R5 Reviewer 2: comparer ma technique avec cet article

Date of publication Dec. 03, 2020, Date of current version Jan. 23, 2021

*Digital Object Identifier (DOI): 10.46470/03d8ffbd.19888ce7*

# An Advanced Non-Orthogonal Multiple Access Security Technique for Future Wireless Communication Networks

**MUHAMMAD FURQAN ZIA[1], JEHAD M. HAMAMREH[2]**

[1]Department of Electrical and Computer Engineering, Antalya Bilim University, Antalya, Turkey (e-mail: muhammad.zia@std.antalya.edu.tr)
[2]Department of Electrical and Electronics Engineering, Antalya Bilim University, Antalya,Turkey (e-mail: jehad.hamamreh@antalya.edu.tr)
Authors are from WISLAB for Innovations in Wireless Communication Computation laboratory.

Corresponding author: M. F. Zia Author (e-mail: muhammad.zia@std.antalya.edu.tr)

This work was supported in part by the Scientific and Technological Research Council of Turkey (TÜBİTAK), under project grant No. 119E392.
The matlab simulation codes used to generate the results in this paper can be found at www.researcherstore.com

**ABSTRACT** The future wireless communication systems demand much more enhanced security and reliability compared to currently deployed systems. In this work, we propose a much simpler yet more efficient physical layer security (PLS) technique for achieving reliable and secure communication in the multiple-input single-output non-orthogonal multiple access (MISO-NOMA) systems. This system is capable of providing enhanced confidential communication as well as inter-user interference cancellation without using the successive interference cancellation (SIC) method. The conventional NOMA was previously adopted under the name of multi-user superposition transmission (MUST) in release 13 of 3GPP but recently excluded from 3GPP-release 17 due to its performance degradation. In this work, we analyze the drawbacks in conventional NOMA and present a new kind of NOMA with more improved performance metrics. The proposed algorithm combines the benefit of pre-coder matrices with simultaneous transmission using antenna diversity to provide simple, reliable, and secure communication without complex processing at the receivers in downlink scenarios. The effectiveness of the proposed algorithm is verified and proven by extensive analysis and numerical simulations.

**INDEX TERMS** PLS, MISO, NOMA, SIC, 3GPP, Wireless Communication, Antenna diversity, Simultaneous transmission, Pre-coder, Complex processing, Reliable, Secure, Downlink.

## I. INTRODUCTION

THE fifth generation 5G wireless communication network is an evolution of previous fourth generation 4G networks with several new enhanced services, added reliability beyond the internet to critical communication, and the internet of things (IoT). The major hype of 5G is due to its three main characteristics that include Ultra-Reliable Low Latency Communication (URLLC), Enhanced Mobile Broadband (eMBB), and Massive Machine Type Communication (mMTC) [1]. With these enhanced services and features, 5G communication systems have become more powerful. They will have a remarkable impact on several areas of life [2], which can support many interesting applications such as smart city projects, smart energy networks, remote surgery, drone delivery, self-driven transportation, virtual reality, and many others. Although 5G has a significant impact on future technologies but still due to the broadcast nature of wireless communication, the network security always suffers from the risks to eavesdropping, which can affect the confidentiality and security of signals [3].

The existing solutions to prevent network security issues in wireless communication include cryptography and physical layer security (PLS) based solutions [4]. It is a fact that the nature of future communication is heterogeneous, which will increase the challenges for the process of key sharing and management. Therefore, cryptography-based solutions will fail to provide security for such systems, and the signals will be at risk because it can only offer the binary level of security [5]. However, the future generation's of wireless networks will be more enhanced and expected to support vast services fulfilling high-level security requirements. Moreover, some applications suffer from the poor performance of transceivers

with processing restrictions, power limitations, and sensitive nature due to delay. These drawbacks make the encryption-based algorithm unsuitable for such applications [5].

The problems encountered by encryption-based algorithms can be resolved using techniques based on PLS in future communication systems, which have emerged as the most popular and effective solution and can complement and may even replace security approaches based on cryptography [5]. PLS-based techniques can exploit different wireless channel characteristics such as fading, noise, randomness, and interference to stop unwanted and unauthorized nodes from interrupting or decoding the permitted communication underway. PLS-based security techniques can exploit any random channel between authorized users to extract secret keys, minimizing the need for key sharing. It can also be applied using basic signal processing techniques that can benefit communication devices with minimal processing and delays [6].

The orthogonal frequency division multiplexing (OFDM) waveforms are widely used in such devices. They are also commonly used in existing wireless systems and are expected to form part of future communication systems with several enhanced properties [6]. Therefore, due to its great importance in communication systems, the OFDM waveform's security has earned significant attention among several top research areas in PLS.

In the literature, PLS-based techniques proposed for OFDM can be divided into four main groups. The first one is based on secret key generation algorithms that generate the secret keys on any random wireless channel. The keys can be used on a physical layer, e.g., for channel-dependent interleaving, [7], or on the application layer for encryption [8]. The second group relates to channel adaptation aided techniques in which the fundamental idea is to change the transmission parameters of the authorized transmitter in order to enhance the performance of the authorized receiver, for example, schemes based on automatic repeat request and adaptive modulation [9], OFDM with sub-carrier index selection [10], channel shortening [11], fading based sub-carrier activation [12], pre-coding [13], etc. The third group focuses on techniques based on artificial noise. In these techniques, the artificial noise is added based on the authorized node's channel, so it can degrade the eavesdropper's performance without affecting the authorized receiver's performance [14]. The fourth one is based on algorithms that focus on the OFDM waveform's hidden characteristics [15].

Most of the techniques mentioned above do not fulfill the critical requirements of 5G networks. Besides, future applications will need reliable and secure communication, such as secure URLLC, [10] [16], or ultra-reliable, and secure communication (URSC). However, due to the combination of security and reliability, several issues arise. As the extra addition of reliability can give rise to redundancy, which can harm the communication system and PLS. As a result, PHY and MAC layers together, need to enhance the communication system's reliability and security.

