Physical Layer Security using Time-Reversal Pre-Coding based OFDM-DCSK Communication System with Artificial Noise Injection

Dhuha Hussein Hameed, and Fadhil S. Hasan

***Abstract*—In this paper, Time-Reversal (TR) pre-coding with Artificial Noise (AN) injection is proposed to enhance the physical layer security (PLS) performance in orthogonal Frequency Division Multiplexing-Differential Chaos Shift Keying (OFDM-DCSK) system, which is named the TRAN-OFDM-DCSK system. This approach is provided to achieve high data rates, high PL data security, and high reliability performance. The AN signal does not spoil the transmitted data to the genuine receiver, but it reduces the ungenuine detection performance. This system ensures the secrecy of communication to the genuine receiver when the sender knows the Channel State Information (CSI) of the genuine communication link. Still, the information about the instantaneous CSI of a possible eavesdropper does not know the transmitter. The performance of the proposed TRAN-OFDM-DCSK system is investigated and tested under a Flat Rayleigh Fading Channel (FRFC). An approach is provided for calculating the performance of Bit Error Rate (BER), and the expression of BER analytical is derived and compared with the simulation version. Furthermore, the ergodic Secrecy Rate (SR) is derived and analyzed at the genuine and ungenuine receivers over the FRFC. Our result shows the best performance for the genuine receiver compared with ungenuine receiver regarding secrecy performance for BER and SR.**

***Index terms*—Physical Layer Security, Orthogonal Frequency Division Multiplexing, Differential Chaos Shift Keying, Artificial Noise, Time Reversal Pre-coding, Secrecy Analysis.**

I. Introduction

Due to the nature of broadcasting, wireless communications stay insecure. However, with the development of 5G as a heterogeneous network that possibly incorporates diverse access technologies, the security of the physical layer has significantly expanded recently for wireless communications security [1-3]. Therefore, the PLS is developed as a new knowledge with power and influence that can accompany and even substitute encryption-based methods.

Manuscript received May 9, 2023; revised September 15, 2023. Date of publication October 29, 2023. Date of current version October 29, 2023. The associate editor prof. Toni Perković has been coordinating the review of this manuscript and approved it for publication.

Authors are with the Department of Electrical Engineering, Al-Mustansiriyah University, Baghdad, Iraq (e-mails: eeph006@uomustansiriyah.edu.iq, fadel_sahib@uomustansiriyah.edu.iq).

Digital Object Identifier (DOI): 10.24138/jcomss-2023-0062

The PLS's main goal is to exploit the physical properties of the wireless communication channel and its debility, including noise, fading, interference, dispersion, diversity, etc., to enhancement the communication security against eavesdroppers that potentially without depend on the complexity of computational, mean that, if Eve has unlimited computing capabilities, the security is not influenced, in a way by which the intended use having the successful ability to recover data while forbidding eavesdroppers to recover data. Thus, the basic design idea of PLS is to raise the different performance between the connection from Alice to the legitimate receiver and the connection from Alice to Eve via well-designed transmission systems [4].

In 1949, Shannon had the first investigation on the security of information-theoretic by describing the wiretap channel. The next work in 1975 was by Wyner that presented a further general noisy wiretap channel and exposed that without using any secret keys, the secure communication of information-theoretic can be accomplished, by keeping the 3rd party unaware of the secure message, when the eavesdropping channel is a degraded, i.e., noisier, version of the Bob link, from that point forward, to concentrate on the study of information-theoretic secrecy performance viewpoint, sufficiently attention from both academia and industry was attracted [5]. Furthermore, a multitude of research concentrates on wireless communication systems utilizing chaos as carrier sequence because of their beneficial characteristics of wideband [6].

Secrecy capacity and bit error rate are the most studied curricula of PLS metrics. Theoretical information secrecy capacity is defined as the reliable transmission of the bits number per channel from a legitimate sender (Alice) to a genuine receiver (Bob) while ensuring negligible leakage of information to an eavesdropper [7]. Therefore, communication with high security can be achieved once the eavesdropping channel has deteriorated with respect to the desired channel [5]. This can be accomplished by decreasing the SNR at the eavesdropper site and increasing the SNR at the legitimate site if the channel state information (CSI) is identified mean that an appropriate transmitted channel that is based adaptive transmission system and/or via addition to the AN to a signal located in the null space of the desired receiver's channel. These methods can be executed in the space, time, and/or frequency domains [4], [8], [9]. The concept of adding the AN was

primarily recognized in [10-12]. The knowledge is degraded artificially in the channel of Eve by purposely adding AN signal to the transmitted information. This AN signal is designed not to degrade the Bob channel, resulting in an improved PLS [4]. There are many works that are used the transmitter side multiple antennas to achieve these systems, and only a few works aim to implement these systems with Single-Input Single-Output (SISO) strategies [13-17]. In [13], a method is proposed that combines Time-Domain (TD) symbol waveform optimization to get the wanted SINR at the legal receiver. AN is injected using the available energy remaining in the sender when the eavesdropping CSI is unknown. Another method proposed in [18] is Time Reversal (TR), implemented to raise the SINR in SISO systems. This process can be executed with a simple precoder at the sender. TR accomplishes a gain at the legitimate site only, and it naturally provides the possibility of communication security. TR is accomplished by signal up-sample and down-sample in the TD. Other approaches combined the TD-TR pre-coding with AN injection to improve the secrecy of communication [15-17]. Other methods are utilized by the OFDM system, which can be employed in Time or Frequency Domain (FD) to achieve PLS. In [19], [20], FD OFDM diagrams consisting of index options of sub-carriers are presented. Many subcarriers are only used to transmit data reliant on their channel gain. For more improved confidentiality, there is little work that combines TD or FD pre-coding with AN injection. In [21-23], the initial FD precoders are presented utilizing OFDM and injection of AN. In [8], AN is injected into Bob's null space, but only finite decoding skills have been attributed to Eve. In [22], [23], the idea is to use several OFDM sub-carriers to transmit dummy data, i.e., several sub-carriers are utilized to jam the data.

Nevertheless, the encryption of data must be shared between the sender and the genuine receiver, which leads to further processing required by the receiver. Additionally, security is improved when more subcarriers are utilized for the obfuscation of information at the expenditure of data rate. Moreover, it is supposed that Eve did not know the legitimate connection.

On the other hand, in digital communication systems, there is a lot of research concentrating on the use of the chaos-based signal as the carrier due to its distinctive broadband properties [24-26] that make it appropriate for spread spectrum (SS) systems [24]. Chaotic modulations have advantages over all other SS schemes, including jamming resistance and fading channel alleviation. Moreover, the low probability of intercept (LPI) [27] and good correlation characteristics [28], and non-periodic random characteristic, improves the security of transmission and are robust against the self-interference and multipath effect [24], [29]. permit them to be the natural nominees for communications in military situations. Numerous communication systems based-chaos, with receivers that are coherent or non-coherent, were presented [24]. With receivers that are coherent, the same as Chaos Shift Keying (CSK) scheme [24, 30], the data sequence is sent by using a chaotic signal that carries information bits that provide a secure communication link, while at the receiver, to recover the sending bits, the synchronization of the chaotic sequence is needed to reproduce the chaotic sequence. Fortunately, for non-coherent reception same as the DCSK system [11, 31], it can perform well without needing the chaotic synchronization of the chaotic signal at the receiver side and also illustrates robust resistance against fading of multipath. Some security properties of CSK and DCSK that were presented in [30] and [31, 32], and [33] security of CSK and DCSK were studied from the theoretical information viewpoint.

