Received November 30, 2021, accepted December 30, 2021, date of publication December 31, 2021

*Digital Object Identifier 10.46470/03d8ffbd.b23dc12e*

# Interference Signal Superposition-aided MIMO with Antenna Number Modulation and Adaptive Antenna Selection for Achieving Perfect Secrecy

**MUHAMMET KIRIK[1], JEHAD M. HAMAMREH[1]**

[1]M. Kirik and J. M. Hamamreh are with WISLAB for Wireless Research at the Department of Electrical-Electronics Engineering, Antalya Bilim University, Antalya, Turkey. (web: https://wislabi.com // email: muhammet.kirik@std.antalya.edu.tr and jehad.hamamreh@gmail.com).

Corresponding author: Muhammet Kirik (e-mail: muhammetkirik1997@gmail.com).

The Matlab simulation codes used to generate the results in this paper can be found at https://researcherstore.com with the name ISS-MIMO-ANM.

WISLAB (wislabi.com/solutions) offers solutions for building and deploying fully secure, cloud-based, and low-cost end-to-end 4G/5G networks along with providing consultations on helping companies reduce their networks CAPEX/OPEX cost and determine which solutions are best suited for their needs and use cases.

**ABSTRACT** In this paper, a novel secure data transmission method called interference signal superposition-aided multiple-input multiple-output with antenna number modulation and adaptive antenna selection (ISS-MIMO-ANM-AAS) is presented to defend transmission systems against eavesdropping attacks or to share secret information between two communication parties in scenarios, where perfect secrecy and ultimate confidentiality are required to be achieved. In the proposed method, while data is transmitted to the legitimate receiver by exploiting the features of MIMO-ANM through transmitting additional data bits with the number of active antennas along with those bits sent by using conventional M-PSK/QAM modulation, the data that the eavesdropper receives is aimed to be mixed by an interference signal superposed (ISS) with the original signal to eliminate the possible wiretapping activities. The conducted theoretical analysis along with the obtained numerical simulations for the proposed ISS-MIMO-ANM-AAS method proves the effectiveness of the scheme, where MIMO-ANM transmission is shown to be fully secured through the ISS algorithm. Thus, the introduced ISS-MIMO-ANM-AAS method can be considered a strong potential candidate method for scenarios where ultra-security is the main requirement of wireless systems including WiFi, 5G, 6G, and beyond technologies.

**INDEX TERMS** MIMO, MIMO-ANM-AAS, ISS, antenna number modulation, adaptive antenna selection, interference signal superposition, wireless security, secrecy, wireless communication, 5G, 6G.

## I. 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 need, many different types of secure data communication solutions are developed, that contribute to the secrecy of digital communication systems [4]–[7].

One of the solutions offered by Wyner [8] 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 [9]. In the following years, Wyner's study was supported by Csiszár and Körner [10]. 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 [11].

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 can't, this encryption/decryption and cryptography based approaches can't be satisfactory to provide the data security in today's conditions [12]–[17].

The reason behind it is the massive number of devices that are powered by 5G and beyond wireless technologies [18]–[20]. Within the advent of the 5G based technologies such as spatial modulation (SM) [21], [22], index modulation (IM) [23], [24], antenna number modulation (ANM) [25]–[28] and 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]–[34]. 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 [35]–[38].

In this paper, a novel secure data transmission method called *"Interference Signal Superposition MIMO with Antenna Number Modulation and Adaptive Antenna Selection (ISS-MIMO-ANM-AAS)"* is proposed to create an environment during the data transmission, that can manipulate 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 [39], [40]. In this method, by inheriting the features of conventional MIMO-ANM-AAS, transmitted data is aimed to be sent with high spectral efficiency, low BER, and capability of channel and data dependent antenna selection at the same time, while the data secrecy is provided against the wire-tapper by adding an artificial interference signal, which is specifically created according to the legitimate receiver's CSI, to the actual signal that is intended to be sent.

The remaining parts of this paper are organized as follows. In section II, the system model of the ISS-MIMO-ANM-AAS concept and its properties are indicated, and the concept is explained in detail. In section III, the simulation results are exhibited and explained. Lastly, part IV concludes the paper.

## II. SYSTEM MODEL

Within this section, design of the *Interference Signal Superposition MIMO with Antenna Number Modulation and Adaptive Antenna Selection (ISS-MIMO-ANM-AAS)* is explained in a profound manner. To do that, a single user point to point MIMO scheme with the existence of an eavesdropper under Rayleigh fading channel is considered. At the transmission side, number of antennas is considered to be $T$, and at the reception side number of antennas is considered to be $R$. In addition to the transmitter and receiver, in this study, also the existence of an eavesdropper is taken into account with $E$ number of antennas, to investigate the secrecy capacity of the proposed ISS-MIMO-ANM-AAS. For a straight forward explanation, number of receiving antennas and eavesdropper's antennas are considered to be singular, $i.e., R = 1, E = 1$.

