Received May 23, 2021, 2021, accepted June 5, 2021, date of publication June 8, 2021

Digital Object Identifier 10.46470/03d8ffbd.92a40b85

Multi-User Auxiliary Signal Superposition Transmission (MU-AS-ST) for Secure and Low-Complexity Multiple Access Communications

MOHAMEDOU ABEWA¹, JEHAD M. HAMAMREH²

^{1,2}J. M. Hamamreh and M. Abewa are with WISLAB for Wireless Research at the department of Electrical-Electronics Engineering, Antalya Bilim University, Antalya, Turkey.

Corresponding author: Mohamedou Abewa and Jehad Hamamreh (email: mohamedou.abewa@std.antalya.edu.tr, jehad.hamamreh@gmail.com)

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK), under project grant No. 119E392. The Matlab simulation codes used to generate the results in this paper can be found at <https://researcherstore.com>

ABSTRACT Beyond 5G (B5G) and future 6G systems are expected to serve a massive number of interconnection links between base stations and Internet of Thing (IoT) devices. Thus, it is critical to develop new effective multiple access techniques, which can serve the demands of this massive number of connections. In this regard, power domain non-orthogonal multiple access (PD-NOMA), which was studied extensively by both academia and industry, was perceived as a potential candidate to the problem of serving more devices while having limited resources; however, the PD-NOMA design was eliminated from the list of the 17th release of 3GPP work items. Even though PD-NOMA proves efficient compared to OMA systems in certain scenarios and under specific conditions, it suffers from many issues including: low reliability due to having inter-user-interference, security vulnerability to both internal and external eavesdropping, the complexity of the transceiver due to the use of successive interference cancellation (SIC), and the inapplicability in power-balanced scenarios, where the superimposed users have the same distance from the base station. To address the aforementioned problems related to PD-NOMA, in this work, we propose and develop a novel new alternative non-orthogonal transmission design through the use of specially designed auxiliary signals superimposed with the users' data. The proposed design is termed and coined as MU-AS-ST (Multi-User Auxiliary Signal Superposition Transmission) and is featured with a very simple transceiver design, where all the processing is done at the base station, thus freeing the receiver from any complex processing. The offered advantages by the proposed design make from it an ideal candidate for low-power and processing-limited devices such as IoT applications.

INDEX TERMS B5G, IoT, Low complexity, Modulation, Multiple access, NOMA, Non-coherent, OFDM, Spectral efficiency, Wireless communication, 6G.

I. INTRODUCTION

A. MOTIVATION

DUE to the massive connectivity that shapes the future wireless world, greater importance is given to communication strategies which support multi-user setups. In this regard, power domain non-orthogonal multiple access (PD-NOMA) was investigated thoroughly in the literature, and took part in many standardization activities for the 5G radio access.

In power-domain NOMA, scheduled users are assigned dif-

ferent power levels based on their channel conditions while sharing the same time, frequency or code resources. At the transmitter, the data of the considered users is superimposed and sent where at the receiver, successive interference cancellation (SIC) is used for separating scheduled users' data. In particular, PD-NOMA has proven very efficient in many aspects when compared to orthogonal multiple access (OMA)-based schemes where PD-NOMA achieves benefits such as high throughput, massive connectivity and coverage, low latency and signaling overhead, and relaxed channel

feedback [1].

On the other hand, PD-NOMA was proven inefficient in multi-antenna setups, which could be the reason that lead to its exclusion from the study items of release 17 of the 3rd Generation Partnership Project (3GPP) [2], [3]. Some of the limitations and the shortcomings exhibited by PD-NOMA, which can serve as an explanation for the reason behind its exclusion from the 3GPP project after being considered as a study item from release 13 to release 16 under the name multi-user superposition transmission (MUST), can be summarized in the following points:

- **Inefficiency of NOMA in multi-antenna settings:** PD-NOMA exhibits performance degradation when compared to multi-user multiple input multiple output (MU-MIMO) systems. In this regard, authors in [4] have shown that most of the benefits of power domain NOMA are only valid when the results are compared with OMA. Furthermore, in this detailed review, it is shown that both multi-user linear precoding (MU-LP) and MU-MIMO outperform conventional power domain NOMA.
- **Receiver complexity related to the use of SIC:** the main operation in conventional NOMA is the inter-user interference cancellation through SIC performed by near users, however; this comes at the ultimate cost of receiver complexity. The receiver complexity grows with the number of super-imposed users and as such, NOMA would not be a suitable choice for communication setups where massive connectivity and low-complexity are crucial requirements as in the case of internet of things (IoT) communications.
- **Constrained users' superposition:** one of the limitations of NOMA is the deficiency of working in power-balanced scenarios as it requires a significant path-loss channel difference between paired (or super-imposed) users. This necessitate having a user near to the base station (i.e., strong channel) and another user far from the base station (i.e., weak channel). Consequently, this limits the applicability of NOMA in scenarios where two users may have the same path-loss due to being located at a similar distance from the base station (BS).
- **Security of the NOMA waveform:** Another concern is the security of the NOMA waveform where using SIC for decoding users' data can yield internal eavesdropping risks in the presence of un-trusted users in the superimposed data. Moreover, there is a need for securing NOMA against external eavesdropping [5].