In this paper, the following contribution points are presented:

- A new version of OFDM-DCSK with high security is proposed, named the Time Reversal Artificial Noise OFDM-DCSK (TRAN-OFDM-DCSK) system. The PLS based on the wiretap communication system is applied for the OFDM-DCSK system using TD-TR pre-coding with an injection of AN to improve the secrecy of the communication system by maximizing the secrecy rate (SR), under the supposition that the eavesdropper is passive whose CSI is assumed to be unknown. It can be utilized in SISO schemes, and therefore it is suitable for resource-limited nodes, the same as those in the Internet of Things (IoT), for example.

- The BER analysis of the proposed system at the legitimate user is derived and compared with the simulation results. The proposed TRAN-OFDM-DCSK system is compared with the TRAN-DCSK system.

- The ergodic SNR's analytical expressions at Bob and Eve positions are derived to estimate the communication secrecy rate (SR), where the optimal amount of AN energy to maximize the C_S is derived. Also, the secrecy rate of the TRAN-OFDM-DCSK system is compared with the TRAN-DCSK system.

The rest of this paper is ordered as follows: Section II presents the proposed TR pre-coding SISO OFDM-DCSK communication with the AN scheme and the technique to design and inject the AN. Section III offers the BER Theoretical Performance Analysis of the legitimate users, and Section IV gives Secrecy Capacity (SC) performance. System simulation results and discussion are provided in section V. Finally, the paper's conclusion is given in section VI.

Notation: The I_N is the identity matrix of the $N \times N$ dimension. The complex conjugate, the Hermitian transpose, the inverse, the real part and the imaginary part are denoted by $(.)^*$,$(.)^H$, $(.)^{-1}$, $\Re(.)$ and $\mathcal{J}(.)$, respectively.

II. The Proposed TRAN-OFDM-DCSK Communication System

A general PLS model constructed with a wiretap system model for the eavesdropping issue, whereby Alice attempts to secretly communicate with Bob without permitting Eve to obtain any useful data from the ongoing communication between the legitimate parties (Alice and Bob). The proposed TR pre-coding SISO OFDM-DCSK communication with an Artificial Noise system is demonstrated in Fig. 1. The

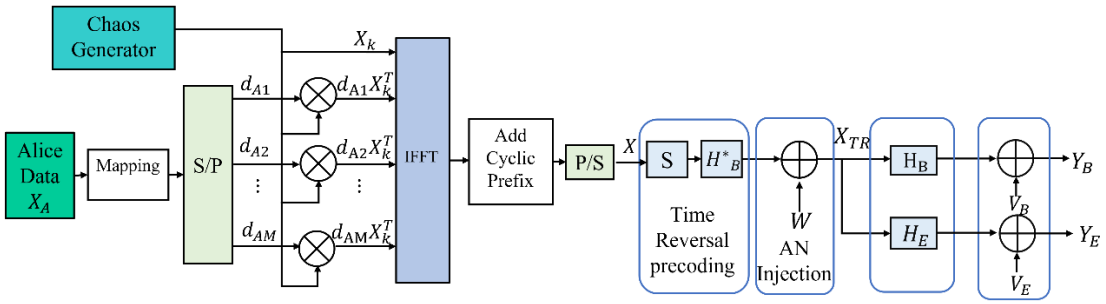

Fig. 1. The Transmitter of the TRAN-OFDM-DCSK communication system.

communication system is intended to transmit the information from Alice's position and focused on the Bob situation, i.e., at the genuine receiver. An eavesdropper, Eve, attempts to interrupt the data. Under the assumption that Alice does not have any information about CSI Eve.

The OFDM-DCSK symbol transmission system transports the data with $(M+1)$ subcarriers, and we deliberate that only one block L is transmitted over the TR pre-coding SISO OFDM-DCSK scheme. In the OFDM-DCSK system, the number of modulated bits is M bits in each frame; therefore, the produced signal for each frame consists of $(M+1)$ signals. The first signal is the Chaotic Reference (CR) sequence, X_k, which is sent in the first subcarrier, and the following M signals that carry M bits are sent to the remaining M subcarriers. Each signal has length β, which is the spreading factor. Therefore, the signal of block L of OFDM-DCSK consists of M bits $d_{(A,m)}$ (for $m = 0,\ldots, M\text{-}1$), can be represented by the baseband matrix of dimension $((M+1)\times\beta)$ given as:

$$T_{M,k} = \begin{bmatrix} X_k \\ d_{A1}X_k^T \\ d_{A2}X_k^T \\ \vdots \\ d_{AM}\,X_k^T \end{bmatrix}, \quad where \;\; k = 1, \ldots, \beta \tag{1}$$

For generating the chaotic samples X_k, the Chebyshev polynomial function (CPF) is used, which is described by the equation $x_{k+1} = 1 - 2x_k^2$ for $(k = 1, \ldots \beta)$ [34] with zero mean and variance unity.

Then each column in the matrix T is modulated by an OFDM technology in which the signal is sent over different carrier frequencies by using IFFT. Therefore, there are β IFFT functions to generate one block. After adding the guard interval (gur), each column of length $N = (N_{FFT} + gur)$ is applied to the up-sample process via the factor $U = Q/N$ by the matrix S of size $Q \times N \; with \; N \leq Q$. The matrix S consists of U times $N \times N$ diagonal matrices, with diagonal elements taken from the set $\{\pm 1\}$ and presence independently and identically distributed. In order to have $S^H S = I_N$, the matrix S is normalized by the $\sqrt{U}$ factor. Therefore, the length of each column after the up-sample process is $1 \times Q$.

$$S = \frac{1}{\sqrt{U}} \begin{pmatrix} \pm 1 & 0 \ldots & 0 \\ 0 & \pm 1 \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 \ldots & \pm 1 \\ \vdots & \vdots & \\ \pm 1 & 0 \ldots & 0 \\ 0 & \pm 1 \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 \ldots & \pm 1 \end{pmatrix} \tag{2}$$

As mentioned in [14], the reason behind the process of up-sampling a signal in TD is tantamount to the repeating and shifting of its FD spectrum. Then the pre-coded process will be done on the up-sampled sequence before the addition of the AN signal and sent it. The pre-coded process needs to be the complex conjugate of Bob's channel information.

The channel information between Alice and Bob is denoted by (H_B), and the channel information between Alice and Eve is denoted by (H_E). Both H_B and H_E are $Q \times Q$ diagonal matrices; their elements are $H_{B,q}$ and $H_{E,q}$ for $(q = 0, \ldots, Q - 1)$ and follow a zero-expectation unity variance normal distribution., i.e., they are Rayleigh distribution modulus. For every channel realization, the total energies are normalized to unity.

Subsequently, the pre-coding matrix is a diagonal matrix with elements of Bob's channel complex conjugate $H^*_{B,q}$. Then, the AN signal will be generated to more secure the communication link between the genuine transmitter (Alice) and the desired recipient (Bob); the AN signal is denoted by (W) is added to the useful transmitted signal X after the pre-coding process at the transmitter side. Since the genuine transmitter doesn't know any information about CSI Eve, therefore, the AN signal is seen as interference everywhere but would not have any influence on Bob's site. Moreover, this signal should be predicted at the intended (desired) recipient situation only to certify the security of communication. Under this assumption, the transmitted sequence is expressed by:

$$X_{TR} = \sqrt{1-\alpha}\; H^*_B\, S\, X + \sqrt{\alpha}\; W \tag{3}$$

where $\alpha \in [0,1]$ describes the ratio of the total power denoted to the AN signal while ensuring that the total transmitted power remains constant, and equals 1 per transmitted symbol for any value of α, described that $E[|H^*_B\, S\, X|^2] = E[|W|^2]$.

