Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations

Preprint · May 2019

CITATIONS
0

READS
749

3 authors:

Muhammad Furqan
Istanbul Medipol University
29 PUBLICATIONS **329** CITATIONS
SEE PROFILE

Jehad Hamamreh
Antalya Bilim University
63 PUBLICATIONS **622** CITATIONS
SEE PROFILE

Huseyin Arslan
University of South Florida & Istanbul Medipol University
444 PUBLICATIONS **12,010** CITATIONS
SEE PROFILE

Physical Layer Security for Downlink NOMA: Requirements, Merits, Challenges, and Recommendations

Haji M. Furqan*, Jehad M. Hamamreh†, and Huseyin Arslan* §
School of Engineering and Natural Sciences, Istanbul Medipol *School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey
†Department of Electrical and Electronics Engineering, Antalya Bilim University, Antalya, Turkey
§Department of Electrical Engineering, University of South Florida, Tampa, USA

***Abstract*—Non-orthogonal multiple access (NOMA) has been recognized as one of the most significant enabling technologies for future wireless systems due to its eminent spectral efficiency, its ability to provide an additional degree of freedom for ultra reliable low latency communications (URLLC), and grant free random access. Meanwhile, physical layer security (PLS) has got much attention for future wireless communication systems due to its capability to efficiently complement the cryptography-based algorithms for enhancing overall security of the communication system. In this article, security design requirements for downlink power domain NOMA and solutions provided by PLS to fulfil these requirements are discussed. The merits and challenges which were encountered while employing PLS to NOMA are identified. Finally, future recommendations and prospective solutions are also presented.**

I. INTRODUCTION

NOn-orthogonal multiple access (NOMA) has received significant attention for 5G and beyond wireless systems due to its unique properties such as high spectral efficiency, low latency, improved coverage, massive connectivity, fairness and so on [1]. However, compared to orthogonal multiple access (OMA), there are some critical security risks in NOMA. More specifically, due to the broadcast of superimposed messages from multiple users at the same time over the same resources, there is a risk that an eavesdropper can overhear the information of multiple users if NOMA transmission is successfully intercepted. Moreover, in NOMA, there is a need of securing confidential messages from each other in case of untrusted users [2].

To cope up with these security risks, physical layer security (PLS) techniques have emerged as a promising solution that can complement and (in some cases) may even replace the cryptography-based approaches [2] [3]. PLS exploits the dynamic features of wireless communications, for example, random channel, fading, interference, and noise, etc., to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully. PLS approaches can be exploited to extract keys from the channel, thus avoiding key management issues. Furthermore, in PLS, channel-dependent resource allocation and link adaptation can be designed to provide flexible and scenario-specific security for 5G and beyond [2].

Based on the potential of PLS for future networks and security concerns in NOMA, designing PLS techniques for NOMA is a promising area of research. However, there is still a paucity of research works in this direction [4][5]. In this article, we first provide a quick overview of NOMA flavors and basic principles to explain security concerns more clearly. This is followed by security design objectives and solutions provided by PLS. Then, we present the merits of PLS in NOMA as compared to OMA. Challenges of PLS in NOMA, possible solutions, and future directions are addressed in the following section. The final section concludes the article.

II. DOMINANT FLAVORS AND SYSTEM MODEL FOR NOMA

In this section, different types of NOMA, basic system model, and NOMA principles are presented to explain the security designs more clearly.

A. NOMA Dominant Flavors

NOMA supports massive connectivity and enhanced spectral efficiency by allowing resource allocation in a non-orthogonal manner. There are two basic types of NOMA schemes: Power-domain (PD) NOMA and code-domain (CD) NOMA [1]. In PD-NOMA, different users' signals are directly superimposed by assigning channel quality-based power allocation to them, while sharing the same frequency-time resources. CD-NOMA, on the other hand, is like Code Division Multiple Access (CDMA), where different users are allowed to share the same frequency-time resources by using unique orthogonal code. However, CD-NOMA uses non-orthogonal codes with lower cross-correlation or sparse sequences. While uplink NOMA [6] has also been studied, more focus is given to downlink NOMA, especially by the standardization bodies, such as the third generation partnership project (3GPP) and IEEE. For example, a downlink version of PD-NOMA has been proposed for 3GPP-LTE-Advanced [7]. Hence, this paper will mainly focus on PLS techniques applied to downlink PD-NOMA to elaborate on the novel challenges and future recommendations for it.[1]

[1]Note that we will use the term NOMA in the remaining part of the paper to represent PD-NOMA [1].

