Received: 26 December 2021 | Revised: 12 September 2022 | Accepted: 10 October 2022

DOI: 10.1002/ett.4678

RESEARCH ARTICLE

WILEY

A novel interference signal superposition algorithm for providing secrecy to subcarrier number modulation-based orthogonal frequency division multiplexing systems

Muhammet Kırık | **Jehad M. Hamamreh**

WISLAB-TELENG for Wireless Research at the Department of Electrical-Electronics Engineering, Antalya Bilim University, Antalya, Turkey

Correspondence
Muhammet Kırık, WISLAB-TELENG for Wireless Research at the Department of Electrical-Electronics Engineering, Antalya Bilim University, Antalya 07190, Turkey.
Email: muhammetkirik1997@gmail.com

Funding information
Türkiye Bilimsel ve Teknolojik Araştirma Kurumu, Grant/Award Number: 119E392

Abstract

Orthogonal Frequency Division Multiplexing with Subcarrier Number Modulation (OFDM-SNM) is a transmission scheme that aims to convey additional data bits by exploiting the number of active subcarriers. Even though OFDM-SNM creates many advantages, such as low bit error rate (BER), high spectral efficiency, and high reliability, it suffers from the security vulnerabilities against eavesdroppers and malicious wire-tappers. The reason why OFDM-SNM is vulnerable against security threats is that the nature of subcarrier number-based additional data transmission differs from the conventional data modulation techniques, which makes the existing physical layer security (PLS) applications to be inapplicable for OFDM-SNM. Therefore, novel PLS techniques must be developed for OFDM-SNM to secure the data that is transmitted by exploiting the number of subcarriers. In this paper, a novel interference signal superposition security algorithm for OFDM-SNM is proposed at the physical level to overcome its security vulnerabilities. The proposed security application aims to provide the data secrecy by embedding an artificial interference signal into the data that are meant to be conveyed by the active subcarriers. This artificial interference signal is created by exploiting the channel state information of the legitimate user, and deliberately included into the transmitted data to create a confusion for those who try to infiltrate the communication system, such as eavesdroppers or malicious wire-tappers. In this paper, the transmission of data for both the legitimate user and eavesdropper is operated by M-ary PSK/QAM modulation over a Rayleigh fading channel. The theoretical calculations and simulation results prove that the proposed security application for OFDM-SNM is a strong candidate to provide the security requirements of such cases in future wireless networks, where providing data secrecy is among the top priorities.

KEYWORDS

5G, 6G, interference signal superposition, ISS, OFDM, OFDM-SNM, physical layer security, PLS, secrecy, subcarrier number modulation, wireless communication, wireless security

1 | INTRODUCTION

The security capacity of the communication devices in the presence of an eavesdropper has been an important notion since it is first introduced by Shannon.[1,2] Throughout the passing years, the importance of this secure communication necessity has enlarged within the unstoppable data traffic growth around the world.[3] To satisfy this necessity, many different types of secure data communication solutions have been developed, that contribute to the secrecy of digital communication systems.[4]

One of the solutions offered by Wyner[5] suggested the wire-tap channel for the first time, which considers the difference between legitimate receiver's and wire-tapper's noises. With this work, assuming that the wire-tapper is receiving a corrupted version of the legitimate receiver's signal, the possibility of secure communication is proved by characterizing the trade-off between the transmitted signal to the receiver and the level of ignorance at the wire-tapper.[6] In the following years, Wyner's study was supported by Csiszár and Körner.[7] With this work, Wyner's results are extended in terms of robustness to transmission errors by creating less noisy channels, and capability of confidentiality by creating an environment that allows the common information to be sent to both legitimate receiver and wire-tapper, while the private data is sent to the legitimate receiver only.[8]

Even though the key factor of the secure communication is achieved by creating a disadvantage at the wire-tapper's side compared to the legitimate receiver, and ensures the legitimate receiver can achieve successful decoding while the eavesdropper cannot, this encryption/decryption and cryptography-based approaches cannot be satisfactory to provide the data security in today's conditions.[9-13]

The reason behind it is the massive number of devices that are powered by 5G and beyond wireless technologies.[14-16] Within the advent of the 5G-based technologies such as spatial modulation,[17,18] index modulation (IM),[19,20] antenna number modulation,[21-24] and subcarrier number modulation (SNM),[25-28] etc., the need for novel security solutions stands out for the sake of modern communication application's secrecy.[29] In this manner, physical layer security (PLS) and the secure data transmission techniques based on PLS draw great attention nowadays, since the PLS gives the opportunity to detect channel state information (CSI) of transmitter.[30-33] This CSI at the transmitter can be manipulated by a suitable optimization on the transmitted data to create an environment that can offer perfect secrecy.[34,35]

Even though there are a lot of data transmission techniques that have been proposed in the literature as mentioned in the above paragraph, to improve the spectral efficiency, data rate, and reliability, the secrecy capabilities of these schemes are also an intriguing topic for the researchers. In this manner, one of the most worth mentioning OFDM-based data transmission schemes is the SNM. OFDM-SNM is a number-based transmission scheme where the number of active subcarriers depends on the data symbols, and exploits the number of active subcarriers as a third dimension to transmit additional data symbols alongside the conventionally modulated M-ary symbols. The main advantage of OFDM-SNM over those other competitor schemes in the literature such as OFDM-IM is the capability of subcarrier selection that is dependent on both channel and the incoming data. Since the additional data symbol transmission is operated by the number of the subcarriers rather than their indices, OFDM-SNM creates a possibility to choose those subcarriers that can provide the highest channel gain during the transmission, which is a unique feature of OFDM-SNM and OFDM-IM is not capable of.[25,28,36]

In this paper, a novel secure data transmission method called Interference Signal Superposition OFDM with Subcarrier Number Modulation (ISS-OFDM-SNM) is proposed to create an environment during the data transmission, that can exploit the CSI of the legitimate user to offer perfect secrecy against the wire-tapper at the physical layer level by exploiting the uniqueness of the channel between the transmitter and legitimate receiver.[37,38] In this method, by inheriting the features of conventional OFDM-SNM, the transmitted data is aimed to be sent with high spectral efficiency, and low BER by utilizing the capability of SNM to offer channel and data-dependent subcarrier selection at the same time, while the data secrecy is provided against a wire-tapper by adding an artificial interference signal, which is specifically designed according to the legitimate receiver's CSI and embedded into the actual signal that is intended to be sent.

The remaining parts of this paper are organized as follows. In Section 2, the system model of the ISS-OFDM-SNM concept is explained in detail and its properties are specified. In Section 3, the performance analysis of the proposed security algorithm is mathematically exhibited. In Section 4, simulation results are exhibited and their performances are commentated. Lastly in Section 5, the paper is concluded.*

2 | SYSTEM MODEL

The system model of the proposed OFDM-SNM-ISS security application is given in Figure 1. The procedure starts in a similar way as the conventional OFDM-SNM.[28] The incoming data stream with m bits enters to the transmitter of Alice who desires to transmit a secure data to a legitimate receiver Bob. These m bits are split into G groups, in which each group contains $p = p_1 + p_2$ bits. While the $p_1 = \log_2(N)$ represents the SNM mapper to define the number of active subcarriers, K, out of N subcarriers, $p_2 = K(\log_2(M))$ represents those bits modulated by conventional M-ary constellation order and transmitted via K active subcarriers. For the case where $N = 4$, the possible subcarrier activation patterns for $p_1 = \log_2(4) = 2$ and $K \in [1, 2, 3, 4]$ is given in Table 1. After this step is successfully operated for all the G subblocks, the combined OFDM block can be represented as $\mathbf{x_F} = [x_F(1)x_F(2)\cdots x_F(N_F)]$.

At this point, each index value of $\mathbf{x_F}$ is affected by an additive artificial interference signal, $\mathbf{n_F} = [n_F(1)n_F(2)\cdots n_F(N_F)]$, that is specifically designed according to the CSI of Bob. This purposefully added artificial interference signal creates the security factor against the eavesdropper, Eve, who tries to breach the communication system.

In order to eliminate any confusion about how the additive artificial interference signal is obtained, the following explanation is provided. In this study, a point-to-point communication is considered where both the transmitter and receiver have perfect CSI. This means that the transmitter has the capacity to create some random signals, namely the additive artificial interference signal, that contains the CSI of the communication channel between the transmitter and legitimate receiver. This additive artificial interference signal is created in a way that it can be canceled when it interacts with the channel of the transmitter and legitimate receiver. However, this is not the case when the channel between the transmitter and illegitimate receiver is considered. The reason for that is this the created additive artificial interference signal contains only the CSI between the transmitter and legitimate receiver. Thus, the added interference cannot be canceled by the eavesdropper. This process is explained further in detail in the following paragraphs with examples.

The next step is operated by the conventional OFDM. After taking the inverse fast fourier transform (IFFT), the acquired signal becomes $\mathbf{x_G} + \mathbf{n_G} = IFFT(\mathbf{x_F} + \mathbf{n_F})$ with dimension $N_F \times 1$, where $\mathbf{x_G} = [x_G(1)x_G(2)\cdots x_G(N_F)]$ is the transmitted data and $\mathbf{n_G} = [n_{G1}n_{G2}\cdots n_{GN}]$ is the artificial interference signal vector added in a superposition way to the data vector in frequency domain.

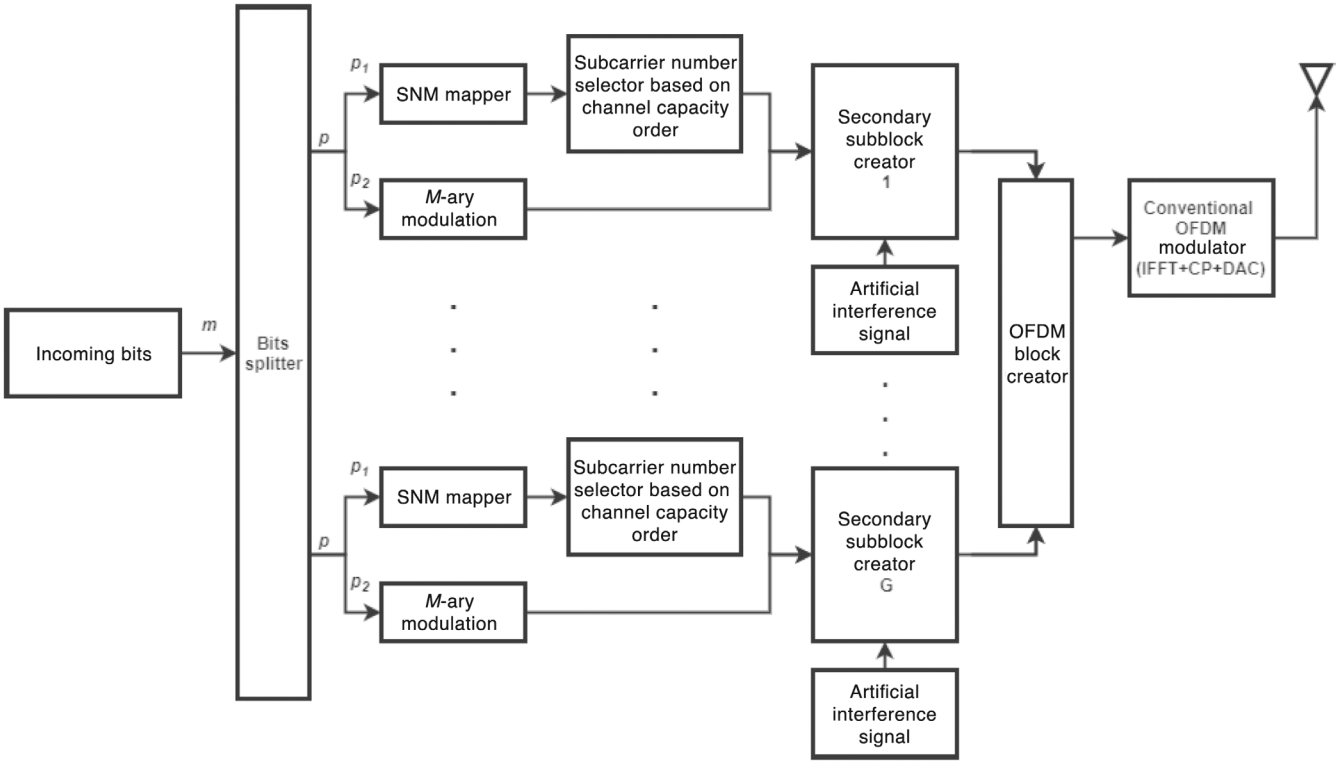

FIGURE 1 Transmitter structure of orthogonal frequency division multiplexing with subcarrier number modulation with the proposed interference signal superposition algorithm

TABLE 1 Orthogonal frequency division multiplexing with subcarrier number modulation interference signal superposition mapper with $p_1 = 2$bits and $N = 4$ subcarriers in each subblock, where the final active subcarrier pattern is determined by the largest channel gains among all possible subcarrier numbers

