Secure Beamforming for IRS-Enhanced NOMA Networks

Wei Wang, Yang Cao, Min Sheng, *Senior Member, IEEE,* Jie Tang, *Senior Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* Dusit Niyato, *Fellow, IEEE,* and Kai-Kit Wong, *Fellow, IEEE*

***Abstract*—Owing to the increasing demand of higher spectrum efficiency and large-scale connectivity, non-orthogonal multiple access (NOMA) has become a highly competitive candidate for the upcoming sixth-generation (6G) systems. Nevertheless, the instable wireless propagation environment and potential wireless security risk become bottlenecks in applications of NOMA. Fortunately, intelligent reflecting surface (IRS) that can construct the three-dimensional beamforming and reconfigure the channels emerges as a highly efficient technology to break through the limitations of NOMA. Thus, in this article, we first present an overview of NOMA, and particularly illustrate its main shortcomings and security risks. Then, we introduce the IRS technology and provide further enhancement by applying IRS to NOMA networks. In addition, typical security threats in IRS-NOMA networks are shown, followed by two countermeasures based on the joint transmit beamforming and IRS reflecting beamforming towards external and internal eavesdropping, respectively. Simulation results are carried out to demonstrate the feasibility and effectiveness of these two schemes. Several challenges and future directions are also discussed.**

***Index Terms*—Intelligent reflecting surfaces, non-orthogonal multiple access, physical layer security, secure beamforming.**

I. Introduction

Multiple access (MA) plays an essential role in every generation of wireless communications, which can be classified into two main schemes: orthogonal multiple access (OMA) and non-orthogonal multiple access (NOMA). In contrast to OMA, power-domain NOMA enables multiple users to simultaneously share one orthogonal resource block while decoding the information via successive interference cancellation (SIC) at each receiver. Thus, NOMA can provide high spectrum efficiency and large-scale connectivity, which has been deemed as a competitive candidate for the future wireless communications [1]. Nevertheless, NOMA owns several limitations even though its significant advantages. First, NOMA needs distinct channel difference among users, which may not be satisfied in practice. More importantly, how to guarantee secure transmission is still challenging in NOMA networks. In order to prevent the information intercepted by potential eavesdroppers, physical layer security (PLS), that mainly depends on the inherent characteristics of wireless channels, has been adopted as a strong strategy [2]. However, existing PLS schemes are limited by uncontrollable wireless propagation channels, expensive hardware and high energy consumption, which drives researchers to find a new cost-efficient solution to overcome these limitations.

With the rapid development of metamaterial and microelectronic technologies, smart metasurfaces have been widely utilized recently [3]. Among all kinds of metasurfaces, intelligent reflecting surface (IRS), a two-dimensional (2D) surface printed with numerous passive reconfigurable reflecting elements, has attracted tremendous attentions from both academia and industry [4]. Specifically, IRS can effectively control the characteristics of incident signal, i.e., the phase, even the amplitude, and thus change the signal propagation direction via reconfigurable elements. Compared with traditional relays, the main advantage of IRS-enhanced wireless systems relies on that it can be flexibly deployed on available infrastructures and establish an intelligent and reconfigurable wireless environment with extremely low power consumption. In addition, due to IRS's high capacity of shaping the signal propagation, the integration of PLS and IRS has attracted significant interests [5]–[7]. To limit the legitimate information leakage, various PLS techniques such as intelligent jammer [5], artificial noise [6] and beamforming [7], have been applied to IRS systems.

Motivated by the advantages of IRS and NOMA, they have been incorporated recently [8]–[11]. Specifically, IRS has the reconfigurable ability to control the channel gain to create disparities in channel strength among users. Furthermore, the SIC condition can be designed more flexibly by adjusting the active beamforming and the phase shifts of IRS elements. Thus, with the help of IRS, the performance of NOMA can be well enhanced. Nevertheless, the security of IRS-NOMA networks is still critical due to the fact that the potential adversaries may also obtain the additional reflecting link via the assistance of IRS. To the best of our knowledge, the secure beamforming optimization for IRS-enhanced NOMA networks is still not well analyzed. Beamforming has been utilized extensively to enhance the security of NOMA [2]. In contrast to the conventional active beamforming via multiple antennas, IRS can provide reconfigurable beamforming with more flexibility and lower hardware cost. However, it is

W. Wang, Y. Cao and N. Zhao (Corresponding Author) are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China (email: 21809066@mail.dlut.edu.cn, cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

M. Sheng is with the State Key Laboratory of ISN, Xidian University, Xi'an 710071, China (e-mail: msheng@mail.xidian.edu.cn).