The new proposed data scheme ISS-MIMO-ANM-AAS focuses on the security of transmitted data by embedding an artificial interference signal into the transmitted signal. By embedding this artificial interference signal, which is specifically created according to the CSI of legitimate receiver, data reception of the eavesdropper can be corrupted, since the CSI of the eavesdropper has a different value than the legitimate receiver. This creates an opportunity to deploy the ANM scheme in such cases that require high spectral efficiency, low bit error rate, and high data secrecy at the same time.

### A. DESIGN OF THE TRANSMISSION END OF ISS-MIMO-ANM-AAS

The general structure of the proposed ISS-MIMO-ANM-AAS transmitter is shown in Fig. 1.

At the beginning of the procedure, given data stream of incoming bits is separated into two different sub-streams. Portion of the bits that is located at the end of the data stream is the part where number of antenna activation patterns is mapped. Thus this portion is named as "ANM Bits". Portion of the bits that is located at the beginning of the data stream is the part where the signal constellation points are mapped. Thus, this portion is named as "Main Bits".

After this separation is achieved for the given data stream of total number of bits $N = N_1 + N_2$ as Main bits ($N_1$), which is determined by the signal constellation modulation order $N_1 = log_2(M)$; and ANM bits ($N_2$), which is determined by number of available transmit antennas $T$ as per this formula $N_2 = log_2(T)$, each bit in the main bits group is modulated by conventional BPSK, while the symbols in the ANM bits group are exploited to decide how many antennas will be used for the transmission of main bits by using a look-up table that maps ANM bits group for specific bit combinations. To exemplify this process, the mapping process for such a case where the total number of antennas for the transmission is four ($T = 4$) is given in Table I.

To make the Table I more straight forward, it can be said that, if the ANM bits group or couple is "00", then the number of active antennas is one; if ANM bits group is "01", then the number of active antennas is two; if ANM bits group is "10", then the number of active antennas is three; and if ANM bits group is "11", then the number of active antennas is four. The mapping numbers of each antenna are specifically determined by the number of antennas in the system by assuming the $T = 2^{N_2}$ is the number of the transmit antennas in the system, where $N_2$ represents the number of data bits for each ANM group. In order to be able to have a decent comparison between MIMO-ANM-AAS and ISS-MIMO-ANM-AAS and observe the data secrecy merits of ISS-MIMO-ANM-AAS, the case composed of four transmit antennas ($T = 4$) and one receive antenna ($R = 1$) under the existence of one eavesdropper ($E = 1$) is considered in the