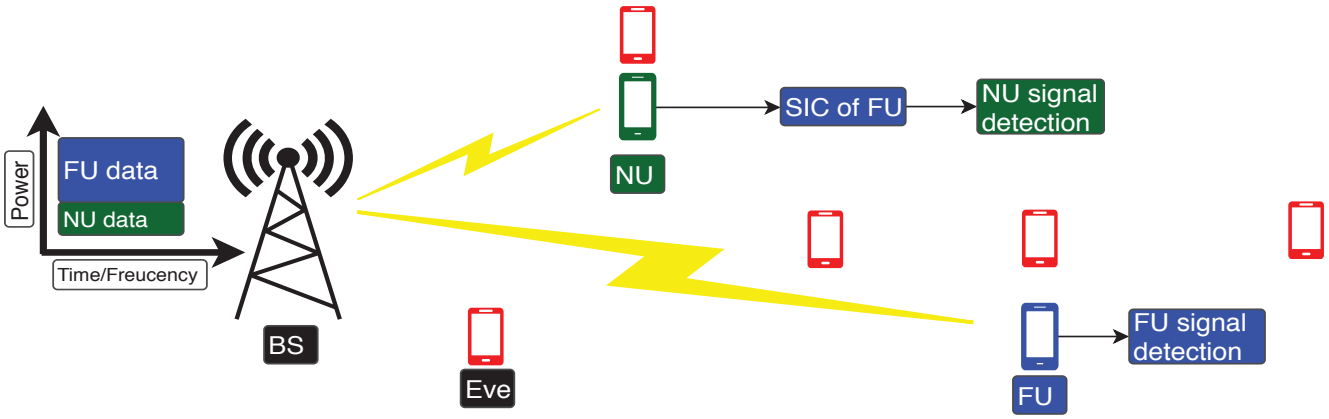

Fig. 1. Downlink NOMA detailed model which consists of a single Base Station (BS) with one Near User (NU) and one Far User (FU) in the presence of an external eavesdropper (cloned at different possible positions).

B. System Model and Principles of NOMA

Consider a simple two-user downlink NOMA scenario that consists of a single base station (BS) with one near user (NU) and one far user (FU) in the presence of an external eavesdropper (cloned at different possible positions) as shown in Fig. 1. The BS first superimposes the users' signals by allocating them different power levels and broadcasts the mixture to all users using the same time-frequency resources. The power allocation in NOMA is done in such a way that the FU (user with lower channel gain) is allocated more power and NU (user with higher channel gain) is given low power. The receivers of NOMA employ different strategies for different users in accordance with their channel characteristics. More specifically, the NU has to decode the signal intended for FU first, and afterward, it subtracts the detected signal from the received signal and then decodes its intended data. This process is known as successive interference cancellation (SIC). On the other hand, the FU directly decodes its information while considering the information of its partner as noise. It should be noted that for the sake of explanation two users case is considered here; however, the discussion is also applicable to multiple (more than two) users case. The above-mentioned case is for single-input-single-output (SISO)-NOMA, where channels are represented by scalars. However, matrices are used to represent the channels of multi-input-multi-output (MIMO)-NOMA. In the case of matrices, ordering of users based on power is quite challenging [1]. In the literature, two main designs are proposed for MIMO-NOMA case: 1) *Beamformer based MIMO-NOMA*, where different beams are allocated to different users and SIC is employed at users sharing the same resource block [1], 2) *Cluster based MIMO-NOMA*, where users are divided into clusters and a single beam can serve all the users in the cluster. In this approach, SIC is adopted among users sharing the same cluster [1].

III. SECURITY DESIGNS OBJECTIVES

In this section, different security design objectives for NOMA are presented and explained. To evaluate the secrecy performance of any security algorithm, the secrecy rate is one of the popular metrics in PLS. It is defined as the difference between the capacity of the legitimate user channel (main channel) and the capacity of the eavesdropper channel (wiretap channel).