J. Tang is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. (e-mail: eejtang@scut.edu.cn).

D. Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, Block N4-02a-32, Nanyang Avenue, Singapore (e-mail:dniyato@ntu.edu.sg).

K.-K Wong is with the Department of Electronic and Electrical Engineering, University College London, London, United Kingdom (e-mail:kai-kit.wong@ucl.ac.uk).

This research was supported in part by the National Key R&D Program of China under Grant 2020YFB1807002. *(Corresponding author: Nan Zhao.)*

still not clear how to combine them together to guarantee the security of IRS-NOMA networks. Thus, in this article, beamforming-based security schemes are carefully designed for IRS-NOMA networks. In Section II, we first present an overview of NOMA. Then, the promising advantages by combining IRS and NOMA are illustrated in Section III. In Section IV, potential security threats in IRS-NOMA networks are presented. In Sections V, an artificial jamming aided joint BS and IRS beamforming scheme is proposed to disrupt the external eavesdropping. In Section VI, the joint precoding and IRS reflecting beamforming is carefully designed to guarantee the internal privacy. In Section VII, we highlight some open issues and future challenges, following by conclusions drawn in Section VIII.

II. An Overview of NOMA

Recalling the development history of wireless communications, the system performance of both validity and reliability has a huge improvement in every generation evolution. From the first generation (1G) to the fifth generation (5G), one of the most important techniques is the MA. The common idea between these conventional MA schemes is to allocate different users distinct resource blocks, which results in higher spectrum efficiency and less inter-user interference. Although OMA schemes are quite mature and effective, they may be still difficult to support the exponential growth of the data and the demand of wireless access in the future.

In view of this, several potential technologies have been proposed and investigated towards the upcoming sixth-generation (6G) systems. Among them, NOMA has been deemed as a more competitive MA candidate for 6G. Unlike OMA, NOMA can share one resource block with multiple users, and thus enhance the spectrum efficiency and user capacity significantly. Particularly, the power-domain NOMA employs the superposition code at the base station (BS), and utilizes the SIC receiver to subtract the MA interference and decode the desired message. The primary study on the power-domain NOMA, named as multi-user superposition transmission (MUST), has been studied by 3GPP from Release 14 to 16. However, the power-domain NOMA is not included in 3GPP Release 17 due to its limitations on applications and performance degradation.

The main shortcomings of conventional power-domain NOMA lie in the following points.

- *Restriction*: NOMA is not always preferable than OMA schemes, when the channel disparity among the served users is not distinctive, the NOMA cannot approach such spectrum efficiency gain than OMA as high as the theoretical value. In practical implementation, the random and uncontrollable signal propagation further restricts the application of NOMA [8].
- *Security Risks*: NOMA utilizes the channel difference of users for multiplexing and performs SIC to cancel the MA interference and decode the intended message. As shown in Fig. 1, typical secure scenarios in downlink power-domain NOMA networks with two users are presented, where the BS serves two users simultaneously over the same resource block. In general, the weaker user should be allocated more power to guarantee its QoS, which accordingly attracts the external eavesdropper. Moreover, the user with stronger channel strength always decodes the message of the weaker user. Thus, the stronger user easily turns to be an adversary, and the information of the weaker user is more likely to be leaked according to the predetermined SIC rule, which results in the limited internal security.

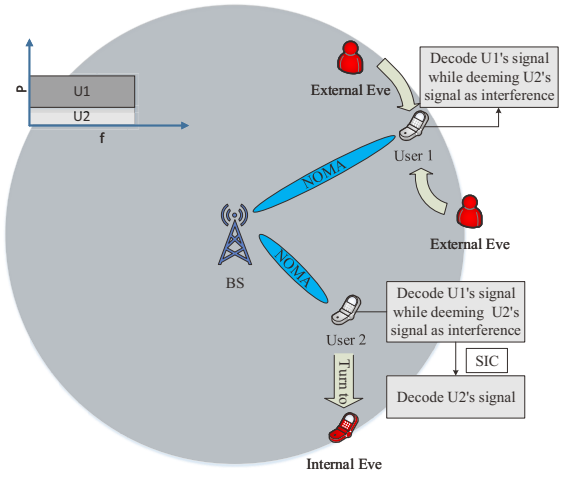


Fig. 1: Typical secure scenarios in downlink power-domain NOMA networks taking two users as an example.

