An overview of methods to combat eavesdropping in NOMA-based networks through physical layer security

D Mihaylova\textsuperscript{1}, V Stoynov\textsuperscript{1}, A Ivanov\textsuperscript{1}, Z Valkova-Jarvis\textsuperscript{1}

\textsuperscript{1}Department of Communication Networks, Technical University of Sofia, bul. Kl. Ohridski 8, Sofia 1000, Bulgaria

E-mail: dam@tu-sofia.bg

Abstract. Thanks to their potentials in providing reliable communications for a large number of devices, 5G non-orthogonal multiple access (NOMA) techniques have recently been the subject of considerable research interest. Accordingly, research of Physical Layer Security approaches in NOMA is essential. A primary purpose and challenge for security at the physical level of NOMA-based systems is to protect the information transmitted against both external and internal eavesdropping attacks. To this end, it is necessary to develop PLS schemes which allow each user to decode the signals transmitted by other users, thus guaranteeing normal operation of the successive interference cancellation, while also providing privacy of the information exchange. In this paper, different types of eavesdropping are studied and a summary of existing approaches to improve security at the physical layer in 5G NOMA networks is provided.

1. Introduction

One way to answer the need for high data rate and low latency communications in fifth-generation wireless networks is by applying new multiplexing techniques for channel access. Since NOMA provides efficient spectrum utilization, it is envisaged as a key enabling technology for future radio access. Depending on the multiplexing employed, NOMA can be realized in either the code or power domain. Code-domain NOMA provides the same transmit resources to several users through the assignment of spreading sequences with low mutual correlation [1]. Power-domain NOMA, as an alternative, shares the entire radio resource by allocating different transmit powers to users conforming to the estimated channel gain [2]. This paper aims attention at power-domain NOMA, for brevity called NOMA.

Conventionally-used orthogonal-multiple access (OMA) schemes share the available resources in time, frequency, code or space domain in such a way that the signals received at different users are orthogonal to each other. Although orthogonality ensures interference mitigation, the limited transmission resources make hard the support of high data rates and low latency. To improve system throughput and user fairness, NOMA can be employed instead, as an effective multiple access that permits multiple users to transmit simultaneously on the same frequency band by means of superposition coding (SC) at the transmitter and successive interference cancelation (SIC) at the receiver side [2], [3]. Furthermore, different novel types of waveforms can be applied collaboratively with NOMA, e.g. filter bank multiearrier (FBMC) and universal filtered multiearrier (UFMC), in order to improve signal performance and spectral efficiency of 5G mobile communication systems. Since the carriers are not yet orthogonal to each other, the innovative waveform design could lead to more
flexible control of the bandwidth of each subcarrier and the degree of overlap between them. It is also to a certain extent capable of avoiding adjacent subcarrier interference, thereby leading to improved usage of spectrum resources [4]. However the operation principles of NOMA impose new challenges for the privacy enhancement of information exchange. Attractive solutions to protect the NOMA network against eavesdropping by unauthorized and/or untrusted users are the physical layer security (PLS) methods, which profits by the channel randomness to establish security instead of relying on complex computational algorithms. Moreover, PLS significantly reduces the complexity of cryptography approaches and obviates the need for secret key management, which makes it applicable in resource-constrained NOMA networks. In this paper, the PLS approaches that can be used to improve the security of downlink NOMA transmissions are investigated.

2. Main principles of NOMA
In NOMA, user ordering is established concerning their channel gains. In general, NOMA is investigated in a paired-users scenario, since increasing the number of users sharing a single resource block enlarges the complexity of SIC algorithm and increases the interference between users. According to the estimated CSI, the paired users are referred to as near user and far user, as shown in figure 1. The transmit power is shared between paired users in accordance with the following requirements: \( \alpha_f > \alpha_n \) and \( \alpha_f + \alpha_n = 1 \), where \( \alpha_f \) is the transmit power, assigned to the far user (Uf), and \( \alpha_n \) is the power factor of the near user (Un). During downlink transmission the base station (BS) performs SC of the signals \( x_f \) and \( x_n \) intended to Uf and Un respectively and broadcasts the resultant composite signal \( x \), determined by (1), to both users in the pair [2], [3]. P stands for the total transmit power, intended for the NOMA pair:

\[
x = \sqrt{P \alpha_n} x_n + \sqrt{P \alpha_f} x_f.
\]  (1)

![Figure 1. A model of downlink NOMA principles.](image)

The signals received at Uf and Un – \( y_f \) and \( y_n \) respectively are given in equation (2), where \( h_f \) stands for the channel between the BS and Uf, \( h_n \) is the downlink channel from the BS to Un, \( w_f \) and \( w_n \) are noise variables [2], [3].

\[
y_f = h_f x + w_f,
\]

\[
y_n = h_n x + w_n.
\]  (2)

As higher power weight is allocated to the \( x_f \) component of \( x \), at the far user \( x_f \) is obtained by directly decoding the received signal \( y_f \), Uf treats the \( x_n \) component of \( x \) as interference and ignores its
presence. On the Un side, in order to decode its own signal, the near user has first to decode $x_f$, considered as interference, and subtract it via SIC from the received signal $y_n$, following equation (3):

$$y'_n = y_n - h_n \sqrt{P_{f}} x_f.$$  \hspace{1cm} (3)

The residual signal after SIC, $y'_n$, is then decoded to obtain $x_n$.