B. CONTRIBUTIONS OF THE PROPOSED DESIGN

All the the aforementioned shortcomings of conventional power domain NOMA have motivated the design of novel multiple access alternatives with varying degrees of success in addressing the requirements of future wireless systems. Different designs were proposed by the actors in the wireless domain such as multi-user shared access (MUSA) [6], pattern division multiple access (PDMA) [7], resource spread

multiple access (RSMA) [8], interleave-grid multiple access (IGMA) [9], interleave division multiple access (IDMA) [10], sparse-code multiple access (SCMA) [11], and many others that were included in different releases of the 3rd Generation Partnership Project (3GPP).

In this scope, we propose a novel physical layer security based design for future wireless systems. The proposed design makes use of auxiliary signal superposition where channel-dependent auxiliary signals are added on top of the multiplexed users' (or IoT devices) signals, which are transmitted from two different antenna sources as shown in Fig.1., in such a way that a completely (inter-user interference)-free, secure and reliable transmission is achieved.

The proposed design was originally presented in [12] along with other multiple access designs proposed for efficient and secure multi-user communications. In [12], two of the proposed designs are based on signal precoding and two are employing auxiliary signals in their design.

The developed designs, in [12], were studied thoroughly in the following papers:

- In [13], the authors proposed an algorithm which combines the benefit of pre-coder matrices with simultaneous transmission using antenna diversity to provide simple, reliable, and secure communication without complex processing.
- A physical layer security version of the design proposed in [13] was developed in [14] for multi-cell, multi-user, and multi-carrier IoT communication setups.
- In [15], the authors proposed a design based on auxiliary signals that are precisely designed and superimposed on top of the users' data. The superimposed signal is then sent from a dual-transmitter system to provide perfect secrecy against external and internal eavesdroppers, while providing low complexity at the receiver.

Furthermore, Since in [12] a basic presentation of the design principles of MU-AS-ST where highlighted, this publication is devoted for studying MU-AS-ST in depth and proving its capacity in addressing the challenging requirements of future wireless communication systems.

In summary, the contribution points of the proposed design can be presented as follows:

- **Working in general scenarios:** Unlike conventional NOMA where only users having different distance from the base station can be super-imposed, this design works for the combination of any two users regardless of their distances from the base station.
- **Perfect information secrecy against both external and internal eavesdropping:** The design of the auxiliary signals ensures perfect secrecy with zero information leakage against both external illegitimate users and amongst the legitimate users one another.
- **Reduced receiver complexity:** Unlike conventional NOMA where successive cancellation at the receiver side leads to a complexity of the system, in this tech-

nique the specific design of the auxiliary signals solves the interference problem effectively making it a strong candidate for applications with limited processing capabilities and low complexity design requirements such as IoT devices.

- **Reduced transmission latency:** Since this design is featured with its simple transceiver design, the transmission latency is reduced. At the transmitter the design of the auxiliary signals employs diagonal matrices making the computational cost lower, while at the receiver simply a conventional OFDM receiver is used and thus freeing the receiver from any complex processing.

Outline: The remaining sections of this paper are organized as follows. Section II illustrates and explains the system model of the proposed design. In Section III, the performance analysis is carried out. Section IV provides simulation results. Finally, Section V presents the conclusion.

Notation: Vector and matrix notations are given in Table 1.

TABLE 1: Notation

	Time domain notation	Frequency domain notation
Vectors	x	$\mathbf{x}$
Matrices	H	$\mathbf{H}$

II. SYSTEM MODEL OF MU-AS-ST

FIGURE 1: General system model of MU-AS-ST.

The general system model design of the proposed scheme is shown in Fig.1. The downlink setup consists of a base station of two antennas A_1 and A_2 trying to communicate with two legitimate user equipments UE_1 and UE_2 in the presence of an illegitimate, eavesdropper UE_X .

At the transmitter, the proposed design uses data superposition where specifically designed auxiliary signals are added to the super-imposed users' data to prevent inter-user interference and internal eavesdropping. Moreover, the special design of these signals ensures the impossibility of external eavesdropping tried by the external device UE_X .

FIGURE 2: Transmitter of MU-AS-ST.

A. MU-AS-ST TRANSMITTER

As shown in the transmitter diagram of Fig.2., the design is based on orthogonal frequency division multiplexing (OFDM). First, the data for the legitimate user equipments (i.e., UE_1 and UE_2) is modulated using binary phase shift keying (BPSK), then the specifically designed r_1 and r_2 signals are super-imposed over the users' data and the combined signal is passed from the IFFT block. Finally, the BS transmits the superposition coded signals u_1 and u_2 simultaneously from antenna A_1 and antenna A_2 , respectively. The transmitted signals u_1 and u_2 are given as:

$$u_1 = x_1 + x_2 + r_1 \quad (1)$$

$$u_2 = x_1 + x_2 + r_2 \quad (2)$$

B. CHANNEL MODEL

The channel between the transmitter and any receiver is assumed to be a slowly-varying, frequency selective Rayleigh type channel with L multi-path exponentially decaying taps, denoted by $H_{ji} = [H_0, H_1, \dots, H_{L-1}]$, $i \in (1, 2)$, $j \in (1, 2, X)$.