In general, different users in NOMA can have different requirements in terms of reliability, throughput, and security, etc. which implies that the design of PLS techniques should consider these requirements. Moreover, there are two types of eavesdroppers: 1) External, and 2) Internal. An internal eavesdropper is from the set of legitimate users of the network, while the external one is not from that set [3]. The eavesdropper can be considered 1) active, or 2) passive. The active eavesdropper can interrupt wireless communication by launching jamming or channel estimation attacks while passive eavesdropper just spies on the communication without interfering with the ongoing communication.

This work is focused on both internal eavesdropping as well as passive external eavesdropping. The objectives of security design for NOMA can be divided into three major categories based on its requirements as follows:

- Security designs against external eavesdroppers.
- Security designs against internal eavesdroppers.
- Security designs against both internal and external eavesdroppers.

The details of security designs and solutions provided by PLS are presented in the subsequent part.

A. Security Designs against External Eavesdroppers

In this scenario, NU and FU are trusted. So, the design goal here is to secure the messages of NU and FU from an external eavesdropper. Based on the basic model presented in Fig.1, there are different possibilities for Eves location. In some cases, Eve is closer to BS compared to users, and her channel is better than far legitimate users. Hence, the location of Eve can affect the security performance of NOMA system and should be considered while designing security algorithms. Moreover, different users are allocated different power levels,

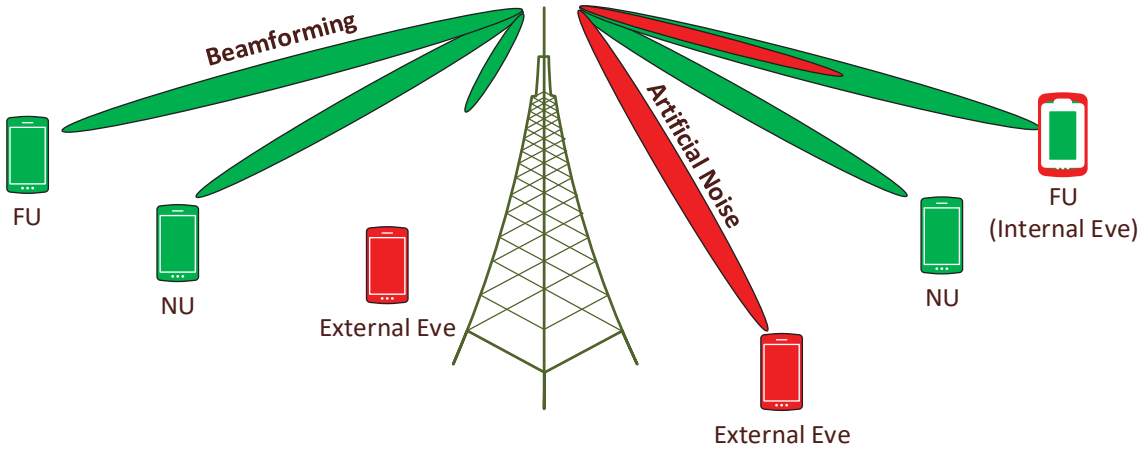

Fig. 2. Security based approaches for internal and external eavesdropper based on beamforming and AN.

due to which they are protected in an unequal manner with respect to Eve's location. More specifically, Eve can eavesdrop their signals to different extents.

The necessary conditions that need to be taken into consideration while designing algorithms for this scenario are as follows: **Firstly**, the basic SIC should be normally operated with the security algorithm, which means that the proposed algorithm should not affect the basic SIC process and the performance of normal NOMA. **Secondly**, the algorithm is also expected to work even in the case of having strong spatial similarity between channels of legitimate and illegitimate parties.

The popular PLS techniques for external eavesdropping in the literature include channel-based optimization of the power allocation for each user, subcarrier assignment to users, channel ordering of NOMA users along with the decoding order, optimization of beamforming policies, adding interfere signal, key generation, phase manipulation, transmit antenna selection (TAS) approaches and inter-user interference exploitation, etc. [2][4]. The brief details of popular approaches are as follows:

1) Beamforming: The basic idea of the beamforming-based security approach in OMA is to enhance the power of the signal at the legitimate users while suppressing it in other directions [2] as presented in Fig. 2 (left). However, this approach may not be able to fulfill the above-mentioned design requirements for secure NOMA. For example, the beamforming design matrices based on maximum ratio transmission for near and far users increase the strength of both users' signals which may not guarantee perfect SIC processing at near user [8]. Hence, these techniques need to be intelligently modified.