III. What Can IRS Bring to NOMA?

A. Principles of IRS

IRS can provide reconfigurable wireless environment and flexibly manipulate the incident signal by adjusting its phase shifts, which has been deemed as an innovative technology for wireless communications. The primary application of IRS is to provide an additional BS-user link, especially for those blocked by an obstacle or located in a dead zone. With the development of IRS, its remarkable capability can be utilized to construct the three-dimensional (3D) passive beamforming for signal enhancement or weakness, through which it can be combined with existing wireless techniques to further enhance the rate performance, energy efficiency and security.

Specifically, IRS as a 2D smart surface is made of electromagnetic material. The structure of IRS is composed of three layers and an embedded micro-controller. The first layer consists of numerous low-cost passive reflecting elements and tunable chips or PIN switches printed on a dielectric material. Each reflecting element and tunable chip can interact together to manipulate the phase shift of the incident signal. Thus, the characteristics of its reconfiguration and programmability can be realized by the joint control of reflecting elements and tunable chips. The second layer is a copper plate designed to prevent the energy leakage of signal to other layers. Finally, the third layer includes the inter-cell communication circuits to deliver the real-time commands from the embedded micro-controller. In general, the reflecting elements are passive and only with limited signal processing capability. The embedded micro-controller can receive and response configuration

TABLE I: Physical Layer Security Realizations in IRS-NOMA Networks

Reference	CSI of Eavesdropper	Optimization	Main Contribution
[12]	No CSI	–	Evaluate the secure performance of IRS-assisted NOMA networks with the one-bit coding scheme
[13]	Perfect CSI	Maximize minimal secrecy rate	Secure beamforming via jointly optimizing the active beamforming and the phase shifts of IRS
[14]	Imperfect CSI	Minimize transmit power	The jamming power is minimized to confuse the eavesdropping while reducing its interference to legitimate users
[15]	No CSI	Maximize sum rate	The jamming signal can be perfectly cancellated at legitimate users via joint BS and IRS beamforming design

requests from the external BS that can afford high computational power. Then, it distributes the phase controls to all the reflecting elements. The detailed structure of IRS is available in Fig. 2 of [4]. Therefore, IRS can realize fully controllable beams via its passive elements with low cost and power consumption, which is different from the multi-antenna systems. Furthermore, IRS does not perform information decoding but only reflects the incoming signal passively without involving interference, which incurs less power consumption compared to the conventional relays.

B. Advantages of IRS-NOMA Networks

Inspired by the IRS, it is promising to exploit IRS to address the dilemmas of NOMA, the main advantages of which are summarized as follows.

Coverage Enhancement: With the assistance of IRS, the desired signal of cell-edge NOMA users can be well enhanced. The reconfigurable capability enables the rate requirement of weak users to be effectively guaranteed in a low-cost way instead of increasing the transmit power to fight against the high signal attenuation. For example, Ding *et al*. presented a novel IRS-NOMA system in [8] to satisfy the QoS requirements of cell-edge users by aligning their effective channel vectors.

Rate Performance Improvement: IRS can provide turnable channel gain to guarantee the achievable NOMA performance. The joint BS active beamforming and the IRS reflecting beamforming can artificially enlarge the differences of the channel conditions, which greatly motivates NOMA's potential. For instance, the joint IRS deployment and power allocation optimization was investigated by Mu *et al*. in [9], which unveils that the optimal IRS deployment can enlarge the differences among channels for NOMA. In [10], Zhu *et al*. investigated an IRS-aided NOMA system with the quasi degradation satisfied, which guarantees that NOMA can approach equivalent performance as dirty paper coding (DPC).

More Flexibility for Decoding: IRS introduces new degree of freedoms (DoFs) for the SIC decoding order of NOMA users. In NOMA, the SIC order is determined by the different channel strength of users, which is greatly limited by the randomness and uncontrollability of wireless channels. However, by employing IRS, the SIC order of NOMA users can be changed more flexibly by controlling the IRS's phase shifts, which provides more DoFs to enhance the performance of IRS-aided NOMA system. In [11], Cheng *et al*. evaluated the rate performance of IRS-NOMA and IRS-OMA networks under downlink and uplink scenarios, and revealed that the utilization of IRS can achieve larger diversity order.