Information bits (p_1)	Possible active subcarriers pattern (v)	Artificial interference signal vector ($\mathbf{n_G}$)
[0 0]	[1 0 0 0]	$[\frac{A}{h_{G1}}\ \frac{-A}{h_{G2}}\ 0\ 0]$
[0 0]	[0 1 0 0]	$[\frac{A}{h_{G1}}\ \frac{-A}{h_{G2}}\ 0\ 0]$
[0 0]	[0 0 1 0]	$[\frac{A}{h_{G1}}\ 0\ \frac{-A}{h_{G3}}\ 0]$
[0 0]	[0 0 0 1]	$[\frac{A}{h_{G1}}\ 0\ 0\ \frac{-A}{h_{G4}}]$
[0 1]	[1 1 0 0]	$[\frac{A}{h_{G1}}\ \frac{-A}{h_{G2}}\ 0\ 0]$
[0 1]	[1 0 1 0]	$[\frac{A}{h_{G1}}\ 0\ \frac{-A}{h_{G3}}\ 0]$
[0 1]	[1 0 0 1]	$[\frac{A}{h_{G1}}\ 0\ 0\ \frac{-A}{h_{G4}}]$
[0 1]	[0 0 1 1]	$[0\ 0\ \frac{A}{h_{G3}}\ \frac{-A}{h_{G4}}]$
[0 1]	[0 1 0 1]	$[0\ \frac{A}{h_{G2}}\ 0\ \frac{-A}{h_{G4}}]$
[0 1]	[0 1 1 0]	$[0\ \frac{A}{h_{G2}}\ \frac{-A}{h_{G3}}\ 0]$
[1 0]	[1 1 1 0]	$[\frac{A}{h_{G1}}\ \frac{B}{h_{G2}}\ \frac{-(A+B)}{h_{G3}}\ 0]$
[1 0]	[1 1 0 1]	$[\frac{A}{h_{G1}}\ \frac{B}{h_{G2}}\ 0\ \frac{-(A+B)}{h_{G4}}]$
[1 0]	[1 0 1 1]	$[\frac{A}{h_{G1}}\ 0\ \frac{B}{h_{G3}}\ \frac{-(A+B)}{h_{G4}}]$
[1 0]	[0 1 1 1]	$[0\ \frac{A}{h_{G2}}\ \frac{B}{h_{G3}}\ \frac{-(A+B)}{h_{G4}}]$
[1 1]	[1 1 1 1]	$[\frac{A}{h_{G1}}\ \frac{-A}{h_{G2}}\ \frac{B}{h_{G3}}\ \frac{-B}{h_{G4}}]$

After that, cyclic prefix (CP) of length (N_{CP}) is appended on the data vector in time domain to alleviate the inter symbol interference (ISI) effect caused by mutipath channels. As a result, the output signal for Bob becomes

$$(\mathbf{x_G} + \mathbf{n_G})_{\mathrm{CP}} = [(\mathbf{x_G} + \mathbf{n_G})(N_F - N_{\mathrm{CP}} + 1 : N_F)\mathbf{x_G} + \mathbf{n_G}]. \tag{1}$$

Next, the obtained $\mathbf{x_G} + \mathbf{n_G}$ is affected by the channel impulse response, $\mathbf{h_G} = [h_{G1}h_{G2}\cdots h_{GL}] \in \mathbb{C}^{1\times L}$, where L is the number of taps in the time domain channel impulse response.

In this regard, the mathematical expression of this process for Bob in the time-domain can be given in convolution as follows.[28]

$$\mathbf{y_{b_G}} = [(\mathbf{x_G} + \mathbf{n_G})_{\mathrm{CP}}] \circledast \mathbf{h_G} + \mathbf{z_{b_G}}, \tag{2}$$

$$\mathbf{y_{b_G}} = \int_{-\infty}^{\infty} [(\mathbf{x_G} + \mathbf{n_G})_{\mathrm{CP}}] \times \mathbf{h_G} dt + \mathbf{z_{b_G}}, \tag{3}$$

where ($\mathbf{z_{b_G}}$) is the additive white Gaussian noise affecting the received signal at Bob.

A similar mathematical transmission expression can also be formulated for Eve with a different channel impulse response in each subblock $\mathbf{e_G} = [e_{G1}e_{G2}\cdots e_{GL}] \in \mathbb{C}^{1\times L}$.

The received signal at the eavesdropper can be given in both convolution and integration form as shown below.

$$\mathbf{y_{e_G}} = (\mathbf{x_G} + \mathbf{n_G})_{\mathrm{CP}} \circledast \mathbf{e_G} + \mathbf{z_{e_G}}, \tag{4}$$

$$\mathbf{y_{e_G}} = \int_{-\infty}^{\infty} (\mathbf{x_G} + \mathbf{n_G})_{\mathrm{CP}} \times \mathbf{e_G} dt + \mathbf{z_{e_G}}, \tag{5}$$

It should be noted that K is not always stable, where as the number of active subcarriers changes by the incoming data stream, the value of K defers accordingly. Also, for different channel amplitude values, indices of $\mathbf{h_G}$ may vary even

in the same number of subcarrier activation cases since the transmission of Bob's data is conducted by those subcarrier channels that can offer the highest possible channel amplitude, which creates different scenarios for the addition of artificial interference signal. Possible cases for different subcarrier activation patterns are given in Table 1 and some of their mathematical transmission correspondences are formulated for both Bob and Eve in the following example.

Example: Consider a communication system that consists of one transmitter, Alice, one legitimate receiver, Bob, and one eavesdropper, Eve. In this system, while Alice is trying to transmit a secret data to Bob by using an OFDM system with four subcarriers in one subblock ($G = 1, N = 4$), under binary phase shift keying (BPSK) modulation, Eve is trying to infiltrate the system. The corresponding data to be transmitted by Alice in one subblock is given in Figure 2 with its separated form as p_1 and p_2.

During this transmission, channel gains of each subcarrier between Alice and Bob in one subblock are sorted according to the subcarriers' channel gains as $|h_{13}| > |h_{14}| > |h_{11}| > |h_{12}|$. In such a case, transmission of each symbol of p_2 under BPSK modulation is explained as follows for both Bob and Eve.

By referring to Figure 2, it can be inferred that the transmission of the first symbol in p_2 ($x_{11} = 1$) will be operated by three subcarriers as the corresponding p_1 symbol is 10. A general illustration of this process is shown in Figure 3A. As it is stated before, the subcarrier channel activation order is $|h_{13}| > |h_{14}| > |h_{11}| > |h_{12}|$, which means the possible active subcarriers pattern for this transmission case is $\mathbf{v} = [1011]$, and the artificial interference signal vector is $\mathbf{n_1} = [\frac{A}{h_{11}} 0 \frac{B}{h_{13}} \frac{-(A+B)}{h_{14}}]$. Under these conditions, by referring to (2) and (3), the mathematical form of the transmission of the first symbol of Bob's data by activating three subcarriers is derived as below.

$$y_{b_{11}} = \int_{-\infty}^{\infty} (x_{11} + n_{11}) \times h_{11} + (x_{11} + n_{13}) \times h_{13} + (x_{11} + n_{14}) \times h_{14} dt, \tag{6}$$

$$y_{b_{11}} = \int_{-\infty}^{\infty} \left(x_{11} + \frac{A}{h_{11}}\right) \times h_{11} + \left(x_{11} + \frac{B}{h_{13}}\right) \times h_{13} + \left(x_{11} - \frac{A+B}{h_{14}}\right) \times h_{14} dt, \tag{7}$$

$$y_{b_{11}} = \int_{-\infty}^{\infty} x_{11} h_{11} + x_{11} h_{13} + x_{11} h_{14} dt, \tag{8}$$

where the A and B represent any two arbitrary values to create the confusion, as they are canceled during the transmission.

On the other hand, since Eve is trying to reach to the Alice's transmitted data from a different location with a different channel impulse response, $\mathbf{e_1}$, and the artificial interference signal, $\mathbf{n_1}$ is created specifically and only for the channel impulse response of Bob, $\mathbf{h_1}$, the transmitted data to the Eve's location will be a complicated signal with no meaning. By referring (4) and (5), this transmission process for Eve is given below in mathematical form as follows.

$$y_{e_{11}} = \int_{-\infty}^{\infty} (x_{11} + n_{11}) \times e_{11} + (x_{11} + n_{13}) \times e_{13} + (x_{11} + n_{14}) \times e_{14} dt, \tag{9}$$

$$y_{e_{11}} = \int_{-\infty}^{\infty} \left(x_{11} + \frac{A}{h_{11}}\right) \times e_{11} + \left(x_{11} + \frac{B}{h_{13}}\right) \times e_{13} + \left(x_{11} - \frac{A+B}{h_{14}}\right) \times e_{14} dt, \tag{10}$$

$$y_{e_{11}} = \int_{-\infty}^{\infty} x_{11} e_{11} + \frac{A}{h_{11}} e_{11} + x_{11} e_{13} + \frac{B}{h_{13}} e_{13} + x_{11} e_{14} - \frac{A+B}{h_{14}} e_{14} dt. \tag{11}$$

For the transmission of the second symbol of p_2 ($x_2 = 0$), it can be inferred from Figure 2 that the corresponding subcarrier activation mapper p_1 is 01, which means the activation of two subcarriers. This process is illustrated in Figure 3B. In this case, the possible active subcarrier pattern is $\mathbf{v} = [0011]$ and the artificial interference signal vector

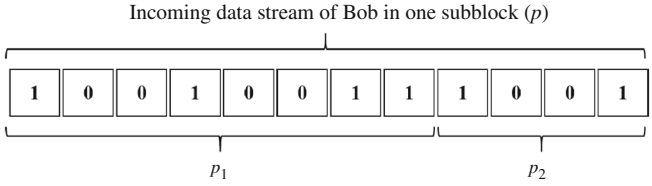

FIGURE 2 Transmitted data by alice with four subcarriers under BPSK modulation

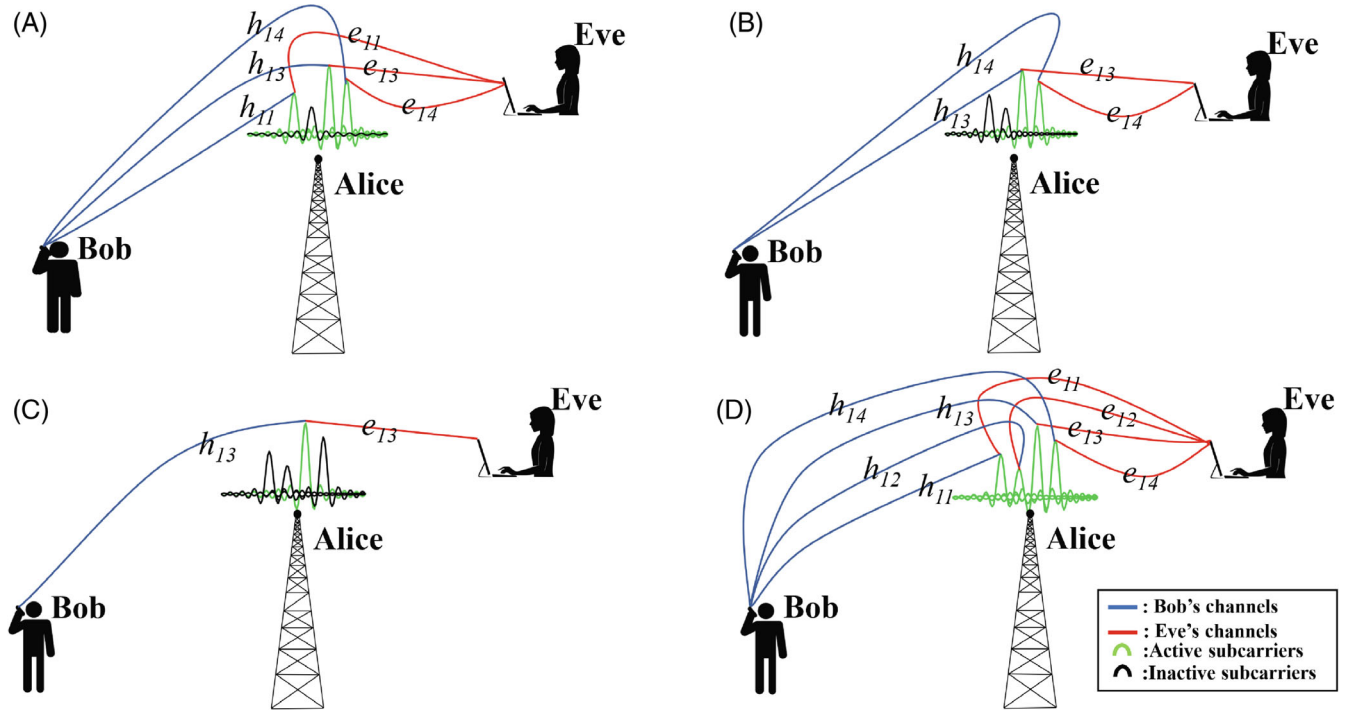

FIGURE 3 Simple visualization of the transmission of each symbol in p_2 for different subcarrier activation patterns given in the example

is $\mathbf{n_1} = [00\frac{A}{h_{13}}\frac{-A}{h_{14}}]$. Under these conditions, by referring (2) and (3), the mathematical form of the transmission of 0 by activating two subcarriers for Bob can be derived as follows.

$$y_{b_{12}} = \int_{-\infty}^{\infty} (x_{12} + n_{13}) \times h_{13} + (x_{12} + n_{14}) \times h_{14} dt, \tag{12}$$

$$y_{b_{12}} = \int_{-\infty}^{\infty} \left(x_{12} + \frac{A}{h_{13}}\right) \times h_{13} + \left(x_{12} - \frac{A}{h_{14}}\right) \times h_{14} dt, \tag{13}$$

$$y_{b_{12}} = \int_{-\infty}^{\infty} x_{12} h_{13} + x_{12} h_{14} dt. \tag{14}$$

On the other hand, by referring (4) and (5), the mathematical form of the erroneously transmitted symbol to Eve's receiver can be given as follows.