As such, the received symbols in time domain are given as:

$$y_j = \left(\sum_{i=1}^2 H_{ji} \otimes u_i \right) + n_j \quad (3)$$

where $\otimes$ represents the convolution operator. H_{ji} stands for the channel impulse response between the antenna A_i and the user equipment UE_j . u_i , and n_j are column vectors representing the transmitted time domain samples from antenna A_i , and the additive white Gaussian noise, respectively. The noise n_j samples are drawn from a normal distribution with zero mean and variance equal to N_0 ; $n_j \sim \mathcal{N}(0, N_0)$. Moreover, it is assumed that the transmitter has no knowledge about the channel of a passive eavesdropper.

The channels corresponding to the transmission to each user end are specified in the general system model of Fig.1.

C. MU-AS-ST RECEIVER

The receiver of the proposed design is shown in Fig.3. below where the signal reception is analyzed at the legitimate nodes UE_1 and UE_2 and at the external eavesdropping node, UE_X .

FIGURE 3: Receiver of MU-AS-ST.

1) Received signal at the legitimate node, UE_1

The received signal at the legitimate user equipment UE_1 , y_1 , is the sum of the individually received signals y_{11} and y_{12} corresponding to the transmitted signals u_1 , u_2 , respectively. The received signal y_1 can be written as:

$$y_1 = y_{11} + y_{12} + n_1 \quad (4)$$

$$y_1 = H_{11}u_1 + H_{12}u_2 + n_1 \quad (5)$$

$$y_1 = H_{11}(x_1 + x_2 + r_1) + H_{12}(x_1 + x_2 + r_2) + n_1 \quad (6)$$

$$y_1 = (H_{11} + H_{12})x_1 + (H_{11} + H_{12})x_2 + H_{11}r_1 + H_{12}r_2 + n_1 \quad (7)$$

2) Received signal at the legitimate node, UE_2

Similarly, the received signal at the second legitimate user, UE_2 , is also the combined transmitted signal from antennas A_1 and A_2 (i.e., channels H_{21} , H_{22} , respectively), calculated as:

$$y_2 = y_{21} + y_{22} + n_2 \quad (8)$$

$$y_2 = H_{21}u_1 + H_{22}u_2 + n_2 \quad (9)$$

$$y_2 = H_{21}(x_1 + x_2 + r_1) + H_{22}(x_1 + x_2 + r_2) + n_2 \quad (10)$$

$$y_2 = (H_{21} + H_{22})x_1 + (H_{21} + H_{22})x_2 + H_{21}r_1 + H_{22}r_2 + n_2 \quad (11)$$

3) Received signal at the external eavesdropping node, UE_X

The eavesdropper user equipment UE_X receives the broadcasted signals from antenna A_1 and antenna A_2 . As such, the received signal at the eavesdropper device can be written as follows:

$$y_X = H_{X1}u_1 + H_{X2}u_2 + n_X \quad (12)$$

$$y_X = H_{X1}(x_1 + x_2 + r_1) + H_{X2}(x_1 + x_2 + r_2) + n_X \quad (13)$$

$$y_X = (H_{X1} + H_{X2})x_1 + (H_{X1} + H_{X2})x_2 + H_{X1}r_1 + H_{X2}r_2 + n_X \quad (14)$$

After the signal reception at the receiver, conventional OFDM operations such as CP removal and performing FFT are carried out. Then, the symbols are demodulated as shown in the receiver in Fig.3. where the legitimate users are able to recover their data while the decoding of the eavesdropper signal is extremely challenging as it involves the combination of many variables that are unknown to UE_X .

In the next section, the specific design of the auxiliary signals is presented where it is shown that the proposed waveform is secure against both internal and external eavesdropping trials.

D. DESIGN OF THE AUXILIARY SIGNALS

The auxiliary signals should cancel the interference caused, by UE_2 on UE_1 and vice versa. From (7), the term including the factor x_1 (i.e., $(H_{11} + H_{12})x_1$) is the only term desired with respect to UE_1 whereas the left terms in (7) represent:

- the interference caused by UE_2 on UE_1 (i.e., $(H_{11} + H_{12})x_2$)
- the effect of the auxiliary signals (i.e., $H_{11}r_1 + H_{12}r_2$)
- a noise term (i.e., n_1).

