Received March 4, 2021, accepted March 28, 2021, date of publication April 6, 2021

Digital Object Identifier (DOI): 10.46470/03d8ffbd.08b7bd1d

Multi-cell, Multi-user, and Multi-carrier Secure Communication Using Non-Orthogonal Signals' Superposition with Dual-Transmission for IoT in 6G and Beyond

MUHAMMAD FURQAN ZIA[1], HAJI M. FURQAN[2], 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]School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey (e-mail: hamadni@st.medipol.edu.tr)
[2]Department of Electrical and Electronics Engineering, Antalya Bilim University, Antalya,Turkey (e-mail: jehad.hamamreh@antalya.edu.tr)
Authors Zia, M. F and Hamamreh, J. M. are also with WISLAB-TELENG for Wireless Research at ABU (web: https://sites.google.com/view/wislab).

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 Considering the advancements of the internet of things (IoT) in 6G and beyond communications, data transmission security in IoT devices has received extensive interest because of their significant features, such as low computational complexity, led by low power requirements. In such devices, the conventional cryptographic techniques may fail to provide secure communication. To fight this drawback, physical layer security (PLS) has remarkable potential to provide security solutions suitable for such applications. In this work, a highly effective PLS technique is proposed for providing secure communication against external and internal eavesdroppers in a downlink multi-cell, multi-user, and multi-carrier IoT communication system. In our proposed system, we considered two base stations, where each base station uses a single radio frequency (RF) chain to link two antennas that are used for the transmission of data. Further, we transmit the data in two rounds, and each round of transmission occurs through a single active antenna of each base station. A different antenna is used for each round of transmission to communicate with two single antenna IoT devices/users in the presence of a passive eavesdropper. In the proposed algorithm, frequency selective channel-based pre-coder matrices and the dual transmission approach are jointly employed. The dual-transmission is performed simultaneously from two base stations to provide security against internal and external eavesdroppers. The proposed system is suitable for IoT-based applications. Also, the potential capabilities of our proposed algorithm are proved by extensive mathematical and simulation analysis.

INDEX TERMS 6G, IoT, PLS, NOMA, Wireless Communication, Dual Transmission, Simultaneous Transmission, Pre-coder, Reliability, Security, PLS

I. INTRODUCTION

THE internet of things (IoT) in 6G is expected to support higher performance metrics than 5G along with the ever-changing service requirements. It is expected that 6G networks will support the requisite IoT applications by leveraging its networking, computing, and processing capabilities [1]. The main features of 6G would include, but not limited to network densification, high throughput, high efficiency, low energy consumption, and huge networking [2]. As a result of its widespread effects, 6G will have a wide range of applications, including autonomous vehicles, virtual reality, smart city, smart energy networks, remote surgery, drone delivery, computing reality devices, and sensing [3] [4].

The key technologies in 6G include artificial intelli-

gence AI-based software, molecular communication, quantum communication, blockchain, the TeraHertz (THz) technology, and visible light communication (VLC) technology [5]. These emerging technologies will play a key role in advancing 6G networks, but they are also prone to several security and privacy issues for example AI is threatened to access control [6], malicious behavior [7], authentication [8] and communication [9]. Molecular communication suffers from the risks of malicious behavior [10], encryption [11], and authentication [12]. The quantum communication also suffers from privacy issues such as encryption [13] and communication [14]. The current emerging technology of blockchain is prone to authentication [15], access control [16], and communication issues [17]. THz technology has the problem of authentication [18] and malicious behavior [19], and finally VLC is again prone to communication [20] and malicious behavior problem [21]. Yet wireless communication has a broadcast nature, so the data protection will still be a question mark due to the possibility of eavesdropping, which could breach the wireless contact's confidentiality [22] [23].

A. WIRELESS SECURITY TECHNIQUES

In the past orthogonal multiple access (OMA) techniques have been used in wireless communication systems [24]. Though orthogonal multiple access techniques provide excellent signal-to-noise ratio performance with complete robustness to interference due to the orthogonality between consumer subcarriers, they have still been proven unable to meet potential 5G plus requirements [25].

As a potential replacement to OMA, several studies have focused on enhancing physical layer security (PLS) for non-orthogonal multiple access NOMA-based communication systems to improve their confidentiality against eavesdropping or illegitimate access by unintended devices, [26] [27] [28], including power-domain NOMA (PD-NOMA) [29], sparse code multiple access (SCMA) [30], pattern division multiple access (PDMA) [31], resource spread multiple access (RSMA) [32], multi-user shared access (MUSA) [33], interleave-grid multiple access (IGMA) [34], welch-bound equality spread multiple access (WSMA) [35], and interleave division multiple access (IDMA) [36].

The non-orthogonal multiple access (NOMA) scheme is considered one of the most important enabling technologies for 6G and beyond, due to its ability to achieve high spectral performance, low latency, increased coverage, massive convergence, and fairness [37] [38]. These effective services of NOMA scheme can revolutionize the performance of wireless communication networks in the future. However, the conventional power-domain PD-NOMA has already been implemented under the title of multi-user superposition transmission (MUST) in 3GPP release 13, but later omitted from 3GPP release 17, due to efficiency degradation of the wireless signal arising from channel estimation errors because it was using successive interference cancellation (SIC) at the receiver [39]. Also, the conventional NOMA scheme requires power-sharing among multiple NOMA users, which causes latency and degradation of signal-to-interference-plus-noise ratio (SINR) for each user [39] [40] [41].

However, current industry-wide approaches for implementing safe communication in NOMA and other such wireless technologies are based on cryptography, and PLS [42]. Cryptography-based solutions can be decrypted by a spy who wants to hear the private information no matter how long or difficult the secret keys are generated. This also adds on an extra disadvantage of large processing at the receiver. Considering this drawback cryptography-based approaches are not suitable for future IoT-based applications because the key sharing and management is very challenging and increases complexity, requiring high computational power to operate. While on the other hand, the IoT-based applications that operate with low power will not handle much complexity, making cryptography-based approaches unsuitable [43].

Moreover, the conventional NOMA schemes suffers from two major drawbacks, i.e., it is prone to external and internal eavesdropping [44]. This means that the transmitted signal is at risk of eavesdropping both by an external eavesdropper and un-trusted user present during the communication who is internally trying to eavesdrop the information [45]. This problem is quite alarming for the society, including multiple sectors such as transportation, power distribution networks, banking, financial services, mobile tele-medicine, tele-work applications, industrial control and monitoring systems.

PLS techniques have emerged as an important alternative to conventional cryptography-based approaches to resolve potential communication system problems [43]. PLS ensure reliable data transmission between intended network nodes, while malicious nodes that try to eavesdrop the communication will obtain extremely degraded signal. This is because it can use wireless channel properties such as randomness, fading, noise, and interference. PLS strategies can also exploit the channel statistics between authorized transmitter and eavesdropper, eliminating the need for key sharing. Also, only simple signal processing can be used to implement PLS techniques in IoT devices [23].

One of the top research areas in PLS is methods to protect the orthogonal frequency division multiplexing (OFDM) waveform. The topic is important because OFDM is one of the most prominent and widely employed waveforms in the modern wireless communication system. It is also planned to be used in advanced communication systems with various enhanced specifications [23]. There are several PLS techniques proposed for OFDM, but many of them do not comply with future low complexity communication systems' requirements [46].