$$y_{e_{12}} = \int_{-\infty}^{\infty} (x_{12} + n_{13}) \times e_{13} + (x_{12} + n_{14}) \times e_{14} dt, \tag{15}$$

$$y_{e_{12}} = \int_{-\infty}^{\infty} \left(x_{12} + \frac{A}{h_{13}}\right) \times e_{13} + \left(x_{12} - \frac{A}{h_{14}}\right) \times e_{14} dt, \tag{16}$$

$$y_{e_{12}} = \int_{-\infty}^{\infty} x_{12} e_{13} + \frac{A}{h_{13}} e_{13} + x_{12} e_{14} - \frac{A}{h_{14}} e_{14} dt. \tag{17}$$

The transmission process of the third symbol of p_2 ($x_3 = 0$) is visually given in Figure 3C. As it can be seen from Figure 2, third symbol of p_2 is sent by activating only one subcarrier as the subcarrier activation mapper, p_1, is 00. In this case, the possible active subcarriers pattern is $\mathbf{v} = [0010]$ and the artificial interference signal vector is $\mathbf{n_1} = [\frac{A}{h_{11}} 0 \frac{-A}{h_{13}} 0]$. Under these circumstances, by referring (2) and (3), the mathematical form of the transmission of 0 to Bob's receiver by activating one subcarrier can be presented as follows.

$$y_{b_{13}} = \int_{-\infty}^{\infty} n_{11} \times h_{11} + (x_{13} + n_{13}) \times h_{13} dt, \tag{18}$$

$$y_{b_{13}} = \int_{-\infty}^{\infty} \frac{A}{h_{11}} h_{11} + \left(x_{13} - \frac{A}{h_{13}}\right) \times h_{13} dt, \tag{19}$$

$$y_{b_{13}} = \int_{-\infty}^{\infty} x_{13} h_{13} dt. \tag{20}$$

By referring (4) and (5), the mathematical form of the erroneously transmitted symbol to Eve's receiver for this case can be given as follows.

$$y_{e_{13}} = \int_{-\infty}^{\infty} n_{11} \times e_{11} + (x_{13} + n_{13}) \times e_{13} dt, \tag{21}$$

$$y_{e_{13}} = \int_{-\infty}^{\infty} \frac{A}{h_{11}} e_{11} + \left(x_{13} - \frac{A}{h_{13}}\right) \times e_{13} dt, \tag{22}$$

$$y_{e_{13}} = \int_{-\infty}^{\infty} \frac{A}{h_{11}} e_{11} + x_{13} e_{13} - \frac{A}{h_{13}} e_{13} dt. \tag{23}$$

Even though the subcarrier activation pattern dictates to activate only one subcarrier for this case, as it can be inferred from (18) and (21), there are two subcarriers deployed for the transmission. The reason behind this is that there is a necessity to activate one more subcarrier to create an availability for the cancellation of the value A. While the first channel is deployed only for the transmission of the artificial interference signal to create such an environment that allows the system to be secure, the third channel is deployed for the transmission of data.

The transmission of the last symbol of p_2 ($x_4 = 1$) must be operated by four subcarriers as the subcarrier activation mapper, p_1, is 11, which can be seen in Figure 2. The visual illustration of this transmission is given in Figure 3D. In this case, the possible active subcarrier pattern is $\mathbf{v} = [1111]$ and the artificial interference signal vector is $\mathbf{n_1} = [\frac{A}{h_{11}} \frac{-A}{h_{12}} \frac{B}{h_{13}} \frac{-B}{h_{14}}]$. Under these circumstances, by referring (2) and (3), the mathematical form of the transmission of 1 for Bob by activating four subcarriers can be presented as follows.

$$y_{b_{14}} = \int_{-\infty}^{\infty} (x_{14} + n_{11}) \times h_{11} + (x_{14} + n_{12}) \times h_{12} + (x_{14} + n_{13}) \times h_{13} + (x_{14} + n_{14}) \times h_{14} dt, \tag{24}$$

$$y_{b_{14}} = \int_{-\infty}^{\infty} \left(x_{14} + \frac{A}{h_{11}}\right) \times h_{11} + \left(x_{14} - \frac{A}{h_{12}}\right) \times h_{12} + \left(x_{14} + \frac{B}{h_{13}}\right) \times h_{13} + \left(x_{14} - \frac{B}{h_{14}}\right) \times h_{14} dt, \tag{25}$$

$$y_{b_{14}} = \int_{-\infty}^{\infty} x_{14} h_{11} + x_{14} h_{12} + x_{14} h_{13} + x_{14} h_{14} dt. \tag{26}$$

By referring (4) and (5), the mathematical form of the erroneously transmitted symbol to Eve's receiver for this case can be given as follows.

$$y_{e_{14}} = \int_{-\infty}^{\infty} (x_{14} + n_{11}) \times e_{11} + (x_{14} + n_{12}) \times e_{12} + (x_{14} + n_{13}) \times e_{13} + (x_{14} + n_{14}) \times e_{14} dt, \tag{27}$$

$$y_{e_{14}} = \int_{-\infty}^{\infty} \left(x_{14} + \frac{A}{h_{11}}\right) \times e_{11} + \left(x_{14} - \frac{A}{h_{12}}\right) \times e_{12} + \left(x_{14} + \frac{B}{h_{13}}\right) \times e_{13} + \left(x_{14} - \frac{B}{h_{14}}\right) \times e_{14} dt, \tag{28}$$

$$y_{e_{14}} = \int_{-\infty}^{\infty} x_{14} e_{11} + \frac{A}{h_{11}} e_{11} + x_{14} e_{12} - \frac{A}{h_{12}} e_{12} + x_{14} e_{13} + \frac{B}{h_{13}} e_{13} + x_{14} e_{14} - \frac{B}{h_{14}} e_{14} dt. \tag{29}$$

As it can be inferred from this example by adding an artificial interference signal into Bob's data, it is possible to create such a transmission environment for Bob that the differentiation of the transmitted symbol and the artificial interference signal is operated at the transmitter, which minimizes the receiver complexity, especially for those Internet of Things (IoT) cases where the battery life is short and processing capabilities are limited. However, the generated transmission formulations for Eve show that since the artificial interference signal does not match with the channel impulse response of Eve and her receiver cannot differentiate the transmitted data from the embedded artificial interference signal, the resulting output of the transmission turns into a meaningless corrupted signal. The illustration of these data differentiations

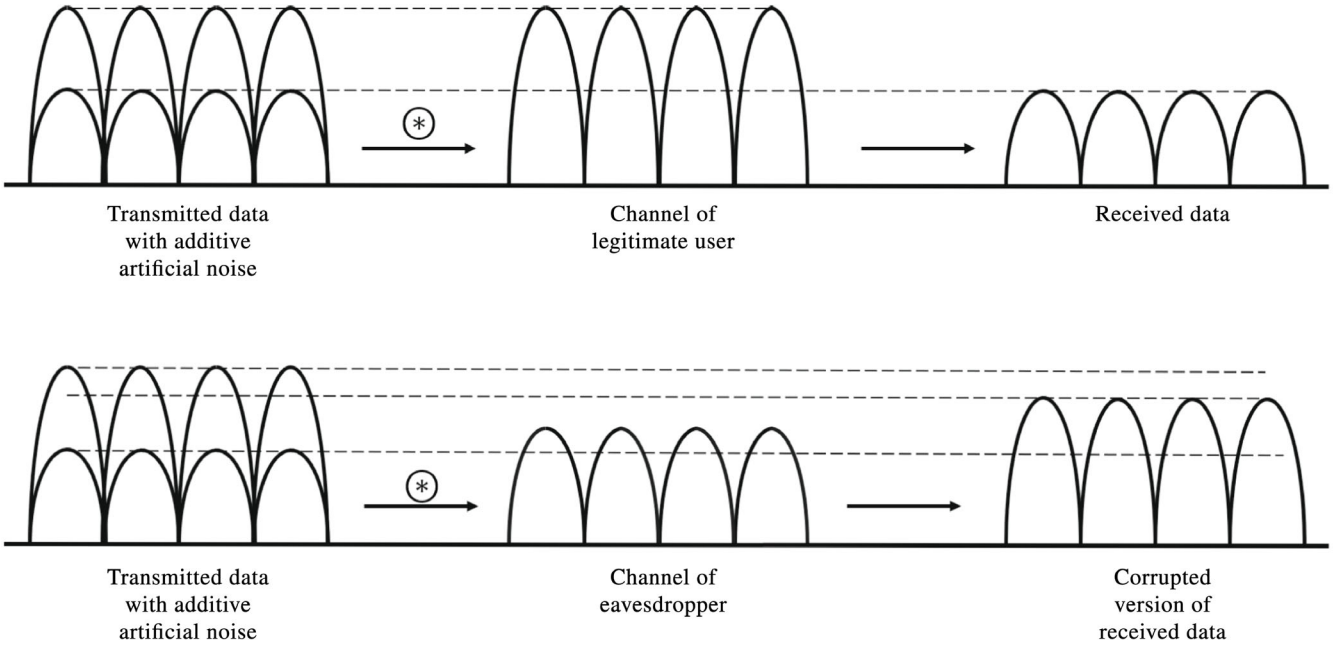

FIGURE 4 Illustration of the artificial interference signal differentiation at the transmitter

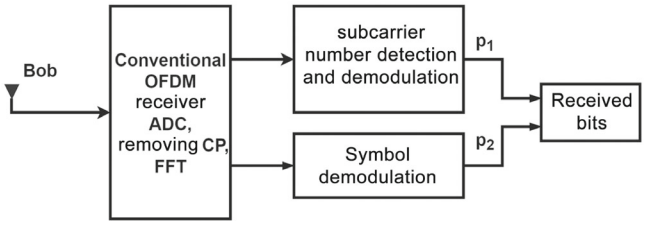

FIGURE 5 Receiver structure of orthogonal frequency division multiplexing with subcarrier number modulation with the proposed interference signal superposition algorithm for Bob

are shown in Figure 4. As it can be seen, the artificial interference signal perfectly matches with the CSI of Bob, which leads the OFDM-SNM system to perfectly cancel the artificial interference signal. On the other hand, since the artificial interference signal does not match with the channel of Eve, differentiation cannot be operated at the transmitter and the receiver of Eve receives a corrupted version of the transmitted data.

Receiver structure of proposed ISS algorithm of OFDM-SNM for Bob is given in Figure 5. The receiving operation of Bob is initiated after this point by reversing the transmission operation, that is, performing the fast fourier transform (FFT), and demapping the SNM as they are performed in a similar way as Reference 28. A simple detector that utilizes the spacial energy as a threshold parameter is used to determine the active subcarriers pattern. As the next step, the set of active subcarriers is mapped at the receiver by receiver demapper, which is the reversed version of SNM mapper at the transmitter. Now, each constellation symbol acquired from the active subcarriers can be detected. At last, both data that acquired from SNM demapper and symbol detection are combined and same procedure is repeated for all subblocks to obtain the whole OFDM block.

3 | PERFORMANCE ANALYSIS

In this section, performance of the proposed ISS algorithm is analysed for both Bob and Eve, and the acquired results are mathematically presented in terms of the statistics of Bob's and Eve's effective SNR, their average BER, and the secrecy performance. In order to analyze the secrecy performance of the proposed ISS algorithm, firstly, the statistics

of the effective instantaneous SNR values of Bob and Eve must be calculated, which are provided as $\gamma_b = \frac{||H_{b_i}||^2 \times P}{\sigma_b^2}$ and $\gamma_e = \frac{||H_{e_i}||^2 \times P}{\sigma_e^2}$ where P is the power allocated to each subcarrier, $||H_{b_i}||$ and $||H_{e_i}||$ are the magnitudes of subchannels for Bob and Eve, respectively.

3.1 | Statistics of Bob's effective SNR

In this section the effective SNR of Bob's data is analyzed under two different perspective. At the beginning, the first portion of Bob's data, p_1, that defines the number of active subcarriers is taken under consideration for the effective SNR analysis, then SNR analysis of the second portion of Bob's data, p_2, that is modulated by M-ary modulation and transmitted over those active subcarriers that are defined by p_1 is operated.

3.1.1 | Effective SNR statistics of the first portion of Bob's data

In this part of the paper, analytical SNR statistics of the first portion of Bob's data, p_1, that is responsible of defining the number of active subcarriers are evaluated. In order to be able to prove the applicability of the proposed scheme into such OFDM systems that contain higher number of subcarriers in each subblock, derivations are generalized for any number of subcarriers, N, instead of four subcarriers, which are mainly considered in the scenario of this paper. The conditional pair-wise power distribution function (PDF) expression is given as

$$P_{\gamma b_s p_1}(\gamma_{b_s}) = 2\frac{N-1}{N} Q_f(\sqrt{2Z\gamma_{b_s}}), \tag{30}$$

where $Z = 3/(N^2-1)$, $\gamma_{b_s} = \gamma_b \log_2(M)$, and $Q_f(.)$ is the Q function defined as

$$Q_f(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt. \tag{31}$$

It is also possible that the representation of this PDF can be done in an exponential distribution form. Distribution of the instantaneous SNR in the exponential form can be formulated as

$$P_{\gamma_{b_s} p_1}(\gamma_{b_s}) = 2\frac{N-1}{N\pi} \int_0^{\pi/2} \exp\left(-\frac{Z\overline{\gamma}_{b_s}}{\sin^2\phi}\right) d\phi. \tag{32}$$

3.1.2 | Statistics of the second portion of Bob's effective SNR

In the proposed ISS algorithm of OFDM-SNM, the effective fading channel distribution is not always the same. This is due to the fact that in the given data stream, the effective channels of OFDM-SNM to transmit one portion of the data are always decided randomly by the other portion of the data to exploit the number of active subcarriers for additional data transmission. Because of this reason, we used numerical data fitting methods to determine the amplitude and power distribution of the effective fading channels. In order to do this determination, we simulated 32 000 realizations generated from a standard Rayleigh distribution with zero mean and unity variance. After that, the proposed OFDM-SNM with ISS algorithm is applied to determine the optimal set of active subcarriers that are deployed to transmit Bob's data. As the last step, the most convenient fading amplitude and power distributions that will be used in the subchannels are detected by utilizing the fitting tools.