This is achievable with the non-orthogonal multiple access (NOMA) scheme, which has received significant attention for 5G and beyond wireless communication systems due to its unique properties and desirable features such as high spectral efficiency, low latency, improved coverage, massive connectivity, fairness, etc. These multiple advantages of NOMA make it a suitable candidate scheme for future massive machine type communication (m-MTC) to be served and provided by 5G and beyond networks [17]. In the literature, multiple PLS schemes have been proposed for NOMA. Xiang et al. [18] proposed a NOMA network with multiple primary and secondary users. This work focuses on PLS design in cognitive radio. In this technique, firstly, the primary and secondary users are paired following their channel gain, and afterwards, the signal is transmitted using power-domain NOMA. This research suggests that by pairing the primary users with the most excellent gains or by minimizing the number of secondary users, the secrecy of data can be improved. Furthermore, Lv et al. [19], proposed new secrecy beamforming (SBF) technique by using artificial noise to secure private data of the two users within a NOMA network. This model is designed for MISO-NOMA systems such that only the eavesdropper receives a degraded version of the signals. Nevertheless, the proposed power-domain technique still suffers from SINR degradation.

In addition, S¸ahin et al. [20] proposed a waveform-domain NOMA. This proposed model presents the idea for the utilization of multiple waveforms in the same resource element, where the most appropriate waveform is allocated to each user and then decoded at the receiver. Thus, this system suffers from the drawback that it requires additional processing at the receiver, resulting in high power consumption with enhanced complexity.

Several other NOMA schemes have also been investigated in literature [21] [22] [23], including power-domain NOMA (PD-NOMA) [24], sparse code multiple access (SCMA) [25], pattern division multiple access (PDMA) [26], resource spread multiple access (RSMA) [27], multi-user shared access (MUSA) [28], interleave-grid multiple access (IGMA) [29], Welch-bound equality spread multiple access (WSMA) [30], and interleave division multiple access (IDMA) [31].

Therefore, the above mentioned NOMA schemes allows multiple users signals to be superimposed on the same resources, this leads to interference and security issues [32]. Furthermore, the existing physical layer security schemes for NOMA are either limited to the case of external eavesdropping or based on cryptography-based approaches that require key sharing and high processing with computational complexity, making it not suitable for loT requirements. Besides, the conventional NOMA in its current form suffers from several security risks and drawbacks, such as being prone to external eavesdropping and internal eavesdropping. Due to the broadcast of messages to multiple users at the same time over the same resources, there is a risk that an external eavesdropper (i.e., unauthorized, illegitimate user) can overhear and access the information of multiple users

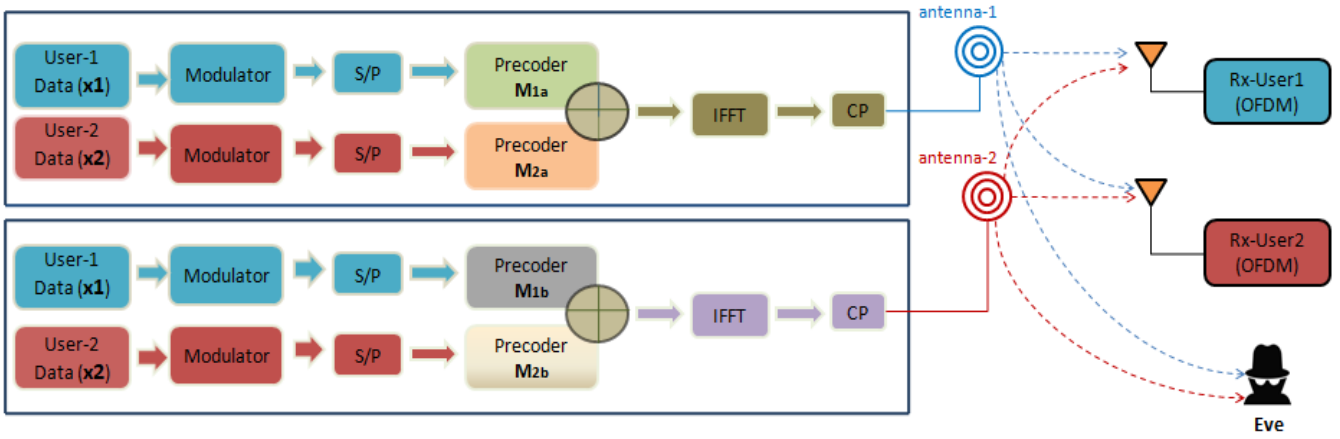



**FIGURE 1.** Basic block diagram of NOMA with signal precoding using spatial diversity based system (i.e., simultaneous transmission from two antennas enabled by MISO)

if NOMA transmission intercepts successfully. In addition, the conventional NOMA is also prone to internal eavesdropping where there is a need to secure confidential messages intended for multiple users from each other, especially in the case when untrusted users are present. Therefore, the conventional methods for sharing of data are unable to provide perfect secrecy.

From the above facts, we are inspired to propose a new kind of NOMA scheme with a simple technique of simultaneous transmission from two antennas to ensure secure and reliable communication in an OFDM system with two users. Our technique's fundamental principle is to make the simultaneous transmission more useful for the authorized receivers and useless for the eavesdropper. However, by introducing joint reliability and security through cross-layer approaches, we aim to improve both the security and reliability beyond what is achievable alone by PHY and MAC security. More specifically, NOMA, [33] inspired super-position along with pre-coder matrices, is used with simultaneous transmission from two antennas to achieve reliable and secure communication. The proposed algorithm does not require any processing at the authorized receiver, making it suitable for low-complexity communication systems that require limited processing at the receiver.

The remainder of the manuscript is organized as follows: In section II, the proposed system model is explained. The proposed algorithm and respective details are presented in section III. The performance analysis of the proposed algorithm is provided with proven mathematical expressions in section IV. The computer simulations and discussion are presented in Section V. Finally, Section VI presents the conclusion of the work.

*Notation*: Bold, lowercase letters are used for column vectors while capital letters are used for matrices.

## II. PROPOSED SYSTEM MODEL

In this section, we provide a brief description of our proposed system and its transmitter, channel model and receiver design.

### A. THE TRANSMITTER DESIGN

The transmitter design in our proposed system consists of a two-user two-antenna multi-carrier down-link authorized transmitter (Tx) that aims to communicate with two single-antenna authorized users in the presence of a passive single antenna eavesdropper as can be seen in Fig. 1. Our MISO system employs spatial diversity enabled by transmitting the same composite signal (i.e., two user signals) simultaneously from two antennas. Furthermore, we considered that the transmitter has no information regarding the channel of a passive eavesdropper.

### B. CHANNEL MODEL

It is supposed that the channel between Tx and any random user is slowly varying multi-path Rayleigh fading with the exponentially decaying function that we presume is known at the transmitter. Also, channel reciprocity property is adopted, where channel sounding techniques have the potential to be implemented to estimate the channel from the Tx to the receiver using the channel from the receiver to transmitter in time division duplexing (TDD) method. The communication system employs a simultaneous transmission of two user signals from two antennas. The authorized transmitter is responsible for the security of communication within the users so that the external eavesdropper cannot receive the user's signal information, nor the users get each other's data.