3. Security concerns in NOMA-based networks

The SIC algorithm as applied in NOMA makes the concept of PLS different from that in OMA networks. On the one hand, Un, whose channel with the BS outperforms the downlink channel of $U_f$, successfully decodes $U_f$'s signal, $x_f$, which is required for proper SIC implementation. Moreover, $U_f$ is capable of partly decoding Un’s signal, $x_n$. On the other hand, the air interface of the downlink NOMA channel makes it vulnerable to eavesdropping outside the network. Therefore, NOMA downlink transmission is exposed to both external and internal eavesdropping attacks and its security enhancement can be studied separately depending on in which of the subsequent three groups it belongs [5]:

3.1. PLS to counteract external eavesdropping

When the eavesdropper (ED) is not from the users of the NOMA system, the BS is not familiar with his location and channel state information (CSI). Depending on ED’s location in the cell and the transmit power allocated to both users in the NOMA pair, different amounts of their private data can be eavesdropped by the unauthorized user. The most common PLS techniques to counteract external eavesdropping in NOMA-based networks include [5]:

- Power allocation corresponding to the estimated channel gains of $U_f$ and $U_n$;
- Beamforming aimed at $U_f$ and $U_n$;
- Artificial noise-aided (AN) beamforming to degrade the quality of the signals being eavesdropped;
- Distributed beamforming by cooperative relays with or without cooperative jamming.

The problem of eavesdropping from outside the single-input single-output (SISO) NOMA network was investigated in [6], where sharing of the total transmit power between users in the pair, so that to achieve maximal secrecy sum rate (SSR), is studied. The improved efficiency of NOMA compared to OMA is numerically proven. In [7] the SSR optimization problem under SIC and transmission power constraints of multiple-input multiple-output (MIMO) NOMA is solved by the alternating optimization method. Different strategies for choosing optimal transmit antenna in both SISO-NOMA and multiple-input single-output (MISO) NOMA scenarios are proposed in [8], where the relation between secrecy outage probability (SOP) and CSI availability is shown.

In [9] the eavesdropping of large-scale NOMA systems with one or multiple antenna elements and random user pairing is investigated. In both scenarios, it is assumed that a region exists around the BS where ED is not present, while in the multiple-antenna system, eavesdropping is additionally suppressed by generating AN. A novel beamforming scheme which exploits AN for safeguarding the downlink transmission of MISO-NOMA system is suggested in [10]. Unlike [9] and [10], in [11] AN is not induced in the system and security enhancement is accomplished by employing only the inter-user interference. Two different approaches for null-steering jamming beamforming are proposed in [12]. In the first scheme, called self-cooperative jamming, the BS sends the jamming signal during downlink transmission phase together with the information signal of legitimate users. The concept of the other scheme, nonself-cooperative jamming, includes two-stage communication of idle legitimate users for sending interfering signals towards the eavesdropper.

In [13] the privacy of unicasting data is achieved by specific beamforming and power allocation while multicasting is also accomplished. In [14] the NOMA network works cooperatively with a multi-antenna decode-and-forward relay node and a two-stage full-duplex jamming scheme with relay beamforming is proposed to improve secrecy performance. When it comes to practical cognitive radio network implementations the issue of PLS is substantial, due to their dynamic spectrum access (DSA)
mode of operation. Its complexity depends on the degree of cooperation between the incumbent and cognitive networks, where the most sophisticated PLS will be necessary for interweave deployments. If an external malicious eavesdropper is not accurately detected, this can lead to unauthorized communications or throughput degradation for the cognitive and/or incumbent users [15]. MISO-NOMA in cognitive radio scenario with simultaneous wireless information and power transfer is examined in [16], where security enhancement against multiple eavesdroppers is realized by cooperative jamming. In [17], millimetre wave NOMA is considered with imperfect SIC, where security enhancement is proposed by two maximum ratio transmission beamforming strategies. A user pairing scheme based on minimal angle difference is also introduced to protect the system against external eavesdroppers.