As a result of the simulation outputs of the fitting tools, the effective fading channel amplitude distribution of Bob for the proposed technique with the scale parameter u is determined as Nakagami as shown in Figure 6. Similarly, the effective fading channel distribution with the mean parameter $\psi \cong 1$ shown in Figure 7 is found to be Nakagami as well. PDF of the effective subchannel fading amplitude, where the $\alpha_b = ||H_{b_i}||$ for each subcarrier can be formulated as

$$P_{\alpha_{b_{p_2}}}(\alpha_b) = \left(\frac{1}{2u^2}\right) \frac{1}{\Gamma(\mu)} \alpha_b^{(2u-1)} \exp\left(-\frac{1}{2u^2}\alpha_b^2\right), \tag{33}$$

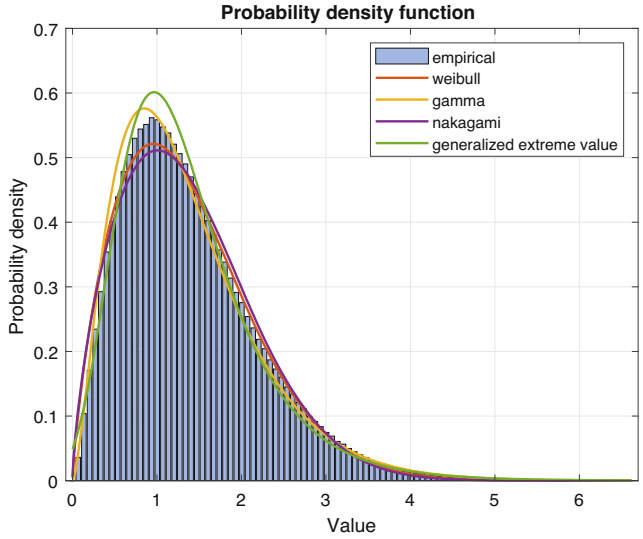

FIGURE 6 The amplitude distribution of the effective channels for Bob using the proposed technique with scale parameter $u = 0.576$

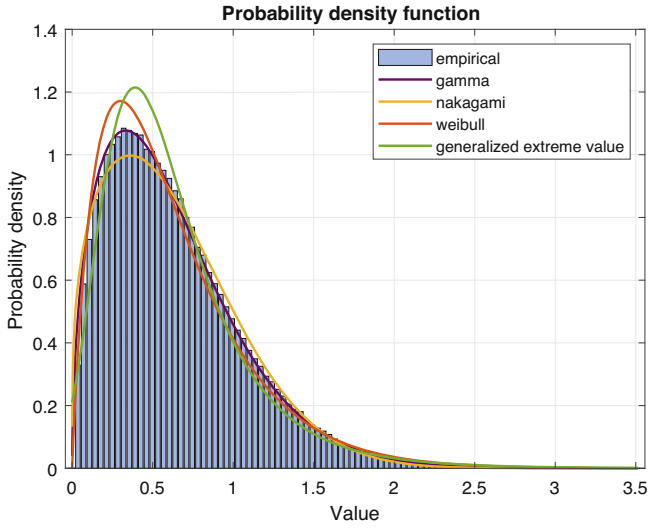

FIGURE 7 The power distribution of the effective channels for Bob using the proposed technique with scale parameter $u = 0.576$

where $\Gamma(\mu)$ is the Gamma function. Also Ω is considered to be the mean square of the subchannel fading amplitude of α_b where $\Omega_b = E\{\alpha_b^2\}$.

After this point, by substituting the effective instantaneous SNR of Bob, γ_{b_s}, in place of α_b the PDF function of the Bob can be determined as

$$P_{\gamma b_s p_2}(\gamma_{b_s}) = \frac{P_{\alpha_b}\left(\sqrt{\frac{\Omega_b \gamma_{b_s}}{\overline{\gamma}_{b_s}}}\right)}{\frac{1}{u^2}\sqrt{\frac{\gamma_{b_s}\overline{\gamma}_{b_s}}{\Omega_b}}}. \tag{34}$$

It should be noted that the scale parameter in the proposed scheme is not always constant. The reason for this is that the fading distribution of the effective subchannels are defined by the number of subcarriers which is mapped by the incoming data stream of Bob. In the transmission environment that is considered in this paper, the possible scale

parameter and mean square values for Bob are defined for each number of active subcarriers, respectively, as

$$K = 1 \Rightarrow u = 0.561, \quad \Omega_b \approx 1, \tag{35}$$

$$K = 2 \Rightarrow u = 0.623, \quad \Omega_b \approx 1, \tag{36}$$

$$K = 3 \Rightarrow u = 0.760, \quad \Omega_b \approx 1, \tag{37}$$

$$K = 4 \Rightarrow u = 0.937, \quad \Omega_b \approx 1. \tag{38}$$

It should also be noted that it is possible to represent the approximated PDF of the effective SNR in an exponential distribution form. For a spatial case where only one subcarrier is active for the transmission and the scale parameter $u = 0.576$ in Nakagami distribution, the distribution of the instantaneous SNR can be formulated as

$$P_{\gamma_{b_s p_2}}(\gamma_{b_s}) \approx \left(\frac{1}{2u^2}\right) \frac{1}{\Gamma(\mu)} \frac{\Omega_b^{\frac{3}{2}} \sqrt{\gamma_{b_s}}}{\frac{1}{u} \overline{\gamma}_{b_s}^{\frac{3}{2}}} \exp\left(-\frac{1}{2u^2} \frac{\Omega_b \gamma_{b_s}}{\overline{\gamma}_{b_s}}\right). \tag{39}$$

3.2 | Statistics of Eve's effective SNR

The PDF of the Eve is not expected to be same as the Bob's PDF. The reason behind this is the fact that the subcarriers that are activated to convey data to Bob are selected by their subchannels that can offer the strongest channel amplitude. However, this is not the case for the Eve since the subcarriers that can provide the strongest set of subchannels to Bob correspond to a random set of subcarriers with respect to Eve. For this reason, the channel distribution of Eve is considered to be same as the original Rayleigh distribution. Simulation results that are obtained from the fitting tools confirm that this assumption is accurate and show the effective amplitude distribution of Eve's subchannel is Rayleigh with scale factor β as shown in Figure 8. Moreover, the effective power distribution of Eve with mean factor $\psi \cong 1$ is given in Figure 9. The mathematical expression of amplitude subchannel distribution can be given as

$$P_{\alpha_e}(\alpha_e) = \frac{\alpha_e}{\beta^2} \exp\left(-\frac{\alpha_e^2}{2\beta^2}\right), \tag{40}$$

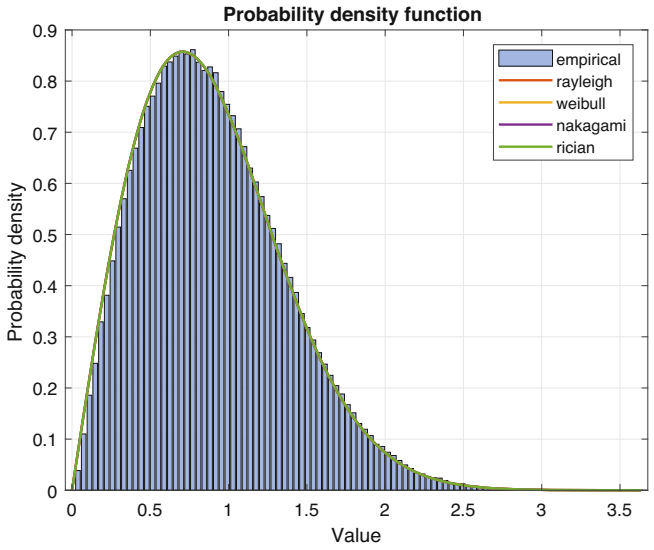

FIGURE 8 The amplitude distribution of the effective channels for Eve using the proposed technique with scale parameter $\beta = 0.71$

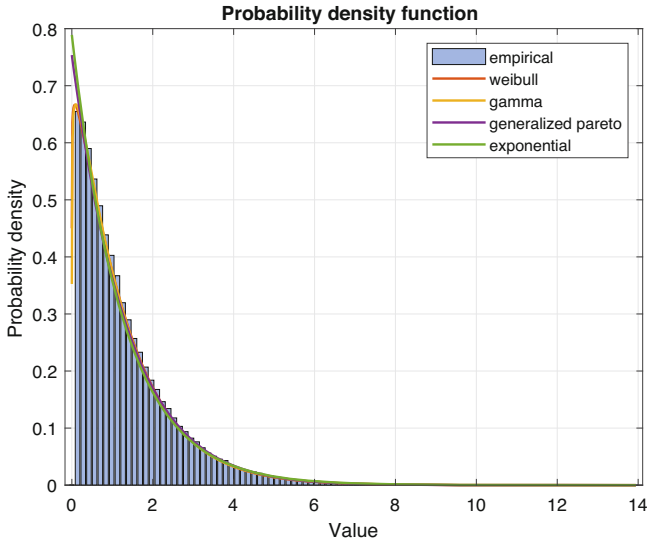

FIGURE 9 The power distribution of the effective channels for Eve using the proposed technique with scale parameter $\beta = 0.71$

In the proposed ISS algorithm, subcarriers are randomly selected for the Eve since the activation of these subcarriers are solely dependent on Bob's data. Therefore, the scale parameter of Eve, β, is not stable and it varies for different subcarrier activation cases, whereas the mean square value of $\alpha_e = ||H_{b_e}||$ where $\Omega_e = E\{\alpha_e^2\}$ is considered to be equal ψ. The distribution parameters for different subcarrier activation cases of Eve that are adopted in this paper are approximated as follows.

$$K = 1 \Rightarrow \beta = 0.710, \quad \Omega_e \approx 1, \tag{41}$$

$$K = 2 \Rightarrow \beta = 1.000, \quad \Omega_e \approx 1, \tag{42}$$

$$K = 3 \Rightarrow \beta = 1.230, \quad \Omega_e \approx 1, \tag{43}$$

$$K = 4 \Rightarrow \beta = 1.420, \quad \Omega_e \approx 1. \tag{44}$$

In the next step, the PDF function of Eve can be obtained by substituting the effective instantaneous SNR of Eve γ_e in place of α_e. Regarding PDF function can be formulated as

$$P_{\gamma_{e_s}}(\gamma_{e_s}) = \frac{P_{\alpha_e}\left(\sqrt{\frac{\Omega_e \gamma_{e_s}}{\overline{\gamma}_{e_s}}}\right)}{\frac{1}{\beta^2}\sqrt{\frac{\gamma_{e_s}\overline{\gamma}_{e_s}}{\Omega_e}}}, \tag{45}$$

where $\gamma_{e_s} = \gamma_e \log_2(M)$.

The approximated PDF of the Eve's effective SNR can also be written in exponential distribution form. For an example case where the number of active subcarriers is one, $K = 1$, $P_{\gamma_{e_s}}(\gamma_{e_s})$ can be written in exponential form as

$$P_{\gamma_{e_s}}(\gamma_{e_s}) = \left(\frac{1}{\Omega_e \overline{\gamma}_{e_s}}\right) \exp\left(\frac{\gamma_{e_s}}{\Omega_e \overline{\gamma}_{e_s}}\right). \tag{46}$$

By using the distribution functions that are calculated in (39) and (46) now it is possible to evaluate and analyze the BER performance, and examine the advantages of the proposed scheme.

3.3 | Average symbol error rate of Bob

Calculation of the symbol error rate (SER) of Bob is not as easy as the conventional OFDM to apply. The reason for this is that there are two different estimations that is needed to be clarified. The first estimation is the determination of the number of subcarriers that are selected for the transmission of Bob's data. The second one is the estimation of the transmitted symbol of Bob. Even though these two processes are considered to be independent from each other this assumption is not applicable in most of the times because of the fact that in most of the cases the correlated channel paths lead these two estimations to be dependent to each other.

Detection of the Bob's transmitted data can be successfully operated only in those cases where both of the estimations are correct. In order to investigate the probability of both these estimations to be simultaneously correct, let A_1 and A_2 to represent the first and second estimation processes, respectively. Since the first portion of the data stream of Bob that is responsible of defining the number of active subcarriers, p_1, and the second portion of the data stream of Bob, p_2, that is modulated by one of the i-ary modulation orders to be sent over these active subcarriers that are defined by p_1 are not equal in length, because of the fact that their lengths are dependent on different parameters such as number of subcarriers in each subblock and the modulation order of the transmission, it is not possible to generalize certain values for these possibilities. However, for the case that is adopted in this paper where the number of subcarriers in each subblock is four ($N = 4$) and the modulation order for the transmission of p_2 is selected as BPSK ($M = 2$), the correct estimation probabilities of A_1 and A_2 can be represented as $P(A_1) = 2/3$ and $P(A_2) = 1/3$. After this point, by setting $P_{\mathrm{SNM}}(E)$ as the error probability of $A1$ (ie, the subcarrier pattern activity) and $P_{\mathrm{BPSK}}(E)$ as the error probability for $A2$ (ie, the BPSK symbol recovery) at the receiver side, the overall error probability $P_T(E)$ can be formulated as

$$P_{\mathrm{T}}(E) = P_{\mathrm{T}}(E|A_1)P(A_1) + P_{\mathrm{T}}(E|A_2)P(A_2), \tag{47}$$

$$P_{\mathrm{T}}(E) = \frac{2}{3}P_{\mathrm{SNM}}(E) + \frac{1}{2}P_{\mathrm{BPSK}}(E). \tag{48}$$

In the following two subsections, the error probability of each estimation process is considered separately for a more realistic investigation.