### C. THE RECEIVER DESIGN

The receiver model consists of user-1, user-2, and external eavesdropper. Both the users decode their authorized precoded data, as explained in section III, which helps in keeping the data entirely secret. While eavesdropper trying to intercept and access the data from user-1 and user-2 receives the degraded version of signals as can be seen in the next sections.

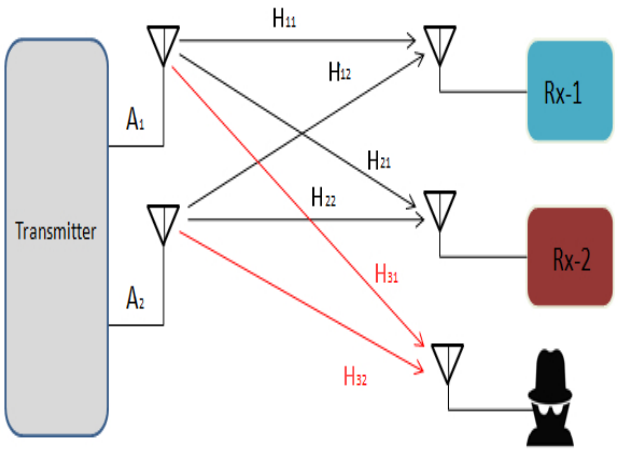



**FIGURE 2.** Channel between the transmitter, authorized users and the eavesdropper.

## III. PROPOSED ALGORITHMS

In this section, we discuss and explain our proposed algorithm and its extension for future communication systems.

### *A. ALGORITHM FOR RELIABLE AND SECURE COMMUNICATION*

This work's primary objective is to meet the requirement for future applications that need secure, reliable communication and limited processing capability at the receiver [10]. It is important to note that improving the reliability of communication makes communication riskier to eavesdropping. A common solution for providing efficient communication is the space-time code [34]. It cannot, however, ensure secure communication based on channel-independent precoder.

In our proposed technique, we superimpose two users' signals along side pre-coder matrices and transmit them simultaneously from two antennas. However, it should ensure that this simultaneous transmission occurs in different channels and not on the same channel. It also allows us to develop and find a specific set of pre-coder that can simultaneously protect against internal and external eavesdroppers. Besides, compared to a single-user channel-based security algorithm, two user signals that transmit simultaneously from two antennas create more difficulty for the eavesdropper. The explanation for this is that, in simultaneous transmission from two antennas of the proposed algorithm, the pre-coders used are a function of various authorized user channels. However, in the case of single-user based algorithms, the pre-coder is a single-user channel function only. So, the simultaneous transmission role makes it more difficult for the eavesdropper to decode the legitimate user signal while making it easier for authorized users to decode the required information.

Moreover, in conventional NOMA [33], there is only one transmission used with interference cancellation at the authorized receiver. But in our proposed technique, interference cancellation is not required. We transmit the signal simultaneously from two antennas, which results in an automatic interference cancellation because of the specially designed precoding matrices. In our proposed method, we ensure reliability and security through joint PHY and MAC mechanisms. In particular, NOMA inspired pre-coded superposition coding, together with cross-layer principles of simultaneous transmission with antenna diversity, is implemented. It made communication more secure and reliable for downlink scenarios without requiring any additional computational processing at the receiver.

The details of the proposed algorithm are as follows: We consider a two-user and two antenna multi-carrier system as shown in Fig.1. At the transmitter (Tx), the total number of modulated symbols in one OFDM block for each user is $N_f$. Thus, the frequency response of each OFDM symbol for user-1 and user-2 can be represented as $\mathbf{x_1} = [x_0 x_1 ..... x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$ and $\mathbf{x_2} = [x_0 x_1 ..... x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$, respectively. Note that $\mathbf{y_{km}} \in \mathbb{C}^{[N_f \times 1]}$, $\mathbf{H_{km}} \in \mathbb{C}^{[N_f \times N_f]}$ and $\mathbf{z_{km}} \in \mathbb{C}^{[N_f \times 1]}$, respectively, present the received signal, the diagonal matrix for frequency response of the channel and Additive White Gaussian Noise (AWGN) between $k_{th}$ user and $m_{th}$ antenna of the transmitter.

The basic steps for the design of pre-coder matrices for the proposed algorithm are presented in the subsequent discussion. On the basis of the proposed algorithm, the superimposed pre-coded transmitted signal from antenna-1 is given as:

$$\mathbf{u_1} = \mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}. \quad (1)$$

Similarly, the superimposed pre-coded transmitted signal from antenna-2 can be given as:

$$\mathbf{u_2} = \mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}, \quad (2)$$

where $\mathbf{x_1}$ and $\mathbf{x_2}$ are data vectors in frequency domain intended for user-1 and user-2, respectively, with the total power divided equally between them, while $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ are specially designed pre-coder matrices based on the channel of authorized nodes. These pre-coders will make sure that the user-1 and user-2 will get reliable signals which are also secure from internal and external eavesdropping. We will first explain the details about the received signal at user-1, user-2, and eavesdropper in the following two subsections. Afterward, the details about designing the pre-coding matrices will be explained.

#### 1) Received Signal at User-1

The received signal in the frequency domain at user-1 from transmission through antenna-1 can be given as:

$$\mathbf{y_{11}} = \mathbf{H_{11}u_1} + \mathbf{z_{11}}, \quad (3)$$

where $\mathbf{H_{11}}$ and $\mathbf{z_{11}}$ are the frequency response of the channel and Additive White Gaussian Noise (AWGN) between user-1 and antenna-1.

Similarly, the received signal at user-1 from transmission using antenna-2 is given as:

$$\mathbf{y_{12}} = \mathbf{H_{12}u_2} + \mathbf{z_{12}}, \tag{4}$$

where $\mathbf{H_{12}}$ and $\mathbf{z_{12}}$ are the frequency response of the channel and AWGN between user-1 and antenna-2.