At the receiver, as shown in Fig. 2, applying S^H on the parallel received sequence for down-sampling operation, then the sequence pass to OFDM demodulation by FFT after eliminating the guard interval. We contemplate that the decoding capabilities for both Bob and Eve are identical; this means that they can recognize the up-sampled sequence and then apply the conventional OFDM-DCSK received system.

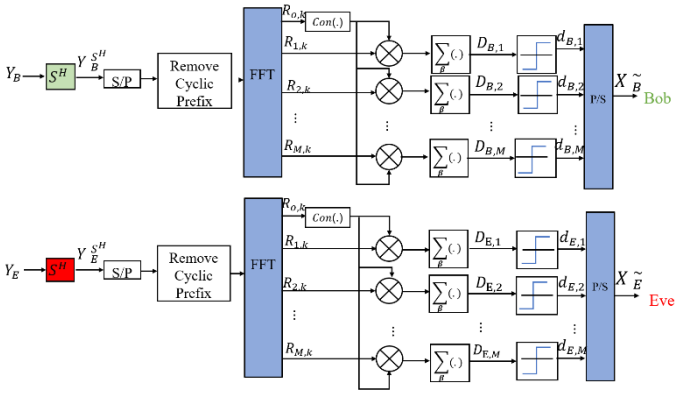

Fig. 2. The Receiver of TRAN-OFDM-DCSK for Bob and Eve.

A. AN Design

In order to prevent any influence at the desired recipient site, the following condition is necessary to be satisfied:

$$AW = 0 \tag{4}$$

where

$$A = S^H \; H_B \qquad \in c^{N \times Q} \tag{5}$$

Eq. (4) certifies that W lies in the right null space of A; this can be done by employing the process of singular value decomposition (SVD) on A, resulting in [35]:

$$A = P\left(\sum 0_{Q-N \times Q}\right)\begin{pmatrix} V_1^H \\ V_2^H \end{pmatrix} \tag{6}$$

where the left singular vectors are represented by $P \in \mathbb{C}^{N \times N}$, $\Sigma \in \mathbb{C}^{N \times N}$ is a diagonal matrix encompassing singular values, $V_1 \in \mathbb{C}^{Q \times N}$contains right singular vectors related to non-zero singular values, and $V_2 \in \mathbb{C}^{Q \times Q-N}$ encompasses the right singular vectors that span the right null space of A. Consequently, the AN signal can be articulated as follows:

$$W = V_2 \widetilde{W} \tag{7}$$

For any arbitrary vector of $\widetilde{W} \in \mathbb{C}^{N \times N}$, that certifies the Eq. (4) is satisfied. Since $Q = NU$, and $U \geq 2$, there are possibilities of the infinite set to produce $\widetilde{W}$, and consequently, the AN signal is then produced thanks to Eq. (7). Under the assumption that $\widetilde{W}$ is white complex Gaussian noise with zero expectation value.

B. Received Data Sequence at the Desired Recipient (Bob)

The received data sequence at the desired recipient (Bob), after de-spreading and OFDM demodulating by FFT with eliminating the guard interval, is $Y_B^{S^H}$ with a length of N given by:

$$Y_B^{S^H} = \left(\sqrt{1-\alpha}\, S^H \;\; |H_B|^2 \;\; S\,X + S^H V_B\right) \tag{8}$$

where V_B is the complex AWGN sequence with an average value is zero and standard deviation $\sqrt{N_O}$ i.e., $E[|V_B|^2] = \sigma_{V_B}^2$. Under the assumption that the transmitted signal X_n and noise $V_{B,n}$ are independent. In Eq. (8), since the product $H_B \times {H_B}^*$ is a real diagonal matrix, therefore, at the position of the genuine receiver, every sent frame is influenced by a real gain $\sqrt{1-\alpha}\;\;|H_B|^2$. It is also noted that no AN signal contribution exists in Eq. (8) by satisfying the condition of Eq. (4). Therefore, for high SNR, perfect data detection can be achieved.

C. Received Data Sequence at the Ungenuine Position (Eve)

After down-sampling and OFDM demodulation by FFT with eliminating the guard interval, the received data at the unintended situation is expressed as:

$$Y_E^{S^H} = \sqrt{1-\alpha}\; S^H H_E\, {H^*}_B \;\; S\,X + \sqrt{\alpha}\; S^H H_E W + S^H V_E \tag{9}$$

where V_E is a complex (AWGN) noise with variance is $E[|V_E|^2] = \sigma_{V_E}^2$. From Eq. (9), the value of $H_E\, {H^*}_B$ is a matrix with a complex diagonal element; therefore, every transmitted frame is affected by a random complex coefficient, which leads to the absence of the gain of TR at the position of unintended. Also, it is clear from Eq. (9) that AN signal contribution exists. The addition of the AN spoiled the detection of data in any unintended locations and to secure the connection. As a result, the worse performance of decoding is determined at the unintended situation as compared to the intended.

Eq. (9) shows that the security of transmitted data over the TR SISO OFDM-DCSK communication can be achieved via the addition of AN. The security degree relies on the energy amount of AN, α, that is injected into the link of communication, with respect to the energy amount of data via $(1-\alpha)$. It is notable that since W is produced from an infinite set of possibilities, even if Eve recognizes its equivalent channel $H_E\, {H^*}_B$ and the up-sampling sequence, he cannot guesstimate the AN signal to attempt to recover the data.

III. Theoretical Performance Analysis at the Legitimate Users

Under the assumption that β is large sufficient, and thus the Gaussian approximation (GA) process [36] is used to determine and derive the theoretical BER expressions over FRFC with additional noise in the channel. The coherent time of the channel is greater than the duration of the symbol, so the channel is slowly fading, i.e., the channel remains time-invariant for the

entire period of the symbol. As a result, the channel frequency response is no longer affected by the OFDM subcarrier index.

The Bob's observation signal ${D_{B,m}}^{l}$ for the m^{th} subcarrier of the l^{th} block is given by:

$${D_{B,m}}^{l} = \Re\{R_{m,k}.\,conj(R_{0,k})\} \tag{10}$$

where $R_{0,k}$ signifies to the CR chip, $R_{m,k}$ is the chip of modulated data.

$${D_{B,m}}^{l} = R\left\{[(\sqrt{1-\alpha}\ S^H\ |H_B|^2 S\ X\ + S^H\ V_{B,m}).(\sqrt{1-\alpha}\ S^H\ |H_B|^2 S\ X\ +\ S^H\ V_B)^*]\right\} \tag{11}$$

$${D_{B,m}}^{l} = R\left\{\sum_{k=0}^{\beta-1}[\left(\frac{1}{U}\sqrt{1-\alpha}\ \ |H_B|^2\ x_k\ + \frac{1}{\sqrt{U}}V_{B,m,k}\right).\left(\frac{1}{U}\sqrt{1-\alpha}\ \ |H_B|^2\ x_k\ + \frac{1}{\sqrt{U}}\ V_{B,0,k}\right)^*]\right\} \tag{12}$$

where $V_{B,m,k}$ and $V_{B,0,k}$ are independent AWGN of information-bearing bit and CR bit, respectively.