Some of the existing security mechanisms are successful approaches, but they will not fulfill the 6G networks' demands. Nevertheless, the lack of security and reliability have contradictory consequences [47]. When the wireless transmission quality is made reliable, security tends to be decreased since reliability encompasses a wide range of redundancy, making communication signals more vulnerable to

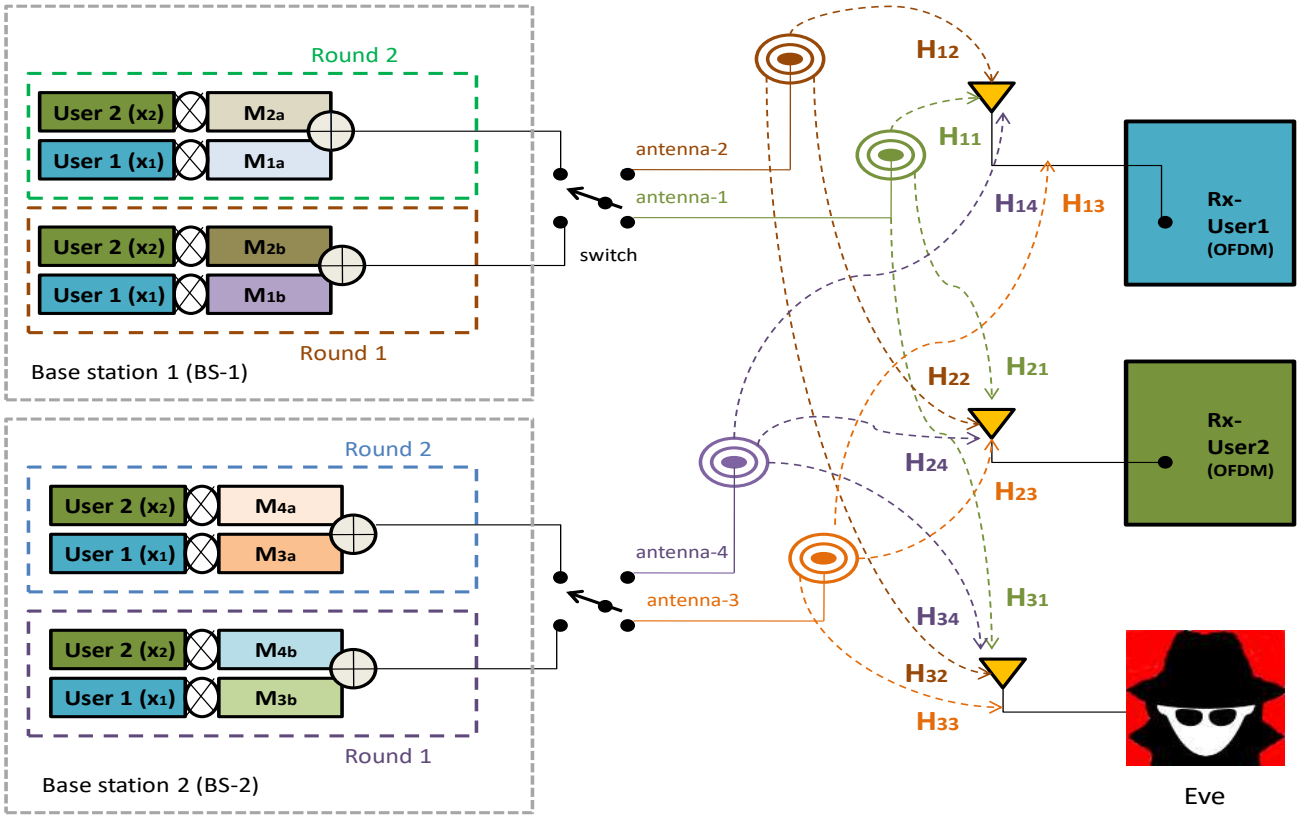

FIGURE 1. A simplified block diagram of the proposed system employing dual-transmission in a multi-cell, multi-user and multi-carrier IoT communication system.

eavesdropping [48] [49]. For instance, space-time codes [50], may improve the transmission system's reliability, but the system is more prone to possible security threats. Moreover, most of the existing security algorithms require complex processing at both transmitter and receiver, making them infeasible for applications with a simple low-power receiver.

Based on the above discussion regarding communication security, in this work, we propose a new kind of non-orthogonal transmission in an OFDM system with two base-stations that utilize small-scale fading. In our proposed technique, the data from both base-stations is simultaneously transmitted to the two authorized users at the receiver in the presence of a passive eavesdropper. Each authorize user consists of one antenna at the receiver. The data from each base station is transmitted following a simple dual-transmission technique using a single active antenna transmitter from each base station for each round of transmission. The data received at both the authorized users from the two base-stations are then added and demodulated at the receiver to provide secure and reliable communication in low-complexity communication systems that require limited processing at the receiver (IoT-based applications). More specifically, IoT devices' data are superimposed using channel-based pre-coder matrices and sent in two transmissions from two base stations simultaneously to achieve reliable and secure communication against internal and external eavesdroppers.

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 ARCHITECTURE

A communication strategy is designed to support multiple users in a downlink scenario. To provide a simple explanation of our proposed scheme, we consider only two users. The proposed system is constituted of two base stations[1], and each base station consists of two-transmit antennas and two single-antenna IoT devices/users.

The two base-stations are labeled as base-station-1 (BS-1) and base-station-2 (BS-2), each with a multi-carrier downlink transmitter and a single active antenna attempting to communicate with two single-antenna IoT devices (receivers), but

[1]The proposed multi-cell communication system resembles the CoMP concept that exist in the literature.

in the presence of a passive external eavesdropper (Eve) as shown in Fig. 1.

More precisely, the transmitter on each base-station has two antennas, and one single radio-frequency (RF) chain links them together. On each base station, one of the antennas (antenna 1 or antenna 2) at BS-1 and (antenna 3 or antenna 4) at BS-2 is made active for the transmission with the help of switch to artificially increase the randomness of the wireless channel for security enhancement. Additionally, it is presumed that users are untrustworthy, which implies the fact that even the individual user information is not protected from one another. The transmitter is believed to have no information about the channel of Eve. The channel connecting transmitter (Tx) and receiver (Rx) is supposedly rayleigh fading with exponentially decaying power delay profile and known by the transmitter before transmission. Channel reciprocity properties are used, where the transmitter and receiver's communication channel is calculated using channel sounding methods in time division duplexing (TDD) wireless systems [51]. The authorized transmitter needs to communicate with the users so that neither eavesdroppers nor the users listen to each others' information.

III. PROPOSED ALGORITHMS

This work's fundamental objective is to satisfy the expected IoT application requirements in 6G and beyond communication networks that would need efficient and robust communication and have minimal processing capability at the receiver [48]. In this study, the signals of user 1 data ($\mathbf{x_1}$) and user 2 data ($\mathbf{x_2}$) are superimposed or mathematically multiplied with the pre-coder matrices. Afterwards, this superimposed data is transmitted to the receiver in two rounds. Each round of transmission occurs from a different active antenna so that different channels are used in each transmission. The dual- transmission simultaneously occurs from both the base stations, i.e. BS-1 and BS-2. To make it possible, we ought to devise and develop specific kinds of pre-coders that could concurrently provide protection against internal and external snoopers.

