Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission

Conference Paper · August 2020

DOI: 10.1109/PIMRC48278.2020.9217261

CITATIONS
0

READS
15

3 authors:

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

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

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

Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission

Haji M. Furqan*, Jehad M. Hamamreh†, and Huseyin Arslan *‡*Fellow, IEEE*
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey
†Department of Electrical and Electronics Engineering, Antalya Bilim University, Antalya, Turkey
‡Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620

***Abstract*—Ensuring secure communication for internet of things (IoT) has drawn much attention because of the limitation in the use of conventional cryptographic techniques owing to the unique features of IoT devices such as low complexity, lightweight computing, and power constraints. Physical layer security (PLS) has the potential to provide security solutions that are suitable for such applications. In this article, an efficient PLS approach is proposed for providing secure communication against external and internal eavesdroppers in a downlink multi-carrier IoT communication system. The system consists of a transmitter with a single active antenna (and a single radio frequency chain) that is trying to communicate with two single-antenna IoT devices in the presence of a passive eavesdropper. In the proposed algorithm, frequency selective channel based pre-coder matrices and dual-transmission approach are jointly employed to provide simple and secure communication without complex computational processing at the IoT devices. Simulation results showed that the proposed algorithm can provide security against internal and external eavesdroppers and is suitable for IoT devices.**

I. Introduction

Fifth-generation (5G) wireless systems are not just simple evolution of conventional fourth-generation (4G) networks, but they are also expected to offer many new services beyond internet to critical communication and internet of things (IoT). The three main services of 5G include ultra-reliable low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine type communication (mMTC) [1]. Overall, 5G will have a significant impact in many areas of life and will bring a lot of interesting applications such as autonomous driving, virtual reality, smart city, smart energy networks, remote surgery, drone delivery, and so on. However, due to the broadcast nature of wireless communication, it is vulnerable to eavesdropping and intervention [2] [3], which may compromise the confidentiality of the signals.

The solutions to tackle security issues in wireless communication include cryptography and physical layer security (PLS) solutions [4]. Cryptography-based solutions are not suitable enough for future communication systems, especially for IoT-based applications. This is due to the fact that the heterogeneous nature of future communication makes the key sharing and management processes very challenging. Moreover, transceivers in some applications are processing restricted and power limited, making encryption-based algorithms unsuitable for them [5].

978-1-7281-4490-0/20/$31.00 © 2020 IEEE

To solve the issues related to encryption-based solutions for future communication systems, PLS techniques have emerged as an effective solution that can complement the cryptography-based approaches [5]. PLS techniques can exploit the characteristics of wireless communication such as randomness, fading, noise, and interference to prevent unauthorized and illegitimate node to intercept or decode the legitimate communication. PLS techniques can exploit random channel between the legitimate parties to extract secret keys, thus, alleviating the need for key sharing. Moreover, various PLS techniques can be implemented by simple signal processing techniques and can support devices with limited processing and delay constraints such as IoT devices [3].

Among many top research areas in PLS, securing the orthogonal frequency division multiplexing (OFDM) waveform has got much attention. This is due to the fact that OFDM is not only one of the most popular and commonly used waveforms in the current wireless communication system but it is also expected to be part of future communication with a wide variety of different numerologies [3]. The techniques proposed in the literature for PLS in OFDM can be grouped into four main classes. The first class is based on secret key generation algorithms in which the random wireless communication channel is exploited to generate secret keys [6]. The second class is related to channel adaptation assisted techniques in which the basic idea is to adapt the transmission parameters of the legitimate transmitter to enhance the performance of the legitimate receiver, for example, adaptive modulation and automatic repeat request based schemes [7], channel shortening [8], OFDM with sub-carrier index selection [9], etc. The

978-1-7281-4490-0/20/$31.00 ©2020 IEEE

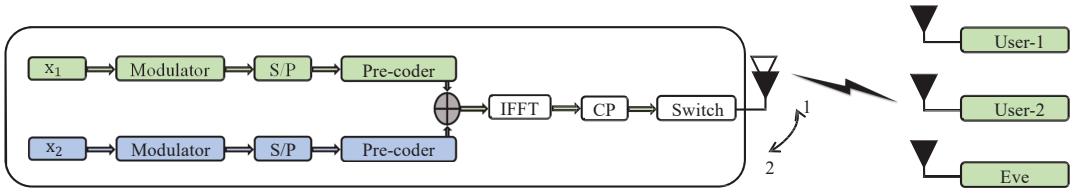

Fig. 1. Basic block diagram of pre-coder based multi-carrier IoT communication system with a single radio frequency chain and a single active antenna.

third class is based on artificial noise-based techniques. In these techniques, the artificial noise is added based on the channel of the legitimate nodes in such a way that it can degrade the performance of eavesdropper without affecting the performance of the legitimate receiver [10]. The fourth class is based on algorithms that are based on concealing features of the OFDM waveform [11].