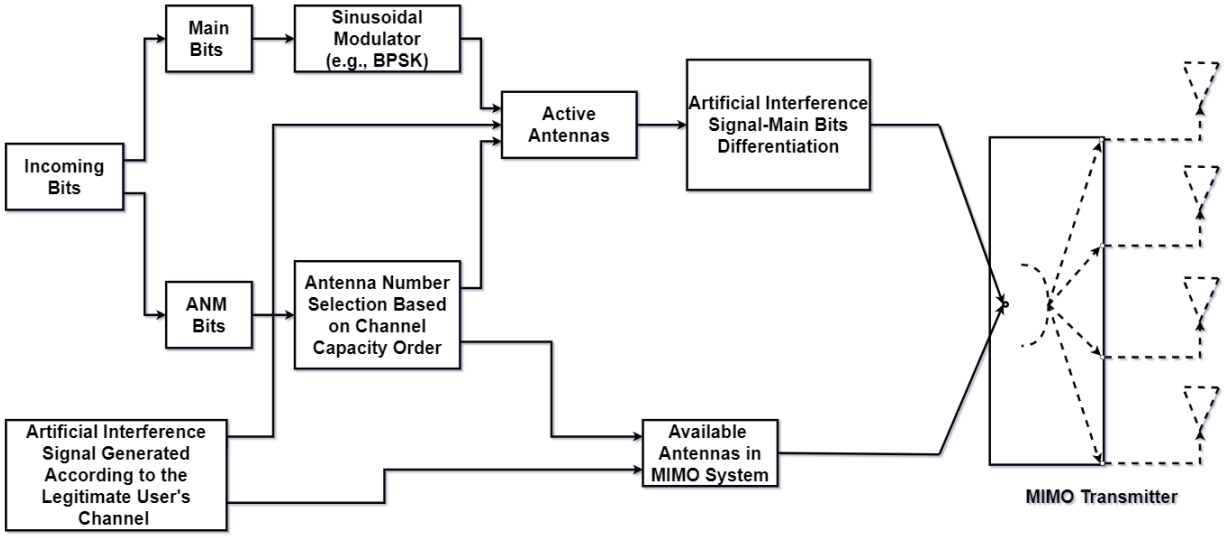


**FIGURE 1.** Transmitter Structure of ISS-MIMO-ANM-AAS.

description of the proposed scheme throughout the coming sections of this paper.

The next step is to determine the channel capacities of each antenna, so the antenna selection process of the ISS-MIMO-ANM-AAS can be enabled in a descending order as from the highest channel capacity offering antenna, to the lowest channel capacity offering antenna, to be not only data dependent as MIMO-SM, but also be channel dependent at the same time, which is an inherited feature of ISS-MIMO-ANM-AAS from MIMO-ANM-AAS [25]. Possible antenna activation patterns for this adaptive antenna selection procedure are given in Table I.

After the channel capabilities of the antennas are defined, and each antenna is labeled as low quality and high quality antennas according to their channel capacities, main bits, which are modulated by BPSK for the data transfer of the legitimate user are conveyed by the high channel capacity offering antennas with an artificial interference signal, that is specifically created according to the channel values of the legitimate user, which leads to the eavesdropper to receive a corrupted version the transmitted data, since the CSI of the eavesdropper does not match with the CSI of the legitimate receiver. The transmission of main bits for the legitimate receiver is given in the following formula.

$$\mathbf{y_l} = \sqrt{\frac{P}{V}} \times \mathbf{h} \times \mathbf{v} \times (x + \mathbf{n}) + w, \tag{1}$$

In this formula, $P$ is defined as the transmit power per data symbol, while $V = \|\mathbf{v}\|_2 = \sum_{i=1}^{T} v_i^2$ is defined as total number of active antennas selected for transmission out of $T$ available antennas in each channel use. The flat fading channel vector is considered to be $\mathbf{h} = [h_{11}, h_{12}, h_{13}, h_{14}] \in \mathbb{C}^{1\times 4}$ in which, each element represents a circularly symmetric complex Gaussian channel coefficient with zero mean and unity variance, corresponding to the response between $R^{th}$ receive antenna and $T^{th}$ transmit antenna. $\mathbf{v} \in \mathbb{R}^{4\times 1}$ is the activation pattern vector that is designed as zeros for inactive antennas and ones for active antennas, which are determined according to $N_2$ bits and the mapping/lookup process given in Table I. $x$ is the each symbol of main bits sub-stream, which is modulated by BPSK. The artificial interference signal vector is represented by $\mathbf{n} = [n_1, n_2, n_3, n_4] \in \mathbb{C}^{1\times 4}$, and $w$ is the white Gaussian noise.

*Example:* Consider a group of people that consists of three individuals, Alice, Bob, and Eve. In this group, while Alice is trying to transmit a secret data with four transmit antennas ($T = 4$) to Bob, who has a singular receive antenna ($R = 1$), Eve is trying to infiltrate the system with one receive antenna ($E = 1$). The regarding data to be transmitted by Alice is given in Fig. 2 with its separated form as Main bits and ANM bits.

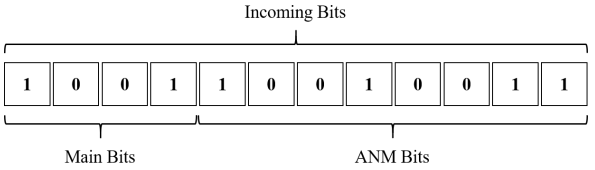


**FIGURE 2.** Transmitted data by Alice from 4 Transmit Antennas with Main Bits and ANM Bits Separation under BPSK modulation.

During this transmission, channel qualities of each transmit antenna between Alice and Bob are sorted as $|h_3| > |h_4| > |h_1| > |h_2|$, which means that the antenna activation pattern of the system will be in a descending order as $T_3 > T_4 > T_1 > T_2$. In such a case, transmission of each symbol of the main bits group under BPSK modulation is explained as follows for both Bob's and Eve's perspective.