Let,

$$P_1 = \Re\left\{\sum_{k=0}^{\beta-1}\frac{1}{U^2}(1-\alpha)\ \ d_{A,m}^{l}\ \ |H_B|^4\ \ {x_k}^2\right\} \tag{13}$$

$$P_2 = \Re\left\{\sum_{k=0}^{\beta-1}\ (\frac{1}{U\sqrt{U}}\ \sqrt{1-\alpha}\ |H_B|^2\ \ d_{A,m}^{l}x_k\left(V_{B,0,k}\right)^* + \frac{1}{U\sqrt{U}}\sqrt{1-\alpha}\ |H_B|^2 x_k V_{B,m,k})\right\} \tag{14}$$

$$P_3 = \Re\left\{\sum_{k=0}^{\beta-1}\ \frac{1}{U}V_{B,m,k}\ \left(V_{B,0,k}\right)^*\right\} \tag{15}$$

The P_1 signal refers to the desired signal, while P_2 is the inter-signal-interference and P_3 is the noise-to-noise correlation. Since P_1, P_2, and P_3 are statistically independent, the expectation and variance of ${D_{B,m}}^{l}$ can be simply determined by:

$$\mathbb{E}\{{D_{B,m}}^{l}|(d_{A,m}^{l} = \mp 1)\} = \sum_{w=1}^{3}\mathbb{E}\{P_w|(d_{A,m}^{l} = \mp 1)\} \tag{16}$$

$$var\{{D_{B,m}}^{l}|(d_{A,m}^{l} = \mp 1)\} = \sum_{w=1}^{3} var\{P_w|(d_{A,m}^{l} = \mp 1)\} \tag{17}$$

where $\mathbb{E}\{\cdot\}$ signifies to the expectation operator and $var\{\cdot\}$ signifies to the variances. The derivation of the statistical characteristics of P_1, P_2 and P_3 can be determined as follows:

$$\begin{aligned}\mathbb{E}\{P_1|(d_{A,m}^{l} = +1)\} &= -\mathbb{E}\{P_1|(d_{A,m}^{l} = -1)\}\\ &= \sum_{k=0}^{\beta-1}\frac{1}{U^2}(1-\alpha)\mathbb{E}\{|H_B|^4\}\ \mathbb{E}\{{x_k}^2\}\\ &= \frac{1}{U^2}\beta(1-\alpha)\mathbb{E}\{|H_B|^4\}\mathbb{E}\{{x_k}^2\}\end{aligned} \tag{18}$$

$$\mathbb{E}\{P_2|(d_{A,m}^{l} = \pm 1)\} = \mathbb{E}\{P_3|(d_{A,m}^{l} = \pm 1)\} = 0 \tag{19}$$

$$\begin{aligned}&var\{P_1|(d_{A,m}^{l} = \pm 1)\}\\ &= \frac{1}{U^4}\ \beta(1-\ \alpha)^2 var\{|H_B|^4\}var\{{x_k}^2\}\end{aligned} \tag{20}$$

$$\begin{aligned}&var\{P_2|(d_{A,m}^{l} = \pm 1)\}\\ &= \frac{1}{U^3}\ 2\beta\ (1-\alpha)^2\ var\{|H_B|^2 x_k\ \Re(V_B)\}\\ &= \frac{1}{U^3}2\beta(1-\alpha)^2\mathbb{E}\{|H_B|^4\}\ \mathbb{E}\{{x_k}^2\}\ \mathbb{E}\left\{\left(\Re(V_B)\right)^2\right\}\\ &= \frac{1}{U^3}\beta(1-\alpha)^2\ \mathbb{E}\{|H_B|^4\}\ \mathbb{E}\{{x_k}^2\}\ N_O\end{aligned} \tag{21}$$

$$\begin{aligned}&var\{P_3|(d_{A,m}^{l} = \pm 1)\}\\ &= \frac{1}{U^2}\beta var\{\Re(V_{B,m,k}[V_{B,0,k}]^*)\} =\\ &\frac{1}{U^2}\beta\left(var\{\Re(V_{B,m,k}).\Re(V_{B,0,k})\}var\{\Im(V_{B,m,k}).\Im(V_{B,0,k})\}\right)\\ &= \frac{1}{U^2}\beta\left(\frac{N_O}{2}.\frac{N_O}{2}+\frac{N_O}{2}.\frac{N_O}{2}\right) = \frac{1}{U^2}\beta\left(\frac{{N_O}^2}{4}+\frac{{N_O}^2}{4}\right)\\ &= \frac{1}{U^2}\beta\left(2.\frac{{N_O}^2}{4}\right) = \frac{1}{U^2}\ \frac{1}{2}\ \beta\ {N_O}^2\end{aligned} \tag{22}$$

Then the BER of the proposed TR pre-coding SISO OFDM-DCSK communication with the Artificial Noise system can be derived as:

$$\begin{aligned}P_{r\ TRAN-OFDM-DCSK} &= \frac{1}{2}erfc\left\{\frac{\mathbb{E}\{{D_{B,m}}^{l}|(d_{A,m}^{l}=\mp 1)\}}{\sqrt{2\ var\{{D_{B,m}}^{l}|(d_{A,m}^{l}=\mp 1)\}}}\right\}\\ &= \frac{1}{2}erfc\left\{\left(\frac{2.var\{{D_{B,m}}^{l}|(d_{A,m}^{l}=\mp 1)\}}{\mathbb{E}\{{D_{B,m}}^{l}|(d_{A,m}^{l}=\mp 1)\}^2}\right)^{-\frac{1}{2}}\right\}\end{aligned} \tag{23}$$

where $\mathbb{E}\{{D_{B,m}}^{l}|(d_{A,m}^{l} = \mp 1)\}$ and $var\{{D_{B,m}}^{l}|(d_{A,m}^{l} = \mp 1)\}$ can be determined using Eq. (16) and Eq. (17), respectively. From Eq. (23), we can perceive that the BER of the proposed TR pre-coding SISO OFDM-DCSK communication with AN is reliant on the higher-order statistics of $|H_B|$ and x_k. The sequence of the chaos is produced by a CPF that has the statistical characteristics of $\mathbb{E}\{{x_k}^2\}$= 1/2, $var\{{x_k}^2\}$= 1/8 $\mathbb{E}\{{x_k}^4\}$= 3/8[37]. Also, we suppose that the power spectral density (PSD) of the channel is unity, which means that $\mathbb{E}\{|H_B|^2\} = 1$ and $\mathbb{E}\{|H_B|^4\} = 2$.

The average transmitted bit energy E_b is given by:

$$E_b = \frac{U(M+1)\beta\mathbb{E}\{{x_k}^2\}\ \mathbb{E}\{|H_B|^2\}}{MU} = \frac{(M+1)\beta\ \mathbb{E}\{{x_k}^2\}}{M} \tag{24}$$

Therefore, Eq. (23) can be rearranged in terms E_b as:

$$BER_{TRAN-OFDM-DCSK} = \frac{1}{2}erfc\left\{\left(\frac{var\{|H_B|^4\}}{\beta\ E^2\{|H_B|^4\}} + \frac{2(M+1)UN_O}{(1-\alpha)\ M\ E\{|H_B|^4\}E_b} + \frac{(M+1)^2\beta U^2 {N_O}^2}{(1-\alpha)^2 M^2 E^2\{|H_B|^4\}{E_b}^2}\right)^{-\frac{1}{2}}\right\} \tag{25}$$

Define the average signal power to noise power ratio at the receiver side, γ_D as:

$$\gamma_D = \frac{(1-\alpha)\ \mathbb{E}\{|H_B|^4\}E_b}{N_O} = \frac{\beta(1-\alpha)\ \mathbb{E}\{|H_B|^4\}\ \mathbb{E}\{{x_k}^2\}}{N_O} \tag{26}$$

Thus, the BER expression can be simplified as:

$$BER_{TRAN-OFDM-DCSK} = \frac{1}{2} erfc \left\{ \left(\frac{var\{|H_B|^4\}}{\beta\, \mathbb{E}^2\{|H_B|^4\}} + \frac{2(M+1)U}{M\gamma_D} + \frac{(M+1)^2 U^2\, \beta}{M\, {\gamma_D}^2} \right)^{-\frac{1}{2}} \right\} \quad (27)$$