The aforementioned algorithms are effective security techniques but some of them were introduced without considering the unique requirements of 5G services. Moreover, there will be applications in the 5G and beyond networks that will require reliable and secure communication with processing limited receivers [9]. However, reliability and security conflict with each other [12]. This is because when the communication link quality is made very reliable, security is usually reduced because reliability comes with a lot of redundancy, which can increase the probability of eavesdropper for decoding the received data successfully [13]. Moreover, some of the security algorithms require complex processing at both transmitter and receiver which makes them infeasible for applications with a simple receiver. Based on the aforementioned discussion, in this work, we propose a simple dual-transmission based technique with a single active antenna transmitter for providing secure and reliable IoT communication systems. More specifically, data of IoT devices are superimposed using channel-based pre-coder matrices and sent in two transmissions to achieve reliable and secure communication against internal and external eavesdroppers. The remainder of the manuscript is organized as follows: In section II, the system model assumptions are explained. The proposed algorithm and respective details are presented in section III while the computer simulations and discussion are presented in section IV. Finally, section V presents the conclusion of the work.[1]

II. System Model Assumptions

The considered system model consists of a multi-carrier downlink legitimate transmitter (Tx) with a single active antenna that is trying to communicate with two single-antenna legitimate IoT devices (users) in the presence of a passive single antenna external eavesdropper (Eve) as shown in Fig. 1. More specifically, the transmitter is equipped with two antennas and a single radio-frequency chain, where one of the antenna (antenna 1 or antenna 2) is made active for any transmission with the help of switch to artificially increase the randomness of the wireless channel for security enhancement. Furthermore, the users are assumed to be untrusted (internal eavesdropper), which means that the individual user's data is also needed to be secured from each other. It is also assumed that the transmitter has no knowledge about the channel of Eve. The channel between Tx and any user is assumed to be slowly varying multi-path Rayleigh fading with exponentially decaying power delay profile (PDP) and assumed to be known at the transmitter. Moreover, channel reciprocity property is also adopted, where the channel from the transmitter to the receiver and vice versa can be estimated by channel sounding techniques in time division duplexing (TDD) systems [8]. The legitimate transmitter wants secure communication with the users such that neither the external eavesdropper gets the information of the users' signals nor the users get each other's information.

III. Proposed Algorithm for Reliable and Secure Communication

The basic goal of this work is to fulfill the needs of those future applications that require reliable and secure communication and have limited processing capability at the receiver [9]. In this work, we superpose the signal of two users along with pre-coder matrices and sent the resultant signal in two transmissions while alternating the active antenna in each round. Having two transmission rounds, with each being transmitted from a different active antenna, is necessary to ensure different channels during different transmissions. This, in turn, enables us to design and find a special type of pre-coders that can provide security against internal and external eavesdroppers simultaneously. Moreover, compared to the single-user channel-based security algorithm, two users with two transmissions introduce more difficulties to an eavesdropper. The reason is that in each round of the proposed algorithm the used pre-coders are function of different legitimate users' channels. However, in the case of single-user based algorithms, the pre-coder is a function of a single user's channel only. So, the

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

two rounds job is to make it more difficult for an eavesdropper to decode the legitimate user's signal while making it easy for the legitimate users to decode the intended data. Moreover, the proposed algorithm just requires a single radio frequency chain at the transmitter.

The details of the proposed algorithm are as follows: As explained earlier, we consider a two-user single antenna multi-carrier system as presented in Fig. 1.