2) Artificial noise (AN) with beamforming: AN based techniques with beamforming are very effective against external eavesdropping in NOMA, especially when Eve is closer to BS compared to the legitimate user. The basic idea is to transmit intentional interference simultaneously with the desired signal by using the beamforming approach to degrade the performance of eavesdropper while fulfilling the above mentioned basic security design requirements for NOMA as presented in Fig. 2 (right bottom). The performance of such types of techniques is highly dependent on the availability of channel state information (CSI) of the eavesdropper. In the case of full CSI availability at the BS, optimal and efficient beamformers can be designed to enhance the security [4]. However, when CSI is not available, the beamformer should be designed to send AN in all directions except in the direction of the desired user while sending the intended signal in the direction of the desired user [8]. The major challenge here is to ensure secure communication while fulfilling the above-mentioned conditions.

3) Power allocation: Power allocation approaches based on channel conditions of legitimate users can make the interception of users signals difficult for eavesdropper under certain settings in NOMA [9]. In the case of full CSI availability, the power allocation can be optimized to maximize the secrecy rate (security) of the legitimate users [9]. However, in the case of imperfect CSI, optimal power allocation for maximizing secrecy rate (security) is not possible [4]. So, in such cases, the goal is to maximize the difference in data rate between Eve and users as much as possible.

4) Cooperative beamforming and jamming: Cooperative communication can enhance the reliability of NOMA systems by cooperative diversity. Moreover, it can also enhance the security of the NOMA system by distributed beamforming with and without cooperative jamming. In the case of distributed beamforming, the signal is directed towards the desired direction by collaborative action of relays [10]. On the other hand, in case of distributed beamforming with cooperative jamming, a group of relays is selected to focus the desired signal in the intended direction while the remaining relays are used to degrade the performance Eve by sending AN [10].

B. Security Designs against Internal Eavesdroppers

In this scenario, no external eavesdropper is assumed; however, the users are untrusted. The design goal here is to secure information of users from each other, while making sure that the SIC operation works normally. Moreover, in this case, the channel is known at the BS, which makes the design process different than the previous case. Internal eavesdropping can be divided into two types:

- Eavesdropping of FU by NU
- Eavesdropping of NU by FU

1) Eavesdropping of FU by NU: In the basic NOMA principle, the main security risk for FU is that the NU has to decode (or demodulate) the signal of FU in order to apply SIC. Another important thing is that the FU's signal is allocated more power, which makes its detection easier for the NU. The design goal here is to avoid leakage of information of FU to NU, while making sure that SIC works normally. To further elaborate on this issue, it should be pointed out that there are two types of SIC receiver: The first one is **symbol-level SIC receiver**, in which FUs signal is demodulated but not decoded in order to apply SIC, while the other one is **codeword-level SIC receiver**, where FU's signal is demodulated and decoded in order to apply SIC. In the codeword-level-SIC case, the data can only be secured by cryptography-based techniques. However, for the case of symbol-level-SIC, PLS techniques can be applied. In symbol-level based SIC, security can be provided to FUs data by transforming its data into another domain by using a special sequence such that NU can apply SIC normally, but cannot decode the information of FU [11]. Moreover, this transformation can also be done by using channel-dependent features. Note that there are not too many contributions to the literature in this direction.

2) Eavesdropping of NU by FU: In the basic NOMA principle, the FU can decode its signal directly, considering the information of near as noise. However, after obtaining its own signal, it may detect the signal of NU. The design goal here is to secure the data of NU from FU while making sure that SIC works normally. In this case, designing security methods is easier as compared to the security problem of FUs data. The BS can employ PLS techniques based on power allocation, beamforming, or any other adaptation-based algorithm to satisfy the security requirement of NU while making sure that the basic data rate requirement of FU is fulfilled. For example, in the case of beamforming, the design should consider the balance between ensuring security at the near user while reliability at the far user, as presented Fig. 2 (right top).