C. Physical Layer Security in IRS-NOMA Networks

PLS is another potential advantage of IRS-NOMA networks. The utilization of IRS can simultaneously create enhanced beams to the intended legitimate receivers while the eavesdropping signal-to-noise ratio can be effectively suppressed, and thus achieving a higher secrecy rate. Motivated by this, robust and secure beamforming with IRS has been investigated to benefit the PLS of NOMA networks [12]–[15]. The secrecy performance of IRS-NOMA networks was studied by Gong *et al*. in [12] under circumstance of one-bit coding scheme, which demonstrated potential security advantages of utilizing IRS in NOMA. In [13], with perfect channel state information (CSI), Feng *et al*. investigated the max-min fairness problem of uplink IRS-NOMA system with an eavesdropper, where artificial noise is transmitted together with confidential messages and the minimal secrecy rate is maximized by jointly optimizing the active beamforming at users and passive beamforming at IRS. In [14], to confuse the eavesdropper with imperfect CSI, Zhang *et al*. proposed an artificial noise aided secure beamforming scheme for IRS-NOMA networks, in which the artificial noise is carefully designed to disrupt eavesdropping while its power is minimized to reduce the negative impact on legitimate users. In [15], when the eavesdropping CSI is unknown, artificial jamming is injected into NOMA signals to guarantee the security of IRS-NOMA networks. Different from [13], [14], owing to the new DoFs introduced by the joint BS and IRS beamforming design, the jamming can be fully eliminated via legitimate SIC receiver, while having no impact on the receiving quality of legitimate users. A comparison of aforementioned realizations for secure IRS-NOMA networks is presented in Table I.

In terms of this, the secure beamforming towards IRS-NOMA networks as a promising direction deserves further investigation. In the following sections, two typical scenarios for secure IRS-NOMA networks are further discussed.

IV. Security Threats in IRS-NOMA Networks

As mentioned earlier, the weaker NOMA user with more power is threatened by external eavesdropping, while the broadcasted NOMA information may be leaked at the internal untrusted user due to the SIC. Similarly, the security issues still exist in IRS-NOMA networks. Except the security risk

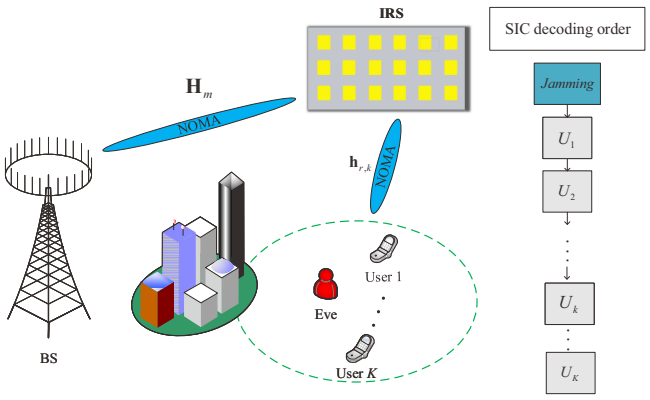


Fig. 2: Secure IRS-enhanced NOMA network via artificial jamming with a passive eavesdropper.

from the SIC, an additional link provided by IRS may also enhance the signal intensity at the eavesdropper. To further discuss this issue, two typical scenarios of external and internal eavesdropping are presented as follows.

- *External Eavesdropping*: IRS can effectively enhance the wireless BS-user links, which may also make the catched signals stronger at the potential eavesdropper owing to its unavailable CSI. When the BS owns sufficient transmit power, the artificial jamming can be broadcasted together with the confidential NOMA information, which is an effective way to suppress the external eavesdropping with less influence on the legitimate transmission via the BS active beamforming and IRS reflecting beamforming.
- *Internal Eavesdropping*: NOMA utilizes the channel disparity of users for multiplexing and performs SIC to remove the MA interference and decode the intended message. Thus, the information of the user with weaker channel strength is possible to be intercepted by the stronger user according to SIC. This security problem may become more serious due to the enhancement of IRS, which results in that the stronger user easily turns to be an adversary. To reduce the information leakage, joint optimization of BS precoding and IRS reflecting can be exploited to guarantee the internal security.

Thus, in order to limit the information leakage in IRS-NOMA networks, secure beamforming and the SIC decoding condition can be flexibly designed with the help of IRS. In the following two sections, two secure beamforming based countermeasures for these two typical scenarios in IRS-NOMA networks are discussed.

V. Artificial Jamming Aided Beamforming With External Eavesdropper

A. Problem Formulation

An IRS-assisted downlink NOMA network is presented in Fig. 2, a BS transmits the information to multiple legitimate users via NOMA in the presence of a passive eavesdropper. The BS has multiple antennas, and both the legitimate users and eavesdropper are with a single antenna. The total number of legitimate users is K, and let U_k represent the kth user. The legitimate NOMA users are located in a remote area where the direct links from BS are blocked. Thus, the IRS is deployed to strengthen the information propagation via its reconfigurable capability. An external eavesdropper exists to overhear the confidential communication, and its CSI is unknown at the BS because of the passive eavesdropping. For the secure transmission, the artificial jamming and NOMA signals are superposed and broadcasted together by the BS to confuse the eavesdropper.