For a large value of β, the first term inside the parentheses in the above expression may be ignored. Thus, the conditional BER can be simplified as:

$$BER_{TRAN-OFDM-DCSK} = \frac{1}{2} erfc \left\{ \left(\frac{2(M+1)U}{M\gamma_D} + \frac{(M+1)^2 U^2\, \beta}{M\, {\gamma_D}^2} \right)^{-\frac{1}{2}} \right\} \quad (28)$$

It should be noted that for the proposed TR pre-coding DCSK communication with AN scheme (TRAN-DCSK), the number of transmitted bits for each frame is one, therefore $M = 1$. Thus, the BER conditional for TRAN-DCSK can be simplified as follows:

$$BER_{TRAN-DCSK} = \frac{1}{2} erfc \left\{ \left(\frac{4U}{\gamma_D} + \frac{4U^2\, \beta}{{\gamma_D}^2} \right)^{-\frac{1}{2}} \right\} \quad (29)$$

Then the average BER over the FRFC can be determined by obtaining the BER expectation, i.e. [38]

$$\overline{BER}_{flat} = \int_0^\infty BER\ f(\gamma_D)\ d\gamma_D \quad (30)$$

where $f(\gamma_D)$ is dedicated to the probability distribution function (PDF) of γ_D.

IV. Secrecy Capacity Performance

The Secrecy capacity (C_S) is defined as the maximum rate of transmission that a legitimate receiver channel can support while certifying that the data cannot be recovered by an eavesdropper [39]. For the wiretap system model, the instantaneous C_S is stated as the difference between the desired channel capacity C_D (from Alice to Bob) and the eavesdropper channel capacity C_E (from Alice to Eavesdropper).

$$C_S = [C_D - C_E]^+ \quad (31)$$

The ergodic concept of C_S can be given as:

$$C_S = \mathbb{E}[C_D - C_E]^+ = \mathbb{E}[log_2(1 + M\gamma_D) - log_2(1 + M\gamma_E)]^+ \quad (32)$$

where $[x]^+ = \max(0, x)$, γ_D and γ_E are the SNR at the position of Bob and Eve's, respectively. It was exposed in [40], Lemma 1, that an achievable ergodic secrecy rate (SR), i.e., a positive rate less than or equal to the C_S, is expressed by:

$$SR = \{\mathbb{E}[log_2(1 + M\gamma_D) - log_2(1 + M\gamma_E)]\}^+ \quad (33)$$

$$\approx \{[log_2(1 + M\mathbb{E}[\gamma_D]) - log_2(1 + M\mathbb{E}[\gamma_E])]\}^+ \quad (34)$$

In the following sections, the ergodic SNR's analytical expressions at Bob and Eve positions are derived to estimate the communication SR.

Under the following assumption, the analytical expression of ergodic SNR's is derived:

- The data and noise are independent of each other.
- $h_{B,i} \perp\!\!\!\perp h_{B,j}, \forall i \neq j$, i.e., no correlation between subcarriers of Bob's channel subcarriers
- $h_{E,i} \perp\!\!\!\perp h_{E,j}, \forall i \neq j$, i.e., no correlation between the subcarriers Eve's channel.
- $h_{B,i} \perp\!\!\!\perp h_{E,j}, \forall i, j$, i.e., no spatial correlation between Bob and Eve; they are suitably spaced.

The transmitted energy per bit is normalized to equal 1.

A. At the Intended (Bob) Position

At the Bob side, a simple down-sample process is accomplished. Each received data frame is influenced by a real gain due to the pre-coding at the transmitter side, as expressed in (8). The express of the ergodic SNR for the transmitted frame is given by:

$$\mathbb{E}[\gamma_D] = \mathbb{E}\left[\frac{|D_1 x_n|^2}{|D_2|^2}\right] = \frac{\mathbb{E}[|D_1|^2]\,\mathbb{E}[|x_n|^2]}{\mathbb{E}[|D_2|^2]} \quad (35)$$

$$\mathbb{E}[|D_1|^2] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\, S^H\ |H_B|^2\ S\right|^2\right] = \mathbb{E}\left[\left|\frac{\sqrt{1-\alpha}}{U}\sum_{i=0}^{U-1}|h_{D,iN}|^2\right|^2\right] = \frac{(1-\alpha)}{U^2}\mathbb{E}\left[\left(\sum_{i=0}^{U-1}|h_{D,iN}|^2\right)\left(\sum_{i=0}^{U-1}|h_{D,iN}|^2\right)^H\right] = \frac{(1-\alpha)}{U^2}\left\{E\left[\sum_{i=0}^{U-1}|h_{D,iN}|^4\right] + E\left[\sum_{i=0}^{U-1}|h_{D,iN}|^2\right] E\left[\sum_{\substack{j=0 \\ j\neq i}}^{U-1}|h_{D,jN}{}^*|^2\right]\right\} = \frac{(1-\alpha)}{U^2}\big(2U + U(U-1)\big) = \frac{(1-\alpha)(U+1)}{U} \quad (36)$$

$$\mathbb{E}[|x_n|^2] = E_b \quad (37)$$

$$\mathbb{E}[|D_2|^2] = \mathbb{E}[|S^H V_B|^2] = \mathbb{E}[|(S^H V_B)(S^H V_B)^H|] = \mathbb{E}[S^H V_B V_B{}^* S] = \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}|V_{B,iN}|^2\right] = \sigma_{V_B}^2 \quad (38)$$

$$\therefore \mathbb{E}[\gamma_D] = \frac{(1-\alpha)(U+1)}{U}\frac{2U\beta\mathbb{E}(x_k{}^2)}{\sigma_{V_B}^2} = \frac{(1-\alpha)(U+1)}{U}\gamma_D \quad (39)$$

B. At the Unintended (Eve) Position

After the down-sample process, the received signal at the unintended situation is expressed by Eq. (9), where the data component is $E_1 = \sqrt{1-\alpha}\, S^H H_E H^*{}_B\, S\, X$, the noise component is $E_2 = S^H V_E$, and the AN component is $E_3 = \sqrt{\alpha}\, S^H H_E$. The averaged SNR of the transmitted data with an approximation of a lower-bound, using Jensen's inequality, can be derived as:

$$\mathbb{E}[\gamma_E] = \mathbb{E}\left[\frac{|E_1 x_n|^2}{|E_2|^2 + |E_3|^2}\right] = \frac{\mathbb{E}[|E_1|^2]\mathbb{E}[|x_n|^2]}{\mathbb{E}[|E_2|^2] + \mathbb{E}[|E_3|^2]} \quad (40)$$

$$\mathbb{E}[|E_1|^2] = \mathbb{E}\left[\left|\sqrt{1-\alpha}\, S^H H_E H^*{}_B\, S\right|^2\right]$$

$$= \frac{(1-\alpha)}{U^2}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{E,iN}\right|^2\left|h_{D,jN}{}^*\right|^2\right]$$
$$= \frac{(1-\alpha)}{U} \quad (41)$$

$$\mathbb{E}[|x_n|^2] = E_b \quad (42)$$

$$\mathbb{E}[|E_2|^2] = \mathbb{E}[|S^H V_E|^2] = \mathbb{E}[|(S^H V_E)(S^H V_E)^H|]$$
$$= \mathbb{E}[S^H V_E V_E{}^* S]$$
$$= \frac{1}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|V_{E,iN}\right|^2\right] = \sigma_{V_E}^2 \quad (43)$$

$$\mathbb{E}[|E_3|^2] = \mathbb{E}\left[\left|\sqrt{\alpha}\, S^H H_E W\right|^2\right]$$
$$= \alpha\,\mathbb{E}[S^H H_E H_E{}^* W W^* S]$$
$$= \frac{\alpha}{U}\mathbb{E}\left[\sum_{i=0}^{U-1}\left|h_{E,iN} W_{iN}\right|^2\right] = \frac{\alpha}{U} \quad (44)$$

$$\therefore \mathbb{E}[\gamma_E] = \frac{(1-\alpha)E_b}{U\left(\sigma_{V_E}^2+\frac{\alpha}{U}\right)} = \frac{(1-\alpha)E_b}{\left(U\,\sigma_{V_E}^2+\alpha\right)} \quad (45)$$

Then Secrecy rate is

$$SR \approx \left[log_2\left(1+\frac{M(1-\alpha)(U+1)}{U}\gamma_D\right) - log_2\left(1+\frac{M(1-\alpha)E_b}{\left(U\,\sigma_{V_E}^2+\alpha\right)}\right)\right]^+ \quad (46)$$

It should be noted that for TRAN-DCSK, the number of transmitted bits for each frame is one; therefore $M = 1$ in secrecy rate for TRAN-DCSK modulated scheme.