As such, for achieving secure and interference-free communication for UE_1 , the effect of the auxiliary signals should act against the interference term and cancel it. This is expressed by the following equation:

$$(H_{11} + H_{12})x_2 + H_{11}r_1 + H_{12}r_2 = 0 \quad (15)$$

Similarly, by looking at (11), we can write the following equation which ensures interference-free and eavesdropping-free communication for UE_2 :

$$(H_{21} + H_{22})x_1 + H_{21}r_1 + H_{22}r_2 = 0 \quad (16)$$

The values for the auxiliary signals r_1 and r_2 , which completely cancel the interference between the users are found by solving the following system of equations S_{r_1, r_2} composed of (15) and (16):

$$S_{r_1, r_2} \begin{cases} (H_{11} + H_{12})x_2 + H_{11}r_1 + H_{12}r_2 = 0 \\ (H_{21} + H_{22})x_1 + H_{21}r_1 + H_{22}r_2 = 0 \end{cases} \quad (17)$$

The solution of the system S_{r_1, r_2} yields the following values for r_1 and r_2 :

$$F = H_{22} - H_{21}H_{11}^{-1}H_{12} \quad (18)$$

$$g = -(H_{21} + H_{22})x_1 + H_{21}(I_{64} + H_{11}^{-1}H_{12})x_2 \quad (19)$$

$$r_2 = F^{-1}g \quad (20)$$

$$r_1 = (I_{64} + H_{11}^{-1}H_{12})x_2 - (H_{11}^{-1}H_{12}r_2) \quad (21)$$

Note that the size of the diagonal matrices $H_{ij, (i,j)=(1,2)}$ is 64×64 , I_{64} is the 64×64 identity matrix. x_1 , x_2 , r_1 , r_2 are 64×1 column vectors.

These specific values of the auxiliary signals r_1 and r_2

allow each user equipment to receive its own data without interference and without eavesdropping from other users in the network. In particular, We can see that the designed auxiliary signals are functions of the users channels and users' data and as such the external eavesdropper is extremely challenged in this case since it has no knowledge about the users' channels ($\mathbf{H}_{11}, \mathbf{H}_{12}, \mathbf{H}_{21}, \mathbf{H}_{22}$), users data (i.e., $\mathbf{x}_1, \mathbf{x}_2$) and the auxiliary signals (i.e., $\mathbf{r}_1, \mathbf{r}_2$).

III. CONVENTIONAL POWER DOMAIN NOMA

In the conventional power domain NOMA setup, the base station (BS) transmits the same superimposed signal from both antennas simultaneously. The transmitted combined signal, $\mathbf{q}$ can be written as:

$$\mathbf{q} = \sqrt{P}(\sqrt{\alpha_1}\mathbf{x}_1 + \sqrt{\alpha_2}\mathbf{x}_2) \quad (22)$$

where P is the total transmit power. α_1 and α_2 denote the power allocation coefficients for the transmission to UE_1 and UE_2 respectively. In the following analysis for PD-NOMA, we assume that UE_1 is the far user and UE_2 is the near user and thus $\alpha_1 > \alpha_2$.

Let y_{1N}, y_{2N} and y_{XN} denote the signals received by UE_1 , UE_2 and UE_X , respectively, using conventional power domain NOMA as the communication technique.

The received signal at each user equipment can be written as:

$$\begin{bmatrix} y_{1N} \\ y_{2N} \\ y_{XN} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_{11} & \mathbf{H}_{12} \\ \mathbf{H}_{21} & \mathbf{H}_{22} \\ \mathbf{H}_{X1} & \mathbf{H}_{X2} \end{bmatrix} \begin{bmatrix} \mathbf{q} \\ \mathbf{q} \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \mathbf{n}_X \end{bmatrix} \quad (23)$$

which can be simplified as:

$$\begin{bmatrix} y_{1N} \\ y_{2N} \\ y_{XN} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_{11} + \mathbf{H}_{12} \\ \mathbf{H}_{21} + \mathbf{H}_{22} \\ \mathbf{H}_{X1} + \mathbf{H}_{X2} \end{bmatrix} \mathbf{q} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \mathbf{n}_X \end{bmatrix} \quad (24)$$

or,

$$\begin{bmatrix} y_{1N} \\ y_{2N} \\ y_{XN} \end{bmatrix} = \begin{bmatrix} (\mathbf{H}_{11} + \mathbf{H}_{12})\mathbf{q} + \mathbf{n}_1 \\ (\mathbf{H}_{21} + \mathbf{H}_{22})\mathbf{q} + \mathbf{n}_2 \\ (\mathbf{H}_{X1} + \mathbf{H}_{X2})\mathbf{q} + \mathbf{n}_X \end{bmatrix} \quad (25)$$

Replacing $\mathbf{q}$ with its value expressed by (22), (25) becomes:

$$\begin{bmatrix} y_{1N} \\ y_{2N} \\ y_{XN} \end{bmatrix} = \begin{bmatrix} (\mathbf{H}_{11} + \mathbf{H}_{12})\sqrt{P}(\sqrt{\alpha_1}\mathbf{x}_1 + \sqrt{\alpha_2}\mathbf{x}_2) + \mathbf{n}_1 \\ (\mathbf{H}_{21} + \mathbf{H}_{22})\sqrt{P}(\sqrt{\alpha_1}\mathbf{x}_1 + \sqrt{\alpha_2}\mathbf{x}_2) + \mathbf{n}_2 \\ (\mathbf{H}_{X1} + \mathbf{H}_{X2})\sqrt{P}(\sqrt{\alpha_1}\mathbf{x}_1 + \sqrt{\alpha_2}\mathbf{x}_2) + \mathbf{n}_X \end{bmatrix} \quad (26)$$