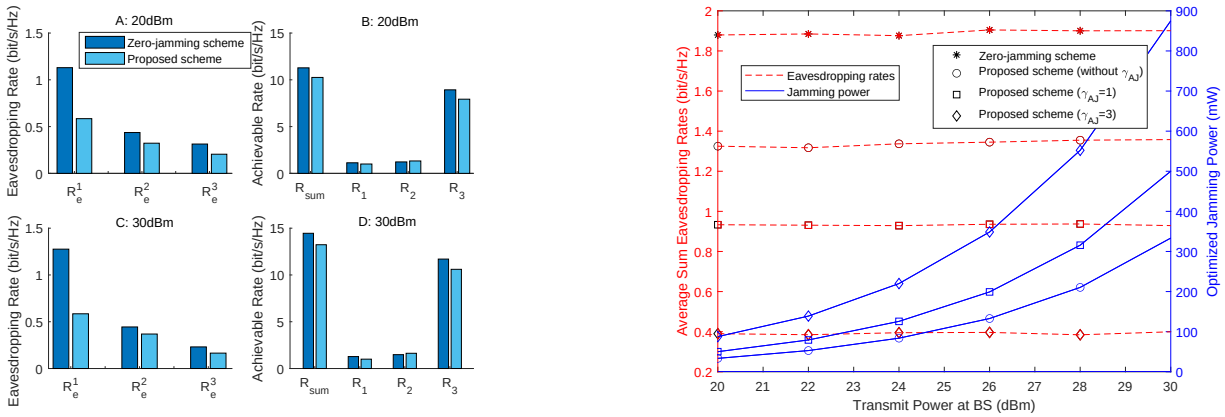
In NOMA networks, SIC is implemented to cancel the MA interference. For instance, the SIC decoding order at each receiver follows $U_1 \Rightarrow U_2 \Rightarrow \cdots \Rightarrow U_K$, which is determined by their channel quality. However, with the introduction of IRS, the SIC is decided not only by the BS active beamforming, but also by the phase shifts of IRS elements. Based on this, we can flexibly adjust the reflecting elements of IRS to control the phase shift and beam the desired signal at each legitimate receiver, i.e., making the received power of jamming at each legitimate receiver higher than that of legitimate information, and resulting in the SIC order as $Jamming \Rightarrow U_1 \Rightarrow U_2 \Rightarrow \cdots \Rightarrow U_K$. Following this condition, the injected jamming signal can be removed in the first layer of SIC at each legitimate receiver, but disrupting the external eavesdropping effectively [15].

The sum rate maximization is achieved via joint optimization of the BS active beamforming including the artificial jamming and the IRS reflecting beamforming, satisfying the QoS requirement of legitimate users, the SINR threshold of artificial jamming, the BS transmit power condition, the SIC order and the unit constraint for each IRS element. To tackle this non-convex problem, we first reformulate the sum rate in terms of product. The rate expression for each user can be replaced by an auxiliary variable. In this way, maximizing the product of these variables can be simplified into finding their maximum geometric mean. Next, the simplified problem can be directly changed into two separate subproblems of alternately optimizing the BS active beamforming and the IRS reflecting beamforming. For each subproblem, the non-convex constraints can be approximated into convex by applying successive convex approximation. Finally, both of them can be further converted to second-order-cone programming and effectively solved in the manner of alternating optimization.

B. Simulation Results

Simulations are carried out to demonstrate the secure IRS-NOMA scheme via artificial jamming. The BS is set at $(5, 0, 5)$ with $M = 4$ antennas and the IRS is deployed at $(0, 50, 20)$ in meters. Three legitimate users are arbitrarily distributed on the ground near the IRS. The passive eavesdropper is located at $(2, 50, 0)$, which is only for performance analysis.

Fig. 3(a) illustrates the average rate versus different transmit power for the proposed scheme, and the benchmark "Zero-jamming scheme" where the allocated jamming power is equal to zero. The results show that the average eavesdropping rate of all users in the proposed scheme can be suppressed via artificial jamming in contrast to the benchmark. On the other hand, in Fig. 3(a)-B, the transmission rate for the proposed



(a) (b)

Fig. 3: (a) The proposed IRS-NOMA scheme versus zero-jamming scheme with different transmit power. (b) Comparison of the average sum eavesdropping rate and the optimized jamming power with different transmit power.