C. The Optimal Amount of AN Energy to Maximize the C_S

As introduced in Eq. (49), the analytical expression of the SR is a function of α. Therefore, in order to maximize the ergodic SR, determined the amount of injected AN energy in the communication that maximizes the SR, with respect to data.

$$SR = \left[log_2\left(\frac{U+M(1-\alpha)(U+1)\gamma_D}{U}\right) - log_2\left(\frac{\left(U\,\sigma_{V_E}^2+\alpha\right)+M(1-\alpha)E_b}{\left(U\,\sigma_{V_E}^2+\alpha\right)}\right)\right]$$
$$= \left[log_2\left(\frac{U+M(1-\alpha)(U+1)\gamma_D}{U}\cdot\frac{\left(U\,\sigma_{V_E}^2+\alpha\right)}{\left(U\,\sigma_{V_E}^2+\alpha\right)+M(1-\alpha)E_b}\right)\right] \quad (47)$$

Let

$A = M\gamma_D(U+1)$, $B = U + M\gamma_D(1+U-U\,\sigma_{V_E}^2 - U^2\,\sigma_{V_E}^2)$, $C = U^2\,\sigma_{V_E}^2 + M\gamma_D\left(U^2\,\sigma_{V_E}^2 + U\,\sigma_{V_E}^2\right)$, $D = U(1-M\gamma_D)$, $E = U^2\,\sigma_{V_E}^2 + UME_b$

$$\therefore SR = \left[log_2\left(\frac{-\alpha^2 A+\alpha B+C}{\alpha D+E}\right)\right] \quad (48)$$

To maximize the SR in term of the parameter α, we determined the zeroes of:

$$\frac{\partial SR}{\partial \alpha} = \frac{-\alpha^2 AD - 2\alpha AE + (BE-CD)}{(\alpha D+E)^2}\cdot\frac{1}{\frac{-\alpha^2 A+\alpha B+C}{\alpha D+E}}\cdot\frac{1}{ln2} \quad (49)$$

Then the result, after some manipulations of algebraic:

$$\frac{\partial SR}{\partial \alpha} = 0 \Leftrightarrow \alpha_{opt} = \frac{-AC \pm \sqrt{A^2C^2+ABCD-ABD^2}}{AD} \quad (50)$$

Then select the positive roots as the results since $\alpha \in [0,1]$.

V. Simulation Results and Discussion

In this section, SISO TRAN-OFDM-DCSK system performance is obtained. MATLAB simulation results with theoretical performance are determined with the spreading factor $\beta = 150$. The parameters of simulations are set as follows, the data rate R is M. The value of M is related to the number of FFT size ($NFFT = 16$), $M = N_{FFT} - 1 = 15$ and the guard interval $Ng = 0.25NFFT = 4$. A stream of bits is pre-coding TRAN-OFDM-DCSK modulated, and the AN signal is generated under the assumption that the channels of Bob and Eve are uncorrelated. Also, the subcarriers are not correlated, and every subcarrier is Rayleigh distributed. For every channel realization, the total energy is normalized to unity. Bob's CSI is supposed to be perfectly well-known in Alice.

A. BER Performance Evaluation

Figures 3 and 4 show the BER performance of the proposed system. The energy per bit, E_b, is determined after spreading and up-sampling, and N_o is the noise PSD. Various levels of AN energy are studied with up-sampling by $U = 2$. Eve is influenced by a random complex coefficient due to pre-coding by Bob is CSI at Alice; therefore, the BER is so high at Eve's position**,** and it can be observed that as the AN radiated energy amount is increased, Eve's BER increases. At the intended (Bob) position, each sample is influenced by a real gain due to pre-coding by Bob is CSI at Alice, but as the AN radiated energy amount is increased, the BER also increases. The higher energy percentage dedicated to AN cause the lower the useful received power signal at Bob. Also, it can be detected that the BER performance of the proposed TRAN-OFDM-DCSK scheme is better than the TRAN-DCSK almost by 3 dB at $BER = 10^{-3}$.

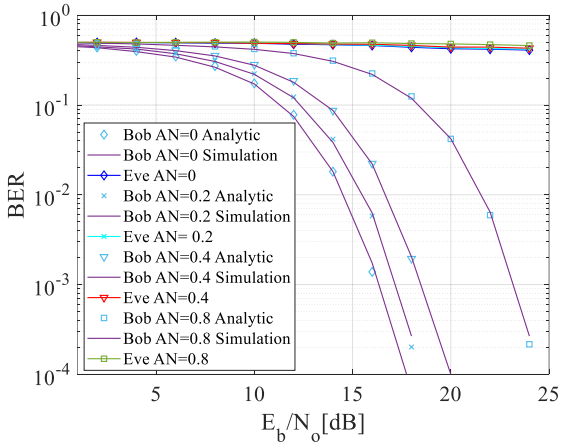

Fig. 3. BER performance proposed TRAN-OFDM-DCSK for Bob and Eve without AN injected $AN = 0$ and with different levels of injected AN power.

B. Ergodic Secrecy Rate Performance Evaluation

Fig. 5 depicts the Ergodic Secrecy rate of TRAN-OFDM-DCSK performance comparison with TRAN-DCSK versus γ_D with regard to the selected value of γ_E over RFC. It's clear that the SR for TRAN-OFDM-DCSK proposed scheme is higher than the SR of the TRAN-DCSK scheme. It can also be observed that as the γ_E of the eavesdropping channel increases,

the SR will decrease for all systems, and as γ_E increases to 20 dB, the SR of the TRAN-OFDM-DCSK proposed scheme is matched to the SR of the TRAN-DCSK scheme.

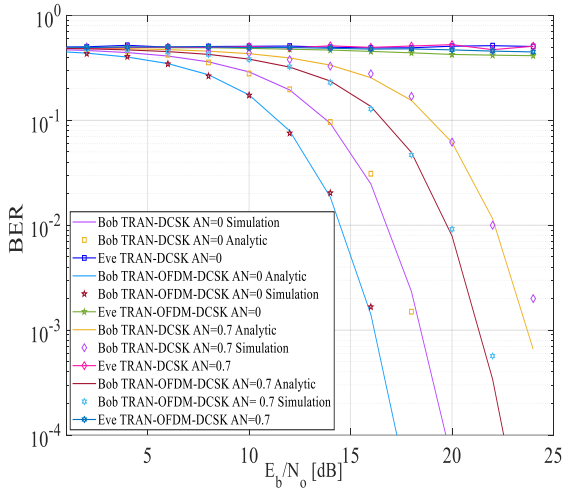

Fig. 4. BER performance comparison of proposed TRAN-OFDM-DCSK with TRAN-DCSK for Bob and Eve without AN and with AN at 70% of Total Transmit Power.