Since UE_1 is the strong user (i.e., higher power share), this user equipment decodes its own signal $\mathbf{x}_1$ by treating the signal of the weak user, $\mathbf{x}_2$, as interference / noise. The received signal at UE_1 can be written as:

$$y_{1N} = (\mathbf{H}_{11} + \mathbf{H}_{12})\sqrt{P\alpha_1}\mathbf{x}_1 + (\mathbf{H}_{11} + \mathbf{H}_{12})\sqrt{P\alpha_2}\mathbf{x}_2 + \mathbf{n}_1 \quad (27)$$

On the other hand, the user equipment UE_2 which is the near user receives the following signal:

$$y_{2N} = (\mathbf{H}_{21} + \mathbf{H}_{22})\sqrt{P\alpha_1}\mathbf{x}_1 + (\mathbf{H}_{21} + \mathbf{H}_{22})\sqrt{P\alpha_2}\mathbf{x}_2 + \mathbf{n}_2 \quad (28)$$

where the signal of UE_1 is dominating and thus, this user employs successive interference cancellation (SIC) to remove the effect of the signal of the far user. The received signal at UE_2 after the application of SIC can be written as follows:

$$y_{2N, \text{SIC}} = (\mathbf{H}_{21} + \mathbf{H}_{22})\sqrt{P\alpha_2}\mathbf{x}_2 + \mathbf{n}_2 \quad (29)$$

Moreover, at the eavesdropper device UE_X , the received signal can be expressed as:

$$y_{XN} = (\mathbf{H}_{X1} + \mathbf{H}_{X2})\sqrt{P\alpha_1}\mathbf{x}_1 + (\mathbf{H}_{X1} + \mathbf{H}_{X2})\sqrt{P\alpha_2}\mathbf{x}_2 + \mathbf{n}_X \quad (30)$$

IV. PERFORMANCE ANALYSIS

In this section, the performance analysis of the proposed design is studied. A comparative analysis with conventional power domain NOMA is performed taking as a reference the configuration displayed in Fig.1 where, for the case of NOMA, UE_1 is considered as the far user and user equipment UE_2 is considered as the near user.

A. BER ANALYSIS

Since BPSK is the modulation used in this design, the bit error rate of a legitimate user can be expressed as shown in [16] as:

$$BER_{UE_1, UE_2} = \frac{1}{2} \int_0^\infty \text{erfc}(\sqrt{\gamma_b}) P_{\gamma_b}(\gamma_b) d\gamma_b \quad (31)$$

where $\text{erfc}(\cdot)$ is the complementary error function. $P_{\gamma_b}(\gamma_b)$ stands for the probability distribution function (PDF) of the effective instantaneous signal to noise ratio of a legitimate user (i.e., UE_1, UE_2). $P_{\gamma_b}(\gamma_b)$ is related to the fading distribution through the following change of variable [17]:

$$P_{\gamma_b}(\gamma_b) = \frac{P_\alpha(\sqrt{\frac{\Omega\gamma_b}{\bar{\gamma}_b}})}{2\sqrt{\frac{\bar{\gamma}_b\gamma_b}{\Omega}}} \quad (32)$$

where $\alpha = \|\mathbf{H}_{UE_i}\|$, $i = (1, 2)$. α is the channel fading amplitude of a legitimate user. $\mathbf{H}_{UE_i} = \sum_{j=1}^2 \mathbf{H}_{ij}$. Ω is defined as the mean square of the channel fading amplitude, i.e., $\Omega = \mathbb{E}\{\alpha^2\}$. $\bar{\gamma}_b$ denotes the average SNR.

Fig.4. shows the fading distribution of a legitimate user fitted with different known distribution functions. As shown, the effective channel can be fit with a Nakagami distribution with shape and scale parameters μ and ω . The fading distribution can be described by the following system (S_α).

$$(S_\alpha) \begin{cases} P_\alpha(\alpha) = 2 \left(\frac{\mu}{\omega}\right)^\mu \frac{1}{\Gamma(\mu)} \alpha^{2\mu-1} \exp\left(-\frac{\mu}{\omega} \alpha^2\right) \\ (\mu, \omega) = (2.12853, 3.65843) \end{cases} \quad (33)$$

where $\Gamma(\cdot)$ is the gamma function.

After getting the expression for the fading amplitude, the PDF of the effective SNR expressed by Eq.(32) can be written as:

$$\begin{cases} P_{\gamma_b}(\gamma_b) = F\sqrt{\gamma_b}^{2(\mu-1)} \exp\left(-\frac{\mu}{\omega} \frac{\Omega}{\bar{\gamma}_b} \gamma_b\right) \\ F = \left(\frac{\Omega}{\bar{\gamma}_b} \frac{\mu}{\omega}\right)^\mu \frac{1}{\Gamma(\mu)} \end{cases} \quad (34)$$

FIGURE 4: Amplitude distribution of the effective fading channel for the legitimate users UE_1 and UE_2 .