The combined received signal at user-1 from simultaneous transmission through antenna-1 and antenna-2 can be given as:

$$\hat{\mathbf{y}}_1 = \mathbf{y_{11}} + \mathbf{y_{12}}, \tag{5}$$

where $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$ are the received signals at user-1 from simultaneous transmission through antenna-1 and antenna-2, respectively. After putting the values of $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$, the combined signal can be presented as follows:

$$\hat{\mathbf{y}}_1 = \mathbf{H_{11}u_1} + \mathbf{z_{11}} + \mathbf{H_{12}u_2} + \mathbf{z_{12}}. \tag{6}$$

Substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (1) and (2) and simplifying, we get:

$$\hat{\mathbf{y}}_1 = \mathbf{H_{11}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{11}} + \mathbf{H_{12}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{12}}, \tag{7}$$

$$\hat{\mathbf{y}}_1 = (\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}})\mathbf{x}_1 + (\mathbf{H_{11}M_{2a}} + \mathbf{H_{12}M_{2b}})\mathbf{x_2} + \mathbf{z_{11}} + \mathbf{z_{12}}. \tag{8}$$

The first term in (8) is the desired term with respect to user-1 while the second term is undesired. The pre-coder matrices will make sure that the undesired term as well as the channel effects are removed and canceled at user-1.

### 2) Received Signal at User-2

Similar to user-1, the expression for combined received signal at user-2 from simultaneous transmission through antenna-1 and antenna-2 can be written as:

$$\hat{\mathbf{y}}_2 = \mathbf{y_{21}} + \mathbf{y_{22}}, \tag{9}$$

where $\mathbf{y_{21}} = \mathbf{H_{21}u_1} + \mathbf{z_{21}}$ and $\mathbf{y_{22}} = \mathbf{H_{22}u_2} + \mathbf{z_{22}}$ are the received signals at user-2 from antenna-1 and antenna-2, respectively. $\mathbf{H_{21}}$ and $\mathbf{z_{21}}$ are the frequency response of the channel and AWGN between user-2 and antenna-1 of the trasmitter while $\mathbf{H_{22}}$ and $\mathbf{z_{22}}$ are the frequency response of the channel and AWGN between user-2 and antenna-2. After putting the values of $\mathbf{y_{21}}$ and $\mathbf{y_{22}}$, the combined signal can be presented as:

$$\hat{\mathbf{y}}_2 = \mathbf{H_{21}u_1} + \mathbf{z_{21}} + \mathbf{H_{22}u_2} + \mathbf{z_{22}}. \tag{10}$$

Substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (1) and (2) and simplifying, we get:

$$\hat{\mathbf{y}}_2 = \mathbf{H_{21}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{21}} + \mathbf{H_{22}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{22}}, \tag{11}$$

$$\hat{\mathbf{y}}_2 = (\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}})\mathbf{x}_1 + (\mathbf{H_{21}M_{2a}} + \mathbf{H_{22}M_{2b}})\mathbf{x_2} + \mathbf{z_{21}} + \mathbf{z_{22}}. \tag{12}$$

The first term in equation (12) is the undesired term for user-2 while the second term is desired for it.

### 3) Received Signal at Eavesdropper

For the case of eavesdropper, the combined received signal from simultaneous transmission through antenna-1 and antenna-2 can be written as:

$$\hat{\mathbf{y}}_3 = \mathbf{y_{31}} + \mathbf{y_{32}}, \tag{13}$$

where $\mathbf{y_{31}} = \mathbf{H_{31}u_1} + \mathbf{z_{31}}$ and $\mathbf{y_{32}} = \mathbf{H_{32}u_2} + \mathbf{z_{32}}$ are the received signal at eavesdropper from antenna-1 and antenna-2, respectively. $\mathbf{H_{31}}$ and $\mathbf{z_{31}}$ are the frequency response of the channel and AWGN between eavesdropper and antenna-1 while $\mathbf{H_{32}}$ and $\mathbf{z_{32}}$ are the frequency response of the channel and AWGN between eavesdropper and antenna-2. After putting the value of $\mathbf{y_{31}}$ and $\mathbf{y_{32}}$, the combined signal can be presented as:

$$\hat{\mathbf{y}}_3 = \mathbf{H_{31}u_1} + \mathbf{z_{31}} + \mathbf{H_{32}u_2} + \mathbf{z_{32}}, \tag{14}$$

Substituting values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (1) and (2) and simplifying as follows:

$$\hat{\mathbf{y}}_3 = \mathbf{H_{31}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{31}} + \mathbf{H_{32}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{32}}, \tag{15}$$

$$\hat{\mathbf{y}}_3 = (\mathbf{H_{31}M_{1a}} + \mathbf{H_{32}M_{1b}})\mathbf{x}_1 + (\mathbf{H_{31}M_{2a}} + \mathbf{H_{32}M_{2b}})\mathbf{x_2} + \mathbf{z_{31}} + \mathbf{z_{32}}. \tag{16}$$

The eavesdropper wants to get information about both user-1 and user-2. Hence, for it both first and second terms of (16) are desired terms.

### 4) Pre-coder Design for the Proposed Algorithm

We need to design pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ in such a way that the combined received signal from simultaneous transmission through both antennas at the authorized users will provide reliable data intended for them while keeping the communication secure from internal and external eavesdropping. The design of pre-coder matrices is inspired by several interesting works in the literature such as, [35] [36].

The design procedure of $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ is as follows: Firstly, in order to remove the effect of the channel at user-1, the first term in the equation (8) should be equal to identity matrix and can be given as:

$$\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}} = \mathbf{I}, \tag{17}$$

Also, in order to cancel the interference caused by user-1 on user-2, the first term in equation (12) should be zero and can be given as:

$$\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}} = 0, \tag{18}$$

Equations (17) and (18) can be jointly solved to get the values of pre-coder matrices $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ as follows:

$$\mathbf{M_{1a}} = \mathbf{H_{22}}(\mathbf{H_{22}H_{11}} - \mathbf{H_{21}H_{12}})^{-1}, \tag{19}$$

$$\mathbf{M_{1b}} = -\mathbf{H_{21}}(\mathbf{H_{22}H_{11}} - \mathbf{H_{21}H_{12}})^{-1}. \tag{20}$$

Similarly, in order to design $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$, we will follow similar steps as explained earlier. In order to remove the effect of the channel at user-2, the second term in equation (12) should be equal to identity and can be given as:

$$\mathbf{H_{21}M_{2a} + H_{22}M_{2b} = I}. \tag{21}$$

Also, in order to cancel the interference caused by user-2 on user-1, the second term should be zero in equation (8) and can be given as:

$$\mathbf{H_{11}M_{2a} + H_{12}M_{2b}} = 0, \tag{22}$$

Equations (21) and (22) can be jointly solved to get the values of pre-coder matrices as follows:

$$\mathbf{M_{2a}} = \mathbf{H_{12}}(\mathbf{H_{12}H_{21} - H_{11}H_{22}})^{-1}, \tag{23}$$

$$\mathbf{M_{2b}} = -\mathbf{H_{11}}(\mathbf{H_{12}H_{21} - H_{11}H_{22}})^{-1}. \tag{24}$$

The values of pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ are given in equations (19), (20), (23) and (24), respectively, will be used in the simultaneous transmission to make sure that the user-1 and user-2 will get reliable signals which are secure from internal and external eavesdroppers.