Adding on to it, two users with dual transmission from each base station add greater complexities to an eavesdropper than the single-user channel-based protection algorithm. In every transmission round of the proposed algorithm, the superimposed intelligently devised pre-coder matrix will be decrypted only at the authorized receiver.

A simplified architecture of the proposed system is presented in Fig. 1. The specifications of the proposed algorithm are provided as follows:

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. It is important to note that we consider the frequency response of both user 1 and user 2 data streams, i.e. $\mathbf{x_1}$ and $\mathbf{x_2}$ same at both base stations. But the superimposed precoders are different for each round of the transmission at both base stations. 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, represent 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} active antenna of the transmitter.

The important contribution here is in the devising of channel-dependent pre-coder matrices that will ensure zero interference between the users. The proposed algorithm doesn't require successive interference cancellation (SIC) and instead shifts all the complexity to the base station. To achieve these goals, we multiply the pre-coder matrix with the user's data streams $\mathbf{x_1}$ and $\mathbf{x_2}$, so it is superimposed with the data stream. This superimposed signal is transmitted to the receiver in two rounds simultaneously from BS-1 and BS-2. Finally, when the signal from each transmission is combined at the authorized receiver, the user will automatically get a secure signal by simply demodulating the combined signal without any complex processing. The dual-transmission occurs from two base stations simultaneously with four total antennas at the transmitter and one single antenna at each users' receiver. On the other hand, it will be tough for eavesdroppers to detect the information intended for user-1 and user-2.

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

$$\mathbf{u_1} = \mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}, \tag{1}$$

Similarly, the transmitted signal during the second round that is transmitted from active antenna-2 of BS-1 can be given as:

$$\mathbf{u_2} = \mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}. \tag{2}$$

Now, following the same above principle the transmitted signal during first round from active antenna-3 of BS-2 is given as:

$$\mathbf{u_1'} = \mathbf{M_{3a}x_1} + \mathbf{M_{4a}x_2}, \tag{3}$$

Similarly, the transmitted signal during second round that is transmitted from active antenna-4 of BS-2 can be given as:

$$\mathbf{u_2'} = \mathbf{M_{3b}x_1} + \mathbf{M_{4b}x_2}. \tag{4}$$

where $\mathbf{x_1}$ and $\mathbf{x_2}$ are data vectors in frequency domain intended for user-1 and user-2, respectively, with equal power allocated to them, while $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ at BS-1 and $\mathbf{M_{3a}}$, $\mathbf{M_{4a}}$, $\mathbf{M_{3b}}$ and $\mathbf{M_{4b}}$ at BS-2 are specially designed pre-coder matrices based on the channel of authorized user 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 of devising intelligent pre-coders are explained.

A. RECEIVED SIGNAL AT USER-1

The total combined received signal at user-1 is the combination of signals from BS-1 and BS-2.

1) Received Signal at User-1 from BS-1

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

$$\mathbf{y_{11}} = \mathbf{H_{11}u_1} + \mathbf{z_{11}}, \tag{5}$$

where $\mathbf{H_{11}}$ and $\mathbf{z_{11}}$ are the frequency response of the channel and AWGN noise between user-1 and active antenna-1 of the Tx during round-1.

Similarly, the received signal at user-1 during round-2 of transmission using active antenna-2 of Tx is given as:

$$\mathbf{y_{12}} = \mathbf{H_{12}u_2} + \mathbf{z_{12}}, \tag{6}$$

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

2) Received Signal at User-1 from BS-2

The received signal in the frequency domain at user-1 during round-1 from transmission through active antenna-3 at the transmitter can be given as:

$$\mathbf{y_{13}} = \mathbf{H_{13}u'_1} + \mathbf{z_{13}}, \tag{7}$$

where $\mathbf{H_{13}}$ and $\mathbf{z_{13}}$ are the frequency response of the channel and AWGN noise between user-1 and active antenna-3 of the Tx during round-1.

Similarly, the received signal at user-1 during round-2 of transmission using active antenna-4 of Tx is given as:

$$\mathbf{y_{14}} = \mathbf{H_{14}u'_2} + \mathbf{z_{14}}, \tag{8}$$

where $\mathbf{H_{14}}$ and $\mathbf{z_{14}}$ are the frequency response of the channel and AWGN between user-1 and active antenna-4 of the Tx during round-2.

3) Combined received signal at User-1 from BS-1 and BS-2

The combined received signal from round-1 and round-2 transmission of BS-1 and BS-2 at user-1 can be written as:

$$\mathbf{\hat{y}_1} = \mathbf{y_{11}} + \mathbf{y_{12}} + \mathbf{y_{13}} + \mathbf{y_{14}}. \tag{9}$$

where $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$ are the received signals at user-1 during round-1 and round-2 through antenna-1 and antenna-2 of BS-1. Similarly, $\mathbf{y_{13}}$ and $\mathbf{y_{14}}$ are the received signals at user-1 during round-1 and round-2 through antenna-3 and antenna-4 of BS-2. After putting the values of $\mathbf{y_{11}}, \mathbf{y_{12}}, \mathbf{y_{13}}$ and $\mathbf{y_{14}}$ the combined signal can be given as follows:

$$\begin{aligned}\mathbf{\hat{y}_1} = {} & (\mathbf{H_{11}u_1} + \mathbf{z_{11}}) + (\mathbf{H_{12}u_2} + \mathbf{z_{12}}) + \\ & (\mathbf{H_{13}u'_1} + \mathbf{z_{13}}) + (\mathbf{H_{14}u'_2} + \mathbf{z_{14}}),\end{aligned} \tag{10}$$

Substituting the values of $\mathbf{u_1}, \mathbf{u_2}, \mathbf{u'_1}$ and $\mathbf{u'_2}$ from (1), (2), (3) and (4) and simplifying, we get:

$$\begin{aligned}\mathbf{\hat{y}_1} = {} & \mathbf{H_{11}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{11}} \\ & + \mathbf{H_{12}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{12}} \\ & + \mathbf{H_{13}}(\mathbf{M_{3a}x_1} + \mathbf{M_{4a}x_2}) + \mathbf{z_{13}} \\ & + \mathbf{H_{14}}(\mathbf{M_{3b}x_1} + \mathbf{M_{4b}x_2}) + \mathbf{z_{14}},\end{aligned} \tag{11}$$

$$\begin{aligned}\mathbf{\hat{y}_1} = {} & (\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}} + \mathbf{H_{13}M_{3a}} + \mathbf{H_{14}M_{3b}})\mathbf{x_1} \\ & + (\mathbf{H_{11}M_{2a}} + \mathbf{H_{12}M_{2b}} + \mathbf{H_{13}M_{4a}} + \\ & \mathbf{H_{14}M_{4b}})\mathbf{x_2}.\end{aligned} \tag{12}$$

Note that the noise term is present in the combined signal but for simplicity and to better explain our pre-coder design we didn't write it in equation (12).

At the receiver of user 1, the first term in (12) is the desired term, while the second term is undesired term for it. The pre-coder matrices will make sure that the undesired term as well as the channel effects are removed and canceled at user-1.

B. RECEIVED SIGNAL AT USER-2

The total combined received signal at user-2 is the combination of signals from BS-1 and BS-2.

