover the occurrence of IRIS, and can adjust the RIS phase shifts to reduce the adverse effect brought by IRIS. Meanwhile, IRIS reconfigures its phase shifts to counteract the boost. This can be formulated as a noncooperative strategic game in which the players are the legitimate system and illegitimate system. In this game, the goal of the legitimate system is to maximize the SR by optimizing the beamforming vector at AP and the RIS phase shifts. Conversely, the strategy of illegitimate system is to degrade PLS by tuning IRIS phase shifts. This game can be solved by game theory-based approaches in which RIS and IRIS selfishly adapt their configuration to achieve their own goal, until they reach a Nash equilibrium.

Future Directions about Countermeasures

Although AN technology shows its strong ability in defending against IRIS, the future wireless systems will be more complex and the impact brought by IRIS can be greater with more elaborate deployment and design. Hence, more effective and powerful countermeasures against IRIS still demand further investigation.

Detection Schemes: One potential solution might be detection schemes, such as detection based on the angle-of-arrival database for location-aware users and detection schemes based on random phase-shift keying symbols. .

Deep Reinforcement Learning: Another solution is to adopt deep reinforcement learning (DRL), which is particularly beneficial to wireless systems where the channels are uncertain and time-varying. The DRL framework makes a decision to enhance the system performance only based on the observed rewards and states, i.e., the current secrecy rate and the CSI of legitimate links. By applying valid deep neural network and learning approach, the CSI of illegitimate communication links might be unnecessary for achieving optimal beamforming policy and phase shifts configuration.

Cooperative Nodes: To combat with IRIS-assisted pilot attack, cooperative nodes (CNs) is a promising technology. During the uplink channel estimation stage, each of CNs broadcasts a mutually orthogonal pilot sequence. Then the CNs can jointly try to minimize the pilot contamination in the system.

ACKNOWLEDGMENTS

This work was supported in part by the National Key R&D Program of China under Grant 2020YFA0711400 and the National Science Foundation of China under Grant U19B2044.

REFERENCES

[1] Z. Gu, H. Lu, M. Zhang, H. Sun and C. Chen, "Association and Caching in Relay-Assisted mmWave Networks: From A Stochastic Geometry Perspective," *IEEE Trans. Wireless Commun.*, to be published, doi: 10.1109/TWC.2021.3091815.

[2] F. Guo, H. Lu and Z. Gu, "Joint Power and User Grouping Optimization in Cell-Free Massive MIMO Systems," *IEEE Trans. Wireless Commun.*, to be published, doi: 10.1109/TWC.2021.3100573.

[3] A. Almohamad, *et al.*, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, 2020.

[4] Q. Wu and R. Zhang, "Intelligent Reflecting Surface Enhanced Wireless Network: Joint Active and Passive Beamforming Design," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1-6.

[5] D. Zhao, H. Lu, Y. Wang, H. Sun and Y. Gui, "Joint Power Allocation and User Association Optimization for IRS-Assisted mmWave Systems," *IEEE Trans. Wireless Commun.,* to be published, doi: 10.1109/TWC.2021.3098447.

[6] Y. Omid, *et al.*, "Low-Complexity Robust Beamforming Design for IRS-Aided MISO Systems With Imperfect Channels," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1697-1701, May. 2021.

[7] Y. Wang, H. Lu and H. Sun, "Channel Estimation in IRS-Enhanced mmWave System with Super-Resolution Network," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2599-2603, Aug. 2021,

[8] K. Feng, *et al.*, "Physical Layer Security Enhancement Exploiting Intelligent Reflecting Surface," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 734-738, March. 2021.

[9] 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, June. 2019.

[10] L. Dong and H. Wang, "Secure MIMO Transmission via Intelligent Reflecting Surface," *IEEE Commun. Lett.*, vol. 9, no. 6, pp. 787-790, June. 2020.

[11] 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.

[12] Q. Wang, F. Zhou, R. Q. Hu and Y. Qian, "Energy Efficient Robust Beamforming and Cooperative Jamming Design for IRS-Assisted MISO Networks," *IEEE Trans. Wireless Commun.,* vol. 20, no. 4, pp. 2592-2607, Apr. 2021.

[13] H. -M. Wang, J. Bai and L. Dong, "Intelligent Reflecting Surfaces Assisted Secure Transmission Without Eavesdropper's CSI," *IEEE Signal Process. Lett.,* vol. 27, pp. 1300-1304, 2020.

[14] B. Lyu, D. T. Hoang, S. Gong, D. Niyato and D. I. Kim, "IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power," *IEEE Wireless Commun. Lett.,* vol. 9, no. 10, pp. 1663-1667, Oct. 2020.

[15] K. -W. Huang and H. -M. Wang, "Intelligent Reflecting Surface Aided Pilot Contamination Attack and Its Countermeasure," *IEEE Trans. Wireless Commun.,* vol. 20, no. 1, pp. 345-359, Jan. 2021.

BIOGRAPHIES

YAZHENG WANG received the B.S. degree in 2019 from the USTC, Hefei, China, where he is currently working toward the Graduate degree in the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC). His research interests include RIS-assisted millimeter wave communication.

HANCHENG LU (M'07) received the Ph.D. degree in communication and information systems from the University of Science and Technology of China, Hefei, China, in 2005. He is currently an Associate Professor with the Department of EEIS, USTC. He is also with Institute of Artificial Intelligence, Hefei Comprehensive National Science Center. His research interests include resource optimization in wireless communication systems, such as RIS, NOMA, cell-free (i.e., distributed MIMO), and caching and service offloading at wireless network edges.

DAN ZHAO received the B.S. degree in 2019 from the Shandong University, Weihai, China, where she is currently working toward the Graduate degree in the Department of EEIS, USTC. Her research interests include RIS-assisted wireless network.

YANSHA DENG (S13-M21) is currently a Senior Lecturer (Associate Professor) with the Department of Engineering in King's College London. Her research interests include machine learning for 5G/6G wireless networks and molecular communications.

ARUMUGAM NALLANATHAN is Professor of Wireless Communications and Head of the Communication Systems Research (CSR) group in the School of Electronic Engineering and Computer Science at Queen Mary University of London. His research interests include Beyond 5G Wireless Networks, Internet of Things, and Molecular Communications. He is an IEEE Fellow and IEEE Distinguished Lecturer.