3.2. PLS to counteract internal eavesdropping

Since the internal ED is a user from the NOMA network, the BS is familiar with his CSI. However, the main challenge in this scenario is to establish privacy without preventing the proper accomplishment of SIC algorithm. Depending on whether the $U_f$ or $U_n$ is untrusted, internal NOMA eavesdropping is subdivided into the following types:

3.2.1. Eavesdropping on $U_n$ by $U_f$

According to the NOMA principle, $U_f$ decodes $x_f$ from the received superposed signal $x$, treating the information of the near user as interference. Even with less power, the component of $x_n$ still exists in the composite received signal which enables the far user to partially decode it. To alleviate this security issue, methods from the PLS can be employed such as power allocation, beamforming and AN aided beamforming. However, proper dimensioning of beamforming matrices is of significant importance, so as to guarantee the privacy of $U_n$’s signal, while achieving the basic rate of $U_f$.

In [18] the authors propose combining power allocation with zero-forcing beamforming to avoid information leakage to the far untrusted user of a MISO-NOMA network. An optimization approach is studied that maximizes the SSR of $U_n$ subject to a transmit power constraint at BS and transmission rate requirements for $U_f$. The same optimization problem for MIMO-NOMA is studied in [19]. Closed form expressions of the pair outage probability and the SOP of $U_n$ are derived in [20]. Two optimal schemes for relay selection in cooperative NOMA scenarios are proposed in [21], where closed form expressions of SOP and positive secrecy capacity probability are provided.

3.2.2. Eavesdropping on $U_f$ by $U_n$

As explained in Section 2, before fulfilling SIC operations, the near user $U_n$ has first to decode the signal of $U_f$. Moreover, NOMA principles for power allocation (namely, $\alpha_f > \alpha_n$) additionally facilitate detection of $x_f$ by $U_n$. Therefore, securing the far user’s information from untrusted near user eavesdropping presents a main security concern in NOMA-based networks. Dealing with this security issue is a very challenging task, since information leakage of data from the far user must be prevented, while ensuring the normal operation of SIC decoding.

In [22], a combination of beamforming and power allocation strategies is proposed, whose successful resistance to internal eavesdropping by the near user is evaluated through SOP analysis. In the case of an untrusted near user, the authors of [23] propose an angle conversion method to transform the original signals of users before transmission. Here, the constellation of the original signal differs from that of the transmitted signal, which guarantees successful SIC decoding of the transmitted signals, while maintaining the privacy of the original signals. In order to be secure, the transformations for each user follow different principles, which can be learned by the intended user via the auxiliary mechanism proposed in [23]. However, as stated in [24], this auxiliary mechanism for sharing the transformation sequences between users suffers from key-management issues. A key-less PLS technique against eavesdropping on the far user by the near user of a MISO-NOMA using directional modulation is proposed in [24]. The method simultaneously ensures the privacy of the far user data and the reliability of SIC by distorting the transmitted symbols at the near user to be from a lower order symbol alphabet. Closed-form expressions are obtained for designing the optimal
directional modulation vectors and bit-to-symbol mapping is suggested that improves the secrecy rates.

### 3.3. PLS to counteract both external and internal eavesdropping

The case of both internal and external eavesdropping represents the most severe security issue of NOMA downlink transmission, as it involves the issues of both Section 3.1 and Section 3.2. The signal transformation method, proposed in [23] against internal eavesdropping, can be applied to secure the system in such a scenario [5]. Another solution, that can be used to minimize the SOP of a system with both internal and external eavesdroppers, is the one suggested in [22].

### 4. Conclusion

Despite the numerous advantages provided by non-orthogonal multiple access, the essence of the applied SIC algorithm makes the NOMA system vulnerable to different types of eavesdropping attacks. In this paper, three varied types of NOMA eavesdropping are examined, together with an overview of methods to combat them. As far as the authors know, there is only a small number of works focused on security against internal NOMA eavesdropping on the far user by the near user. The limited number of studies on this severe problem for the security of NOMA, makes it an open research area that needs further comprehensive studies.