3.4 | SER analysis of the active subcarriers that transmit Bob's data

By formulating the PDF of the first portion of the Bob's data, p_1, as shown in (30), the analytical error rate evaluation of the symbols that define the number of active subcarriers for the transmission of the second portion of the Bob's data is now possible. This evaluation can be presented by the following formulation for any number of subcarriers in each subblock.

$$\mathrm{SER}_{b_{p_1}} = \int_0^\infty P_{\gamma_{b_{p_1}}}(\gamma_b)\, d_{\gamma_b}. \tag{49}$$

By substituting the value of $P_{\gamma_{b_{p_1}}}(\gamma_b)$ in (49), the result turns into

$$\mathrm{SER}_{b_{p_1}} = \int_0^\infty 2\frac{N-1}{N} Q_f(\sqrt{2Z\gamma_b}) d_{\gamma_b}. \tag{50}$$

By integrating (50), the resulting formula can be presented as

$$\mathrm{SER}_{b_{p_1}} = \frac{N-1}{N}\left(1 - \sqrt{\frac{Z\overline{\gamma}_b}{1+Z\overline{\gamma}_b}}\right). \tag{51}$$

3.5 | SER analysis of the transmitted symbol of Bob's data

Formulating the PDF of the second portion of the Bob's data, p_2, enables the analytical SER evaluation of the conventionally transmitted data Bob under the proposed OFDM-SNM-ISS scheme. This evaluation is in analysed in both BPSK (ie, $M = 2$) and higher modulation orders such as QPSK and $M-$ary QAM (ie, $M = 4, 8, \ldots$).

BER analysis of Bob's data portion that is conventionally modulated by BPSK modulation ($M = 2$) where $\gamma_{b_s} = \gamma_b \log_2 2 = \gamma_b$ is given as follows.

$$\mathrm{BER}_{b_{p_2}} = \frac{1}{2}\int_0^{\infty} \mathrm{erfc}\left(\sqrt{\gamma_b}\right) P_{\gamma_{b_{p_2}}}(\gamma_b)\, d_{\gamma_b}, \tag{52}$$

where erfc(.) is the error function. By substituting the corresponding value of $P_{\gamma_{b_{p_2}}}(\gamma_b)$ into (52), the obtained integration becomes

$$\mathrm{BER}_{b_{p_2}} = \frac{1}{2}\int_0^{\infty} \mathrm{erfc}\left(\sqrt{\gamma_b}\right) \frac{1}{2u^2}\frac{1}{\Gamma(\mu)}\frac{\Omega_b^{\frac{3}{2}}\sqrt{\gamma_b}}{\frac{1}{u}\overline{\gamma}_b^{\frac{3}{2}}} \times \exp\left(-\frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\overline{\gamma}_b}\right) d\gamma_b, \tag{53}$$

$$\mathrm{BER}_{b_{p_2}} = \frac{1}{2}\frac{1}{2u^2}\frac{1}{\Gamma(\mu)}\frac{\Omega_b^{\frac{3}{2}}}{\frac{1}{u}\overline{\gamma}_b^{\frac{3}{2}}}\int_0^{\infty} \mathrm{erfc}\left(\sqrt{\gamma_b}\right) \sqrt{\gamma_b} \times \exp\left(-\frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\overline{\gamma}_b}\right) d\gamma_b. \tag{54}$$

The integral in (54) can be solved by introducing the variables $G = \frac{1}{2}\frac{1}{2u^2}\frac{1}{\Gamma(\mu)}\frac{\Omega_b^{\frac{3}{2}}}{\frac{1}{u}\overline{\gamma}_b^{\frac{3}{2}}}$ and $\rho = \frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\overline{\gamma}_b}$ for simplicity. The resulting solution of the integral is given as

$$\mathrm{BER}_{b_{p_2}} \approx \frac{G}{2\sqrt{\pi}}\left(\frac{\arctan(\sqrt{\rho})}{2\rho^{\frac{3}{2}}} - \frac{1}{2\rho(1+\rho)}\right), \tag{55}$$

where arctan(.) is the inverse of tangent.

In the following, the error rate analysis is done for higher modulation orders such as QPSK and M-ary QAM. The closed form SER derivation for M-ary QAM in Nakagami distribution is provided as[39]

$$\mathrm{SER}_{b_{p_2}} = \frac{4\left(1-\frac{1}{\sqrt{M}}\right)}{\pi}\int_0^{\pi/2} \exp\left(-\frac{\frac{1.5}{M-1}\gamma_{b_s}}{\sin^2\phi}\right) d\phi - \frac{4\left(1-\frac{1}{\sqrt{M}}\right)^2}{\pi}\int_0^{\pi/4} \exp\left(-\frac{\frac{1.5}{M-1}\gamma_{b_s}}{\sin^2\phi}\right) d\phi. \tag{56}$$

3.6 | SER analysis of the transmitted symbol of Eve's data

As it is stated in the previous sections, subcarrier activations in the proposed scheme are dependent on the Bob's data, and these activations are made in a descending order (ie, from the subcarriers that have higher channel amplitude to lower channel amplitude). For this reason, subcarrier activations of Eve's transmission is randomly operated and the PDF of the instantaneous SNR of Eve is considered to be Rayleigh, which leads the SER performance of Eve under the proposed scheme to be same as the original OFDM. Under these circumstances, the BER performance of Eve under BPSK modulation ($M = 2$) where $\gamma_{e_s} = \gamma_e \log_2 2 = \gamma_e$ can be given as

$$\mathrm{BER}_e = \frac{1}{2}\int_0^{\infty} \mathrm{erfc}(\sqrt{\gamma_e}) P_{\gamma_e}(\gamma_e) d\gamma_e. \tag{57}$$

By substituting the corresponding PDF expression of the effective instantaneous SNR of Eve, (46), into (58), the acquired integration formula becomes

$$\mathrm{BER}_e = \frac{1}{2}\int_0^{\infty} \mathrm{erfc}(\sqrt{\gamma_e})\left(\frac{1}{\Omega_e\overline{\gamma}_e}\right)\exp\left(\frac{\gamma_e}{\Omega_e\overline{\gamma}_e}\right) d\gamma_e. \tag{58}$$

TABLE 2 Simulation parameters

Modulation type (M)	BPSK, QPSK, 8-QAM
Channel type	Rayleigh
IFFT/FFT size (N_F)	64
CP guard interval (samples)	9
Number of subblocks in each OFDM symbol (G)	16
Number of available subcarriers in each subblock (N)	4
Number of bits mapped to each subblock (p_1)	2
Multipath channel delay samples locations	[0 3 5 6 8]
Multipath channel tap power profile (dBm)	[0 -8 -17 -21 -25]
Channel length (L)	9

Abbreviations: CP, cyclic prefix; OFDM, orthogonal frequency division multiplexing.

To obtain the closed-form expression for Eve's BER, the above integral can be solved and its final solution can be presented as

$$\mathrm{BER}_e = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_e}{1+\bar{\gamma}_e}}\right). \tag{59}$$

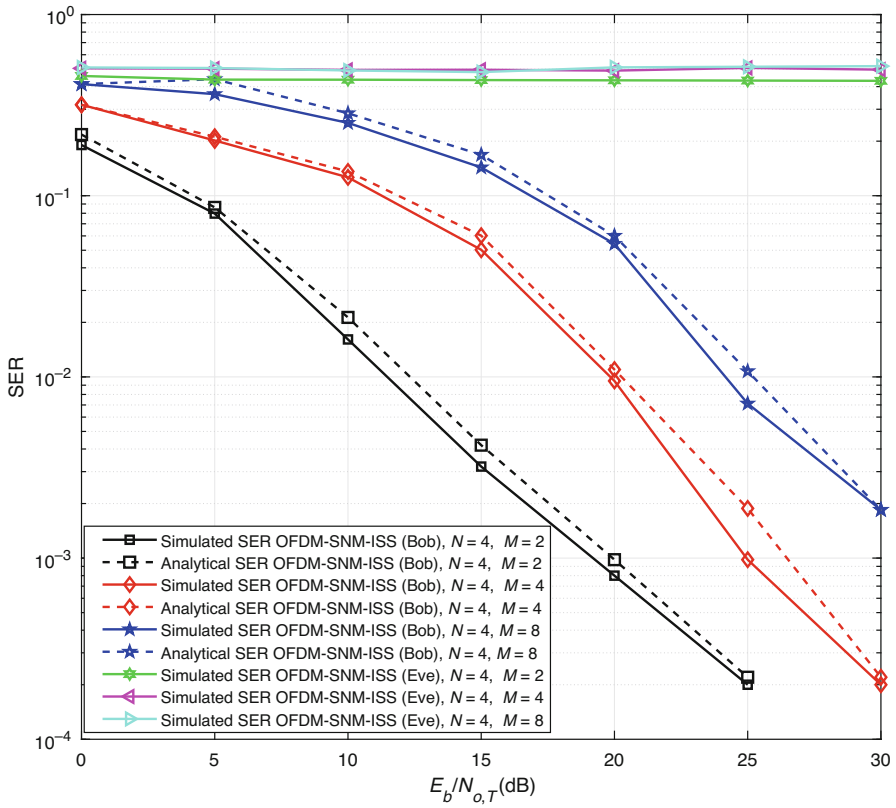

FIGURE 10 Simulation and analytical symbol error rate performances of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation scheme under different M-ary modulation orders for both Bob and Eve

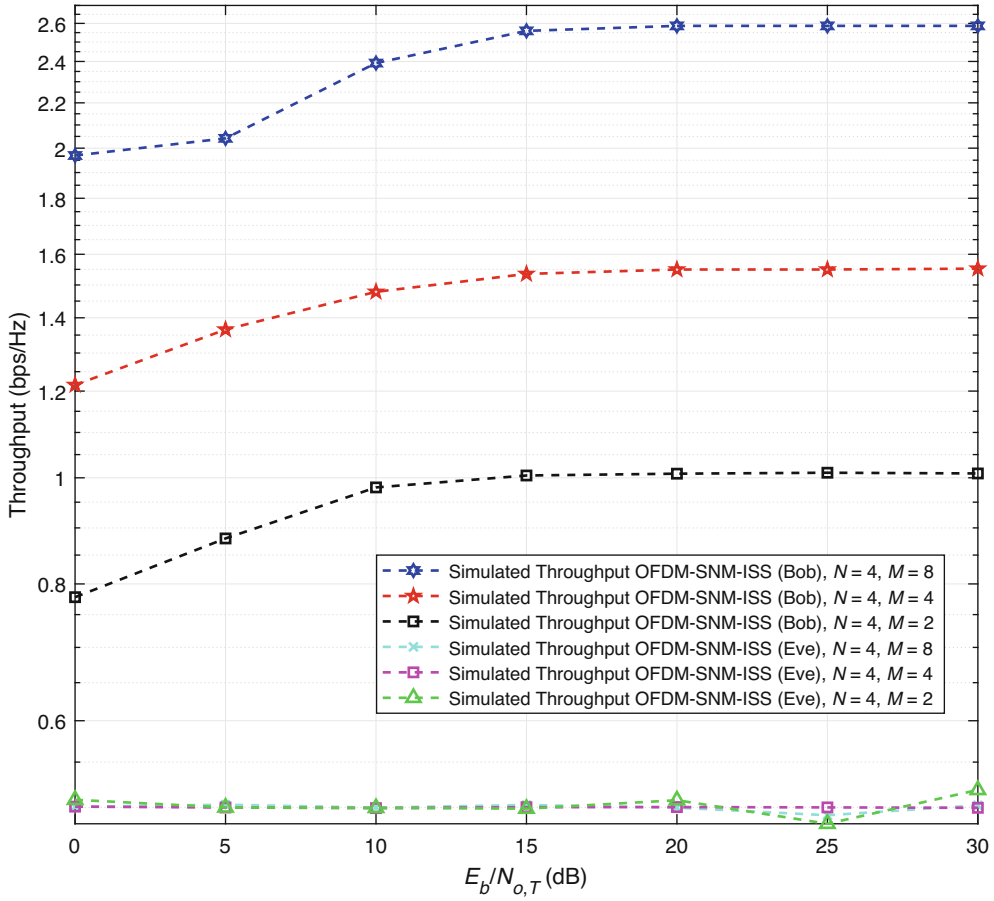

FIGURE 11 Simulation results of the throughput of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation scheme under different M-ary modulation orders for both Bob and Eve

For the transmission of Bob's data to Eve in higher modulation orders, Equation (49) can be adopted from Reference 40 as the closed-form expression of Eve's M-QAM SER derivation over Rayleigh fading channel, which is given as

$$\mathrm{SER}_e = 2\left(\frac{\sqrt{M}-1}{\sqrt{M}}\right)\left(1-\sqrt{\frac{1.5\overline{\gamma}_{e_s}}{M-1+1.5\overline{\gamma}_{e_s}}}\right)-\left(\frac{\sqrt{M}-1}{\sqrt{M}}\right)^2 \times\left[1-\sqrt{\frac{1.5\overline{\gamma}_{e_s}}{M-1+1.5\overline{\gamma}_{e_s}}}\left(\frac{4}{\pi}\arctan\left(\sqrt{\frac{M-1+1.5\overline{\gamma}_{e_s}}{1.5\overline{\gamma}_{e_s}}}\right)\right)\right]. \tag{60}$$

It should be stated that the above derived formulas for the both BER and SER analysis of Eve are only applicable for those cases where the transmitted data, which is empowered by the artificial interference signal matches with the Eve's CSI. However, since the artificial interference signal that is appended on the transmitted data is specifically designed according to Bob's channel, and the adaptive interleaver that activates the subcarriers that transmit Bob's data cannot be reached by Eve, her performance will not be the same as (59) and (60). In fact, performance of Eve will be dramatically decreased due to the fact that she cant have an access to the artificial interference signal vector of Bob.