1) Received Signal at User-2 from BS-1

Similar to user-1, the received signal from round-1 and round 2 transmitted through antenna-1 and antenna-2 at user-2 are provided in equations (13) and (14), respectively:

$$\mathbf{y_{21}} = \mathbf{H_{21}u_1} + \mathbf{z_{21}}, \tag{13}$$

$$\mathbf{y_{22}} = \mathbf{H_{22}u_1} + \mathbf{z_{22}}, \tag{14}$$

where $\mathbf{H_{21}}$ and $\mathbf{z_{21}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-1 of the Tx during round-1. Similarly, $\mathbf{H_{22}}$ and $\mathbf{z_{22}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-2 of the Tx during round-2.

2) Received Signal at User-2 from BS-2

The received signal from round-1 and round-2 transmitted through active antenna-3 and antenna-4 of BS-2 at user-2 can be written as:

$$\mathbf{y_{23}} = \mathbf{H_{23}u'_1} + \mathbf{z_{23}}, \tag{15}$$

$$\mathbf{y_{24}} = \mathbf{H_{24}u'_2} + \mathbf{z_{24}}, \tag{16}$$

where $\mathbf{H_{23}}$ and $\mathbf{z_{23}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-3 of the Tx during round-1. Similarly, $\mathbf{H_{24}}$ and $\mathbf{z_{24}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-4 of the Tx during round-2.

3) Combined received signal at User-2 from BS-1 and BS-2

Now, the combined received signal at user-2 from BS-1 and BS-2 can be written as:

$$\hat{\mathbf{y}}_\mathbf{2} = \mathbf{y_{21}} + \mathbf{y_{22}} + \mathbf{y_{23}} + \mathbf{y_{24}}. \tag{17}$$

After putting the values of $\mathbf{y_{21}}$, $\mathbf{y_{22}}$, $\mathbf{y_{23}}$ and $\mathbf{y_{24}}$ the combined signal can be presented as:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}u_1} + \mathbf{z_{21}} + \mathbf{H_{22}u_2} + \mathbf{z_{22}} + \\ \mathbf{H_{23}u'_1} + \mathbf{z_{23}} + \mathbf{H_{24}u'_2} + \mathbf{z_{24}},\end{aligned} \tag{18}$$

Substituting the values of $\mathbf{u_1}$, $\mathbf{u_2}$, $\mathbf{u'_1}$ and $\mathbf{u'_2}$ from (1), (2), (3) and (4) and simplifying, we get:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{21}} \\ + \mathbf{H_{22}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{22}} \\ + \mathbf{H_{23}}(\mathbf{M_{3a}x_1} + \mathbf{M_{4a}x_2}) + \mathbf{z_{23}} \\ + \mathbf{H_{24}}(\mathbf{M_{3b}x_1} + \mathbf{M_{4b}x_2}) + \mathbf{z_{24}},\end{aligned} \tag{19}$$

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{2} = (\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}} + \mathbf{H_{23}M_{3a}} + \mathbf{H_{24}M_{3b}})\mathbf{x_1} \\ + (\mathbf{H_{21}M_{2a}} + \mathbf{H_{22}M_{2b}} + \mathbf{H_{23}M_{4a}} + \\ \mathbf{H_{24}M_{4b}})\mathbf{x_2}.\end{aligned} \tag{20}$$

It is important to note that we are not considering the noise terms during mathematical calculations for simplicity purposes as it does not affect the results.

The first term in equation (20) is the undesired term for user-2 while the second term is desired term for it.

C. RECEIVED SIGNAL AT EAVESDROPPER

The total combined received signal at Eve is the combination of signals received from BS-1 and BS-2.

1) Received Signal at Eve from BS-1

The received signal from round-1 and round-2 through active antenna-1 and antenna-2 of BS-1 is provided in equations (21) and (22), respectively.

$$\mathbf{y_{31}} = \mathbf{H_{31}u_1} + \mathbf{z_{31}}, \tag{21}$$

$$\mathbf{y_{32}} = \mathbf{H_{32}u_2} + \mathbf{z_{32}}, \tag{22}$$

where $\mathbf{H_{31}}$ and $\mathbf{z_{31}}$ are the frequency response of the channel and AWGN between the eavesdropper and active antenna-1 of the Tx during round-1. Similarly, $\mathbf{H_{32}}$ and $\mathbf{z_{32}}$ are the frequency response of the channel and AWGN between the eavesdropper and active antenna-2 of the Tx during round-2.

2) Received Signal at Eve from BS-2

Now, following the same steps as mentioned above, the received signal at the eavesdropper (Eve) is calculated, the received signal from round-1 and round-2 transmitted through BS-2 is provided in equations (23) and (24), respectively:

$$\mathbf{y_{33}} = \mathbf{H_{33}u'_1} + \mathbf{z_{33}}, \tag{23}$$

$$\mathbf{y_{34}} = \mathbf{H_{34}u'_2} + \mathbf{z_{34}}, \tag{24}$$

where $\mathbf{H_{33}}$ and $\mathbf{z_{33}}$ are the frequency response of the channel and AWGN between the eavesdropper and active antenna-3 of the Tx during round-1. Similarly, $\mathbf{H_{34}}$ and $\mathbf{z_{34}}$ are the frequency response of the channel and AWGN between the eavesdropper and active antenna-4 of the Tx during round-2.

3) Combined received signal at Eve from BS-1 and BS-2

For the case of eavesdropper, the combined received signal from BS-1 and BS-2 can be written as:

$$\hat{\mathbf{y}}_\mathbf{3} = \mathbf{y_{31}} + \mathbf{y_{32}} + \mathbf{y_{33}} + \mathbf{y_{34}}. \tag{25}$$

After putting the value of $\mathbf{y_{31}}$, $\mathbf{y_{32}}$, $\mathbf{y_{33}}$ and $\mathbf{y_{34}}$ the combined signal can be presented as:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{3} = \mathbf{H_{31}u_1} + \mathbf{z_{31}} + \mathbf{H_{32}u_2} + \mathbf{z_{32}} \\ + \mathbf{H_{33}u'_1} + \mathbf{z_{33}} + \mathbf{H_{34}u'_2} + \mathbf{z_{34}},\end{aligned} \tag{26}$$

Substituting the values of $\mathbf{u_1}$, $\mathbf{u_2}$, $\mathbf{u'_1}$ and $\mathbf{u'_2}$ from (1), (2), (3) and (4) and simplifying, we get:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{3} = \mathbf{H_{31}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{31}} \\ + \mathbf{H_{32}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{32}} \\ + \mathbf{H_{33}}(\mathbf{M_{3a}x_1} + \mathbf{M_{4a}x_2}) + \mathbf{z_{33}} \\ + \mathbf{H_{34}}(\mathbf{M_{3b}x_1} + \mathbf{M_{4b}x_2}) + \mathbf{z_{34}},\end{aligned} \tag{27}$$

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{3} = (\mathbf{H_{31}M_{1a}} + \mathbf{H_{32}M_{1b}} + +\mathbf{H_{33}M_{3a}} + \mathbf{H_{34}M_{3b}})\mathbf{x_1} \\ + (\mathbf{H_{31}M_{2a}} + \mathbf{H_{32}M_{2b}} + \mathbf{H_{33}M_{4a}} + \\ \mathbf{H_{34}M_{4b}})\mathbf{x_2}.\end{aligned} \tag{28}$$

The eavesdropper wants to hear both user-1 and user-2 information. Hence, both the first and second terms of (28) are desired terms for it.