### References

[1] Duchemin D, Gorce J-M, Goursaud C 2018 Code Domain Non Orthogonal Multiple Access versus ALOHA: a simulation based study *ICT 2018 - 25th International Conference on Telecommunications (Saint-Malo, France) 2018* pp 445-450

[2] Islam S R, Avazov N, Dobre O A, Kwak K-S 2017 Power-domain non-orthogonalmultiple access (NOMA) in 5G systems: potentials and challenges *IEEE Communications Surveys & Tutorials* vol. 19, no. 2 pp. 721-742

[3] Saito Y, Kishiyama Y, Benjebbour A, Nakamura T, Li A, Higuchi K 2013 Non-orthogonal multiple access (NOMA) for cellular future radio access *Proceedings of the 77th IEEE Vehicular Technology Conference (VTC Spring) 2013* pp. 1–5

[4] Cai Y, Qin Z, Cui F, Li G Y, McCan, J A 2018 Modulation and Multiple Access for 5G Networks *IEEE Communications Surveys & Tutorials* vol. 20 no.1 pp. 629–646

[5] Furqan H M, Hamamreh J, Arslan H 2019 Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations *arXiv preprint arXiv:1905.05064*

[6] Zhang Y, Wang H, Yang Q, Ding Z May 2016 Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access *IEEE Communications Letters* vol. 20 no. 5 pp. 930-933

[7] Tian M, Zhang Q, Zhao S, Li Q, Qin J Aug. 2017 Secrecy Sum Rate Optimization for Downlink MIMO Nonorthogonal Multiple Access Systems *IEEE Signal Processing Letters* vol. 24 no. 8 pp. 1113-1117

[8] Lei H *et al.* 2017 On Secure NOMA Systems With Transmit Antenna Selection Schemes *IEEE Access* vol. 5 pp. 17450-17464

[9] Liu Y, Qin Z, Elkashlan M, Gao Y, Hanzo L March 2017 Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks *IEEE Transactions on Wireless Communications* vol. 16 no. 3 pp. 1656-1672

[10] Lv L, Ding Z, Ni Q, Chen J July 2018 Secure MISO-NOMA Transmission With Artificial Noise *IEEE Transactions on Vehicular Technology* vol. 67 no. 7 pp. 6700-6705

[11] He B, Liu A, Yang N, Lau V K N Oct. 2017 On the Design of Secure Non-Orthogonal Multiple Access Systems *IEEE Journal on Selected Areas in Communications* vol. 35 no. 10 pp. 2196-2206

[12] Alsaba Y, Leow C Y, Abdul Rahim S K 2019 Null-Steering Beamforming for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System *IEEE Access* vol. 7 pp. 11397-11409
[13] Ding Z, Zhao, Peng M, Poor H V July 2017 On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming IEEE Transactions on Communications vol. 65 no. 7 pp. 3151-3163

[14] Cao Y et al. Aug. 2019 Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay IEEE Transactions on Communications vol. 67 no. 8 pp. 5574-5587

[15] Singh P, Pawar P, Trivedi A Dec. 2018 Physical layer security approaches in 5G wireless communication networks 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (Jalandhar, India) pp. 477-482

[16] Zhou F, Chu Z, Sun H, Hu R Q, Hanzo L April 2018 Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT IEEE Journal on Selected Areas in Communications vol. 36 no. 4 pp. 918-931

[17] Huang S, Xiao M, Poor V August 2020 On the Physical Layer Security of Millimeter Wave NOMA Networks IEEE Transactions on Vehicular Technology

[18] Li Y, Jiang M, Zhang Q, Li Q, Qin J Aug. 2017 Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems IEEE Transactions on Vehicular Technology vol. 66 no. 8 pp. 7563-7567

[19] Jiang M, Li Y, Zhang Q, Li Q, Qin J Dec. 2017 Secure Beamforming in Downlink MIMO Nonorthogonal Multiple Access Networks IEEE Signal Processing Letters vol. 24 no. 12 pp. 1852-1856

[20] ElHalawany B M, Wu K Physical-Layer Security of NOMA 2018 Systems Under Untrusted Users 2018 IEEE Global Communications Conference (GLOBECOM), (Abu Dhabi, United Arab Emirates) pp. 1-6

[21] Cao K, Wang B, Ding H, Li T, Gong F Feb. 2020 Optimal Relay Selection for Secure NOMA Systems Under Untrusted Users IEEE Transactions on Vehicular Technology vol. 69 no. 2 pp. 1942-1955

[22] Cao K, Wang B, Ding H, Li T, Tian J, Gong F 2020 Secure Transmission Designs for NOMA Systems Against Internal and External Eavesdropping IEEE Transactions on Information Forensics and Security vol. 15 pp. 2930-2943

[23] Xu D, Ren P, Du Q, Sun L, Wang Y 2017 Combat eavesdropping by full-duplex technology and signal transformation in non-orthogonal multiple access transmission 2017 IEEE International Conference on Communications (ICC), (Paris) pp. 1-6

[24] Christopher R M, Borah D K May 2020 Physical Layer Security for Weak User in MISO NOMA Using Directional Modulation (NOMAD) IEEE Communications Letters vol. 24 no. 5 pp. 956-960

Acknowledgments
This work was supported by the National Program ”Young Scientists and Postdoctoral Students”, PMC No577, 17.08.2018, of Ministry of Education and Science of Bulgaria.