By substituting (34) in the bit error rate equation (31), the following integral is obtained:

$$BER_{UE_1, UE_2} = \frac{F}{2} \int_0^\infty \text{erfc}(\sqrt{\gamma_b}) \sqrt{\gamma_b}^{2(\mu-1)} \exp\left(-\frac{\mu}{\omega} \frac{\Omega}{\gamma_b} \gamma_b\right) d\gamma_b \quad (35)$$

Moreover, the above integral is similar to a solvable integration involving the complementary error function given in [18] as:

$$\int_0^\infty \text{erfc}(\sqrt{x}) \sqrt{x} \exp(-\beta x) dx = \frac{1}{2\sqrt{\pi}} \left(\frac{\arctan(\sqrt{\beta})}{(\beta)^{3/2}} - \frac{1}{\beta(1+\beta)} \right), \beta > 0. \quad (36)$$

where, $\arctan(\cdot)$ is the inverse tangent function.

The bit error rate in (35) can be written in the form of this known integral by making $2(\mu-1) = 1$ which corresponds to setting $\mu = \frac{3}{2}$ instead of its original value, $\mu = 2.12853$. Note that it is feasible to perform this integration by taking $\beta = \frac{\mu}{\omega} \frac{\Omega}{\gamma_b}$ which satisfies the condition $\beta > 0$.

Thus, the bit error rate of a legitimate user can be approximated by the following expression:

$$\left\{ \begin{array}{l} BER_{UE_1, UE_2} \approx \frac{F}{4\sqrt{\pi}} \left(\frac{\arctan(\sqrt{\beta})}{(\beta)^{3/2}} - \frac{1}{\beta(1+\beta)} \right) \\ \beta = \frac{\mu}{\omega} \frac{\Omega}{\gamma_b} \\ F = \frac{\beta^\mu}{\Gamma(\mu)} \\ (\mu, \omega) = \left(\frac{3}{2}, 3.65843\right) \end{array} \right. \quad (37)$$

B. SINR ANALYSIS

1) Legitimate Nodes (UE_1, UE_2)

In the proposed design, the auxiliary signals remove the effect of the interference caused by the data superposition

at the transmitter. Thus the received signals, after the interference cancellation at the legitimate nodes UE_1 and UE_2 expressed by (7) and (11) can be simplified further to the following:

$$y_{1, MU-AS-ST} = (H_{11} + H_{12})x_1 + n_1 \quad (38)$$

for UE_1 , and

$$y_{2, MU-AS-ST} = (H_{21} + H_{22})x_2 + n_2 \quad (39)$$

for the legitimate user UE_2 .

In the following, we will derive the signal to interference plus noise ratio ($SINR$) for the legitimate users using both the proposed MU-AS-ST and the conventional power domain NOMA. The $SINR$ metric for a given user equipment $UE \in \{UE_1, UE_2, UE_X\}$ using a technique $T \in \{MU-AS-ST, NOMA\}$ is defined as follows:

$$SINR_{UE}^T = \frac{S}{I + \sigma_n^2} \quad (40)$$

where S, I and σ_n^2 stand, respectively, for the signal power, the interference power and the noise variance at the corresponding receiver node UE .

From (38) and (39), $SINR$ for the legitimate users UE_1 and UE_2 using MU-AS-ST can be written as:

$$SINR_{UE_1}^{MU-AS-ST} = \frac{\|H_{11} + H_{12}\|^2}{\sigma_{n_1}^2} \quad (41)$$

$$SINR_{UE_2}^{MU-AS-ST} = \frac{\|H_{21} + H_{22}\|^2}{\sigma_{n_2}^2} \quad (42)$$

On the other hand, let's derive the $SINR$ for the legitimate users using conventional power domain NOMA.

First, for the far user the received signal is shown by (27) and as can be seen from this equation it contains the interference from UE_2 however since this user's power share is the highest, this interference term is counted as noise and does not affect the detection of x_1 by UE_1 . The corresponding $SINR$ for this user equipment can be written as:

$$SINR_{UE_1}^{NOMA} = \frac{P\alpha_1 \|H_{11} + H_{12}\|^2}{P\alpha_2 \|H_{11} + H_{12}\|^2 + \sigma_{n_1}^2} \quad (43)$$

Moreover, since the near user removes the interference caused by the far user, the $SINR$ for this user for decoding its own signal x_2 can be derived from (29) as:

$$SINR_{UE_2}^{NOMA} = \frac{P\alpha_2 \|H_{21} + H_{22}\|^2}{\sigma_{n_2}^2} \quad (44)$$

2) Internal Eavesdropping (UE_1 on UE_2) or (UE_2 on UE_1)

Unlike the data superposition principle in power domain NOMA where SIC is employed at the near user for subtracting the dominating far user's signal, in this design every legitimate user receives only its own signal where the interference from all other superimposed users in the network can be fully cancelled through the addition of the auxiliary signals. This presents a more robust design, compared to

conventional NOMA, with no risk of internal eavesdropping activities in the presence of internal eavesdroppers among the superimposed users.