3.7 | Secrecy capacity

In this section, secrecy capacity of the proposed ISS algorithm is investigated. In order to do this, such a transmission environment where Alice transmits data to Bob over a standard additive white Gaussian noise (AWGN) with zero mean

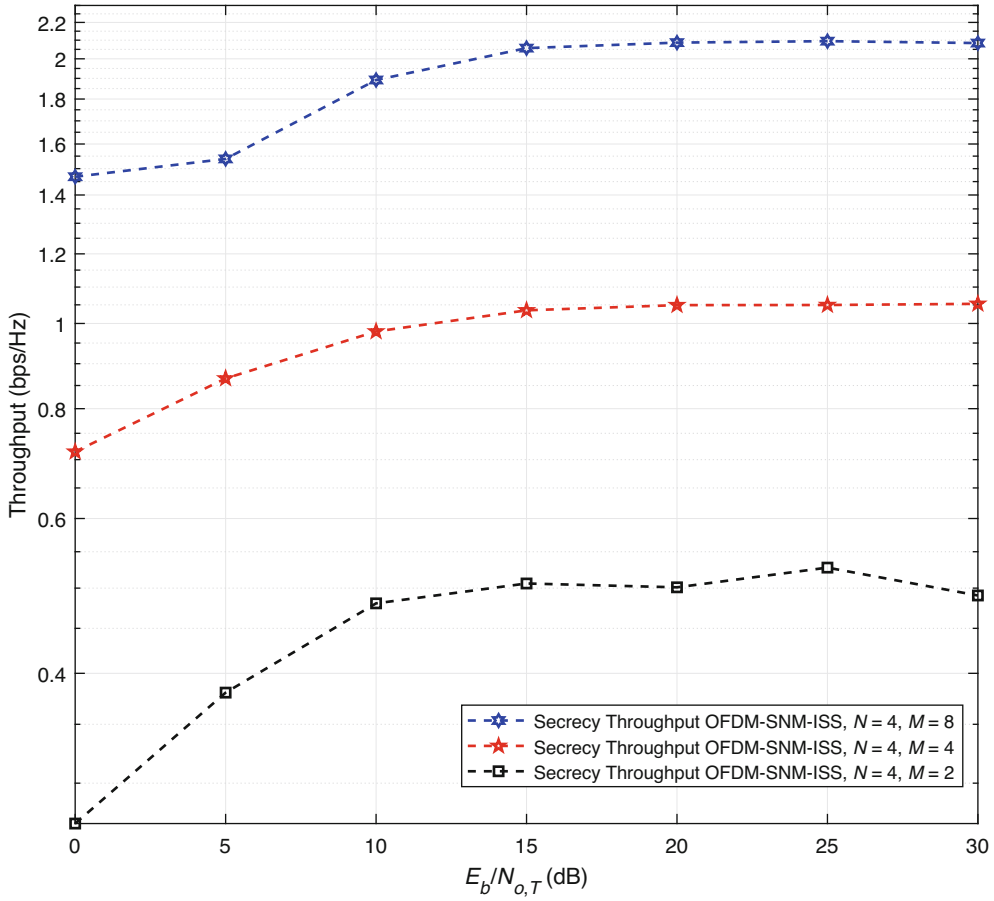

FIGURE 12 Secrecy throughput of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation scheme under different M-ary modulation orders

and unity variance is considered under the existence of an eavesdropper, Eve, where her receiver has lower SNR than Bob's (ie, $||H_{i_b}|| > ||H_{i_i}||$). For this setup the secrecy capacity of the proposed ISS algorithm supported OFDM-SNM scheme can be given as[4]

$$C_s = C_b - C_e, \tag{61}$$

where

$$C_b = \frac{1}{2}\log_2(1+\gamma_b), \tag{62}$$

is the expression of the capacity of Bob's channel and

$$C_e = \frac{1}{2}\log_2(1+\gamma_e), \tag{63}$$

represents the capacity of Bob's channel.

Because of the fact that in each usage of complex AWGN channel the total number of real AWGN channel usage is two, C_b and C_e can also be represented as follows

$$C_b = \log_2(1+\gamma_b), \tag{64}$$

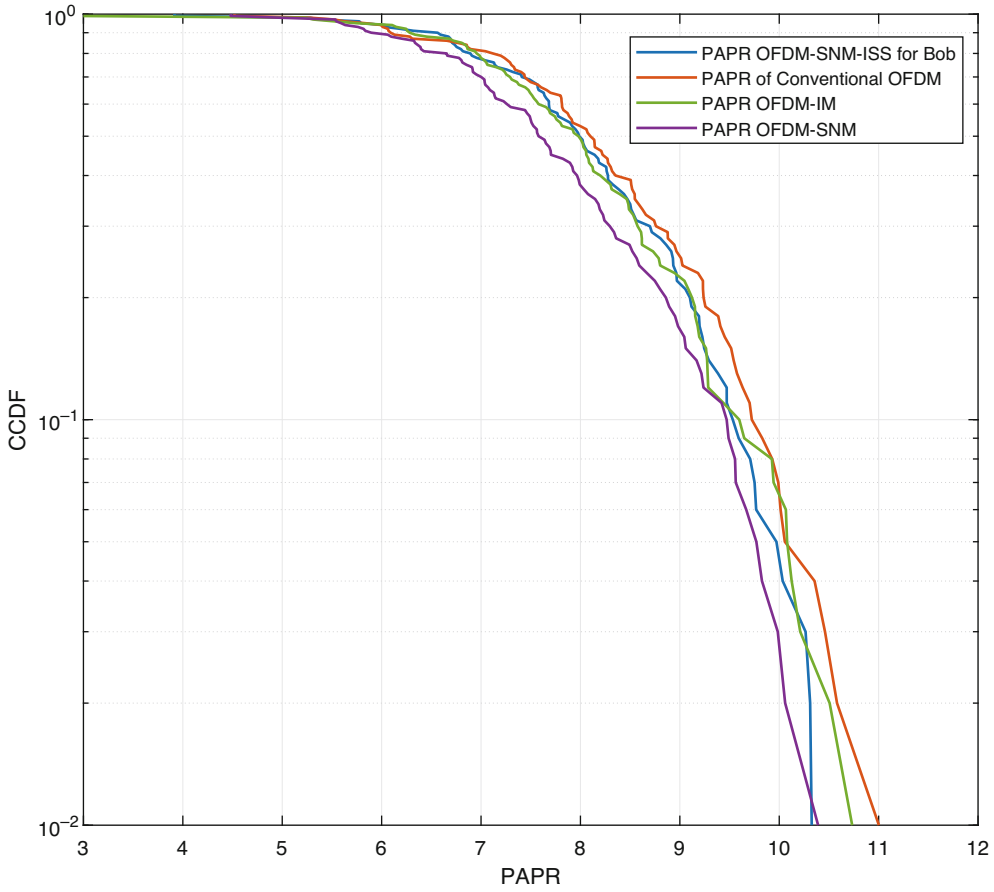

FIGURE 13 Peak to average power ratio (PAPR) performance of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation scheme for Bob and its comparison with the PAPR of the other competitive schemes in the literature

and

$$C_e = \log_2(1 + \gamma_e). \tag{65}$$

By deploying these values given in (64) and (65) in (61), secrecy capacity formulation of the proposed scheme can be finalized as

$$C_s = \begin{cases} \log_2(1 + \gamma_b) - \log_2(1 + \gamma_e), & \gamma_b > \gamma_e \\ 0, & \gamma_b \leq \gamma_e. \end{cases} \tag{66}$$

3.8 | Secrecy outage performance

In this section, the secrecy outage probability of the ISS algorithm supported OFDM-SNM scheme is analytically investigated. The secrecy outage probability can be mathematically expressed as

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(C_s < R_s), \tag{67}$$

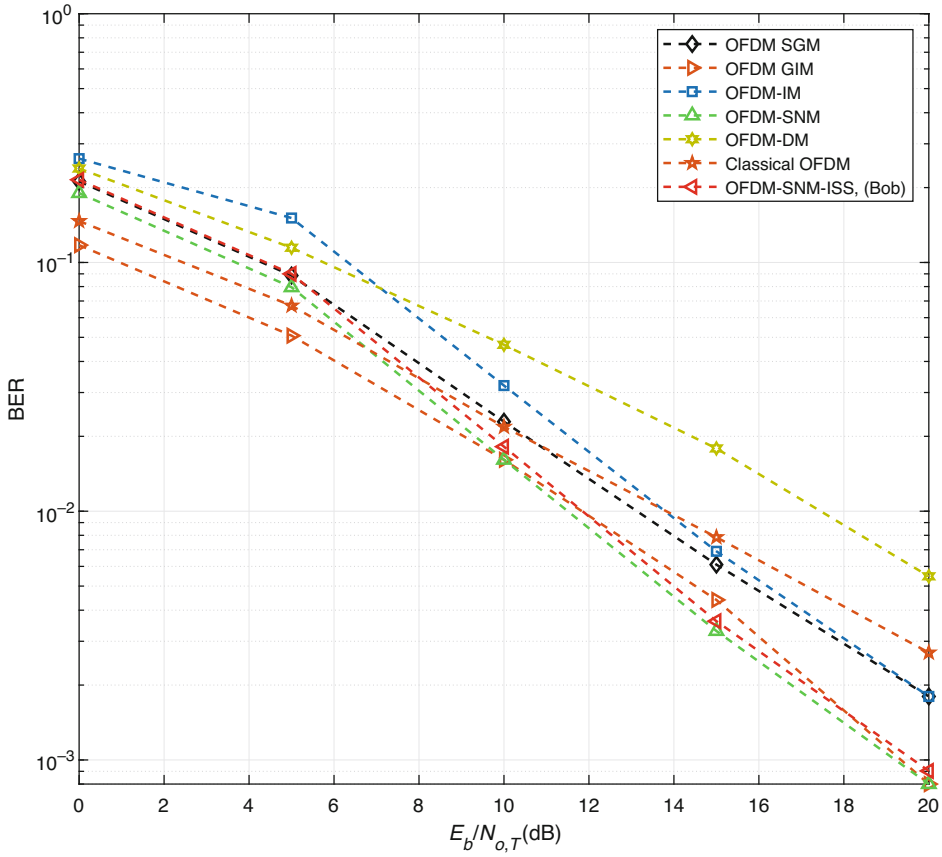

FIGURE 14 Bit error rate comparison of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation for Bob's data with its competitors in the literature

where $R_s > 0$ represents the targeted secrecy rate and desired to be bigger than the instantaneous secrecy capacity, C_s. Secrecy outage probability can be further expressed as[9]

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(C_s < R_s|\gamma_b > \gamma_e)\mathcal{P}(\gamma_b > \gamma_e) + \mathcal{P}(C_s < R_s|\gamma_b \leq \gamma_e)\mathcal{P}(\gamma_b \leq \gamma_e). \tag{68}$$

Since $R_s > 0$, the case where $\gamma_b \leq \gamma_b$, $\mathcal{P}(C_s < R_s|\gamma_b \leq \gamma_e)$ is always considered to be unity, that is, 1. Thus, (68) can be simplified as

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(C_s < R_s|\gamma_b > \gamma_e)\mathcal{P}(\gamma_b > \gamma_e) + \mathcal{P}(\gamma_b \leq \gamma_e). \tag{69}$$

The probability of the case where $\gamma_b > \gamma_e$ can be calculated as

$$\mathcal{P}(C_s > 0) = \mathcal{P}(\gamma_b > \gamma_e) = \int_0^\infty \int_0^\infty P(\gamma_b, \gamma_e) d\gamma_e d\gamma_b, \tag{70}$$

$$\mathcal{P}(C_s > 0) = \mathcal{P}(\gamma_b > \gamma_e) = \int_0^\infty \int_0^{\gamma_b} P_{\gamma_b}(\gamma_b) P_{\gamma_e}(\gamma_e) d\gamma_e d\gamma_b, \tag{71}$$

$$\mathcal{P}(C_s > 0) = \mathcal{P}(\gamma_b > \gamma_e) = \frac{\overline{\gamma}_b}{\overline{\gamma}_b + \overline{\gamma}_e}. \tag{72}$$

The probability of the case where $\gamma_b \leq \gamma_e$ can be calculated by subtracting the probability of $\gamma_b > \gamma_e$ from all the possible cases given as

$$\mathcal{P}(\gamma_b \leq \gamma_e) = 1 - \mathcal{P}(\gamma_b > \gamma_e), \tag{73}$$