At the Tx, the total number of modulated symbols in one OFDM block for each user is N_f. Thus, the frequency response of each OFDM symbol for user-1 and user-2 can be represented as $\mathbf{x_1} = [x_0 \;\; x_1 \;\; ..... \;\; x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$, and $\mathbf{x_2} = [x_0 \;\; x_1 \;\; ..... \;\; x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$, respectively. Note that $\mathbf{y_{km}} \in \mathbb{C}^{[N_f \times 1]}$, $\mathbf{H_{km}} \in \mathbb{C}^{[N_f \times N_f]}$, and $\mathbf{z_{km}} \in \mathbb{C}^{[N_f \times 1]}$, respectively, 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 basic idea is to first multiply each user signal with a specially designed channel-dependent pre-coder matrix. Afterwards, superimpose the pre-coded signals and finally send the resultant signal in two transmissions (rounds) in such a way that when the signals are combined at the legitimate receivers (IoT devices), each user will get its reliable signal by simply demodulating the combined signal without any complex processing. On the other hand, it will be very hard for eavesdroppers to detect the information intended for user-1 and user-2 due to legitimate users' channel-based specially designed pre-coder matrices. Moreover, the specially designed pre-coders will also make sure that the information of the users is also secure from each other.

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

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

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 $\mathbf{M_{2b}}$ are specially designed pre-coder matrices based on the channel of legitimate nodes. These pre-coders will make sure that the user-1 and user-2 will get reliable signals which are also secure from internal and external eavesdropping. We will first explain the details about the received signal at user-1, user-2, and eavesdropper in the following two subsections. Afterward, the details about designing the pre-coding matrices will be explained.

1) Received Signal at User-1: The received signal in the frequency domain at user-1 during round-1 using active antenna-1 can be given as:

$$\mathbf{y_{11}} \;\; = \;\; \mathbf{H_{11}u_1} + \mathbf{z_{11}}, \tag{3}$$

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 using active antenna-2 is given as:

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

where $\mathbf{H_{12}}$ and $\mathbf{z_{12}}$ are the frequency response of the channel and AWGN between user-1 and active antenna-2 of the Tx during round-2. The combined received signal from round-1 and round-2 at user-1 can be written as:

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

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

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

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

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

$$\begin{aligned}\mathbf{\hat{y}_1} = {} & (\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}})\mathbf{x_1} + (\mathbf{H_{11}M_{2a}} \\ & + \mathbf{H_{12}M_{2b}})\mathbf{x_2} + \mathbf{z_{11}} + \mathbf{z_{12}}.\end{aligned} \tag{8}$$

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

2) Received Signal at User-2: Similar to user-1, the combined received signal from round-1 and round-2 for the case of user-2 can be written as:

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

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

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

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

$$\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{21}} + \mathbf{H_{22}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{22}}. \quad (11)$$

$$\hat{\mathbf{y}}_\mathbf{2} = (\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}})\mathbf{x_1} + (\mathbf{H_{21}M_{2a}} + \mathbf{H_{22}M_{2b}})\mathbf{x_2} + \mathbf{z_{21}} + \mathbf{z_{22}}. \quad (12)$$

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

3) Received Signal at Eavesdropper: For the case of eavesdropper, the combined received signal from round-1 and round-2 can be written as:

$$\hat{\mathbf{y}}_\mathbf{3} = \mathbf{y_{31}} + \mathbf{y_{32}}, \quad (13)$$

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

$$\hat{\mathbf{y}}_\mathbf{3} = \mathbf{H_{31}u_1} + \mathbf{z_{31}} + \mathbf{H_{32}u_2} + \mathbf{z_{32}}. \quad (14)$$

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

$$\hat{\mathbf{y}}_\mathbf{3} = \mathbf{H_{31}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{31}} + \mathbf{H_{32}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{32}}, \quad (15)$$

$$\hat{\mathbf{y}}_\mathbf{3} = (\mathbf{H_{31}M_{1a}} + \mathbf{H_{32}M_{1b}})\mathbf{x_1} + (\mathbf{H_{31}M_{2a}} + \mathbf{H_{32}M_{2b}})\mathbf{x_2} + \mathbf{z_{31}} + \mathbf{z_{32}}. \quad (16)$$

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

4) Pre-coder Design for the Proposed Algorithm: We need to design pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ in such a way that the combined 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 $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ is as follows: Firstly, in order to remove the effect of channel at user-1, the first term in the equation (8) should be equal to identity matrix and can be given as:

$$(\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}}) = \mathbf{I}. \quad (17)$$

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

$$(\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}}) = 0. \quad (18)$$

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

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

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

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

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

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

$$(\mathbf{H_{11}M_{2a}} + \mathbf{H_{12}M_{2b}}) = 0. \quad (22)$$

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

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

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

The values of pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ are given in equations (19), (20), (23) and (24), respectively, will be used in round-1 and round-2 to make sure that the user-1 and user-2 will get reliable signals which are secure from internal and external eavesdroppers. Note that, in the proposed method explained earlier, 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. Hence, it can support applications with processing limited receiver (IoT-based applications).

