Manuscript version: Author's Accepted Manuscript

The version presented in WRAP is the author's accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:

http://wrap.warwick.ac.uk/118178

How to cite:

Please refer to published version for the most recent bibliographic citation information.
If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.

Secure Transmission via Beamforming Optimization for NOMA Networks

Yang Cao[*†], Nan Zhao[*†] (Corresponding Author), *Senior Member, IEEE*,
Yunfei Chen[‡], *Senior Member, IEEE*, Minglu Jin[*], Zhiguo Ding[§], *Senior Member, IEEE*, Yonghui Li[¶], *Fellow, IEEE* and F. Richard Yu[∥], *Fellow, IEEE*

[*]School of Information and Communication Engineering, Dalian University of Technology, Dalian, China

[†]State Key Laboratory of Integrated Services Networks, Xidian University, China

[‡]School of Engineering, University of Warwick, Coventry CV4 7AL, U.K.

[§]School of Electrical and Electronic Engineering, The University of Manchester, Manchester, M13 9PL, U.K.

[¶]School of Electrical and Information Engineering, The University of Sydney, Sydney, NSW 2006, Australia

[∥]Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada

Abstract

Owing to the eminent performance gain, non-orthogonal multiple access (NOMA) has been regarded as a promising approach to achieve high throughput and low latency for the next-generation networks. Nevertheless, the potential adversaries can still pose a threat to the secure transmission in NOMA systems. Hence, in this article, secure transmission schemes based on beamforming optimization are designed to combat both internal and external eavesdropping for downlink multi-input single-output NOMA networks. Using the transmit beamforming design, we first propose two schemes to protect the privacy of a specific NOMA user in the presence of untrusted users. Then, the sum secrecy rate optimization problem is studied to combat the external eavesdropper through optimizing the precoding vectors, when the channel state information (CSI) is available. In addition, two secure beamforming strategies with the help of artificial noise and inter-user interference are proposed without eavesdropping CSI, respectively. Simulation results are presented to demonstrate the effectiveness of the proposed schemes, and some open issues are discussed as well.

Index Terms

Beamforming optimization, non-orthogonal multiple access, physical layer security, privacy protection.

I. INTRODUCTION

The scarcity of spectrum resources has always been a bottleneck restricting the development of communications, especially the 5G mobile networks, where efficient spectrum utilization is required to provide higher transmission rate for the prevailing bandwidth-thirsty applications, such as virtual reality, ultra high definition video and self-driving [1]. To this end, non-orthogonal multiple access (NOMA) is emerging as a competitive candidate to improve the spectrum efficiency, in which the transmitter broadcasts the superposed signal of several users through a single resource block, and users' messages can be identified by different power levels with successive interference cancellation (SIC) performed at receivers [2]. Recently, plenty of research efforts have been dedicated to multi-antenna NOMA systems owing to the advantage of prominent array gains and system throughput. In [3], the sum rate maximization problem was investigated for the downlink multi-input single-output (MISO) NOMA system through optimizing linear precoding vectors. In [4], a general structure was presented for multi-input multi-output (MIMO) NOMA networks, and the idea of signal alignment was utilized to improve the performance gains. A novel resource allocation scheme for multi-antenna NOMA was proposed in [5], which can significantly improve the energy efficiency and security. In [6], an effective joint beamforming and power allocation optimization scheme was proposed for satellite-terrestrial integrated networks based on multi-antenna NOMA.

Although NOMA can bring significant performance gains, there still exist some serious challenges threatening its secure transmission [7]. Thus, the secure transmission in NOMA networks has received great attention from both academia and industry. Specifically, internal privacy leakage as well as external eavesdropping are the two main security issues due to

broadcasting and SIC adopted in NOMA. The first issue was tackled in a multi-user NOMA network with hybrid multicast-unicast streaming [8]. Using transmit beamforming design, secrecy rate maximization problem was investigated in [9] to ensure the security of the private user in MISO NOMA networks. For the external eavesdropping, secrecy outage probability (SOP) was derived in [10] for large-scale NOMA networks. In [11], a transmitting zero-forcing-beamforming method was proposed to remove the inter-cell interference at legitimate NOMA users and enhance the secure performance. The secrecy outage performance of two NOMA users was analyzed for a downlink MISO NOMA network assisted by artificial noise (AN) [12]. Based on characteristics of SIC, AN-aided secure beamforming schemes were proposed to fight against the external eavesdropper [13].

Although these works have provided very useful insights on the security issues in NOMA, none of them investigated secure beamforming optimization oriented multi-user NOMA. Thus, in this article, secure transmission based on beamforming is proposed and analyzed for diverse eavesdropping scenarios in downlink MISO NOMA networks. First, exploiting SIC, optimal PA between users is achieved by transmit beamforming to help protect the user privacy. Then, for the external eavesdropping, the sum secrecy rate maximization (SSRM) problem is formulated and solved via beamforming optimization with eavesdropping channel state information (CSI). Furthermore, in the cases when the eavesdropping CSI is not available, secure beamforming schemes assisted by AN or inter-user interference (IUI) can be utilized to enhance the security of NOMA users without affecting their quality of service (QoS). Finally, simulation results of the proposed schemes are presented, and several critical open research issues and challenges are pointed out.