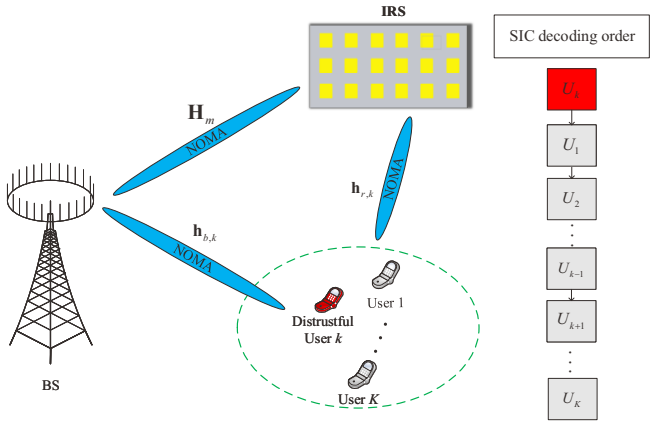


Fig. 4: Secure beamforming assisted IRS-NOMA network with an untrusted user.

scheme is lower than that of the benchmark owing to the power consumption for jamming. However, this rate degradation can be significantly mitigated by increasing the transmit power, as shown in Fig. 3(a)-D.

Then, we introduce the SINR threshold of artificial jamming γ_{AJ} to flexibly adjust the proportion of jamming and further disrupt the eavesdropping. As shown in Fig. 3(b), the average sum eavesdropping rate and the optimized jamming power are presented with different γ_{AJ}. From the results, we can conclude that more transmit power is allocated to the artificial jamming as the growth of γ_{AJ}. Accordingly, higher γ_{AJ} results in lower sum eavesdropping rate.

VI. Secure Precoding Scheme with Untrusted User

A. Problem Formulation

As shown in Fig. 4, an IRS-assisted NOMA network is composed of a BS with mulitple antennas, K users with single antenna and an IRS that is deployed to enhance the transmission. Assume that U_k is the untrusted user that may overhear the information. In this case, the CSI of all the channels is available at the BS.

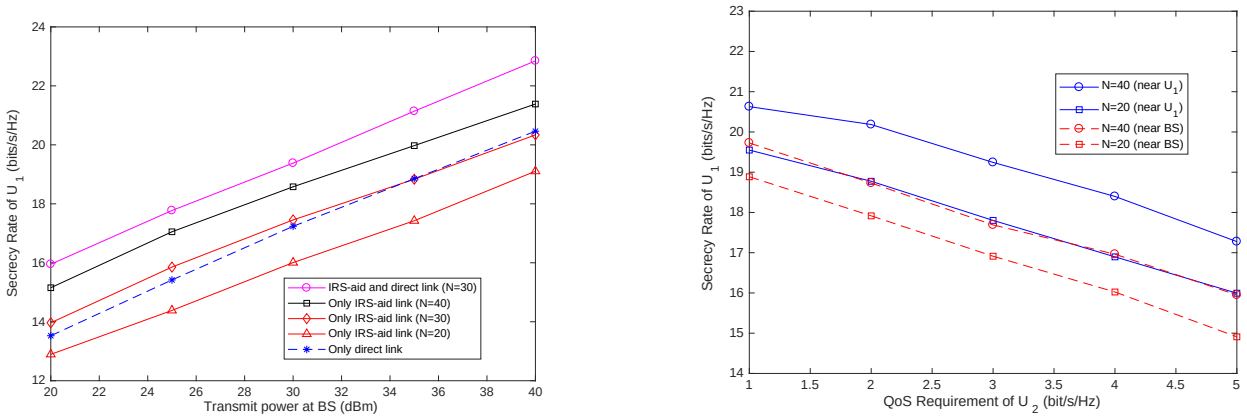
Each NOMA user can receive the broadcasting signal of all users relying on the superposition coding. Relying on the SIC condition, the stronger users always decode the signal of weaker users, and then decode its own, which may drive them to extract the internal message and become an adversary. Besides, with the enhancement of IRS, more confidential information may be leaked. Thus, joint precoding and IRS reflecting beamforming are carefully designed to guarantee the internal privacy, which refers to that the SIC order at legitimate receivers should follow $U_k \Rightarrow U_1 \Rightarrow \cdots \Rightarrow U_{k-1} \Rightarrow U_{k+1} \Rightarrow \cdots \Rightarrow U_K$. In this way, the power allocated for the untrusted user U_k is higher than that of other legitimate users, and thus, the transmitted signals of other legitimate users can be hidden, which greatly mitigates the threat of internal eavesdropping.