### B. SIGNIFICANCE OF THE PROPOSED ALGORITHM

There are significant benefits to the proposed algorithm that can be summarized as follows:

- *Security against external eavesdropping:* The proposed method can provide security against external Eve because the pre-coders are dependent on the channels of the legitimate nodes.
- *Security against internal eavesdropping:* The proposed algorithm can also provide security against internal Eve by ensuring that there will be no leakage of information among users.
- *Less complexity:* Due to the diagonal channel matrices, the inverse operation is simple. Hence, pre-coder matrices can be designed by simple computation.
- *Limited processing:* In our proposed approach, there is no need for interference cancellation because we transmit the signal simultaneously from two antennas at one time and there is an automatic interference cancellation due to the specially designed pre-coding matrices. Hence, it can support applications with processing limited receiver (IoT-based application).
- *Enhanced complexity for eavesdroppers:* Mixture of channel-based pre-coded signals of two users that are transmitted simultaneously from two antennas is more challenging to eavesdrop compared to channel adaptive secure transmission based on a single user.

## IV. PERFORMANCE ANALYSIS FOR THE PROPOSED ALGORITHM

In this section, we present a performance analysis of the theoretical bit error rate (BER) of the authorized node using the proposed algorithm. We also discuss the BER performance details of the eavesdropper, who is supposedly trying to eavesdrop user-1 and user-2 information.

To calculate the analytical results related to the BER performance of the authorized user, we use numerical data fitting methods, similar to the work presented in [37]. In order to calculate BER, we need to find the statistics of the effective instantaneous signal-to-noise ratio (SNR), $\gamma_{\mathbf{b}}$, at the legitimate node. The values of pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ given in equations 19, 20, 23 and 24, respectively, make sure that the interference term as well as the channel effects are removed at both user-1 and user-2 corresponding to equation 8 and 12, respectively. In the first step, we use the numerical data fitting method for finding the statistics of $\gamma_{\mathbf{b}}$ at any user to obtain the distribution of power of sub-channels corresponding to the received signal [37]. More specifically, we simulate 10000 realizations from both AWGN and Rayleigh fading distributions. Subsequently, the proposed scheme is applied, followed by the use of curve fitting tools to obtain the best matching distribution for the power of the sub-channels corresponding to the received signal.

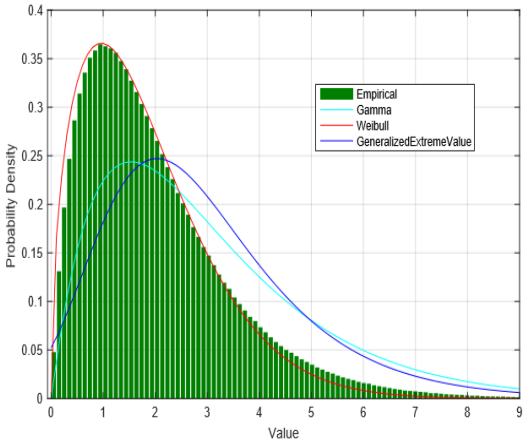



**FIGURE 3.** The power distribution of the sub-channels using curve fitting tools at any user based on proposed technique.

Moreover, as can be seen from Fig. 3, power distribution of the sub-channels using curve fitting tools at any user based on the proposed technique follows the Gamma distribution [38]. Where, the scale and shape parameters are given as w = 1.53 and u = 2.08, respectively.

The probability density function (PDF) for the effective instantaneous SNR, $\gamma_{\mathbf{b}}$ , at the authorized node, with Gamma distributed, [38], sub-channels' power can be given in simplified form similar to the work presented in, [37], with some modifications and approximation as follows:

$$P_{\gamma_b}(\gamma_b) \approx \left(\frac{\mathbf{1}}{\mathbf{w}}\right)^{u} \frac{\mathbf{1}}{\mathbf{\Gamma(u)}} \frac{\mathbf{\Omega^{\frac{3}{2}}}\sqrt{\gamma_{\mathbf{b}}}}{\bar{\gamma}_{\mathbf{b}}^{\frac{3}{2}}} \exp\left(-\frac{\mathbf{1}}{\mathbf{w}}\frac{\mathbf{\Omega}\gamma_{\mathbf{b}}}{\bar{\gamma}_{\mathbf{b}}}\right), \tag{25}$$

where $\mathbf{w}$ and $\mathbf{u}$ are the scale and shape parameters, $\Omega$ is the mean square of sub-channels, $\bar{\gamma_\mathbf{b}}$ is average SNR and $\mathbf{\Gamma(u)}$ is the gamma function.

The BER can be evaluated analytically by using PDF of instantaneous SNR, $\gamma_\mathbf{b}$ , [39] as follows:

$$BER_b = \frac{\mathbf{1}}{\mathbf{2}} \int_0^\infty \mathbf{erfc}(\sqrt{\gamma_\mathbf{b}}) P_{\gamma_\mathbf{b}}(\gamma_\mathbf{b}) d\gamma_\mathbf{b}. \tag{26}$$

By substituting the value of PDF of SNR, $\gamma_\mathbf{b}$, the resultant equation can be given as:

$$BER_b = \frac{\mathbf{1}}{\mathbf{2}} \int_0^\infty \mathbf{erfc}(\sqrt{\gamma_\mathbf{b}}) \left(\frac{\mathbf{1}}{\mathbf{w}}\right)^u \frac{\mathbf{1}}{\mathbf{\Gamma(u)}} \frac{\mathbf{\Omega^{\frac{3}{2}}} \sqrt{\gamma_\mathbf{b}}}{\bar{\gamma_\mathbf{b}}^{\frac{3}{2}}} \times$$

$$\exp\left(-\frac{\mathbf{1}}{\mathbf{w}} \frac{\mathbf{\Omega}\gamma_\mathbf{b}}{\bar{\gamma_\mathbf{b}}}\right) d\gamma_\mathbf{b}. \tag{27}$$