IV. 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 ($L = 9$).

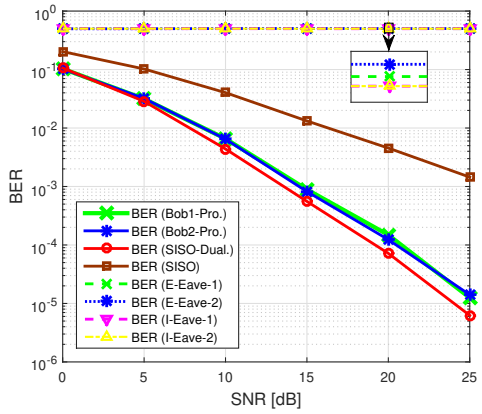

Fig. 2. BER versus SNR performance for the proposed algorithm, SISO with dual-transmission, and SISO-OFDM.

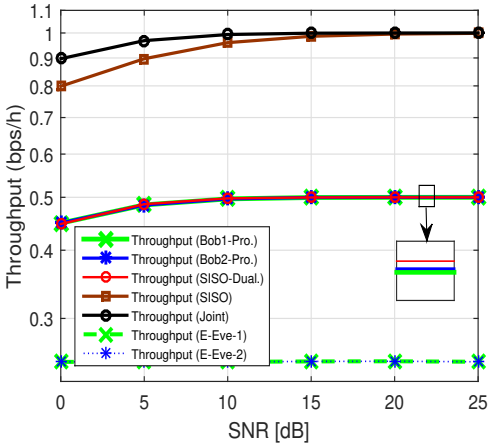

Fig. 3. Throughput versus SNR performance for the proposed algorithm, SISO with dual-transmission, and SISO-OFDM.

Fig. 2 shows the BER versus signal to noise ratio (SNR) plots for the proposed algorithm, single-input single-output (SISO)-OFDM system, and SISO with the dual-transmission (SISO Dual.), where SISO with dual-transmission is used as a benchmark. Note that in SISO with dual-transmission, the OFDM symbol is transmitted two times to have a fair comparison with the proposed algorithm. It should be noted from Fig. 2 that the BER performances of user-1 (Bob1-Pro.) and user-2 (Bob2-Pro.) employing the proposed algorithm are similar to each other. However, there is a significant gap between their BER performances and that of external eavesdropper ones, where labels E-Eve-1 and E-Eve-2 present the BER performances of the external eavesdropper that is trying to eavesdrop the signals intended for user-1 and user-2, respectively. Fig. 2 also shows that there is a significant gain in BER performances of users employing the proposed algorithm and SISO with dual-transmission (SISO Dual.) as compared to SISO-OFDM performance. Moreover, it is also observed that there is a little performance degradation of users employing the proposed algorithm compared to SISO with the dual-transmission (SISO Dual.). However, SISO with the dual-transmission cannot provide secure communication while the proposed algorithm can provide significant gain in terms of security against internal and external eavesdropper.

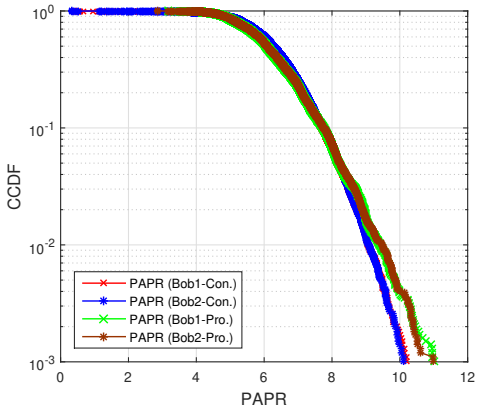

Fig. 4. Comparison of PAPR performances of the conventional OFDM and proposed algorithm.