C. Security Designs against both Internal and External Eavesdroppers

In this scenario, there is an external eavesdropper as well as an internal eavesdropper where the users in the network are not trustable. The design goal here includes the security of signals intended for NU and FU from external eavesdropper as well from each other. This case is the most challenging one with respect to security design. The design algorithms should make sure that SIC will work normally while fulfilling the above goals. One possible way to provide security, in this case, can be by the transformation of the signal of near and far users into another domain by using some randomization sequences [11]. However, this is still an open research area, and a lot of research efforts are needed in this direction. A summary of the objectives of security designs, complexity, and popular solutions for NOMA are presented in Table. I.

IV. MERITS OF PLS IN NOMA

In this section, we present some of the merits of NOMA over OMA with respect to PLS under certain conditions.

A. Higher Sum-Secrecy Rate

In NOMA, the signals are not sent separately like OMA. Hence, multi-user interference and PLS can be processed collaboratively. Moreover, user selection, number of clusters, intra-cluster and inter-cluster power allocation can be designed based on the quality of service requirements of legitimate users such as data rate, reliability, etc. to enhance the secrecy rate of the system. For example, power allocation based on channel conditions of legitimate users can enhance the security of the system under certain settings as presented in Fig. 3 of [9] . It should be noted from the figure that the average sum secrecy rate (ASSR) of the NOMA system improves with the increase in the number of users as compared to OMA under specific settings. The reason for the improvement in ASSR is due to the dominance of legitimate users' high spectral efficiency [9].

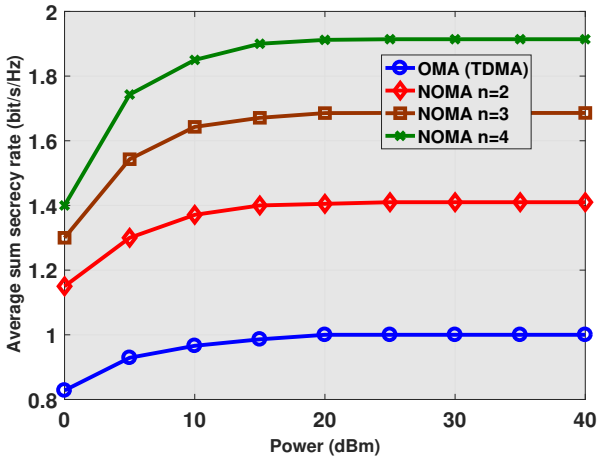

Fig. 3. Average Sum Secrecy Rate (ASSR) versus the transmit power for different number of users (n=2, n=3, n=4).

B. Inter-User Interference Exploitation for Securing Massive MIMO System

In the case of a massive MIMO system, AN-based security techniques face complexity issues. In such cases, NOMA can help us to provide secure communication without using AN [12]. For example, consider a clustering-based Massive MIMO NOMA system employing non-orthogonal channel estimation in the presence of multiple active eavesdroppers [12] as presented in Fig. 4. The nodes in this system suffer from intra-cluster and inter-cluster interference; however, this inter-user interference can be exploited intelligently in NOMA to provide secure communication [12]. More specifically, power allocation coefficients during channel estimation and multiple access stages can be designed in such a way that it will enhance the performance of legitimate users and degrade the

TABLE I
SUMMARY OF THE OBJECTIVES OF SECURITY DESIGNS FOR DIFFERENT SCENARIOS IN NOMA FOCUSING ON PASSIVE EXTERNAL EAVESDROPPER AND ACTIVE INTERNAL EAVESDROPPER.

Scenarios for security	Design objectives	Design Complexity	Candidate solutions
External Eavesdropper	Securing NU and FU data against external Eavesdropper while keeping normal SIC	Normal	Beamforming, Power allocation based, interference exploitation based, TAS, relay selection, etc.
Internal Eavesdropper	Securing users' information from each other while ensuring normal SIC	**Against NU**: High **Against FU**: Normal	**Against NU**: Transformation of FU to other domain **Against FU**: Beamforming Power allocation, TAS etc.
External and Internal Eavesdropper	Securing users' information from each other as well as from external Eve while having normal SIC	Highest	Transformation of users' signal into another domain, channel based phase rotation, interference assisted, etc.

performance of active eavesdroppers [12]. Moreover, this approach can also be extended to full-duplex NOMA to provide secure communication [4].