By simplifying the above equation based on [37], the BER formula can be given as:

$$BER_b \approx \frac{\mathbf{G}}{\mathbf{2}\sqrt{\pi}} \left(\frac{\arctan\left(\sqrt{\rho}\right)}{\mathbf{2}\rho^{\mathbf{3/2}}} - \frac{\mathbf{1}}{\mathbf{2}\rho\left(\mathbf{1}+\rho\right)}\right), \tag{28}$$

where, $G = \left(\frac{1}{\mathbf{w}}\right)^{\mathbf{u}} \frac{\mathbf{1}}{\mathbf{\Gamma(u)}} \frac{\mathbf{\Omega^{\frac{3}{2}}}}{\bar{\gamma_\mathbf{b}}^{\frac{3}{2}}}$ , $\rho = \frac{\mathbf{1}}{\mathbf{w}} \frac{\Omega}{\bar{\gamma_b}}$ and arctan $(\cdot)$ is the tangent inverse.

Finally, for the case of an eavesdropper, it is observed from equation (16) that the eavesdropper is interested in eavesdropping the data of both user-1 and user-2. The signal-to-interference-plus-noise ratio (SINR) at eavesdropper for eavesdropping the information intended for user-1 is given as:

$$SINR_{e1} = \frac{(|\mathbf{H_{22}}|^2|\mathbf{H_{31}}|^2 + |\mathbf{H_{21}}|^2|\mathbf{H_{32}}|^2)|\mathbf{x_1}|^2}{(|\mathbf{H_{11}}|^2|\mathbf{H_{32}}|^2 + |\mathbf{H_{12}}|^2|\mathbf{H_{31}}|^2)|\mathbf{x_2}|^2 + \sigma_{\mathbf{31}}^{\mathbf{2}}} \tag{29}$$

where $\sigma_{\mathbf{31}}^{\mathbf{2}}$ is the variance of noise power corresponding to $\mathbf{H_{31}z_{31}}$. Similarly, the SINR at eavesdropper for eavesdropping the information intended for user-2 is given as:

$$SINR_{e2} = \frac{(|\mathbf{H_{11}}|^2|\mathbf{H_{32}}|^2 + |\mathbf{H_{12}}|^2|\mathbf{H_{31}}|^2)|\mathbf{x_2}|^2}{(|\mathbf{H_{22}}|^2|\mathbf{H_{31}}|^2 + |\mathbf{H_{21}}|^2|\mathbf{H_{32}}|^2)|\mathbf{x_1}|^2 + \sigma_{\mathbf{32}}^{\mathbf{2}}} \tag{30}$$

where $\sigma_{\mathbf{32}}^{\mathbf{2}}$ is the variance of noise power corresponding to $\mathbf{H_{32}z_{32}}$.

It is clear from equations 29 and 30 that there is a severe performance degradation at eavesdropper when it tries to eavesdrop the information intended for either user because of interference terms (inter-user interference) in the denominators of these equations. Moreover, the terms $\mathbf{H_{11}}$ , $\mathbf{H_{12}}$, $\mathbf{H_{21}}$, and $\mathbf{H_{22}}$ are unknown to the eavesdropper, making eavesdropping more challenging. The SINR distribution at eavesdropper by the above-mentioned fitting methods doesn't fit into any appropriate placement. Hence, we explain intuitively about equations 29 and 30.

## V. SIMULATION RESULTS

In this section, we evaluate the performance for superimposed pre-coder matrices with simultaneous transmission using antenna diversity for two users' signals. We present the simulation results for the proposed algorithm and its extension. The simulation of bit error rate (BER), throughput, packet error rate (PER), and peak to average power ratio (PAPR) used as performance metrics, proves the effectiveness of our proposed technique.

We consider that the Tx is employing OFDM with $N_f = 64$ sub-carriers for each user. The added cyclic prefix (CP) helps in avoiding inter-symbol interference (ISI). The channel is assumed to be multi-path rayleigh fading channel between the transmitter and receiving nodes (such as users and eavesdropper) with an equal number of taps ($L = 9$) as shown in Table-I.

**TABLE 1.** System parameters.

| | |
|---|---|
| Channel | Multi-path Rayleigh fading channel |
| Channel length | 9 |
| Cyclic prefix (CP) | 9 |
| FFT size | 64 |
| Modulation type | BPSK |

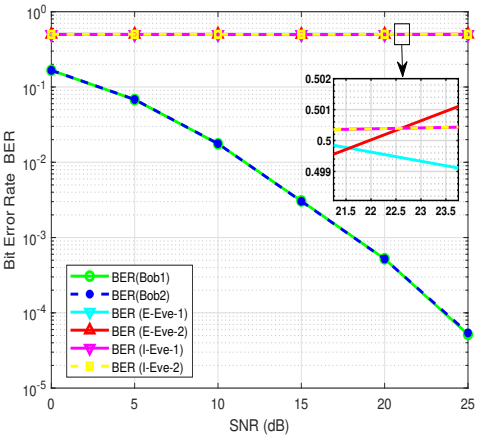



**FIGURE 4.** Bit Error Rate (BER) versus SNR performance analysis for the proposed algorithm.

Figure 4 presents the bit error rate (BER) versus signal to noise ratio (SNR) plots for the proposed algorithm (explained in subsection-III-A), multiple-input single-output (MISO) system. It is clear from Fig. 4 that the BER performances of user-1 (Bob-1) and user-2 (Bob-2) employing the proposed algorithm are similar to each other. However, there is a significant gap between their BER performances and external and internal eavesdropper ones. The labels E-Eve-1 and E-Eve-2 show the BER performance of the external eavesdropper that is trying to eavesdrop the signals intended for user-1 and user-2, respectively. Labels I-Eve-1 and I-Eve-2 represent the BER performance of the internal eavesdropper that is internally trying to eavesdrop the signal between user-1 and user-2. The degraded BER performances of external and internal

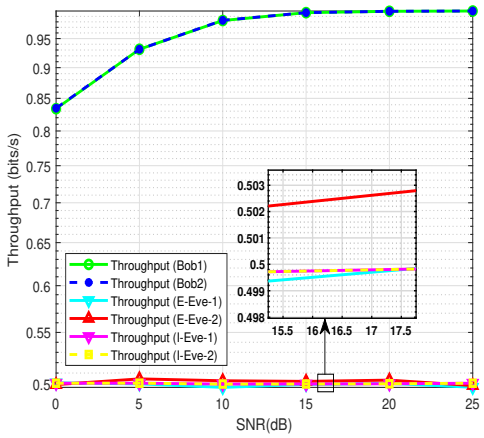



**FIGURE 5.** Throughput versus SNR performance analysis for the proposed algorithm.

eavesdropper show that the proposed algorithm can provide reliable and secure communication.