D. PRE-CODER DESIGN FOR THE PROPOSED ALGORITHM

We need to design the pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2b}}$ for BS-1 and $\mathbf{M_{3a}}$, $\mathbf{M_{4a}}$, $\mathbf{M_{3b}}$, $\mathbf{M_{4b}}$ for BS-2 in such a way that the combined signal during round-1 and round-2 at the legitimate users will provide reliable data intended for them, while keeping the communication secure from internal and external eavesdropping.

The design procedure of $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{3a}}$, $\mathbf{M_{3b}}$ is as follows: Firstly, in order to remove the effect of channel at user-1, the first term in the equation (12) should be equal to identity matrix and can be given as:

$$(\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}} + \mathbf{H_{13}M_{3a}} + \mathbf{H_{14}M_{3b}}) = \mathbf{I}. \tag{29}$$

Also, to cancel the interference caused by user-1 on user-2, the first term in equation (20) should be equal to zero, and it is given as:

$$(\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}} + \mathbf{H_{23}M_{3a}} + \mathbf{H_{24}M_{3b}}) = 0. \tag{30}$$

Equations (29) and (30) can be jointly solved by supposing the values of precoders $\mathbf{M_{3a}}$ and $\mathbf{M_{3b}}$ as matrices '$\mathbf{X}$' and

'$\mathbf{Y}$', respectively, so that we can calculate the values of pre-coder matrices $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ as follows:

$$\mathbf{M_{1a}} = -(\mathbf{H_{22}} + \mathbf{H_{12}H_{23}X} - \mathbf{H_{13}H_{22}X} + \mathbf{H_{12}H_{24}Y} - \mathbf{H_{14}H_{22}Y}) \times (\mathbf{H_{12}H_{21}} - \mathbf{H_{11}H_{22}})^{-1}. \quad (31)$$

$$\mathbf{M_{1b}} = (\mathbf{H_{21}} + \mathbf{H_{11}H_{23}X} - \mathbf{H_{13}H_{21}X} + \mathbf{H_{11}H_{24}Y} - \mathbf{H_{14}H_{21}Y}) \times (\mathbf{H_{12}H_{21}} - \mathbf{H_{11}H_{22}})^{-1}. \quad (32)$$

It is indicated from the above-designed precoders that it has infinitely many solutions and provide us with the freedom to choose any matrix from the infinite number of matrix values for both '$\mathbf{X}$' and '$\mathbf{Y}$'. These intelligent precoders can provide highly secure and reliable communication.

Similarly, in order to design $\mathbf{M_{2a}}$, $\mathbf{M_{2b}}$, $\mathbf{M_{4a}}$ and $\mathbf{M_{4b}}$ we will follow similar steps as explained in the above discussion. So, in order to remove the effect of the channel at user-2, the second term in equation (20) should be equal to identity matrix and can be given as:

$$(\mathbf{H_{21}M_{2a}} + \mathbf{H_{22}M_{2b}} + \mathbf{H_{23}M_{4a}} + \mathbf{H_{24}M_{4b}}) = \mathbf{I}. \quad (33)$$

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

$$(\mathbf{H_{11}M_{2a}} + \mathbf{H_{12}M_{2b}} + \mathbf{H_{13}M_{4a}} + \mathbf{H_{14}M_{4b}}) = 0. \quad (34)$$

Equations (33) and (34) can be jointly solved to get the values of pre-coder matrices. To solve these both equations we suppose the values of precoders $\mathbf{M_{4a}}$ and $\mathbf{M_{4b}}$ as matrices '$\mathbf{A}$' and '$\mathbf{B}$', respectively, so that we can calculate the values of pre-coder matrices $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ as follows:

$$\mathbf{M_{2a}} = -(\mathbf{H_{12}} - \mathbf{H_{12}H_{23}A} + \mathbf{H_{13}H_{22}A} - \mathbf{H_{12}H_{24}B} + \mathbf{H_{14}H_{22}B}) \times (\mathbf{H_{11}H_{22}} - \mathbf{H_{12}H_{21}})^{-1}. \quad (35)$$

$$\mathbf{M_{2b}} = (\mathbf{H_{11}} - \mathbf{H_{11}H_{23}A} + \mathbf{H_{13}H_{21}A} - \mathbf{H_{11}H_{24}B} + \mathbf{H_{14}H_{21}B}) \times (\mathbf{H_{11}H_{22}} - \mathbf{H_{12}H_{21}})^{-1}. \quad (36)$$

Again, it is indicated from the above-designed precoders that they have infinitely many solutions and provides with the freedom to choose any matrix value from 0 to infinity for both '$\mathbf{A}$' and '$\mathbf{B}$'. These calculated equations of precoder matrices will be used in round-1 and round-2 at BS-1 and BS-2 to ensure that user-1 and user-2 will get reliable signals that are secure from internal and external eavesdroppers.

Note that, in this proposed method, we do not need any complex processing at the receiver of user-1 and user-2 and they just simply need to add the signals from round-1 and round-2 of BS-1 and BS-2. Hence, it can support applications with processing limited receiver (IoT-based applications).

E. ADVANTAGES OF THE PROPOSED NOVEL SECURITY SCHEME

There are multiple advantages of the proposed novel security technique that can be summarized as follows:

- No need for successive interference cancellation (SIC).
- Provides security against both internal and external eavesdropping with no leakage of information.
- Does not require having large scale channel gain difference between multiplexed users to make it work (unlike PD-NOMA).
- Offers full data rate for each user with no BER degradation.
- There is no need for interference cancellation because we transmit the signal in multiple transmissions 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).
- Mixture of channel-based pre-coded signals that undergoes dual transmission simultaneously at two base stations is more challenging to eavesdrop compared to channel adaptive secure transmission.

IV. MATHEMATICAL PERFORMANCE ANALYSIS OF THE PROPOSED ALGORITHM

In this part, we first present the performance evaluation for the theoretical bit error rate (BER) of the authorized node employing the proposed algorithm. Then we mathematically compare the SNR performance of OMA and conventional PD-NOMA. And then prove the effectiveness of the proposed algorithm, which is comparable to OMA and better than PD-NOMA.

A. BIT ERROR RATE ANALYSIS

Bit error rate (BER) is a significant indication of communication systems efficiency. It evaluates the certainty that a bit sent from a transmitter is received without any changes at the receiver. 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 [52]. To calculate BER, we need to find the statistics of the effective instantaneous signal-to-noise ratio (SNR), $\gamma_{\mathbf{b}}$, at the authorized node. The values of pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ at BS-1, while $\mathbf{M_{3a}}$, $\mathbf{M_{3b}}$, $\mathbf{M_{4a}}$ and $\mathbf{M_{4b}}$ superimposed with data transmitted from BS-2 are provided in section III.

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 [52]. In addition, 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.