The rest of this article is summarized as follows. In Section II, diverse eavesdropping scenarios for MISO NOMA networks are presented, and secure beamforming schemes on the internal privacy protection are proposed in Section III. The sum secrecy rate is maximized through
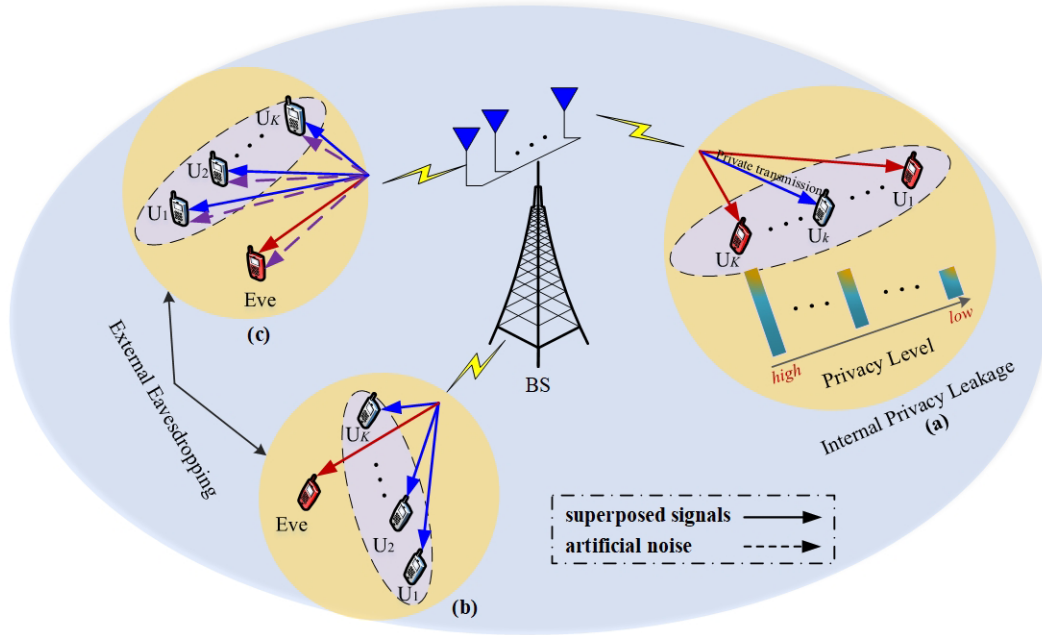
Fig. 1.   Scenarios for secure beamforming-based MISO NOMA Networks.

beamforming design with eavesdropping CSI in Section IV. In Section V, AN and IUI are employed to improve the security without eavesdropping CSI. We discuss open research issues and challenges in Section VI, and conclusions are obtained in Section VII.

II. SCENARIOS FOR SECURE BEAMFORMING-BASED MISO NOMA NETWORKS

In this section, several scenarios for secure beamforming-based MISO NOMA networks are presented as shown in Fig. 1, details of which are described as follows.

- *Internal Privacy Leakage*: In conventional NOMA networks, the messages of users with weaker channel strength are more likely to be leaked at the stronger users, because the signals with higher power from the weaker users will be recovered and cancelled at a stronger receiver according to SIC. Thus, the privacy of users with weaker channel strength are severely threatened. As shown in Fig. 1(a), the strongest user U_K has the highest privacy level, whereas the weakest user U_1 has the lowest one. To reduce the information leakage of a specific NOMA user, power control based on beamforming optimization can be utilized

to fight against the internal eavesdropping.

- *External Eavesdropping with CSI*: We consider the case in which the eavesdropping CSI is available for the legitimate network as shown in Fig. 1(b). This is reasonable for the situations where the eavesdroppers serve as registered users of the network, but they are not allowed to access the confidential information. In this case, we can optimize the sum secrecy rate of all the legitimate users directly, following the conventional SIC decoding order constraints with respect to the transmit beamforming design.

- *External Eavesdropping without CSI*: In the scenario without eavesdropping CSI, there are two main approaches to disturb the eavesdropping, i.e., AN and IUI. When the transmit power of the base station (BS) is high enough as shown in Fig. 1(c), AN can be utilized to degrade the eavesdropping performance without affecting the legitimate transmission via beamforming optimization. On the other hand, IUI can be leveraged to assist the secure transmission when the wireless resource is inadequate as shown in Fig. 1(b). In this case, the beamforming design combined with the modified SIC order can provide novel insights for improving the security of a specific user.

Subsequently, several secure transmission schemes based on the beamforming optimization will be demonstrated in NOMA networks for the aforementioned scenarios in detail.