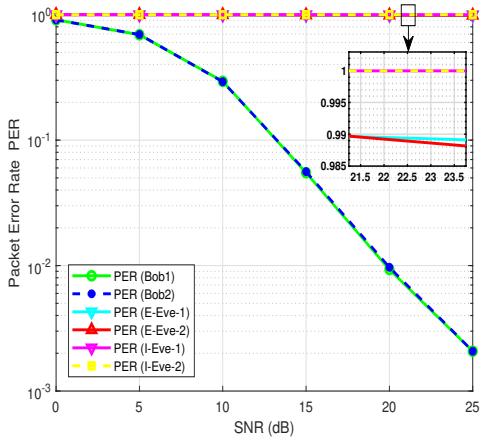



**FIGURE 6.** Packet error rate (PER) versus SNR performance analysis for the proposed algorithm.

Figure 5 presents the throughput plots for the basic proposed algorithm, multiple input single output (MISO) system. Through experiments, we have observed that the number of transmitted packets in the proposed system is equal to the number of time slots, enhancing the joint throughput of authorized users. As can be seen from Fig. 5, the individual throughput performances of user-1 (Bob-1) and user-2 (Bob-2) employing the proposed algorithm are similar to each other. The excellent throughput performance of the authorized user's signals and the deterioration of external and internal eavesdropper's signals proves our proposed algorithm's robustness. It is essential to consider that although eavesdroppers' throughput performance is not zero, it is still possible to provide quality of service (QoS) based security. QoS-based security refers to the protection provided considering the requirements of various communication services such as (voice, video, etc.). Further, different communication services indeed have different QoS requirements for effective communication. Therefore, to enhance a specific service's security, we degrade the performance of eavesdropper below the requirements of QoS for that service.

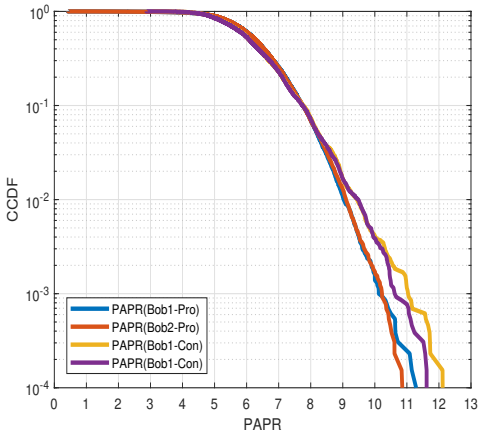



**FIGURE 7.** Comparison of peak to average power ratio (PAPR) performances of the conventional OFDM and proposed algorithm.

Figure 6 shows the simulation of packet error rate PER performance of both users and eavesdroppers, which we calculated from BER as follows: $PER = 1 - (1 - BER)^n$, where $n$ is the block size. It is clear from the result that signal performance for PER of user-1 (Bob-1) and user-2 (Bob-2) are again similar to each other. The Bob-1 and Bob-2 perform exceptionally well than the eavesdroppers trying to eavesdrop the signal intended for the users. And the eavesdropper receives the extremely degraded version of the signal. So, in this work, we target the QoS to provide security for services such as voice and video and ensure that the error rate at Eve is higher than the minimum required error criteria to use that service. For example, voice and video can be kept secure at Bob by ensuring that PER (corresponding to BER) at Bob is less than the minimum required PER (corresponding to BER) to use that service. In contrast, PER at Eve is made higher than the minimum required PER.

Figure 7 depicts a comparison of the peak to average power ratio (PAPR) performances of the conventional OFDM and OFDM with the proposed algorithm for user-1 (Bob-1) and user-2 (Bob-2). We can observe in Fig. 7 that the proposed method's PAPR performance outperforms the conventional method at high SNR values. The developed scheme gets improved PAPR because the precoder matrices, when designed at the transmitter, change the signal's distribution from being gaussian to something less random than gaussian and close to uniform. Therefore, it resolves one of the significant challenges faced by OFDM systems [40] by reducing the PAPR, which results in improved spectral and energy efficiency.

Overall, as can be seen from the above-detailed analysis, the proposed algorithm can be a good solution for providing secure communication, especially for the low processing IoT-based devices.

## VI. CONCLUSION

We have proposed a new technique for reliable and secure communication in this paper. Our proposed method provides the benefit of channel-dependent pre-coders with the simultaneous transmission from two antennas to ensure reliable and secure communication against both internal and external eavesdroppers. Firstly, the pre-coded data of the users is superimposed. Then this pre-coded data is transmitted to the receivers in simultaneous transmission from two antennas, and the signals from the simultaneous transmission are combined and sent to the receiver in such a way that only the authorized users receive its data. At the same time, the eavesdropper gets the degraded data. The simulation results prove that our proposed method is suitable for secure and reliable communication at receiver nodes without complex operations, making it ideal for applications with low complexity and less power limits (IoT-based applications).

## REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 1617–1655, 2016.

[2] M. F. Khan, F. A. Bhatti, A. Habib, S. Jangsher, M. I. Khan, I. Zafar, S. M. Shah, M. A. Jamshed, and J. Iqbal, "Analysis of macro user offloading to femto cells for 5G cellular networks," in Int. Symposium on Wireless Systems and Networks (ISWSN), Nov 2017, pp. 1–6.

[3] M. F. Zia and J. M. Hamamreh, "An Advanced NOMA Security Technique for Future Wireless Communication," Workshop on Information and Communications Technologies, International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Sep. (2020), pp. 38–43.

[4] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," IEEE Access, vol. 6, pp. 4850–4874, 2018.

[5] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," China Commun., vol. 14, no. 12, pp. 1–14, December 2017.

[6] 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.

[7] H. Li, X. Wang, and J. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," IEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 1155–1165, Feb 2015.

[8] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," Journal of Commun. and Netw., vol. 14, no. 4, pp. 385–395, Aug 2012.

[9] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Adaptive OFDM-IM for enhancing physical layer security and spectral efficiency of future wireless networks," Wireless Commun. and Mobile Computing, vol. 2018, 2018.

[10] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," IEEE Access, vol. 5, pp. 25 863–25 875, 2017.