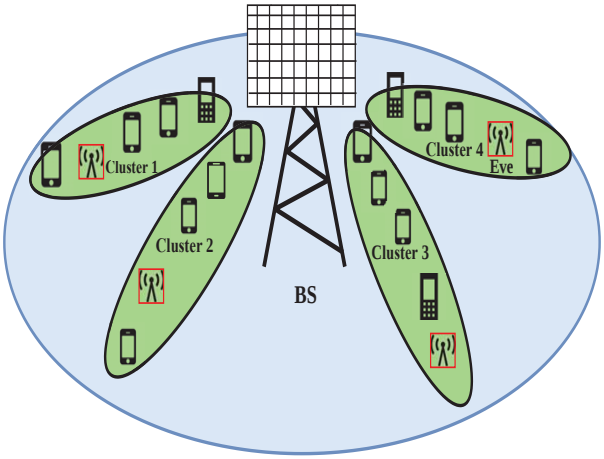

Fig. 4. Secure massive MIMO with NOMA by using inter-user interference, where users are divided into four clusters [12].

C. Securing Uni-Cast Message from Multi-Cast Receivers

An interesting advantage of NOMA is to secure a uni-cast message from interception by the untrusted multi-cast receivers while improving spectral efficiency [13] as presented in Fig. 5, where uni-cast message is for a specific receiver while the multi-cast message is for all the receivers in the set of specific receivers. In OMA, uni-casting and multi-casting are transmitted separately and can be intercepted easily by multi-casting receivers as presented in Fig. 5. However, the NOMA principle can be used to degrade the intercepting capabilities of the multi-casting receivers similar to the case of securing NU message from untrusted FU receiver [13]. More specifically, joint power allocation and beamforming strategies can be used to enhance the secrecy of uni-cast message while preserving the reliability of multi-cast message [13]. Moreover, in OMA, two slots are required to send uni-casting and multi-casting information while in NOMA both information types can be transmitted simultaneously by using a single slot [13] as presented in Fig. 5.

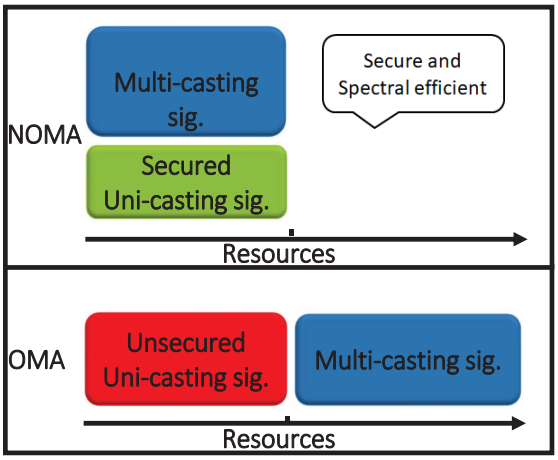

Fig. 5. Multi-casting and Uni-casting in NOMA and OMA [13].

D. Channel Correlation and Security

Most, if not all, PLS techniques (based on small scale fading) assume that the received signals at Eve and Bob will experience independent fading if they are roughly half a wavelength apart. This assumption is valid only in a sufficiently rich scattering environment. In the case of a poor scattering environment, these algorithms will not ensure secure communication. However, NOMA with large scale fading based security algorithms can provide secure communication under certain circumstances even in a poor scattering environment [5][12]. Moreover, in the case of a rich scattering environment, both the small and large scale fading based security algorithms can be applied in NOMA.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section presents the challenges in securing NOMA using PLS alongside some of the proposed solutions and research directions.