III. Secure Beamforming Based Privacy Protection

In NOMA networks, each user receives the messages of all the users from BS due to the superposition coding, and the stronger users with better channel conditions have to decode and subtract the messages of weaker users from the signals before decoding its own, which will cause privacy leakage, as shown in Fig. 1(a). Hence, in this section, beamforming with PA is employed to guarantee the security of a prescribed private user, considering SIC [9].
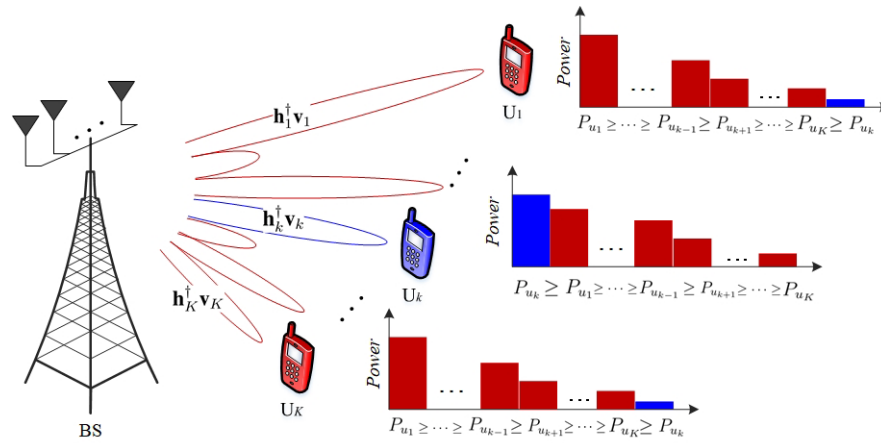
Fig. 2. Diagram of beamforming based private protection for MISO NOMA Networks.

A. Power Allocation Based on Beamforming

Considering a downlink MISO NOMA system, the BS equipped with M antennas broadcasts the messages to K single-antenna users as in Fig. 2. For clarity, let $\mathcal{K}$ denote the index set of users, i.e., $\mathcal{K} \triangleq \{1, 2, \ldots, K\}$, and U_i represents the ith user. Assume that only one specific user requires private transmission during each time slot, while others do not need secure transmission. When more than one user requires private transmission, it can be further scheduled by the BS over different time slots. Without loss of generality, we assume U_k as the private user, and the distances from the BS to all the users follows $d_K < \cdots < d_i < \cdots < d_1$. $\mathbf{h} = d^{-\frac{\alpha}{2}}\mathbf{g}$ denotes the channel gain vector with M dimensions between the BS and a certain NOMA user, where $d^{-\frac{\alpha}{2}}$ represents the large scale fading with the distance d and the path loss exponent α, and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the Rayleigh fading channel vector. According to NOMA, the BS transmits the superposed signals combining the confidential message together with other messages to the users, and the SIC at other receivers will severely threaten the privacy of U_k.

To safeguard the privacy of U_k, a novel PA strategy can be designed based on the beamforming optimization. Specifically, we optimize the PA via precoding vectors, to minimize the private information leakage at other common users and maximize it at U_k. To achieve this, the PA

constraints at common users should be expressed as $|\mathbf{h}_i^\dagger \mathbf{v}_k|^2 \leq |\mathbf{h}_i^\dagger \mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_{k+1}|^2 \leq |\mathbf{h}_i^\dagger \mathbf{v}_{k-1}|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_1|^2$, $i \in \mathcal{K}, i \neq k$, where $\mathbf{v}_i$ denotes the precoding vector of U_i. In addition, the order of the assigned power at the private receiver should satisfy the condition $|\mathbf{h}_k^\dagger \mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_k^\dagger \mathbf{v}_{k+1}|^2 \leq |\mathbf{h}_k^\dagger \mathbf{v}_{k-1}|^2 \leq \cdots \leq |\mathbf{h}_k^\dagger \mathbf{v}_1|^2 \leq |\mathbf{h}_k^\dagger \mathbf{v}_k|^2$ for enhancing its own transmission performance. Accordingly, in terms of the proposed PA strategy, the SIC decoding order should follow $U_1 \rightarrow \cdots \rightarrow U_{(k-1)} \rightarrow U_{(k+1)} \cdots \rightarrow U_K \rightarrow U_k$ and $U_k \rightarrow U_1 \rightarrow \cdots \rightarrow U_{(k-1)} \rightarrow U_{(k+1)} \rightarrow \cdots \rightarrow U_K$ at the common receivers and the *k*th receiver, respectively.

B. Privacy Protection Schemes

Based on the proposed PA strategy, two optimization schemes, the secrecy rate maximization (SRM) scheme and zero-forcing based (ZF-based) scheme, can be designed to further boost the secure transmission of U_k as well as guarantee the QoS of other users through optimizing the precoding vectors. When the number of antennas at BS is insufficient, the SRM scheme is applicable to protect the private transmission, i.e., the secrecy rate of the private user can be directly maximized with the transmission rate requirement of common users and the proposed PA constraints satisfied. In addition, it is worth noticing that the achievable rate at the *j*th common user R_j should be denoted as $\min_{j < n \leq K, n \neq K} \{ R_j^j, R_n^j \}$ when $j \in \mathcal{K} \backslash \{k, K\}$ or R_j^j when $j = K, j \neq k$ for the perfect SIC decoding, which indicates that R_j should be no larger than the minimum between the achievable rate R_j^j at U_j itself and R_n^j of U_j at U_n in order to successfully subtract the message of U_j from the received signal at U_n.