The probability density function (PDF) for the effective instantaneous SNR, $\gamma_{\mathbf{b}}$, at the authorized node, with Gamma

distributed, [53], sub-channels' power can be given in simplified form similar to the work presented in, [52], with some modifications and approximation as follows:

$$P_{\gamma_b}(\gamma_b) \approx \left(\frac{\mathbf{1}}{\mathbf{w}}\right)^{u} \frac{\mathbf{1}}{\mathbf{\Gamma(u)}} \frac{\mathbf{\Omega^{\frac{3}{2}}}\sqrt{\gamma_\mathbf{b}}}{\bar{\gamma_\mathbf{b}}^{\frac{3}{2}}} \exp\left(-\frac{\mathbf{1}}{\mathbf{w}}\frac{\mathbf{\Omega}\gamma_\mathbf{b}}{\bar{\gamma_\mathbf{b}}}\right), \quad (37)$$

where $\mathbf{w}$ and $\mathbf{u}$ are the scale and shape parameters, Ω 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, $\gamma_\mathbf{b}$, [54] as follows:

$$BER_b = \frac{\mathbf{1}}{\mathbf{2}} \int_0^\infty \mathbf{erfc}(\sqrt{\gamma_\mathbf{b}}) P_{\gamma_\mathbf{b}}(\gamma_\mathbf{b}) d\gamma_\mathbf{b}. \quad (38)$$

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

$$BER_b = \frac{\mathbf{1}}{\mathbf{2}} \int_0^\infty \mathbf{erfc}(\sqrt{\gamma_\mathbf{b}}) \left(\frac{\mathbf{1}}{\mathbf{w}}\right)^{u} \frac{\mathbf{1}}{\mathbf{\Gamma(u)}} \frac{\mathbf{\Omega^{\frac{3}{2}}}\sqrt{\gamma_\mathbf{b}}}{\bar{\gamma_\mathbf{b}}^{\frac{3}{2}}} \times \exp\left(-\frac{\mathbf{1}}{\mathbf{w}}\frac{\mathbf{\Omega}\gamma_\mathbf{b}}{\bar{\gamma_\mathbf{b}}}\right) d\gamma_\mathbf{b}. \quad (39)$$

By simplifying the above equation based on [52], the BER formula can be given as:

$$BER_b \approx \frac{\mathbf{G}}{\mathbf{2}\sqrt{\pi}} \left(\frac{\arctan\left(\sqrt{\rho}\right)}{\mathbf{2}\rho^{\mathbf{3/2}}} - \frac{\mathbf{1}}{\mathbf{2}\rho\left(\mathbf{1}+\rho\right)}\right), \quad (40)$$

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

B. PERFORMANCE COMPARISON OF CONVENTIONAL OMA AND PD-NOMA WITH PROPOSED NEW NOMA

To understand the difference between conventional OMA and PD-NOMA and compare their performance with the proposed new NOMA, we consider SNR as a performance comparison metric.

Let us consider a multi-user (two-user) conventional downlink PD-NOMA model. In this model, we assign different powers to each user. The power is assigned based on the channel properties, and afterward, the signal is transmitted [55]. In contrast, the proposed design uses antenna diversity and transmits signals in rounds simultaneously from two base stations using four total antennas in the system (as already explained in section III). The enhanced antenna diversity in the proposed new NOMA results in overall efficiency improvements compared to conventional PD-NOMA transmission. Also, the received signal efficiency at user-1 and user-2 is largely dependent on the signal to noise ratio (SNR). The stronger the SNR rating, the greater the reliability. For reference, the SNR of OMA for near user (i.e, $user1$) and far user (i.e, $user2$) is given as:

$$SNR_{_{near}} = \frac{p_{_{near}}}{n_o}, \qquad SNR_{_{far}} = \frac{p_{_{far}}}{n_o}. \quad (41)$$

where $p_{_{near}}$ and $p_{_{far}}$ represents the assigned power to near and far users respectively, while the channel noise is denoted by n_o. In comparison, the SNR of conventional PD-NOMA for both near user and far user can be presented as:

$$SNR_{_{near}} = \frac{p_{_{near}}}{n_o}, \qquad SNR_{_{far}} = \frac{p_{_{far}}}{p_{_{near}} + n_o}. \quad (42)$$

The signal decrypted by the near user includes the channel noise, while that decrypted by the far user has both the channel noise as well as the near user signal (i.e., in PD-NOMA, the far user considers the near user's signal as a noise). We can conclude from equation (42) that the SNR of individual users in PD-NOMA network is more degraded than OMA incase when users are far from the base station. Therefore OMA is more efficient than PD-NOMA in such cases.

In contrast to conventional PD-NOMA, where a combination of signals from far and near consumers is needed, the proposed new NOMA, explained in section III, will also work in power-balanced cases and eventually provide enhanced reliable and secure output signal like OMA system. However, the proposed technique is less complex due to automatic interference cancellation. It eliminates the need for using the successive interference cancellation (SIC) method and makes the data transmission more reliable.

V. SIMULATION RESULTS

In this section, simulation results for the proposed algorithm are presented in order to evaluate the effectiveness of the proposed technique by using bit error rate (BER), throughput, and peak to average power ratio (PAPR) as performance metrics.

We consider that the Tx is employing OFDM with $N_f = 64$ sub-carriers with BPSK modulation for each user and a cyclic prefix (CP) of size L is added in order to avoid 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-1.

TABLE 1. System parameters.

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

Figure 2 presents the BER versus signal to noise ratio (SNR) plots for the proposed algorithm. We transmit the signals in two rounds simultaneously from two base stations in the proposed communication system. It can be observed from Fig. 2 that the BER outputs of user-1 and user-2 employing the proposed algorithm are identical to each other. However, there is a substantial difference between the legitimate users' BER performances and the eavesdropper entities, E-Eve-1 and E-Eve-2 are the external eavesdroppers that

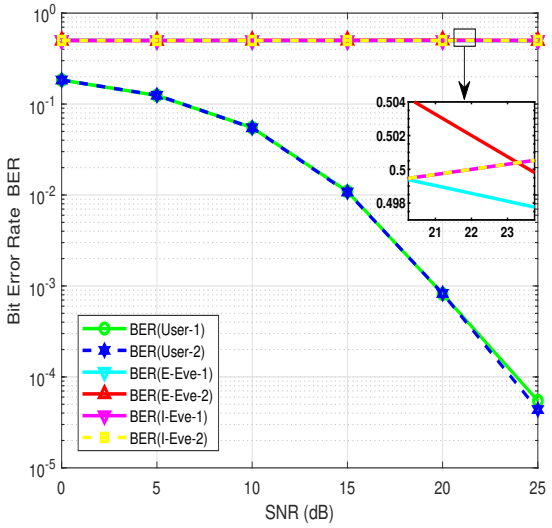

FIGURE 2. BER versus SNR performance for the proposed algorithm.

are spy entities aiming to hear the private communication between legitimate users. On the other hand, I-Eve-1 and I-Eve-2 denote the internal eavesdropper's performance that is internally trying to eavesdrop the signal of other user during the communication. In general, the superior BER performance of legitimate users compared to the degraded BER performance of eavesdroppers proves that the proposed algorithm can significantly provide security against all kinds of eavesdropping.