Fig. 4 presents the throughput versus SNR plots for the proposed algorithm, SISO-OFDM system, SISO with the dual-transmission (SISO Dual.), and joint consideration of users throughput. The reason for the joint consideration of throughput is that the superimposed signals of user-1 and user-2 are sent jointly during each transmission in the proposed algorithm such that the total number of packets sent by the proposed algorithm is similar to the case of SISO. It is observed from Fig. 3 that the individual throughput performances of user-1 (Bob1), user-2 (Bob2), and SISO with the dual-transmission are similar to each other while worst compared to SISO-

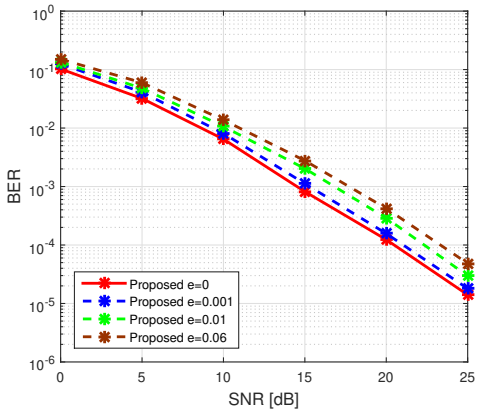

Fig. 5. BER versus SNR performance of the proposed algorithm for imperfect case.

OFDM case and joint case. It is also observed from Fig. 3 that the throughput performance of the joint case outperforms SISO-OFDM at lower values of SNR while it has similar performance to the joint case at high SNR. Moreover, it is observed that the performances of throughput for external eavesdroppers are worse. One important point to be noted here is that although the throughput performances of the external eavesdroppers are not zero, quality of service (QoS) based security can still be ensured. Here, the QoS based security [7] means to provide security based on the requirements of different services (voice, video, etc.) instead of providing perfect security. More specifically, different services have different QoS requirements for reliable communication and if we make sure that eavesdropper is operating below the QoS requirements of a specific service, we can secure that service.

Fig. 4 depicts a comparison of the peak to average power ratio (PAPR) performances of the conventional OFDM and OFDM with the proposed algorithm for user-1 (Bob1) and user-2 (Bob2). It is observed from Fig. 4 that there is a small degradation in the PAPR performances of the users compared to conventional OFDM. Overall, the proposed algorithm can be a good solution for providing secure communication, especially for IoT devices with limited processing receivers.

Analyzing the robustness of the PLS algorithm against the imperfect channel is extremely important. In order to show the effect of the imperfect channel, intentional error ($\Delta\mathbf{h}$) is added to the true channel ($\mathbf{h}$). The imperfect channel is given by $\tilde{\mathbf{h}} = \mathbf{h} + \Delta\mathbf{h}$ [8]. We can model $\Delta\mathbf{h}$ as an independent AWGN with zero mean and variance ($\sigma^2 = e \times 10^{\frac{-SNR_{dB}}{10}}$), where the value of e determines the quality of estimator, with lower values showing a good quality estimator. Fig. 5 shows the BER versus SNR performance under imperfect channel conditions with estimators having different qualities ($e = 0, 0.001, 0.01, 0.06$). It is observed from Fig. 5 that there is a small degradation in the BER performance of the proposed algorithm due to the imperfect estimator. However, it can be improved by increasing the power of training sequence or/and by using a pilot with a longer length. Moreover, there are plenty of algorithms in the literature to enhance the channel estimator's performances [8].

V. Conclusion

An effective technique for reliable and secure communication is presented for IoT devices. Channel-dependent pre-coders with dual-transmission approach are jointly exploited to ensure a reliable as well as secure communication against internal and external eavesdropping. More specifically, users' pre-coded data is superimposed in the first step. Afterward, the mixture is sent in two transmissions in such a way that after combining signals from the first and the second transmissions, the legitimate receivers will get the reliable signal without complex processing while the external eavesdropper will get the degraded version of the signal. Moreover, the proposed algorithm also ensures that the users are also not able to eavesdropper each other's data. Simulation results proved that the proposed algorithm can ensure secure communication and suitable for IoT-based devices because it does not require complex processing at the receivers. For future work, the extension of the proposed algorithm for active eavesdropper case will be considered.

Acknowledgement

The author Jehad M. Hamamreh is supported in part by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 119E392.

References

[1] 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.

[2] H. M. Furqan, M. A. Aygül, M. Nazzal, and H. Arslan, "Primary user emulation and jamming attack detection in cognitive radio via sparse coding," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 141, Jul 2020.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] 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.

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

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

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

[13] 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.