On the other hand, when the number of antennas is adequate at BS, i.e., $M \geq K$, the ZF-based scheme can be feasible. Specifically, the information leakage of U_k can be zero-forced at other common users whereby the beamforming design. Thus, the common users are impossible to obtain the private message of U_k. In this case, the secrecy rate maximization is equivalent to optimize the transmission rate of U_k. Moreover, the QoS constraints of common users, PA

constraints and zero-forcing conditions should also be satisfied in the beamforming problem.

To solve the aforementioned problems, ConCave-Convex Procedure (CCCP) can be applied to convert the non-convex problems into convex ones, and then, competitive Karush-Kuhn-Tucker (KKT) solutions can be obtained via iterations. Particularly, some auxiliary variables should be first introduced to substitute the difference between two exponential functions, and transform the objective function into the concave geometric mean of the introduced variables. The items leading to the non-convexity of the constraints can be replaced with their first-order Taylor approximations, and the non-convex constraints can be reformulated as hyperbolic ones. These steps allow us to cast the original optimization problems as convex second-order cone programming (SOCP) ones by exploiting the fact about hyperbolic constraints. Finally, the KKT solutions can be calculated by handling the SOCP problem iteratively.

C. Simulation Results

Define the distances between the BS and all the users as a set of $\vec{d} = (d_{U_K}, d_{U_{K-1}}, \ldots, d_{U_1})$. We set $\vec{d} = (5, 22.5, 40)$, $K = 3$ and $M = 3$. In Fig. 3(a), we take U_1, U_2 and U_3 as the private user, respectively, and compare the secrecy performance of the SRM scheme with the conventional NOMA scheme. From the results, we can see that U_3 has the highest secrecy rate due to the better channel condition in the SRM scheme, whilst U_1 has the lowest, which verifies our deduction that the users with stronger channel strengths can embrace higher privacy levels. In addition, the secrecy rate of the private user in the SRM scheme is clearly superior to that in the conventional NOMA scheme. In Fig. 3(b), the secrecy performance of the two proposed schemes are compared as the number of antennas increases. The results show that the secrecy rate of U_2 in the ZF-based scheme is zero when $M < K$, because the optimization problem in the ZF-based scheme is not solvable. When $M \geq K$, the two proposed schemes have close performance, and the ZF-based scheme is more attractive due to its lower complexity.
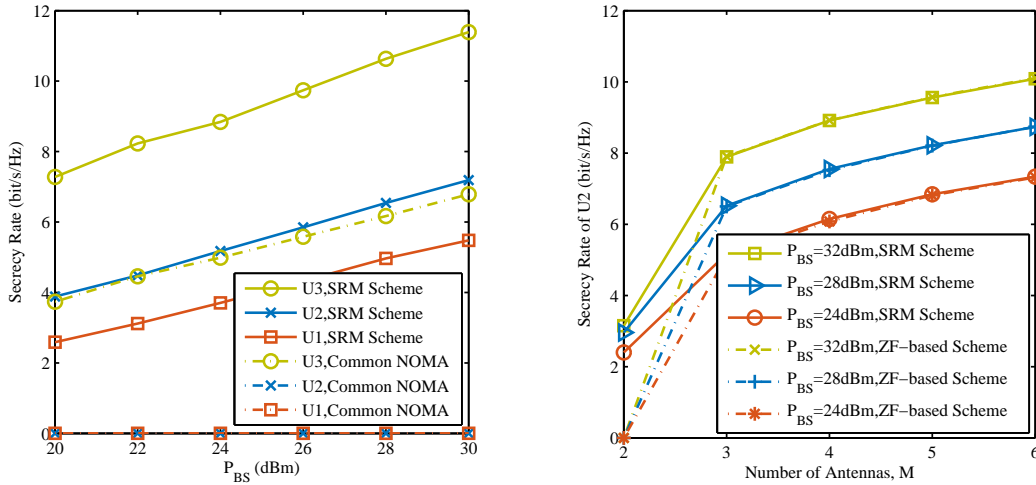
Fig. 3. (a) Secrecy rate comparison of different private users for the SRM and conventional NOMA schemes in a 3-user network. (b) Comparison of secrecy rate of the private user between the SRM and ZF-based Schemes in a 3-user network.

IV. SECURE BEAMFORMING SCHEMES WITH EAVESDROPPING CSI

For the scenarios shown in Fig. 1(b) and Fig. 1(c), secure beamforming based on PA can be designed to alleviate the external eavesdropping. In this section, we first propose the secure scheme for the case with eavesdropping CSI [14].