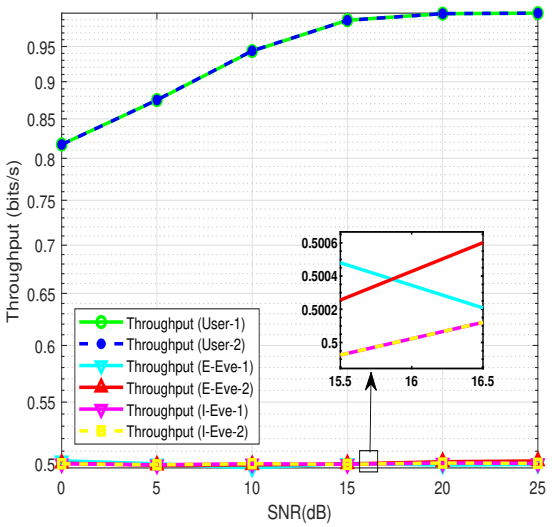

FIGURE 3. Throughput versus SNR performance for the proposed algorithm.

Figure 3 presents the throughput versus SNR plots for the proposed algorithm. The graph provides an analysis of the rate of the successful message that is delivered over a communication channel. As shown in fig. 3, the individual throughput performances of legitimate user-1 and user-2 employing the proposed algorithm are remarkable and equal to 1 bits/sec at high SNR values. While at the same time, it is observed that the throughput performance of external and internal eavesdroppers deteriorates. One essential consideration to be noted here is that while the throughput performances of the external and internal eavesdroppers are not zero, the service providers can still guarantee the quality of service (QoS) based communication security. The term QoS-based protection [56] refers to providing a secure communication channel depending on the specifications of service providers (voice, video, etc.), instead of offering perfect security. More precisely, different network services have different QoS criteria for effective communication. If we make sure the eavesdropper is operating below the QoS requirements of a particular service, we can protect that service.

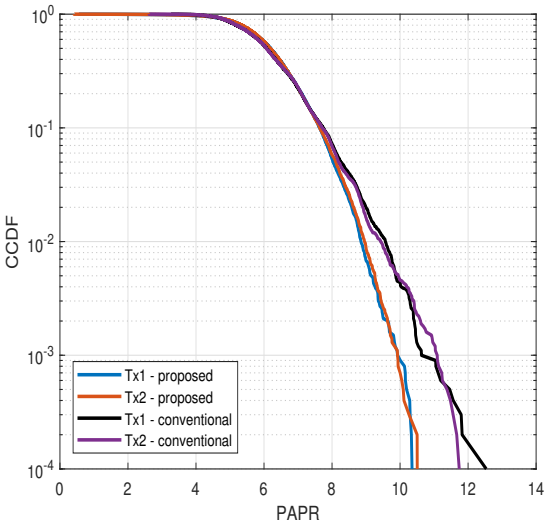

FIGURE 4. Peak-to-Average Power Ratio (PAPR) performance analysis for the proposed system.

Figure 4 shows a comparison of the peak to average power ratio (PAPR) plots of the conventional OFDM and OFDM employing the proposed algorithm for user-1 and user-2, respectively. The Fig. 4 indicates that PAPR performance of OFDM system employing the proposed algorithm surpasses the conventional OFDM at high SNR values. The developed technique gets improved PAPR because the precoder matrices, when devised at the transmitter, shift the signal's propagation from being gaussian to something less arbitrary than gaussian and near to uniform. Consequently, it addresses one of the crucial problems faced by OFDM systems [57] by reducing the PAPR, which leads to improved higher spectral efficiency.

In figure 5 we assess the robustness of the proposed method by deploying it under imperfect channels. To view the effect of the imperfect channel, intentional error (ΔH) is added to the actual channel (H). After adding an intentional error the equation of imperfect channel can be given as $\tilde{H} = H + \Delta H$ [51]. We can project ΔH as an individual

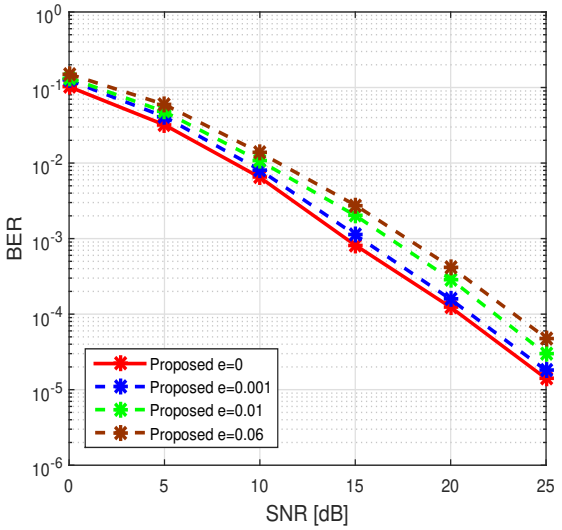

FIGURE 5. Robustness of the proposed algorithm under imperfect channel conditions

AWGN with zero mean and variance ($\sigma^2 = e \times 10^{\frac{-SNRdB}{10}}$), where the value of e dictates the standard of estimator, with lower values indicating a high quality estimator. Fig. 5 displays the BER versus SNR output under imperfect channel set-up with projections offering multiple parameters ($e = 0, 0.001, 0.01, 0.06$). It is evident from Fig. 5 that there is a slight deterioration in the BER efficiency of the proposed method due to the imperfect assessor. Even so, it can be enhanced by increasing the power of the training sequence or using a pilot with a greater range. Besides that, there are plenty of techniques in the literature to improve the channel estimator's outputs [51].

All in all, the proposed algorithm can be an excellent method for providing secure communication, particularly for IoT applications with low processing receivers.

VI. CONCLUSION

A viable IoT communication technique has been proposed, allowing safe and efficient communication between IoT devices that require low computational power. A novel approach is presented where data of users are superimposed after multiplication with the precoder matrices and sent in dual-transmission from two antennas (i.e., different active antenna for each transmission) of two base stations at the same time to ensure a reliable as well as secure communication against internal and external eavesdropping. The transmission occurs so that the mixture of data and pre-coders from both base stations is simultaneously sent. After combining signals from the first and the second transmissions of both base stations, the authorized receivers get the genuine signal without complex processing. In contrast, the external eavesdropper gets the degraded version of the signal. Moreover, the proposed algorithm also ensures that the users cannot eavesdrop each other's data. Simulation results confirmed that the proposed algorithm would allow safe communication and is suitable for IoT-based devices since it does not involve complex processing at the receivers.

REFERENCES

[1] 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.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, June 2014.

[3] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure and reliable iot communications using nonorthogonal signals' superposition with dual-transmission," IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Sep. 2020.

[4] S. Choochotkaew, H. Yamaguchi, T. Higashino, and M. Shibuya, "Requirement-based prioritization system in multi-user iot," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 122–127.

[5] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," Digital Communications and Networks, vol. 6, 07 2020.

[6] E. Peltonen, M. Bennis, M. Capobianco, M. Debbah, A. Ding, F. Gil-Castiñeira, M. Jurmu, T. Karvonen, M. Kelanti, A. Kliks, T. Leppänen, L. Lovén, T. Mikkonen, A. Rao, S. Samarakoon, K. Seppänen, P. Sroka, S. Tarkoma, and T. Yang, "6g white paper on edge intelligence," ArXiv, vol. abs/2004.14850, 2020.

[7] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" 11 2019.

[8] R. Sattiraju, A. Weinand, and H. D. Schotten, "Ai-assisted phy technologies for 6g and beyond wireless networks," arXiv preprint arXiv:1908.09523, 2019.