[11] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in IEEE 28th Annual Int. Symposium on Personal, Indoor, and Mobile Radio Commun. (PIMRC), Oct 2017, pp. 1–5.

[12] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in 2014 IEEE Int. Conf. Commun. Work. ICC 2014. IEEE, jun 2014, pp. 813–818.

[13] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in 13th Int. Wireless Commun. and Mobile Computing Conf. (IWCMC). IEEE, 2017, pp. 1338–1343.

[14] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2717–2729, 2013.

[15] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic feature concealing CP selection for physical layer security," in IEEE military commun. conf. IEEE, 2014, pp. 485–489.

[16] Z. Li, M. A. Uusitalo, H. Shariatmadari, and B. Singh, "5G URLLC: Design challenges and system concepts," in 15th Int. Symposium on Wireless Commun. Systems (ISWCS), Aug 2018, pp. 1–6.

[17] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1773–1828, 2019.

[18] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired noma network," IEEE Journal of Selected Topics in Signal Processing, vol. 13, no. 3, pp. 700–714, 2019.

[19] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure miso-noma transmission with artificial noise," IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6700–6705, 2018.

[20] M. M. Sahin and H. Arslan, "Waveform-domain noma: The future of multiple access," arXiv preprint arXiv:2003.05548, 2020 - arxiv.org.

[21] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5g," IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 2294–2323, 2018.

[22] B. Makki, K. Chitti, A. Behravan, and M.-S. Alouini, "A survey of noma: Current status and open research challenges," IEEE Open Journal of the Communications Society, vol. 1, pp. 179–189, 2020.

[23] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (noma)," 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 611–615, 2013.

[24] P. Xu, Z. Ding, X. Dai, and H. V. Poor, "Noma: An information theoretic perspective," (2015) ArXiv Preprint ArXiv:1504.07751.

[25] Y. Yuan and C. Yan, "Noma study in 3gpp for 5g," 2018 IEEE 10th International Symposium on Turbo Codes Iterative Information Processing (ISTC), pp. 1–5, 2018.

[26] S. Chen, B. Ren, Q. Gao, S. Kang, S. Sun, and K. Niu, "Pattern division multiple access—a novel nonorthogonal multiple access for fifth-generation radio networks," IEEE Transactions on Vehicular Technology, vol. 66, pp. 3185–3196, 2017.

[27] Y. Cao, H. Sun, J. Soriaga, and T. Ji, "Resource spread multiple access - a novel transmission scheme for 5g uplink," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 2017, pp. 1–5.

[28] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for internet of things," 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), pp. 1–5, 2016.

[29] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for internet of things," in 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016, pp. 1–5.

[30] Z. Wu, K. Lu, C. Jiang, and X. Shao, "Comprehensive study and comparison on 5g noma schemes," IEEE Access, vol. 6, pp. 18 511–18 519, 2018.

[31] X. Li, H. Chen, Y. Qian, B. Rong, and M. Soleymani, "Welch bound analysis on generic code division multiple access codes with interference free windows," IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 1603–1607, Apr. 2009.

[32] J. P. Lemayian and J. M. Hamamreh, "A novel small-scale nonorthogonal communication technique using auxiliary signal superposition with enhanced security for future wireless networks," RS Open Journal on Innovative Communication Technologies, 10 2020, https://rs-ojict.pubpub.org/pub/rd8elz19. [Online]. Available: https://rs-ojict.pubpub.org/pub/rd8elz19

[33] 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.

[34] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Sel. Areas Commun., vol. 16, no. 8, pp. 1451–1458, Oct 1998.

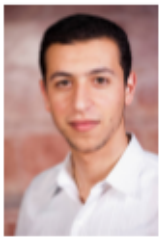
[35] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," IEEE Trans. Signal Process., vol. 52, no. 2, pp. 461–471, Feb 2004.

[36] R. Ghaffar and R. Knopp, "Linear precoders for multiuser MIMO for finite constellations and a simplified receiver structure under controlled interference," in Conf. Record of the Forty-Third Asilomar Conf. on Signals, Systems and Computers, Nov 2009, pp. 1431–1435.

[37] J. M. Hamamreh, E. Basar, and H. Arslan, "Ofdm-subcarrier index selection for enhancing security and reliability of 5g urllc services," IEEE Access, vol. 5, pp. 25 863–25 875, 2017.

[38] V. P. Singh, "Gamma Distribution. In: Entropy-Based Parameter Estimation in Hydrology". Springer, Dordecht, 1998, vol. 30.
[39] J. G. Proakis and D. G. Manolakis, Digital Signal Processing (3rd Ed.): Principles, Algorithms, and Applications. USA: Prentice-Hall, Inc., 1996.
[40] I. Baig, N. ul Hasan, M. Zghaibeh, I. Khan, and A. S. Saand, "A dst precoding based uplink noma scheme for papr reduction in 5g wireless network," 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), pp. 1–4, 2017.

MUHAMMAD FURQAN ZIA received his B.E degree in Electrical engineering from DHA Suffa University, Karachi, Pakistan, in 2017. He is presently pursuing his master's (M.S) degree in Electrical and Computer engineering from Antalya Bilim University, Turkey. Previously, he was associated with the electrical power sector industry in Pakistan. Currently, he is working as a researcher at the Wireless Intelligent Systems laboratory in Antalya Bilim University on the topic of Advanced small-scale NOMA Schemes for Enhancing Communication Security and Reliability of Future Low-complexity, Massive Machine-Type Communications. His research interests include 5G and 6G Communication networks, Physical layer security, Wireless technologies, Signal processing techniques, and the Internet of Things (IoT) applications.



JEHAD M. HAMAMREH received the B.Sc. degree in electrical and telecommunication engineering from An-Najah University, Nablus, in 2013, and the Ph.D.degree in electrical-electronics engineering and cyber systems from Istanbul Medipol University, Turkey, in 2018. He was a Researcher with the Department of Electrical and Computer Engineering, Texas A and M University at Qatar. He is currently an Assistant Professor with the Electrical and Electronics Engineering Department, Antalya International (Bilim) University, Turkey. His current research interests include wireless physical and MAC layers security, orthogonal frequency-division multiplexing multiple-input multiple-output systems, advanced waveforms design, multi-dimensional modulation techniques, and orthogonal/non-orthogonal multiple access schemes for future wireless systems. He is a Regular Reviewer for various IEEE, Elsevier, Wiley, and Springer journals as well as a TPC Member for several international conferences.