A. Sum Secrecy Rate Maximization Scheme

Consider a downlink MISO NOMA system with a single-antenna external eavesdropper, as shown in Fig. 1(b). We assume that the eavesdropping CSI is available at the BS, and the sum secrecy rate maximization (SSRM) problem can be formulated to improve the secure performance of the system via beamforming optimization. Thus, the precoding vectors with power information are optimized to maximize the sum secrecy rate of all the users, with constraints on the limited transmit power at BS, the PA for SIC and the rate. Notice that the IUI introduced by the superposition coding of NOMA can be favorable to confuse the eavesdropping, i.e., the eavesdropper cannot perform the SIC and tends to decode the desired signal by deeming all the other messages as noise, due to the lack of the prior knowledge of the legitimate network. Therefore, the secrecy capability can be enhanced owing to the fact that the attenuation of the
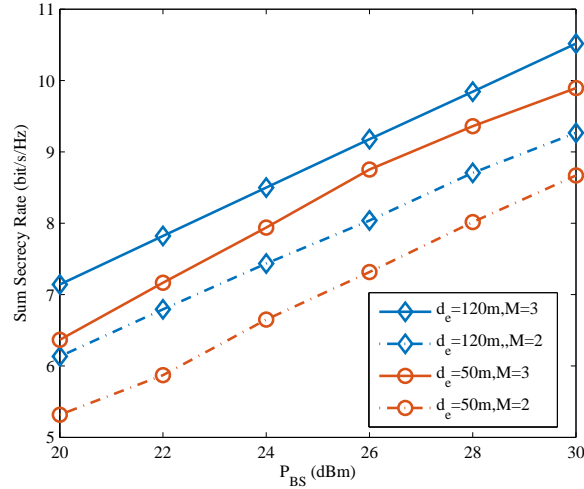
Fig. 4. Comparison of the sum secrecy rate for the proposed SSRM scheme with varying P_{BS} in a 3-user NOMA network.

eavesdropping channel caused by the IUI is worse than that of legitimate channel.

In addition, the beamforming optimization problem formulated in the SSRM scheme is non-convex as well. For the intractable objective function, linear auxiliary variables are first introduced to replace its complicate non-convex items, which are transformed as constraints. Then, the objective function is equivalent to maximizing the product of the linear variables, which can be cast as a series of second-order cone constraints using the fact about hyperbolic constraints. Similar approximation method adopted in the Section III-B can be leveraged for the non-convex items of the constraints in this problem, which are changed into convex ones subsequently. Therefore, the aforementioned iterative algorithm based on the CCCP in the last section can also be extended to solve the problem, the details of which are omitted for the limited space of the article.

B. Simulation results

In this simulation, we set $\vec{d} = (10, 55, 100)$, and the influence of the number of antennas and the eavesdropper's location on the secrecy performance of the SSRM scheme is investigated under different P_{BS}. The results show that the sum secrecy rate becomes higher with the growth of P_{BS}, and the increment of the number of antennas can further enhance the performance gains

using the sufficient spatial degrees of freedom (DoFs). Moreover, when the eavesdropper gets close to the BS, i.e. $d_e = 50$m, the sum secrecy rate declines due to its less path loss.

V. SECURE BEAMFORMING SCHEMES WITHOUT EAVESDROPPING CSI

In many scenarios, the eavesdropping CSI is difficult to obtain at BS due to the fact that the eavesdroppers may be passive during the legitimate transmission. In this case, secure schemes assisted by AN or IUI can be designed to degrade the eavesdropping performance with PA involved. In this section, the secure beamforming schemes based on AN and IUI will be elaborated for downlink MISO NOMA networks.

A. AN Injection

In the AN-based secure scheme, the BS broadcasts AN and the desired signals simultaneously, i.e., part of the transmit power at BS is utilized to send the confidential messages, while the remaining serves as AN to disturb the eavesdropping without affecting the legitimate transmission as in Fig. 1(c). To this end, the transmit power between the AN and useful signals is allocated by the beamforming optimization, and the AN should be removed in SIC before recovering the legitimate signals at receivers [13]. This means the expected PA ordering for SIC should be expressed as $|\mathbf{h}_i^\dagger \mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_1|^2 \leq |\mathbf{h}_i^\dagger \mathbf{v}_{an}|^2, i \in \mathcal{K}$. By doing so, the introduced AN only interferes the eavesdropping channel while has no impact on the information decoding of legitimate signals, and thus, the secrecy performance can be improved. Subsequently, based on the above PA constraints, we aim to maximize the transmit power of AN via optimizing the precoding vectors, subjecting to the limitation of the transmit power at BS and the constraints on the rate of NOMA users. Therefore, the eavesdropping can be disturbed as much as possible while guaranteeing the QoS of the users. In addition, when the relationship between the number of antennas and users satisfies the condition that $M \geq K + 1$, AN can be zero-forced via beamforming. In this case, the expected PA ordering for SIC can be modified as $0 = |\mathbf{h}_i^\dagger \mathbf{v}_{an}|^2 \leq$
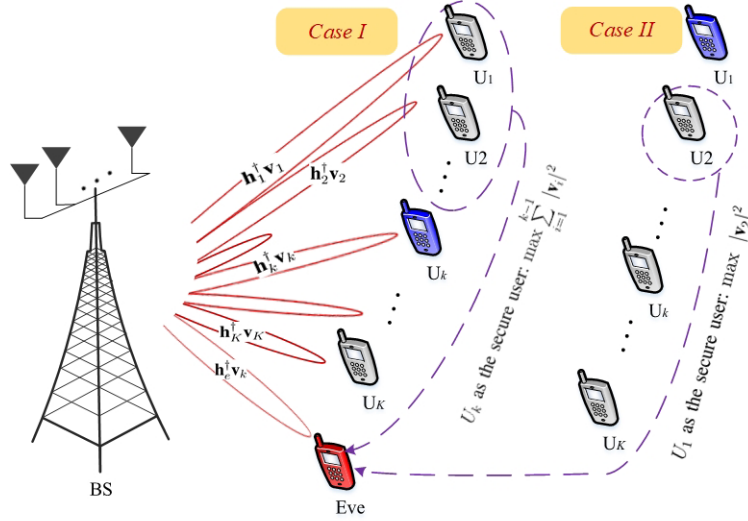
Fig. 5.   Diagram of beamforming-based IUI management for secure MISO NOMA Networks.