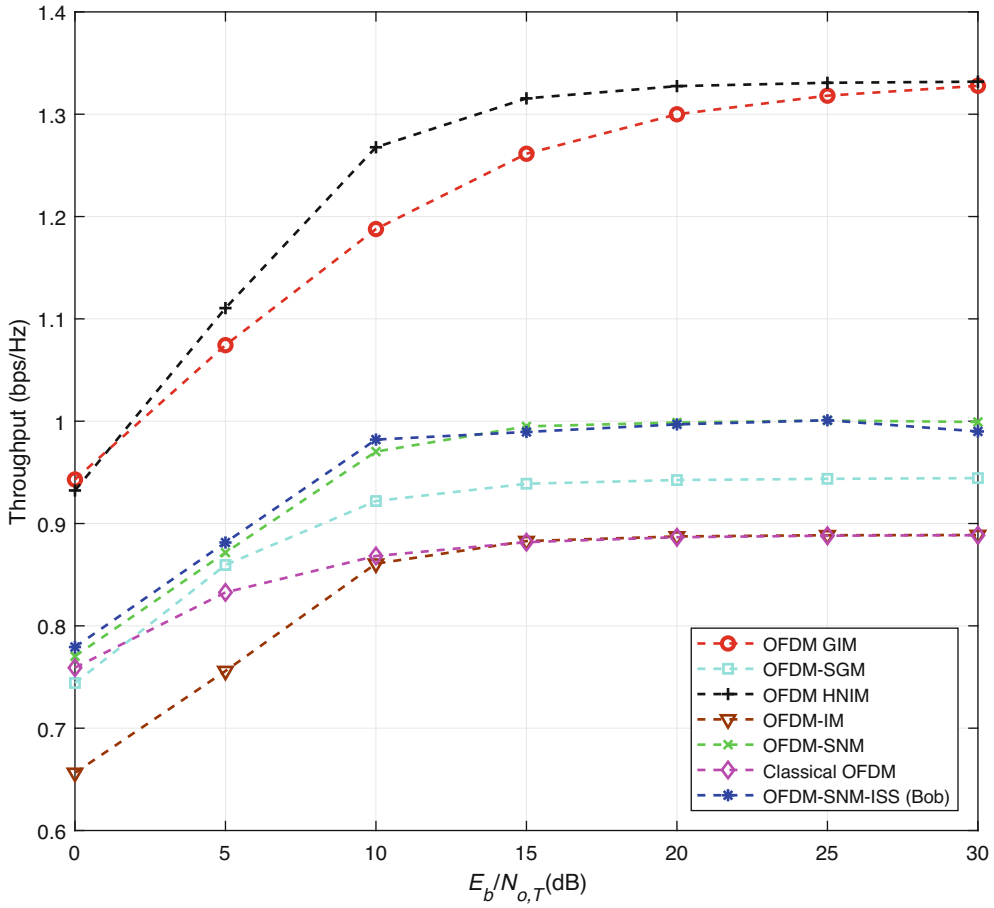

FIGURE 15 Throughput comparison between proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing (OFDM) with subcarrier number modulation with other competitive OFDM schemes under BPSK modulation

$$\mathcal{P}(\gamma_b \leq \gamma_e) = \frac{\overline{\gamma}_e}{\overline{\gamma}_b + \overline{\gamma}_e}. \tag{74}$$

Lastly, the first term of (69) can be given as[4]

$$1 - \frac{\overline{\gamma}_b + \overline{\gamma}_e}{\overline{\gamma}_b + 2^{R_s}\overline{\gamma}_e} \exp\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_b}\right). \tag{75}$$

By substituting (72), (74), and (75) into (69), the resulting secrecy outage probability can be determined as

$$\mathcal{P}_{\text{out}}(R_s) = 1 - \frac{\overline{\gamma}_b}{\overline{\gamma}_b + 2^{R_s}\overline{\gamma}_e} \exp\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_b}\right). \tag{76}$$

4 | SIMULATION RESULTS

In this section, performance metrics of the proposed ISS algorithm supported OFDM-SNM scheme is analyzed in terms of BER, SER, throughput, peak to average power ratio (PAPR), and secrecy outage probability, and power spectral density. Also the metrics of the proposed scheme are compared with the other competitive schemes in the literature. Simulation parameters of the proposed scheme are given in Table 2.

As it can be observed from Table 2, channel type that is used for the transmission of the data between Alice and Bob under the existence of Eve is considered to be Rayleigh with equal length ($L = 9$). The IFFT/FFT size of Bob and Eve's

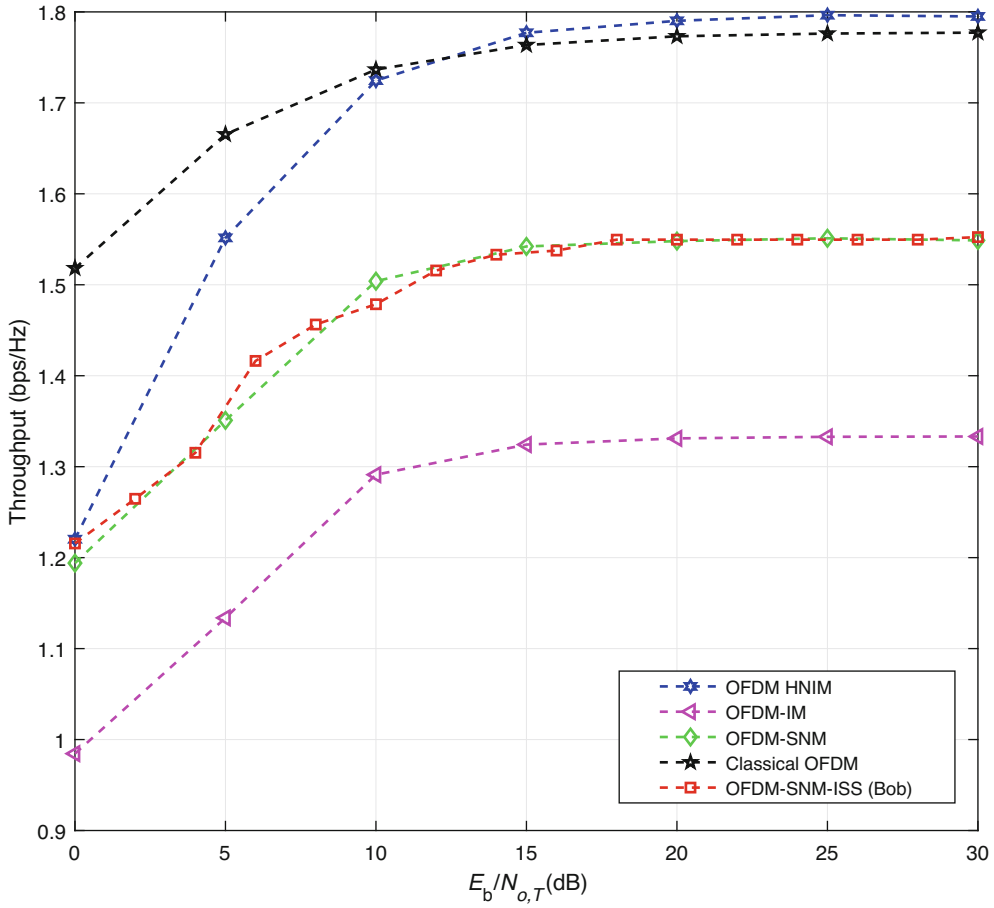

FIGURE 16 Throughput comparison between proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing (OFDM) with subcarrier number modulation with other competitive OFDM schemes under QPSK modulation

receivers are defined as 64, and in order to mitigate the intersymbol interference (ISI), a CP with length of 9 is appended. Moreover, simulated results are generated for both BPSK and higher modulation orders such as QPSK, and 8-QAM.

Figure 10 shows the simulation and analytical BER performances of the proposed ISS algorithm supported OFDM-SNM scheme under different M-ary modulation orders for both Bob and Eve. In this figure while the straight lines represent the simulation outputs, dashed lines represent the theoretically analyzed results for different M-ary modulation orders. It can be inferred from Figure 10 that while the Bob's BER results get better values in each increment of the SNR value, $E_b/N_{o,T}$, Eve's BER performance follows a straight line without any curve at any SNR value. This is due to the fact that while the additive artificial interference signal that is specifically created for Bob's effective channels can be successfully differentiated at the transmitter for the transmission of Bob's data, the differentiation of this artificial interference signal cannot be canceled for the transmission of Eve since the CSI of Eve does not match with the noise vector $\mathbf{n_G}$, which leads the received signal at the Eve's receiver to be a meaningless, corrupted data.

Figure 11 shows the simulated throughput performances of Bob and Eve under different M-ary modulation orders. As it can be observed from the figure, while the throughput performances of Bob under different M-ary modulation orders, black dashed line for BPSK ($M = 2$), red dashed line for QPSK ($M = 4$), and blue dashed line for 8-QAM ($M = 8$), get better values for each increment of SNR, the throughput performances of Eve for different M-ary modulation orders does not change and follows a low path at 0.5 level for any SNR value for both M-ary modulation orders, green dashed line for BPSK ($M = 2$), yellow dashed line for QPSK ($M = 4$), and cyan dashed line for 8-QAM ($M = 8$), that are presented in Figure 11.

Figure 12 represents the secrecy throughput of the proposed ISS algorithm under different M-ary modulation orders. When Figure 12 is compared with Figure 11, it can be seen that the difference between the throughput of Bob and the provided secrecy throughput is not significantly large, which proves the robustness of the proposed scheme against eavesdroppers.

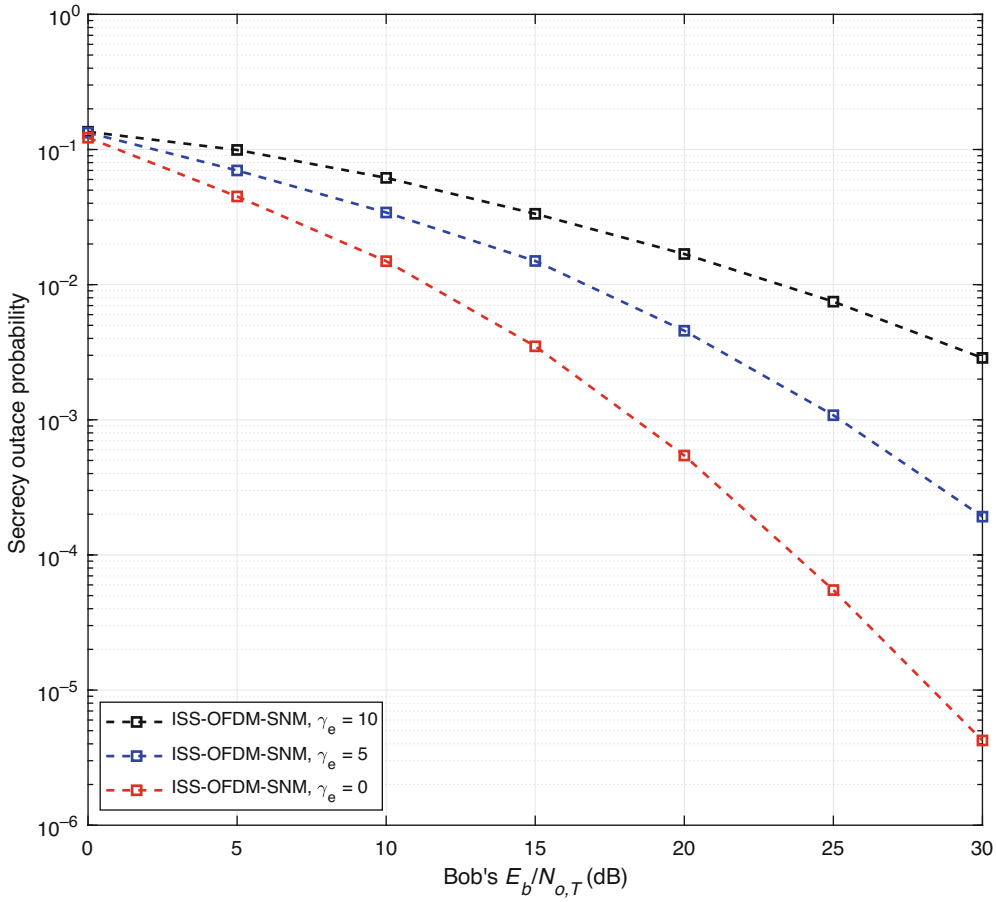

FIGURE 17 Secrecy outage probability of the proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing with subcarrier number modulation for $\gamma_e = 0$, 5, and 10 dB while $R_s = 1$

Another important notion that must be investigated along with the SER and throughput in determining the performance is the PAPR of the proposed scheme. For this reason, the PAPR performance of the proposed scheme for Bob is shown and compared with its competitor schemes in the literature as given in Figure 13. As it can be observed from this figure, while the performance of the proposed scheme, depicted in purple line, exceeds the performance of the classical OFDM, and OFDM-IM, depicted in orange line and green line, respectively, it also shows similar characteristics with plain OFDM-SNM, which is shown in blue line. Thus, Figure 13 proves the fact that the additional artificial interference signal does not create a disadvantage in terms of the PAPR performance during the transmission of Bob's data.

It is also important to compare the BER performance of the proposed scheme with its other competitors to be able to observe the effects of the artificial interference signal on Bob's data and make an inference whether the artificial interference signal ruins Bob's data, even it is a slightly degradation in BER, as well as Eve's data. In order to make this comparison the BER vs $E_b/N_{o,T}$ performance for different modulation options of OFDM is shown in Figure 14. As it can be observed from Figure 14, the performance of the proposed ISS algorithm supported OFDM-SNM shown almost the same performance as the plain OFDM-SNM and it even exceeds the performance of the plain OFDM-SNM at the SNR level 25. It is also possible to observe that the performance of the proposed scheme shows superior performance than the classical OFDM and most of the other competitor transmission techniques that are paired with OFDM. With a simple interpretation from Figure 14, it can be inferred that the ISS algorithm that is applied on the OFDM-SNM scheme does not bring any disadvantage in terms of BER along with the perfect secrecy.