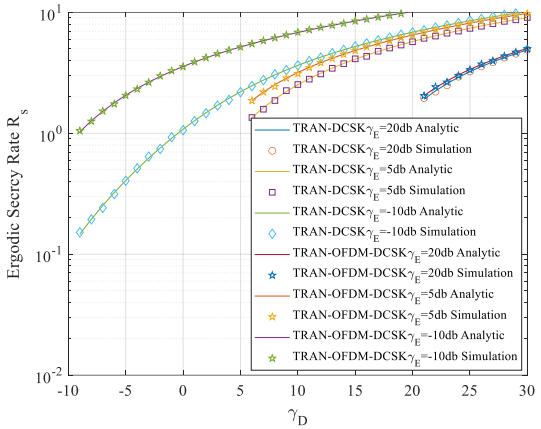

Fig. 5. Ergodic Secrecy rate performance comparison of proposed TRAN OFDM-DCSK with TRAN-DCSK versus γ_D with AN at 20% of Total Transmit Power.

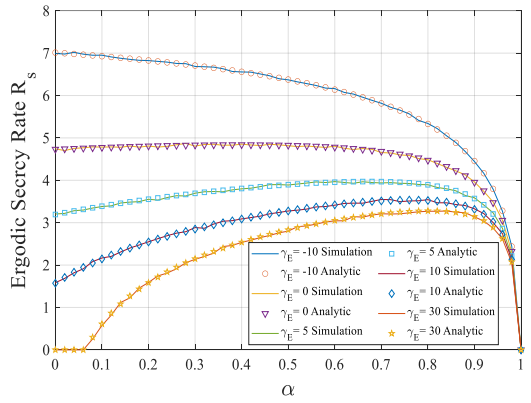

Fig. 6. TRAN-OFDM-DCSK achievable secrecy rate performance for different AN power α with different γ_E values when γ_D is 10dB.

Fig. 6 demonstrates the relationship between the AN energy injected and the ergodic secrecy rate for different values of γ_E, and the selected value of γ_D is 10 dB, which shows that achievable SR is a function of α. which can be seen from point $\alpha = 0$ (i.e., there is no AN) the SR is increased as the value of γ_E is decreased. Also, clear that, as increasing the value of γ_E, the AN energy injected can improve the ergodic system SR significantly, and it has a maximum rate for a certain value of α. Therefore, it is possible to maximize the achievable secrecy rates by optimizing the AN energy injected α. Also, it is demonstrated that the optimal AN energy injected α dependent on the eavesdropper SNR value γ_E. More specifically, it is revealed that the optimal AN energy injected α is increased for the higher SNR of eavesdroppers γ_E.

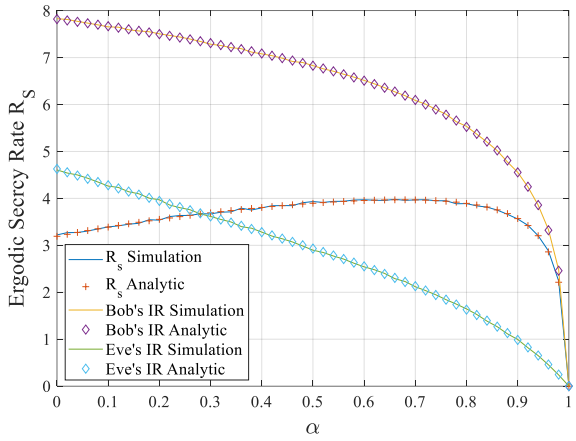

Fig. 7. TRAN-OFDM-DCSK Bob and Eve information rates and achievable secrecy rate for different AN power α with selected γ_E is 5db, and γ_D is 10dB.

Fig. 7 describes the relationship between the AN energy injected α and the Ergodic rate for the fixed value of the legitimate receiver SNR γ_D as 10 dB and the set value of SNR of the eavesdropper receiver as 5 dB. Next, we determined the information rate (IR) via the genuine and ungenuine receivers for different energy levels assigned to the AN injection. It is detected that the injection of AN in the TRAN-OFDM-DCSK proposed method results in a relatively minor deterioration in the IR of the genuine receiver while significantly disrupting the reception upon eavesdropping, and as an outcome, enhanced secrecy rates are achieved.

VI. Conclusion

In this paper, we suggest a new wiretap transmission system based on PLS by using TR pre-coding chaos-based OFDM-DCSK modulation with AN injection, to accomplish high data rate, high security of transmission, high physical layer data security and high-reliability performance. The performance of the proposed scheme is evaluated by considering a passive eavesdropper (Eve), whose CSI is assumed to be unknown at Alice, that trying to eavesdrop on the wireless transmission from Alice to Bob. Alice uses the time-reversal precoder for artificial noise addition to the transmitted data, which falls into Bob's null space but degrades the channel of Eve. The proposed technology needs only one transmitting antenna and is consequently well appropriate for limited abilities devices, like the Internet of

Things, for example. The analytical expression of the bit error rate and ergodic secrecy rate performance is derived over a Rayleigh fading channel, which matches the simulation results. Also, it can be distinguished that the BER performance of the proposed TRAN-OFDM-DCSK scheme is better than the TRAN-DCSK almost by 3 dB at BER= 10^{-3}, and the SR is increased as the value of γ_E is decreased. Also, as increasing the value of γ_E, the AN energy injected can improve the ergodic system SR significantly, and the ergodic system SR can reach a maximum rate for a certain value of α. Furthermore, the determined analytical formulations permit Alice to find the optimal energy value of artificial noise injected to make the most of the secrecy rate.

REFERENCES

[1] H. Alves, R. D. Souza, M. Debbah, and M. Bennis: *Performance of transmit antenna selection physical layer security schemes*, IEEE Signal Process. Lett., Vol.19, No.6, pp. 372-375, Apr. 2012.

[2] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen: *Physical layer security for TAS/MRC with antenna correlation*, IEEE Trans. Inf. Forensics Security, Vol.8, No.1, pp. 254-259, Oct. 2013.

[3] D. D. Tran, D. B. Ha, V. Tran Ha, and E. K. Hong: *Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels*, IETE Journal of Research, Vol. 61, No. 4, pp. 363-371, Jul. 2015.

[4] J. M. Hamamreh, H. M. Furqan and H. Arslan:*Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey*, IEEE Communications Surveys & Tutorials, Vol.21, No.2, pp. 1773-1828, Oct. 2019.

[5] A. D. Wyner: "The wiretap channel " The Bell System Technical Journal, Vol.54, No.8, pp. 1355–1387, 1975.

[6] L. Kong, G. Kaddoum and Mostafa Taha: "Performance Analysis of Physical Layer Security of Chaos-based Modulation Schemes" Eight International Workshop on Selected Topics in Mobile and Wireless Computing, 2015.

[7] M. Bloch and J. Barros: "Physical-Layer Security: From Information Theory to Security" Engineering. Cambridge University Press, 2011.

[8] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen: *A survey on multiple-antenna techniques for physical layer security*, IEEE Communications Surveys Tutorials, Vol.19, No.2, pp. 1027–1053, Nov. 2017.

[9] 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, Feb. 2019.

[10] R. Negi and S. Goel: "Secret communication using artificial noise," IEEE 62nd Vehicular Technology Conference., Vol.3, pp. 1906–1910, Sep. 2005.

[11] S. Goel and R. Negi: "Secret communication in presence of colluding eavesdroppers," IEEE Military Communications Conference, Vol.3, pp. 1501–1506, Oct. 2005.