$|\mathbf{h}_i^\dagger \mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_i^\dagger \mathbf{v}_1|^2, i \in \mathcal{K}$. Then, similar optimization problem can be formulated with the updated PA constraints.

B. IUI Management

When there is no surplus transmit power serving as AN or the spatial DoFs are limited, IUI can be used to confuse the eavesdropper and enhance the security. Thus, via beamforming, IUI-based secure schemes are proposed to ensure the NOMA security [14]. Assume that the only one NOMA user is prescribed to perform secure transmission during each time slot. According to the different locations of users, two secure schemes based on IUI management are designed for Case I and Case II, to combat the eavesdropping, respectively, as in Fig. 5.

In Case I, U_k is the designated secure user, $2 \leq k \leq K$. To effectively fight against the eavesdropping, we aim to maximize the total transmit power from U_1 to U_{k-1} via transmit beamforming design, with the QoS of all the users satisfied. Particularly, the objective function of the problem can be formulated to maximize $\sum_{i=1}^{k-1} |\mathbf{v}_i|^2$, with the constraints including the conventional PA ordering for SIC, users' QoS requirements $R_j \geq r_j$ and the limited transmit power $\sum_{i=1}^{K} |\mathbf{v}_i|^2 \leq P_{BS}$. In this way, the IUI caused by $(k-1)$ users can be managed to

disturb the eavesdropping as much as possible, and will have no influence on the information decoding from U_k to U_K when SIC is perfectly performed. Moreover, it is reasonable to allocate more transmit power to the users with weaker channels, which is beneficial to their transmission reliability.

In Case II, we consider an extreme case of $k = 1$, i.e., the farthest user U_1 is deemed as the secure one who requires the confidential transmission. Generally, U_1 is the most vulnerable user from the view of secure transmission due to the fact that the most proportion of transmit power at BS tends to be allocated to the weakest user in conventional NOMA networks, which means that the power of the intercepted signal for U_1 at the eavesdropper will be higher than that of other users. To tackle this issue, beamforming design can be utilized to manage the IUI and safeguard the secure transmission of U_1, i.e., the transmit power of U_2 can be maximized to conceal the information of U_1 and deteriorate the eavesdropping performance by increasing the interference item of the eavesdropped SINR of U_1. Thus, in this case, the objective function should be expressed to maximize $|\mathbf{v}_2|^2$, with the rate constraints involved to satisfy the QoS of users. In addition, the PA ordering for SIC should be revised as $|\mathbf{h}_i^\dagger \mathbf{v}_2|^2 \geq |\mathbf{h}_i^\dagger \mathbf{v}_1|^2 \geq |\mathbf{h}_i^\dagger \mathbf{v}_3|^2 \geq \cdots \geq |\mathbf{h}_i^\dagger \mathbf{v}_K|^2, i \in \mathcal{K}$, which means that the expected SIC decoding order at each user should subject to $U_2 \to U_1 \to U_3 \to \cdots \to U_K$. By solving the problem, the secure performance of U_1 can be largely improved with the help of the increased IUI from the adjacent user U_2.

To effectively address the optimization problems in both cases, we first need to approximate the non-convex problems as convex ones. Particularly, the objective functions are convex quadratic functions with variables $\mathbf{v}$, which should be converted as concave ones for maximization. To achieve this goal, some linear auxiliary variables are added to make the objective function concave and non-decreasing, and then, the convex items are reformulated as the constraints with their corresponding auxiliary variables. Next, in order to transform the non-convex constraints, the quadratic items that cause non-convexity are approximately linearized by their corresponding
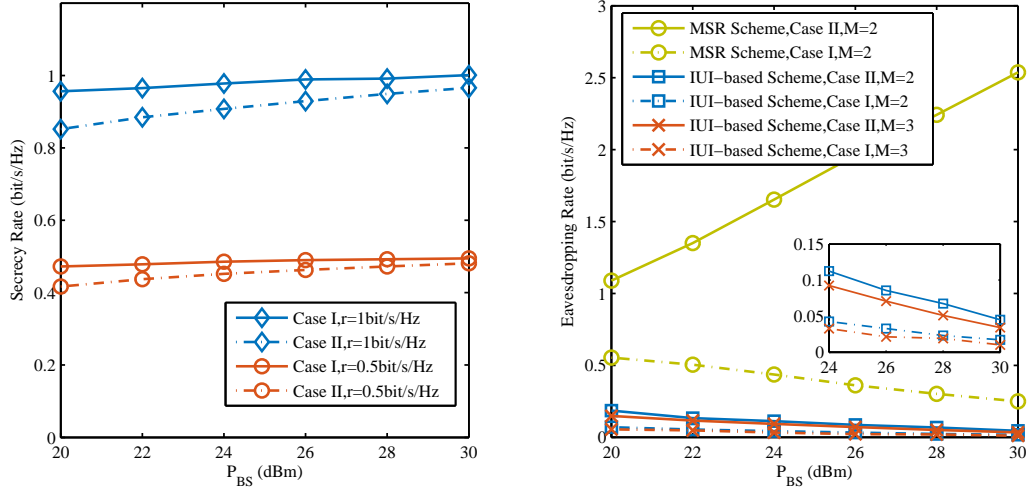
Fig. 6. (a) Secrecy rate comparison for the secure user of Case I and Case II in a 3-user NOMA network. (b) Comparison of eavesdropping rate of the secure user between the MSR and IUI-based Schemes in a 3-user NOMA network.