Based on the SIC condition, the secrecy rate maximization problem is proposed to further suppress the eavesdropping from U_k. The secrecy rate of legitimate users is maximized via joint optimization of the precoding and the IRS reflecting beamforming, satisfying the rate requirement of U_k, the SIC condition, the transmit power constraint and the unit constraint for each IRS element. To solve this non-convex problem, we first decompose it into two separate problems, and then optimizing the precoding vectors and the IRS reflecting matrix with the other fixed. Finally, they can be simplified as convex semidefinite programming and solved iteratively.

B. Simulation Results

Simulations are carried out to demonstrate the proposed secure precoding scheme for an IRS-NOMA network with two users. The BS is set at $(0, 0, 5)$ with $M = 4$ antennas while the legitimate user U_1 and the untrusted user U_2 are located at $(0, 40, 0)$ and $(5, 18, 0)$ in meters, respectively.

The secrecy rate of legitimate U_1 versus different transmit power and number of IRS elements N for three scenarios is shown in Fig. 5(a), i.e., both IRS-assisted and direct link, only IRS-assisted link and only direct link. The results verify that



(a) (b)

Fig. 5: (a) The secrecy rate comparison of U_1 with transmit power and different number of IRS elements. (b) The secrecy rate comparison of U_1 with different IRS deployment and different QoS requirement of U_2.

the secrecy rate of U_1 increases with the growth of transmit power and N. With the assistance of IRS, the IRS-NOMA network can approach the same secrecy rate performance as the conventional NOMA (i.e., only direct link) with less transmit power, which greatly enhances the energy efficiency.

In Fig. 5(b), the secrecy rate of legitimate U_1 is compared with different QoS requirement of untrusted U_2 and different IRS deployment. From the results, the secrecy rate of U_1 decreases with the higher QoS requirement of U_2, and hence, we can conclude that there exists a tradeoff between suppressing the untrusted user and guaranteeing its own performance. In addition, the performance is certainly relevant to the location of IRS. From the results, we can see that when the IRS is near the legitimate U_1, U_1 can achieve better security performance with the same number of IRS elements.

VII. Challenges and Future Directions

Although some of the security issues in IRS-NOMA networks have been discussed above, there still remain some challenges to be addressed as follows.

External and Internal Eavesdropping: For the scenario of both external and internal eavesdropping, the proposed two countermeasures can be jointly implemented to complement each other on the premise of sufficient transmit power and large-sized IRS, which can be utilized to provide flexible beamforming and DoFs for the SIC decoding. In addition to the passive eavesdropping, active eavesdroppers that can overhear and jam the legitimate network simultaneously are much tougher to fight against.

Channel Acquisition: The proposed secure schemes are based on the full CSI of legitimate channels. However, in practice, IRS-related channel estimation is challenging to acquire owing to its limited signal processing capability of IRS passive reflecting elements. Thus, more efficient channel acquisition is expected for IRS-assisted NOMA systems. In addition, the accurate secure beamforming will be put into effect via the cooperation of the BS and IRS, if the eavesdropping CSI can be collected efficiently. However, it is still a tricky problem for current anti-eavesdropping systems.

IRS Deployment and Control: As demonstrated above, the IRS deployment plays an essential role that affects the achievable secrecy rate. Furthermore, the proposed iterative algorithm, that decomposes the BS active beamforming and the IRS reflecting beamforming into two separated problems, can converge to a sub-optimal point based on the alternating optimization. However, this inevitably requires high information exchange overhead and long transmission delay, which is still very challenging in practical scenarios.

Interference Management: In the proposed schemes, only one cluster is considered and the number of users in these two cases is, 2 and 3 respectively. When extending IRS to the multi-cluster scenario, more research is needed to manage the dynamic co-channel/co-cluster interference, and utilize it reasonably to assist the secure transmission, especially the additional interference introduced by the IRS.

VIII. Conclusion

Recently, IRS comes out as an energy and cost efficient solution to releasing the potential of NOMA. In this article, an overview of NOMA is first presented, especially its key limitations. Then, the advantages of IRS and promising realizations of PLS in IRS-NOMA networks are discussed. Subsequently, we illustrate two typical security scenarios in IRS-NOMA networks, following by two countermeasures, i.e., the artificial jamming aided joint beamforming scheme for the external eavesdropping and the joint precoding and reflecting beamforming scheme for the internal untrusted user. Furthermore, the solutions and simulations of these two schemes are carried out. Finally, several challenges and future directions are discussed for the security of IRS-NOMA networks.