A. Challenges for Security against FU and External Eavesdroppers

There are considerable contributions in the literature regarding the provision of secure communication schemes against untrusted FU and external eavesdroppers (in case of trusted internal users), such as channel-dependent power allocation, beamforming, cooperative communication, TAS and inter-user interference, etc.. However, the majority of the research works assumes the availability of full, partial or statistical information about the CSI of Eve, which is difficult to achieve in case of passive eavesdropping. Moreover, some techniques provide security at the cost of performance degradation. Hence, conventional techniques should be intelligently modified, and novel techniques should be proposed to provide security for NOMA. Some of the potentially interesting techniques like multi-dimensional directional modulation scheme, cyclic feature suppression-based techniques, and channel-based interleaving, etc., have not been explored for such cases, whereas these techniques have the potential to be used in such situations [4].

B. Security Challenges against Untrusted NU and both External and Internal Eavesdroppers

The design of security algorithms against untrusted NU and both internal and external eavesdropper is extremely challenging. The only solutions available in the literature so far are based on the transformation of signals into another domain. This transformation is done by using a transformation sequence that needs to be shared between the legitimate parties [11]. The sequence can be shared by PLS approaches, such as full-duplex jamming based techniques for sequence sharing [11] which requires complex hardware. In this direction, the channel-based phase manipulation of symbols, directional modulation and cross-layer security techniques can also be effective. For example, automatic repeat request (ARQ) with AN can be jointly designed to provide security against internal and external eavesdropping in NOMA similar to the work presented in [14]. Moreover, joint composite constellation design and ARQ with adaptive modulation can also be used to provide security against untrusted NU. Furthermore, in the case of a rich scattering environment, channel-based manipulation security techniques can also be employed in such scenarios. This is still an open area and a lot of research efforts are needed to provide security for such cases while making sure the SIC operation works normally.

C. Passivity and Limited Observations

A lot of techniques in the literature of secure NOMA consider that the illegitimate user is just spying the information. However, in future networks, there may exist illegitimate nodes that can interfere with the normal operation of the NOMA system by active attacks, such as pilot spoofing attacks, etc. These attacks are more critical in NOMA because of the broadcast of superimposed messages of multiple users at the same time. Quite a few PLS techniques in the NOMA literature are robust to active eavesdroppers case [12]. Hence, there is a need of designing PLS techniques that are robust to active attacks from eavesdroppers. Moreover, collaborative-eavesdroppers with multiple observations may lead to zero secrecy rate [3]. Hence, there is a need for understanding the implications of collaborative-eavesdroppers and multi-observation cases while developing security techniques for NOMA.

D. SIC and Eve Capability

In the literature, it is assumed that eavesdroppers use the same SIC procedure as legitimate users. However, an eavesdropper can apply alternative strategies for eavesdropping, for example, it may decode a signal in the first step that is decoded in the last stage of SIC at legitimate users, which can affect the overall security performance of the system. Moreover, a powerful eavesdropper can apply parallel interference cancellation to simultaneously decode the users' signal [1]. Possible alternative approaches by eavesdropper should also be considered while designing security algorithms.

E. SIC Error Propagation and Secrecy

The security algorithms in NOMA mainly rely on the assumption that perfect channel estimate is available, and the signals are perfectly separated at the receiver side (perfect SIC). However, if there is an error in any of these signals during SIC, then the remaining signals may also be detected erroneously [15]. Hence, the effect of imperfect SIC and imperfect channel estimation should be considered while designing security algorithms for NOMA, so that these drawbacks can be avoided. Therefore, it is also recommended to use an efficient non-linear detection algorithm at each state of SIC to alleviate the effect of imperfect SIC and practical channel calibration solutions for imperfect channel estimation case. Moreover, new interference cancellation schemes and improvement in signal processing chip technology that can benefit the legitimate receivers are also of special interest [1].

F. AN based Security Schemes

AN-based techniques are one of the popular techniques in the literature. In these techniques, an artificial interference signal is added in the null-space of the legitimate user channel to degrade the performance of Eve. However, in NOMA, when AN is added based on the individual user, it also causes AN leakage in the range space of other NOMA users which degrades their performance. Moreover, AN may increase peak to average power ratio (PAPR), sacrifices some power, and is also sensitive to imperfect channel estimation. Thus, it is recommended to design AN, not only to provide security but also to reduce the amount of out-of-band emission (OOBE), adjacent channel interference and average PAPR, etc. [14].