tangential functions in terms of CCCP. Similar to the method in Section III, the original problems can be reformulated as convex SOCPs, and their solutions can be achieved via iterations.

For the IUI-based secure schemes, when there are multiple secure users during each time slot, the transmit power of some weaker users can still be maximized to disturb the eavesdropping. If all the NOMA users demand the secure transmission simultaneously, we can rely on the AN-based secure schemes to ensure the security of legitimate networks.

C. Simulation Results

Assume that the secure user in Case I and Case II is U_2 and U_1 in a 3-user MISO NOMA network, respectively. $d_e = 20$m. In Fig. 6(a), $M = 3$, r is the QoS requirement for all the users, and the secrecy performance of the secure user in Case I and Case II is compared. From the results, it can be known that both the secrecy rate of the secure user in Case I and Case II become closer to the data rate threshold as the transmit power increases, which means that the eavesdropping performance is deteriorated by the increasing IUI, as shown in Fig. 6(b). In addition, we can also observe that the secrecy rate of U_1 is lower than that of U_2 due to the difference of their channel conditions. In Fig. 6(b), the eavesdropping rate is compared for

the proposed IUI-based scheme and the maximized sum rate (MSR) scheme in [3]. The results show that the eavesdropping rate of the MSR scheme is worse than that of IUI-based scheme since beamforming optimization problem investigated in the former scheme does not consider the security, which will severely threaten the secure transmission. In addition, the eavesdropping rate towards Case II is a little higher than that in Case I, which is consistent with the result in Fig. 6(a).

VI. OPEN RESEARCH ISSUES AND CHALLENGES

Although some preliminary works on the security of NOMA networks have been discussed from the perspective of beamforming optimization, several open research issues and challenges still need to be investigated as follows in the future.

User Clustering: In the aforementioned secure schemes, the number of NOMA users is set as K, $K \geq 2$. Actually, when massive connections are in place, i.e., K is large, the complexity of proposed schemes will increase, and more hardware resources will be required due to SIC. In this case, NOMA users should be divided into different clusters, which means that secure strategies combined with user scheduling are expected to reduce the complexity.

Robust Secure Schemes: Although we considered both cases of known and unknown eavesdropping CSI in this article, the perfect CSI of the legitimate network is assumed to be available at BS, which may be difficult to obtain due to the limited system overhead, non-negligible channel estimation and quantization errors, transmission delay, *etc* [15]. Moreover, the accuracy of the channel estimation can make a huge difference to the system performance. Thus, robust secure schemes should be further investigated for imperfect CSI.

Energy Efficiency: In the AN-based secure scheme, surplus transmit power is served as AN to effectively disturb the eavesdropping, which is directly eliminated at the receivers without affecting the legitimate transmission. This may cause a waste of energy. To solve this issue,

some other techniques like simultaneous wireless information and power transfer can be used in AN-assisted NOMA networks to achieve high energy efficiency.

Interference Management: In the Section IV-B, inter-user interference is utilized to degrade the eavesdropping channel and improve the security. However, when we consider multi-cell networks, how to manage the inter-cell interference in order to assist the secure transmission in NOMA networks is a challenging issue.

VII. CONCLUSIONS

Although NOMA can be deemed as a promising technique for high spectrum-efficiency transmission, secure issues are still inevitable due to the SIC and broadcast of wireless channels. In this article, several anti-eavesdropping schemes are proposed based on beamforming optimization for downlink MISO NOMA networks. We first investigate the internal privacy leakage problem, and design two secure beamforming schemes to safeguard the security of the private user. Then, considering the external eavesdropping, the sum secrecy rate is maximized by optimizing precoding vectors with eavesdropping CSI. Moreover, AN and IUI aided secure beamforming strategies are designed to boost the security capability without eavesdropping CSI. Finally, open issues and challenges are pointed out for secure beamforming based NOMA networks.

REFERENCES

[1] Y. Liu, H. Xing, C. Pan, A. Nallanathan, M. Elkashlan, and L. Hanzo, "Multiple-antenna-assisted non-orthogonal multiple access," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 17–23, Apr. 2018.