Figures 15 and 16 show the throughput performances of the proposed ISS algorithm supported OFDM-SNM scheme and their comparisons with the other competitive OFDM-based schemes under BPSK and QPSK, respectively. As it can be seen from Figure 15, throughput performance of the proposed scheme shows almost the same performance of the plain OFDM-SNM and it also outperforms the performance of classical OFDM as well as OFDM-IM and OFDM-SGM under BPSK conditions. Similarly in Figure 16, it can be observed that the performance of the proposed scheme shows similar

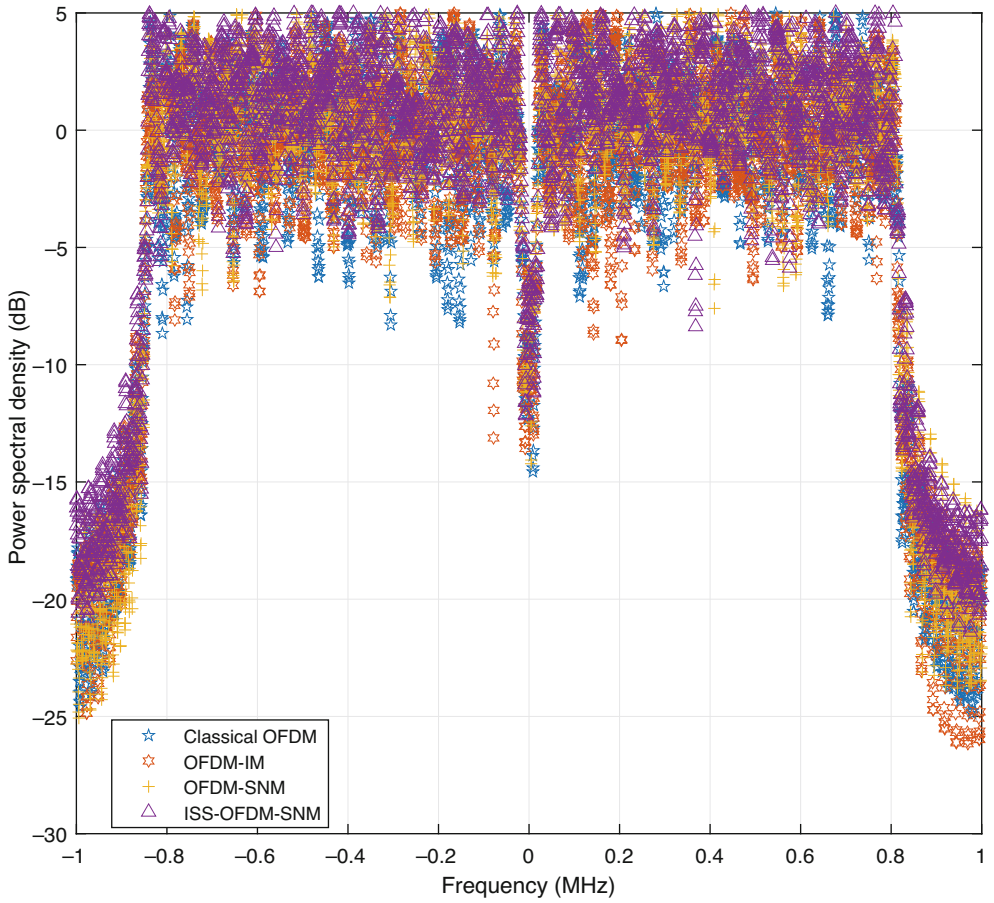

FIGURE 18 Power spectral density of the proposed proposed interference signal superposition algorithm supported orthogonal frequency division multiplexing (OFDM) with subcarrier number modulation scheme and its comparison with the featured competitive modulation options of OFDM

characteristics with the plain OFDM-SNM in terms of throughput under QPSK conditions. It is also possible to infer that the performance of the proposed scheme has the capability to outperform the throughput performance of its competitor scheme OFDM-IM. By depicting these two figures it can be proved that the proposed physical layer security algorithm does not have any effect on the throughput performance of the legitimate user's data and does not cause any degradation during the transmission.

Secrecy outage probability is another necessary parameter to be investigated in order to discover the merits of the proposed ISS algorithm supported OFDM-SNM scheme. For this reason, depiction of the secrecy outage probability of the proposed scheme is given in Figure 17 for different γ_e values, such as 0, 5, and 10, while the desired secrecy rate is defined unity (ie, $R_s = 1$). As it can be inferred from from the figure, as γ_e value decreases, a drastic improvement occurs in terms of secrecy outage probability of the proposed scheme as Bob's SNR value increases, which ensures the secrecy of Bob's data.

Figure 18 depicts the power spectral density of the proposed OFDM-SNM scheme that is supported by the ISS algorithm. As it can be observed from this figure, both classical OFDM, OFDM-IM, OFDM-SNM, and ISS-OFDM-SNM show similar performances in terms of power spectral density.

5 | CONCLUSION

In this paper, a novel ISS algorithm is applied to the OFDM-SNM scheme to abolish the security issue, which OFDM-SNM is not capable of overcoming this issue on its own. The fundamental idea to protect the data of the legitimate receiver relies on embedding an artificial interference signal that is specifically designed according to the legitimate receiver's CSI,

into the transmitted symbols. This creates such an environment that allows to OFDM-SNM system to send additional data by exploiting the number of subcarriers, while the secrecy of the transmitted data is substantially ensured against eavesdroppers. Analytical calculations and simulation results under different M-ary modulation orders prove that by applying such a security algorithm, OFDM-SNM scheme is led to be perfectly protected against external eavesdroppers without any degradation in terms of SER and throughput.

FUNDING INFORMATION

This research was partly funded by Scientific and Technological Research Council of Turkey (TUBITAK) under Grant/Award Number 119E392.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ENDNOTE

*Notation: Bold, lowercase, and capital letters are used for column vectors and matrices, respectively. ⊛ denotes a circular convolution operation.

ORCID

Muhammet Kırık https://orcid.org/0000-0003-2431-8075

REFERENCES

1. Shannon CE. Communication theory of secrecy systems. *Bell Syst Tech J*. 1949;28(4):656-715.
2. Prabhu VU, Rodrigues MR. On wireless channels with m-antenna eavesdroppers: characterization of the outage probability and ε-outage secrecy capacity. *IEEE Trans Inf Forens Secur*. 2011;6(3):853-860.
3. Bloch M, Barros J, Rodrigues MR, McLaughlin SW. Wireless information-theoretic security. *IEEE Trans Inf Theory*. 2008;54(6):2515-2534.
4. Barros J, Rodrigues MR. Secrecy capacity of wireless channels. Proceeding of the 2006 IEEE International Symposium on Information Theory; 2006:356-360.
5. Wyner AD. The wire-tap channel. *Bell Syst Tech J*. 1975;54(8):1355-1387.
6. Gopala PK, Lai L, El Gamal H. On the secrecy capacity of fading channels. *IEEE Trans Inf Theory*. 2008;54(10):4687-4698.
7. Csiszár I, Korner J. Broadcast channels with confidential messages. *IEEE Trans Inf Theory*. 1978;24(3):339-348.
8. Tekin E, Yener A. The gaussian multiple access wire-tap channel. *IEEE Trans Inf Theory*. 2008;54(12):5747-5755.
9. Mukherjee A, Fakoorian SAA, Huang J, Swindlehurst AL. Principles of physical layer security in multiuser wireless networks: a survey. *IEEE Commun Surv Tutor*. 2014;16(3):1550-1573.
10. Güvenkaya E, Hamamreh JM, Arslan H. On physical-layer concepts and metrics in secure signal transmission. *Phys Commun*. 2017;25:14-25.
11. Hamamreh JM, Basar E, Arslan H. Ofdm-subcarrier index selection for enhancing security and reliability of 5g URLLC services. *IEEE Access*. 2017;5:25 863-25 875.
12. Hamamreh JM, Guvenkaya E, Baykas T, Arslan H. A practical physical-layer security method for precoded ostbc-based systems. Proceedings of the 2016 IEEE Wireless Communications and Networking Conference; 2016:1-6; IEEE.
13. Sun L, Du Q. Physical layer security with its applications in 5g networks: a review. *China Commun*. 2017;14(12):1-14.
14. Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Di Renzo M. Safeguarding 5g wireless communication networks using physical layer security. *IEEE Commun Mag*. 2015;53(4):20-27.
15. Khan MF, Bhatti FA, Habib A. Analysis of macro user offloading to FEMTO cells for 5g cellular networks. Proceedings of the 2017 International Symposium on Wireless Systems and Networks (ISWSN); 2017:1-6; IEEE.
16. Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive mimo: an overview on passive eavesdropping and active attacks. *IEEE Commun Mag*. 2015;53(6):21-27.
17. Mesleh RY, Haas H, Sinanovic S, Ahn CW, Yun S. Spatial modulation. *IEEE Trans Veh Technol*. 2008;57(4):2228-2241.
18. Mesleh R, Haas H, Ahn CW, Yun S. Spatial modulation-a new low complexity spectral efficiency enhancing technique. Proceedings of the 2006 First International Conference on Communications and Networking in China; 2006:1-5; IEEE.
19. Basar E. Index modulation techniques for 5g wireless networks. *IEEE Commun Mag*. 2016;54(7):168-175.
20. Basar E, Wen M, Mesleh R, Di Renzo M, Xiao Y, Haas H. Index modulation techniques for next-generation wireless networks. *IEEE Access*. 2017;5:16 693-16 746.
21. Hamamreh JM, Kirik M, Sagman MO, Ishikawa N. Multiple input multiple output with antenna number modulation and adaptive antenna selection. *RS Open J Innovat Commun Technol*. 2020;1(1).

22. Kirik M, Hamamreh JM. Multiple mimo with antenna number modulation. Proceedings of the 2020 International Conference on UK-China Emerging Technologies (UCET); 2020:1-4; IEEE.
23. Karatepe S, Kirik M, Hamamreh JM. Novel nonorthogonal multi-access method for multi-user mimo with antenna number modulation. *RS Open J Innovat Commun Technol*. 2021;2(3):1-11.
24. Kirik M, Hamamreh JM. Multiple mimo with joint block antenna number modulation and adaptive antenna selection for future wireless systems. *RS Open J Innovat Commun Technol*. 2020;1(2):12.
25. Jaradat AM, Hamamreh JM, Arslan H. Modulation options for OFDM-based waveforms: classification, comparison, and future directions. *IEEE Access*. 2019;7:17 263-17 278.
26. Dang S, Guo S, Shihada B, Alouini M-S. Information-theoretic analysis of OFDM with subcarrier number modulation. *IEEE Trans Inf Theory*. 2021;67(11):7338-7354.
27. Dang S, Ma G, Shihada B, Alouini M-S. Enhanced orthogonal frequency-division multiplexing with subcarrier number modulation. *IEEE Internet Things J*. 2019;6(5):7907-7920.
28. Jaradat AM, Hamamreh JM, Arslan H. Ofdm with subcarrier number modulation. *IEEE Wirel Commun Lett*. 2018;7(6):914-917.
29. Huang Z, Gao Z, Sun L. Anti-eavesdropping scheme based on quadrature spatial modulation. *IEEE Commun Lett*. 2016;21(3):532-535.
30. Wang X, Wang X, Sun L. Spatial modulation aided physical layer security enhancement for fading wiretap channels. Proceedings of the 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP); 2016:1-5; IEEE.
31. Yang Y, Guizani M. Mapping-varied spatial modulation for physical layer security: transmission strategy and secrecy rate. *IEEE J Select Areas Commun*. 2018;36(4):877-889.
32. Shiu Y-S, Chang SY, Wu H-C, Huang SC-H, Chen H-H. Physical layer security in wireless networks: a tutorial. *IEEE Wirel Commun*. 2011;18(2):66-74.
33. Bloch M, Barros J. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge: Cambridge University Press; 2011.
34. Khisti A, Wornell G, Wiesel A, Eldar Y. On the Gaussian mimo wiretap channel. Proceedings of the 2007 IEEE International Symposium on Information Theory; 2007:2471-2475.
35. Oggier F, Hassibi B. The secrecy capacity of the mimo wiretap channel. *IEEE Trans Inf Theory*. 2011;57(8):4961-4972.
36. Dang S, Zhou J, Shihada B, Alouini M-S. Relay assisted OFDM with subcarrier number modulation in multi-hop cooperative networks. *IEEE Wirel Commun Lett*. 2020;9(11):1869-1873.
37. Xiao L, Greenstein LJ, Mandayam NB, Trappe W. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans Wirel Commun*. 2008;7(7):2571-2579.
38. Trappe W. The challenges facing physical layer security. *IEEE Commun Mag*. 2015;53(6):16-20.
39. Annamalai A, Tellambura C. Error rates for nakagami-m fading multichannel reception of binary and m-ary signals. *IEEE Trans Commun*. 2001;49(1):58-68.
40. Alouini M-S, Goldsmith AJ. A unified approach for calculating error rates of linearly modulated signals over generalized fading channels. *IEEE Trans Commun*. 1999;47(9):1324-1334.

How to cite this article: Kırık M, Hamamreh JM. A novel interference signal superposition algorithm for providing secrecy to subcarrier number modulation-based orthogonal frequency division multiplexing systems. *Trans Emerging Tel Tech*. 2023;34(1):e4678. doi: 10.1002/ett.4678