G. Multi-Cell Case and Other Technologies

In the case of multi-cell NOMA, there are a lot of challenges to provide secure and reliable communication due to inter-channel interference. However, there is not much work in this

area. Algorithms for joint processing, coordinated beamforming, and coordinated scheduling need to be proposed to ensure reliable and secure multi-cell NOMA. Moreover, there is also the paucity of PLS research works for NOMA integrated with other technologies such as millimeter-wave, full-duplex, visible light communication, cognitive radio, heterogeneous networks, and coordinated multi-point, etc.

H. Cross-layer, Context-Aware and Hybrid Security Techniques for NOMA

In the literature of PLS techniques in NOMA, transmission parameters of the physical layer are optimized according to legitimate users' channel characteristics to provide secure communication without considering upper layer parameters. However, to meet the diverse requirements of NOMA users and for joint design of throughput, secrecy, delay, reliability, and respective trade-off among them, the concept of cross-layer security design from the perspective of physical layer should also be considered such as: 1) Cross MAC-PHY layer: In this approach, MAC layer features (for example, channel accessing, multiplexing, ARQ and control of resource allocation, etc.) can be optimized jointly with physical layer parameters to provide efficient QoS based security solution [14], 2) Cross NET-PHY layer security: In this approach, the network layer features such as relaying, routing and path determination, etc. can be optimized jointly with physical layer parameters for enhancing security of the system [3], 3) Cross APP-PHY layer: In this approach, physical layer parameters of transmission are jointly optimized based on channel characteristics as well as on the basis of applications, services and features of data to provide efficient security solution based on the requirements of users. Finally, designing **hybrid** techniques by combining signals security approaches (PLS) with data security approaches (cryptography) can further enhance the security of the NOMA-based systems.

I. IRS assisted PLS for NOMA

Recently, reconfigurable intelligent surfaces (RIS)-assisted networks have been proposed as a promising power-efficient solution to enable a smart and controllable wireless propagation environment. Basically, the RIS is a large array of passive reflecting elements that intelligently reflect the impinging signals in order to add different signals constructively or destructively at receivers [16]. This feature can be exploited to enhance PLS against external and internal eavesdropper in NOMA [17].

VI. Conclusion

NOMA promises high spectral efficiency, low latency, and massive connectivity, while PLS offers simple and effective security solutions. Together, these two technologies are capable of supporting the exceeding efficiency and security requirements of 5G and beyond networks. In this article, the key security design requirements of NOMA and the strength of PLS as a solution to fulfill these requirements are discussed. By employing PLS to NOMA, spectrally efficient, adaptive, and secure systems can be realized. However, the challenges and future recommendations explained in this work need to be investigated further to address the open issues. Practical secure NOMA systems can be developed by modification of current PLS techniques and/or proposing new novel techniques that do not require extra processing, extra signaling, or major modification in the receiver structure.

References

[1] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, thirdquarter 2018.

[2] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, pp. 1–1, 2018.

[3] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, April 2018.

[5] 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, March 2017.

[6] S. Althunibat, R. Mesleh, and T. F. Rahman, "A novel uplink multiple access technique based on index-modulation concept," *IEEE Transactions on Communications*, vol. 67, no. 7, pp. 4848–4855, July 2019.

[7] 3rd Generation Partnership Project (3GPP), "Study on Downlink Multiuser Superposition Transmission," Technical Report RP-150496, Mar. 2015.

[8] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with noma," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, 2019.

[9] Y. Zhang, H. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[10] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Transactions on Information Forensics and Security*, 2019.

[11] D. Xu, P. Ren, Q. Du, L. Sun, and Y. Wang, "Combat eavesdropping by full-duplex technology and signal transformation in non-orthogonal multiple access transmission," in *2017 IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[12] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 788–801, April 2018.

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

[14] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Sep. 2018.

[15] Z. Ding, M. Xu, Y. Chen, M. g. Peng, and H. V. Poor, "Embracing non-orthogonal multiple access in future wireless networks," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 3, pp. 322–339, Mar 2018.

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

[17] Almohamad, A., Tahir, A. M., Al-Kababji, A., Furqan, H. M., Khattab, T., Hasna, M. O., & Arslan, H. (2020). Smart and Secure Wireless Communications via Reflecting Intelligent Surfaces: A Short Survey. arXiv preprint arXiv:2006.14519.