[2] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[3] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Trans. Signal Process.*, vol. 64, no. 1, pp. 76–88, Jan. 2016.

[4] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4438–4454, Jun. 2016.

[5] Z. Chang, L. Lei, H. Zhang, T. Ristaniemi, S. Chatzinotas, B. Ottersten, and Z. Han, "Energy-efficient and secure resource allocation for multiple-antenna NOMA with wireless power transfer," *IEEE Trans. Green Commun. and Netw.*, vol. 2, no. 4, pp. 1059–1071, Dec. 2018.

[6] Z. Lin, M. Lin, J. Wang, T. De Cola, and J. Wang, "Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 657–670, Jun. 2019.

[7] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[8] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[9] Y. Cao, N. Zhao, Y. Chen, M. Jin, L. Fan, Z. Ding, and F. R. Yu, "Privacy preservation via beamforming for NOMA," *IEEE Trans. Wireless Commun.*, Online, DOI: 10.1109/TWC.2019.2916363.

[10] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[11] N. Nandan, S. Majhi, and H. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, Aug. 2018.

[12] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[13] N. Zhao, W. Wang, J. Wang, Y. Chen, Y. Lin, Z. Ding, and N. C. Beaulieu, "Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2294–2305, Mar. 2019.

[14] N. Zhao, D. Li, M. Liu, Y. Cao, Y. Chen, Z. Ding, and X. Wang, "Secure transmission via joint precoding optimization for downlink MISO NOMA," *IEEE Trans. Veh. Technol.*, Online, DOI: 10.1109/TVT.2019.2920144.

[15] L. Zhou, "QoE-driven delay announcement for cloud mobile media," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 1, pp. 84–94, Jan. 2017.

BIOGRAPHIES

Yang Cao (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.

Nan Zhao [Senior Member, IEEE] (zhaonan@dlut.edu.cn) is an Associate 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 Transactions on Green Communications and Networking.

Yunfei Chen [Senior Member, IEEE] (Yunfei.Chen@warwick.ac.uk) received his B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, P.R.China, in 1998 and 2001, respectively. He received his Ph.D. degree from the University of Alberta in 2006. He is currently working as an Associate Professor at the University of Warwick, U.K. His research interests include wireless communications, cognitive radios, wireless relaying and energy harvesting.

Minglu Jin [Member, IEEE] (mljin@dlut.edu.cn) received the B.S degree from University of Science and Technology in 1982, M.S. and Ph. D degrees from Beijing University of Aeronautics and Astronautics in 1984 and 1995, respectively. He was a Research Fellow in Radio & Broadcasting Research Lab at Electronics Telecommunications Research Institute (ETRI), Korea from 2001 to 2004. He is currently a professor at Dalian University of Technology. His research interests include wireless communication, wireless sensor networks, signal processing for wireless communication system.

Zhiguo Ding [Senior Member, IEEE] (zhiguo.ding@manchester.ac.uk) is currently a Professor in Communications at the University of Manchester. From Sept. 2012 to Sept. 2019, he has also been an academic visitor in Princeton University. Dr Ding research interests are 5G networks, signal processing and statistical signal processing. He has been serving as an Editor for IEEE TCOM, IEEE TVT, and served as an editor for IEEE WCL and IEEE CL. He received the EU Marie Curie Fellowship 2012-2014, IEEE TVT Top Editor 2017, 2018 IEEE COMSOC Heinrich Hertz Award, 2018 IEEE VTS Jack Neubauer Memorial Award, and 2018 IEEE SPS Best Signal Processing Letter Award.

Yonghui Li [Fellow, IEEE] (yonghui.li@sydney.edu.au) is a Professor and Director of Wireless Engineering Laboratory in School of Electrical and Information Engineering, University of Sydney. He is the recipient of the Australian Queen Elizabeth II Fellowship in 2008 and the Australian Future Fellowship in 2012. He is a Fellow of IEEE. His current research interests are in the area of wireless communications, with a particular focus on MIMO, millimeter wave communications, machine to machine communications, coding techniques and cooperative communications. He holds a number of patents granted and pending in these fields. He is now an editor for IEEE transactions on communications, IEEE transactions on vehicular technology. He also served as the guest editor for several IEEE journals, such as IEEE JSAC, IEEE Communications Magazine, IEEE IoT journal, IEEE Access. He received the best paper awards from IEEE International Conference on Communications (ICC) 2014, IEEE PIRMC 2017 and IEEE Wireless Days Conferences (WD) 2014.

F. Richard Yu [Fellow, IEEE] (richard.yu@carleton.ca) is a Professor at Carleton University, Canada. His research interests include connected/autonomous vehicles, security, and wireless. He serves on the editorial boards of several journals, including Co-Editor-in-Chief for Ad Hoc & Sensor Wireless Networks, Lead Series Editor for IEEE Transactions on Vehicular Technology, Area Editor for IEEE Communications Surveys & Tutorials, and IEEE Transactions on Green Communications and Networking. He is a Distinguished Lecturer and the Vice President (Membership) of the IEEE Vehicular Technology Society.