3) External Eavesdropping (UE_X)

From the receiver in Fig.3. and the derivation of the received signal at the eavesdropper node, UE_X , we can see that the decoding of the received signal is a very complex operation for UE_X . This is due to the fact that the received signal at this node contains many unknowns including the legitimate users' data (i.e., x_1, x_2), their channels and the auxiliary signals r_1 and r_2 . Moreover, the auxiliary signals, as can be seen from their derivation in (18) to (21), are a complicated function of the user's channels and user's data signals which makes the decoding of the transmitted signals by an external device an extremely challenging task.

C. DESIGN COMPLEXITY & LATENCY

In conventional NOMA, the main operation is successive interference cancellation where near users perform SIC for the far users' signals and then decode their own signals. This is regarded as one of the main sources of complexity in the NOMA receiver and thus it introduces a delay in the communication. Unlike SIC, this design cancels the interference completely, in one run only. Moreover, the use of diagonal of matrices, in the proposed design, keeps the computational cost very minimal at the transmitter freeing the receiver from any complex processing. Furthermore, performing all the processing at the transmitter makes the proposed paradigm a very appealing choice for internet of things (IoT) applications.

V. NUMERICAL RESULTS

Simulations of the proposed design in terms of bit error rate, throughput and peak-to-average power ratio (PAPR) were conducted in the MATLAB simulation environment. The list of all the parameters used in the simulations are shown in TABLE 2.

TABLE 2: Simulation Parameters

Modulation type	BPSK
IFFT / FFT size	64
Subcarriers for data n	52
Symbols allocated for cyclic prefix	16
Number of inactive sub-carriers for out of band emission	12
Number of OFDM symbols	2×10^4
Channel model	Rayleigh
Multipath channel delay samples locations	[0 3 5 6 8]
Multipath channel tap power profile (dBm)	[0 -8 -17 -21 -25]

In Fig.5., the bit error rate simulation results are displayed. It can be seen that the legitimate receiver devices UE_1 and UE_2 decode their data successfully where in all eavesdropping scenarios a very poor and degraded BER performance is obtained.

The degraded curves simulate the performance of the external eavesdropping where UE_X is trying to decode the

FIGURE 5: Bit error rates; where legitimate users have a good performance while all internal and external eavesdroppers experience severe BER degradation.

data of UE_1 and UE_2 , and internal eavesdropping (i.e., simulating the presence of an un-trusted legitimate user. That's the performance of UE_1 eavesdropping on UE_2 and vice versa).

In Fig.6, the proposed design is compared to conventional

FIGURE 6: MU-AS-ST vs PD-NOMA; under different power allocation scenarios.

power domain NOMA under different power allocation scenarios for a fixed distance. It can be seen that MU-AS-ST achieves better reliability than PD-NOMA, in this case. Distances from the base station used in this simulation are:

$$\begin{cases} \text{distance}(BS, UE_1) = 1000m \\ \text{distance}(BS, UE_2) = 500m \end{cases} \quad (45)$$

Throughput simulations of MU-AS-ST are shown in Fig.6.

It is known that one of the problems with orthogonal frequency division multiplexing is the higher peak to average power ratio. Fig.7. displays the simulation results for the peak to average power ratio for the proposed design along with conventional OFDM where it can be seen that the proposed design does not add further degradation over conventional

FIGURE 7: Throughput of the legitimate/eavesdropper nodes in the network, using the proposed MU-AS-ST.

OFDM. Moreover, at high SNR slightly lower PAPR values are obtained with MU-AS-ST compared to conventional OFDM.

FIGURE 8: PAPR of MU-AS-ST compared to conventional OFDM.

VI. CONCLUSION

In this paper, a novel OFDM-based multiple-access design was presented. The proposed design uses auxiliary signal superposition at the base station for cancelling the inter-user interference of the superimposed users while providing full secrecy for the legitimate users against both external and internal eavesdropping trials.

Moreover, the proposed design has no constraint on the users' superposition, unlike conventional NOMA where the users' superposition is constrained with the distance from the base station.

Furthermore, the use of diagonal matrices in the design keeps the computational cost very minimal at the base station, while doing no extra processing at the receiving nodes where a conventional OFDM receiver is used.

The proposed design proves capable of surpassing the conventional power domain NOMA in many aspects such as

reliability, secrecy and throughput. Moreover, it attains the same PAPR performance as conventional OFDM.