References

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[3] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sept. 2018.
[4] 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, Jan. 2020.
[5] 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.
[6] 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.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.
[7] Y. Xiu, J. Zhao, C. Yuen, Z. Zhang, and G. Gui, "Secure beamforming for multiple intelligent reflecting surfaces aided mmWave systems," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 417–421, Feb. 2021.
[8] Z. Ding and H. Vincent Poor, "A simple design of IRS-NOMA transmission," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1119–1123, May 2020.
[9] X. Mu, Y. Liu, L. Guo, J. Lin, and R. Schober, "Joint deployment and multiple access design for intelligent reflecting surface assisted networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6648–6664, Oct. 2021.
[10] J. Zhu, Y. Huang, J. Wang, K. Navaie, and Z. Ding, "Power efficient IRS-assisted NOMA," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 900–913, Feb. 2021.
[11] Y. Cheng, K. H. Li, Y. Liu, K. C. Teh, and H. Vincent Poor, "Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3988–4000, Jun. 2021.
[12] C. Gong, X. Yue, X. Wang, X. Dai, R. Zou, and M. Essaaidi, "Intelligent reflecting surface aided secure communications for NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2761–2773, Mar. 2022.
[13] Y. Feng, J. Chen, X. Xue, K. Wu, Y. Zhou, and L. Yang, "Max-min fair beamforming for IRS-aided secure NOMA systems," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 234–238, Feb. 2022.
[14] Z. Zhang, L. Lv, Q. Wu, H. Deng, and J. Chen, "Robust and secure communications in intelligent reflecting surface assisted NOMA networks," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 739–743, Mar. 2021.
[15] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for IRS-aided secure NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.

BIOGRAPHIES

Wei Wang [GSM] (21809066@mail.dlut.edu.cn) is currently pursuing Ph.D. degree in the School of Information and Communication Engineering at Dalian University of Technology, China. His current research interests include intelligent reflecting surface, non-orthogonal multiple access, and physical layer security.

Yang Cao [GSM] (cy216@mail.dlut.edu.cn) is currently pursuing Ph.D. degree in the School of Information and Communication Engineering at Dalian University of Technology, China. She received the B.S. degree from HeFei University of Technology, China. Her current research interests include intelligent reflecting surface, non-orthogonal multiple access, interference alignment, physical layer security, wireless energy harvesting, and resource allocation.

Min Sheng [SM] (msheng@mail.xidian.edu.cn) is a full professor with the State Key Laboratory of ISN, Xidian University. Her research interests include intelligent networks, self-organizing networks, and satellite networks. She was awarded the Distinguished Young Researcher from NSFC, Changjiang Scholar from Ministry of Education, China, elected in "Ten Thousand Talents Program" in 2019, and honored with the Second Prize for the State Technological Innovation Award in 2014 and 2017.

Jie Tang [SM] (eejtang@scut.edu.cn) received the B.Eng. degree in Information Engineering from the South China University of Technology, Guangzhou, China, in 2008, the M.Sc. degree in Communication Systems and Signal Processing from the University of Bristol, UK, in 2009, and the Ph.D. degree from Loughborough University, Leicestershire, UK, in 2012. From 2013 to 2015, he was a research associate at the School of Electrical and Electronic Engineering, University of Manchester, UK. He is currently a full professor at the School of Electronic and Information Engineering, South China University of Technology, China. He is currently serving as an Editor for IEEE Systems Journal and IEEE Wireless Communications Letters.

Nan Zhao [SM] (zhaonan@dlut.edu.cn) is a Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. He received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018. He is an Editor for IEEE Wireless Communications (magazine), IEEE Transactions on Green Communications and Networking and IEEE Wireless Communications Letters.

Dusit Niyato [F] (dniyato@ntu.edu.sg) is currently a professor in the School of Computer Science and Engineering, at Nanyang Technological University, Singapore. He received B.Eng. from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999 and Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.

Kai-Kit Wong [F] (kai-kit.wong@ucl.ac.uk) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, UK. He is Chair in Wireless Communications at the Department of Electronic and Electrical Engineering, University College London, UK. His current research centers around 5G and beyond mobile communications. He is a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international best paper awards. He is Fellow of IEEE and IET and is also on the editorial board of several international journals. He is the Editor-in-Chief for IEEE Wireless Communications Letters since 2020.