[9] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6g: A comprehensive survey on technologies, applications, challenges, and research problems," Transactions on Emerging Telecommunications Technologies, 2021. [Online]. Available: https://app.dimensions.ai/details/publication/pub.1135077922

[10] N. Farsad, H. B. Yilmaz, A. Eckford, C.-B. Chae, and W. Guo, "A comprehensive survey of recent advancements in molecular communication," IEEE Communications Surveys Tutorials, vol. 18, no. 3, p. 1887–1919, 2016. [Online]. Available: http://dx.doi.org/10.1109/COMST.2016.2527741

[11] A. O. Kislal, B. C. Akdeniz, C. Lee, A. E. Pusane, T. Tugcu, and C. B. Chae, "Isi-mitigating channel codes for molecular communication via diffusion," IEEE Access, vol. 8, pp. 24 588–24 599, 2020.

[12] V. Loscrí, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," IEEE Transactions on NanoBioscience, vol. 13, no. 3, pp. 198–207, 2014.

[13] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6g communication networks: State-of-the-art and vision for the future," IEEE Access, 2019.

[14] T. Li and G.-L. Long, "Quantum secure direct communication based on single-photon bell-state measurement," New Journal of Physics, vol. 22, no. 6, p. 063017, jun 2020. [Online]. Available: https://doi.org/10.1088/1367-2630/ab8ab5

[15] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. U. Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication in context of molecular communication and terahertz communication for body-centric nanonetworks," IEEE Transactions on Molecular, Biological and Multi-Scale Communications, vol. 6, no. 2, pp. 107–133, 2020.

[16] K. Kotobi and S. Bilen, IEEE Vehicular Technology Magazine, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[17] P. Ferraro, C. King, and R. Shorten, "Distributed ledger technology for smart cities, the sharing economy, and social compliance," IEEE Access, vol. 6, pp. 62 728–62 746, 2018.

[18] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," Physical Communication, vol. 12, pp. 16–32, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874490714000238

[19] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," Nature, vol. 563, no. 7729, p. 89—93, November 2018. [Online]. Available: https://doi.org/10.1038/s41586-018-0609-x

[20] N. Cen, N. Dave, E. Demirors, Z. Guan, and T. Melodia, "Libeam: Throughput-optimal cooperative beamforming for indoor visible light networks," in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019, pp. 1972–1980.

[21] T. Zhu, D. Ye, W. Wang, W. Zhou, and P. Yu, "More than privacy: Applying differential privacy in key areas of artificial intelligence," IEEE Transactions on Knowledge and Data Engineering, p. 1–1, 2021. [Online]. Available: http://dx.doi.org/10.1109/TKDE.2020.3014246

[22] H. M. Furqan, M. A. Aygul, M. Nazzal, and H. Arslan, "Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding," arXiv e-prints, p. arXiv:2006.09231, Jun. 2020.

[23] 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.

[24] M. Aldababsa, M. Toka, S. Gökçeli, G. K. Kurt, and O. Kucur, "A tutorial on nonorthogonal multiple access for 5g and beyond," wireless communications and mobile computing, vol. 2018, 2018.

[25] J. M. Hamamreh, M. Abewa, and J. P. Lemayian, "New non-orthogonal transmission schemes for achieving highly efficient, reliable, and secure multi-user communications," RS Open Journal on Innovative Communication Technologies, vol. 1, no. 2, 12 2020, https://rs-ojict.pubpub.org/pub/tphonik9. [Online]. Available: https://rs-ojict.pubpub.org/pub/tphonik9

[26] 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.

[27] 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.

[28] 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.

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

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] Y. Liu, W. Yi, Z. Ding, X. Liu, O. Dobre, and N. Al-Dhahir, "Application of noma in 6g networks: Future vision and research opportunities for next generation multiple access," arXiv preprint arXiv:2103.02334, 2021.

[38] M. F. Zia and J. M. Hamamreh, "An advanced non-orthogonal multiple access security technique for future wireless communication networks," RS Open Journal on Innovative Communication Technologies, vol. 1, no. 2, 12 2020, https://rs-ojict.pubpub.org/pub/s99ykm90. [Online]. Available: https://rs-ojict.pubpub.org/pub/s99ykm90

[39] 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

[40] J. Lemayian and J. Hamamreh, "Novel small-scale noma communication technique using auxiliary signal superposition," 2020 International Conference on UK-China Emerging Technologies (UCET), Sep. 2020.

[41] U. S. S. S. Arachchillage, D. N. K. Jayakody, S. K. Biswash, and R. Dinis, "Recent advances and future research challenges in non-orthogonal multiple access for 5g networks," in 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), 2018, pp. 1–6.

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

[43] 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.

[44] 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.

[45] M. Furqan, J. Hamamreh, and H. Arslan, "Physical layer security for noma: Requirements, merits, challenges, and recommendations," arXiv preprint arXiv:1905.05064, May 2019.

[46] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on ofdm physical layer security," Physical Communication, vol. 32, pp. 1–30, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874490718302817

[47] Z. Feng, "Security, reliability and performance issues in wireless networks," Ph.D. dissertation, USA, 2013, aAI3559975.

[48] 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.

[49] 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.

[50] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," IEEE Transactions on Information Theory, vol. 44, no. 2, pp. 744–765, 1998.

[51] 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.

[52] 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.

[53] V. P. Singh, "Gamma Distribution. In: Entropy-Based Parameter Estimation in Hydrology". Springer, Dordecht, 1998, vol. 30.

[54] J. G. Proakis and D. G. Manolakis, Digital Signal Processing (3rd Ed.): Principles, Algorithms, and Applications. USA: Prentice-Hall, Inc., 1996.

[55] A. Kassir, R. A. Dziyauddin, H. M. Kaidi, and M. A. Mohd Izhar, "Power domain non orthogonal multiple access: A review," in 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN), 2018, pp. 66–71.

[56] 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.

[57] 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 and M.S. degree in Electrical and Computer engineering from Antalya Bilim University, Turkey in Jan. 2021. Currently, he is working as a researcher at the Wireless Intelligent Systems laboratory in Antalya Bilim University, where he invented new 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, NOMA, Wireless technologies, Signal processing techniques, and the Internet of Things (IoT) applications.

HAJI M. FURQAN received his B.S. degree in electrical engineering (telecommunication), M.S. degree in electrical engineering (wireless communication) from the COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan, in 2013 and 2014, respectively, and the Ph.D. degree in electrical engineering from Istanbul Medipol University, Turkey, in 2020. He was a Trainee Researcher and Teacher Assistant at the Department of Electrical, CIIT. During his PhD, he was a researcher at the CoSiNC research group in Istanbul Medipol University, where he is currently a Post-Doc Researcher. His current research interests include physical layer security, cooperative communication, adaptive index modulation, cryptography, 5G systems, RIS, and wireless channel modeling and characterization.

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. He worked as a Researcher at the Department of Electrical and Computer Engineering in Texas AM University. He is the inventor of 8+ Patents, and He has authored more than 55+ 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, and orthogonal/nonorthogonal multiple access schemes for future wireless systems. He is a regular investigator and referee for various scientific journals as well as a TPC member for several international conferences. He is an Editor at RS-OJICT and Frontiers in Communications and Networks.