[12] S. Goel and R. Negi: *Guaranteeing secrecy using artificial noise*, IEEE Trans. on Wireless Communications, Vol.7, No.6, pp. 2180–2189, Jun, 2008.

[13] M. Li, S. Kundu, D.A. Pados, and S.N. Batalama: *Waveform Design for Secure SISO Transmissions and Multicasting*, IEEE Journal on Selected Areas in Communications, Vol.31, No.9, Sep. 2013.

[14] T-H. Nguyen, J-F. Determe, M. Van Eeckhaute, J. Louveaux, P. De Doncker, and F. Horlin: "Frequency-Domain Time-Reversal Pre-coding in Wideband MISO OFDM Communications Systems", in arXiv e-prints, Apr. 2019.

[15] Q. Xu, P. Ren, Q. Du, and L. Sun: *Security-Aware Waveform and Artificial Noise Design for Time-Reversal-Based Transmission*, IEEE Trans. on Vehicular Technology, Vol.67, No.7, June 2018.

[16] S. Li, N. Li, X, Tao, Z. Liu, H. Wang, and J. Xu: "Artificial Noise Inserted Secure Communication in Time-Reversal Systems", IEEE Wireless Communications and Networking Conference, Apr. 2018.

[17] S. Li, N. Li, Z. Liu, H. Wang, J. Xu, and X. Tao: "Artificial Noise Aided Path Selection for Secure TR Communications", IEEE/CIC International Conference on Communications in China (ICCC), Oct. 2017.

[18] C. Oestges, A.D. Kim, G. Papanicolaou, and A. J. Paulraj: *Characterization of Space-Time Focusing in Time-Reversed Random Fields*, IEEE Transactions on Antennas and Propagation, Vol.53, No.1, Jan. 2005.

[19] Y. Lee, H. Jo, Y. Ko, and J. Choi: *Secure Index and Data Symbol Modulation for OFDM-IM*, IEEE Access, Vol.5, pp. 24 959–24 974, 2017.

[20] 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.

[21] S. Golstein, T. Nguyen, F. Horlin, P. D. Doncker, and J. Sarrazin: "Physical layer security in frequency-domain time-reversal siso ofdm communication," 2020 International Conference on Computing, Networking and Communications (ICNC), pp. 222–227, Febr. 2020.

[22] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong: *Design of an OFDM physical layer encryption scheme*, IEEE Trans. on Vehicular Technology, Vol.66, No.3, pp. 2114–2127, 2017.

[23] K. Umebayashi, F. Nakabayashi, and Y. Suzuki, "A study on secure pilot signal design for ofdm systems," in Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia Pacific, pp. 1–5, Dec. 2014.

[24] F. C. Lau and C. K. Tse: "Chaos-based digital communication systems". Springer-Verlag, 2003.

[25] W. K. Xu, L. Wang, and G. Kolumban: *A novel differential chaos shift keying modulation scheme*, International Journal of Bifurcation and Chaos, Vol.21, No.03, pp. 799–814, 2011.

[26] G. Kaddoum and F. Shokraneh: *Analog network coding for multiuser multi-carrier differential chaos shift keying communication system*, IEEE Trans. Wireless Commun., Vol.14, No.3, pp. 1492–1505, Mar. 2015.

[27] J. Yu and Y.-D. Yao: *Detection performance of chaotic spreading LPI waveforms*, IEEE Trans. Wireless Commun., Vol.4, No.2, pp. 390–396, Mar. 2005.

[28] G. Heidari-Bateni and C. McGillem: "Chaotic sequences for spread spectrum: an alternative to PN-sequences," Proc. IEEE International Conference on Selected Topics in Wireless Communications, pp. 437–440, June 1992.

[29] G. Kaddoum and F. Shokraneh: *Analog network coding for multi user multi-carrier differential chaos shift keying communication system*, IEEE Trans. Wireless Communication., Vol.14, No.3, pp. 1492–1505, Mar. 2015.

[30] Y.-S. Lau, K. Lin, and Z. Hussain: "Space-time encoded secure chaos communications with transmit beamforming," IEEE Region 10 TENCON, pp. 1–5, Nov. 2005

[31] G. Kaddoum, F. Richardson, and F. Gagnon: *Design and analysis of a multi-carrier differential chaos shift keying communication system*, IEEE Trans. on Commun., Vol.61, No.8, pp. 3281–3291, Aug. 2013.

[32] G. Kaddoum, F. Gagnon, and F. Richardson: "Design of a secure multicarrier DCSK system," in Proc. the ninth Intlernational Symposium on Wireless Communication Systems (ISWCS), pp. 964–968, Aug. 2012.

[33] L. Kong, G. Kaddoum and Mostafa Taha: "Performance Analysis of Physical Layer Security of Chaos-based Modulation Schemes" 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 283-288, Oct. ,2015.

[34] G. Kaddoum, P. Charge, D. Roviras, and D. Fournier-Prunaret: "A methodology for bit error rate prediction in chaos-based communication systems", Circuits, System Signal Process, Vol.28, pp. 925– 944, Aug. 2009.

[35] Y. S. Cho, J. Kim, W. Y. Yang and C. G. Kang: "MIMO-OFDM Wireless Communications with MATLAB", John Wiley & Sons (Asia) Pte Ltd, 2010.

[36] M. Dawa, G. Kaddoum, and Z. Sattar: *A generalized lower bound on the bit error rate of DCSK systems over multipath Rayleigh fading channels*, IEEE Trans. Circuits Syst. II, Exp. Briefs, Vol.65, pp. 321– 325, Mar. 2018.

[37] Z. Liu, L. Zhang, Z. Wu and J. Bian,: *A Secure and Robust Frequency and Time Diversity Aided OFDM–DCSK Modulation System Not Requiring Channel State Information*, in IEEE Trans. on Communications, Vol.68, No.3, pp. 1684-1697, March 2020.

[38] Z. Liu, L. Zhang, and Z. Chen: "Low PAPR OFDM-based DCSK design with carrier interferometry spreading codes," IEEE Commun. Lett., Vol.22, pp. 1588–1591, Aug. 2018.

[39] H. Tran, H. Tran, G. Kaddoum, D. Tran, and D. Ha: "Effective secrecy sinr analysis of time reversal-employed systems over correlated multipath channel," IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 527–532, 2015.

[40] D. Hu, W. Zhang, L. He, and J. Wu: *Secure transmission in multi-cell multi-user massive mimo systems with an active eavesdropper*, IEEE Wireless Communications Letters, Vol.8, No.1, pp. 85–88, Feb. 2019.

Dhuha Hussein Hameed was born in Baghdad, Iraq in 1993. She received her B.Sc. degree in Electrical Engineering in 2015 and her M.Sc. degree in Electronics and Communication Engineering in 2018, both from the Mustansiriyah University, Iraq. she is currently pursuing an Ph.D. in Communication Engineering at the department of Electrical Engineering, Al- Mustansiriyah University. Her research interests include wireless communication, spread spectrum, physical layer security, OFDM based DCSK, and chaotic theory.

Fadhil S. Hasan was born in Baghdad, Iraq in 1978. He received his B.Sc. degree in Electrical Engineering in 2000 and his M.Sc. degree in Electronics and Communication Engineering in 2003, both from the Mustansiriyah University, Iraq. He received Ph.D. degree in 2013 in Electronics and Communication Engineering from the Basrah University, Iraq. In 2005, he joined the faculty of Engineering at the Mustansiriyah University in Baghdad. His recent research activities are Wireless Communication Systems, Multicarrier System, Wavelet based OFDM, MIMO System, Speech and Image Signal Processing, Chaotic Cryptography, Chaotic Modulation, FPGA and Xilinx System Generator based Communication System. Now he has been an Assist. Prof. at the Mustansiriyah University.