REFERENCES

- [1] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen and L. Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," in *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2294-2323, thirdquarter 2018, doi:10.1109/COMST.2018.2835558.
- [2] M. M. Şahin and H. Arslan, "Waveform-Domain NOMA: The Future of Multiple Access," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145077.
- [3] —, "Study on Non-Orthogonal Multiple Access (NOMA) for NR," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.812, 12 2018, version 13.0.0.
- [4] Clerckx, B., Mao, Y., Schober, R., Jorswieck, E., Love, D., Yuan, J., Hanzo, L., Li, G., Larsson, E., Caire, G. (2021). Is NOMA Efficient in Multi-Antenna Networks? A Critical Look at Next Generation Multiple Access Techniques. *ArXiv*, abs/2101.04802.
- [5] Furqan, Haji M., Jehad Hamamreh, and Huseyin Arslan. "Physical Layer-Security for NOMA: Requirements, Merits, Challenges, and Recommendations." *arXiv preprint arXiv:1905.05064* (2019).
- [6] Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for internet of things," in *Proc. IEEE VTC Spring'2016*, Nanjing, China, May 2016, pp. 1-5.
- [7] S. Chen, B. Ren, Q. Gao, S. Kang, S. Sun, and K. Niu, "Pattern division multiple access-a novel nonorthogonal multiple access for fifthgeneration radio networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3185-3196, April 2017.
- [8] 3GPP, R1-164688, Resource Spread Multiple Access, Qualcomm, May 2016.
- [9] 3GPP, R1-163992, Non-Orthogonal Multiple Access Candidate for NR, Samsung, May 2016.
- [10] C. Xu, Y. Hu, C. Liang, J. Ma, and L. Ping, "Massive MIMO, nonorthogonal multiple access and interleaved division multiple access," *IEEE Access*, vol. 5, pp. 14 728-14 748, Aug. 2017.
- [11] F. Wei and W. Chen, "Low complexity iterative receiver design for sparse code multiple access," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 621-634, Feb. 2017.
- [12] Hamamreh, J. M., Abewa, M., & Lemayian, J. P. (2020). New Non-Orthogonal Transmission Schemes for Achieving Highly Efficient, Reliable, and Secure Multi-User Communications. *RS Open Journal on Innovative Communication Technologies*, 1(2). <https://doi.org/10.46470/03d8ffbd.324cc0fb>
- [13] Zia, M. F., Hamamreh, J. M. (2020). An Advanced Non-Orthogonal Multiple Access Security Technique for Future Wireless Communication Networks. *RS Open Journal on Innovative Communication Technologies*, 1(2). <https://doi.org/10.46470/03d8ffbd.19888ce7>
- [14] Zia, M. F., Furqan, H. M., Hamamreh, J. M. (2021). Multi-cell, Multi-user, and Multi-carrier Secure Communication Using Non-Orthogonal Signals' Superposition with Dual-Transmission for IoT in 6G and Beyond. *RS Open Journal on Innovative Communication Technologies*, 2(3). <https://doi.org/10.46470/03d8ffbd.08b7bd1d>
- [15] Lemayian, J. P., Hamamreh, J. M. (2020). 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*, 1(2). <https://doi.org/10.46470/03d8ffbd.86b0d106>
- [16] J. M. Hamamreh, E. Basar and H. Arslan, "OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services," in *IEEE Access*, vol. 5, pp. 25863-25875, 2017, doi: 10.1109/ACCESS.2017.2768558.
- [17] M. K. Simon and M.-S. Alouini, *Fading Channel Characterization and Modeling*. Hoboken, NJ, USA: Wiley, 2002, pp. 15-30.
- [18] I.S.Gradshteyn and I.M.Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

JEHAD M. HAMAMREH is currently an Assistant Professor with the Electrical and Electronics Engineering Department, Antalya International (Bilim) University, Turkey. He received the Ph.D. degree in electrical-electronics engineering and cyber systems from Istanbul Medipol University, Turkey, in 2018. Previously, he worked as a Researcher at the Department of Electrical and Computer Engineering in Texas A&M University. He is the inventor of 10+ Patents, and has authored more than 60+ peer reviewed scientific papers along with several book chapters. His innovative patented works won the golden, silver and bronze medals by numerous international invention contests and fairs.

His current research interests include wireless physical and MAC layers security, orthogonal frequency-division multiplexing multiple-input multiple-output systems, advanced waveforms design, multidimensional modulation techniques (MIMO-SNM, OFDM-SNM, OFDM-SPM), and orthogonal/non-orthogonal multiple access schemes for future wireless systems. He is a regular referee, investigator and editor for various scientific journals as well as a TPC member for several international conferences. (web: <https://sites.google.com/view/wislab>)

MOHAMEDOU ABEWA received his B.Sc. degree in Electrical and Electronics Engineering from Antalya Bilim University, Turkey in 2019. Currently, he is pursuing a masters degree in Electrical and Computer Engineering at the same university. He is pursuing his research/thesis work at the Wireless Intelligent Systems Laboratory (WIS-LAB) at Antalya Bilim University. His research interests include Orthogonal Frequency Division Multiplexing (OFDM) related waveform designs, physical layer security algorithms and Non-Orthogonal Multiple Access Techniques (NOMA) for future wireless systems.

• • •