**TABLE 1.** ISS-MIMO-ANM-AAS mapper with $N_2$=2 bits & $T$=4 antennas, where the final active antenna pattern is determined by the largest channel gains among all possible antenna numbers

| ANM bits ($N_2$) | Possible Active Antennas Pattern ($\mathbf{v}$) | Artificial Interference Signal ($\mathbf{n}$) |
|---|---|---|
| [0 0] | [1 0 0 0] | $[\frac{A}{h_1}\ \frac{-A}{h_2}\ 0\ 0]$ |
| [0 0] | [0 1 0 0] | $[\frac{A}{h_2}\ \frac{-A}{h_1}\ 0\ 0]$ |
| [0 0] | [0 0 1 0] | $[\frac{A}{h_3}\ \frac{-A}{h_2}\ 0\ 0]$ |
| [0 0] | [0 0 0 1] | $[\frac{A}{h_4}\ \frac{-A}{h_2}\ 0\ 0]$ |
| [0 1] | [1 1 0 0] | $[\frac{A}{h_1}\ \frac{-A}{h_2}\ 0\ 0]$ |
| [0 1] | [1 0 1 0] | $[\frac{A}{h_1}\ \frac{-A}{h_3}\ 0\ 0]$ |
| [0 1] | [1 0 0 1] | $[\frac{A}{h_1}\ \frac{-A}{h_4}\ 0\ 0]$ |
| [0 1] | [0 0 1 1] | $[\frac{A}{h_3}\ \frac{-A}{h_4}\ 0\ 0]$ |
| [0 1] | [0 1 0 1] | $[\frac{A}{h_2}\ \frac{-A}{h_4}\ 0\ 0]$ |
| [0 1] | [0 1 1 0] | $[\frac{A}{h_2}\ \frac{-A}{h_3}\ 0\ 0]$ |
| [1 0] | [1 1 1 0] | $[\frac{A}{h_1}\ \frac{B}{h_2}\ \frac{-(A+B)}{h_3}\ 0]$ |
| [1 0] | [1 1 0 1] | $[\frac{A}{h_1}\ \frac{B}{h_2}\ \frac{-(A+B)}{h_4}\ 0]$ |
| [1 0] | [1 0 1 1] | $[\frac{A}{h_1}\ \frac{B}{h_3}\ \frac{-(A+B)}{h_4}\ 0]$ |
| [1 0] | [0 1 1 1] | $[\frac{A}{h_2}\ \frac{B}{h_3}\ \frac{-(A+B)}{h_4}\ 0]$ |
| [1 1] | [1 1 1 1] | $[\frac{A}{h_1}\ \frac{-A}{h_2}\ \frac{B}{h_3}\ \frac{-B}{h_4}]$ |

By the Fig.2, transmission of the first symbol in main bits group, 1, will be operated by three antennas, as the regarding ANM bits mapper ($N_2$) is 10. General illustration of this process is shown in Fig.3-a. As it is stated before, the antenna activation order is $T_3 > T_4 > T_1 > T_2$, which means the possible active antennas pattern for this case is $\mathbf{v} = [1, 0, 1, 1]$, and the artificial interference signal vector is $\mathbf{n} = [\frac{A}{h_1}, \frac{B}{h_3}, \frac{-(A+B)}{h_4}, 0]$. By exploiting this information, mathematical form of the transmission of 1 to Bob by activating three antennas is derived as below.

$$y_b = (x_1+n_1)\times h_1+(x_1+n_2)\times h_3+(x_1+n_3)\times h_4+w \quad (2)$$

$$y_b = (x_1 + \frac{A}{h_1}) \times h_1 + (x_1 + \frac{B}{h_3}) \times h_3 + (x_1 + \frac{-(A+B)}{h_4}) \times h_4 + w \quad (3)$$

$$y_b = (x_1 \times h_1) + \frac{A}{h_1} \times h_1 + (x_1 \times h_3) + \frac{B}{h_3} \times h_3 + (x_1 \times h_4) - \frac{A+B}{h_4} \times h_4 + w \quad (4)$$

$$y_b = (x_1\times h_1)+A+(x_1\times h_3)+B+(x_1\times h_4)-A-B+w \quad (5)$$

$$y_b = x_1 \times (h_1 + h_3 + h_4) + w \quad (6)$$

On the other hand, since Eve is trying to reach to the Alice's transmitted data from a different location with a different flat fading channel, $\mathbf{e}$, and the artificial interference noise, $\mathbf{n}$ is designed specifically and only for the flat fading channel of Bob, $\mathbf{h}$, the transmitted data to the Eve's location will be a complicated signal with no meaning. This transmission process from Eve's perspective is given below in mathematical form as follows.

$$y_e = (x_1+n_1)\times e_1+(x_1+n_2)\times e_3+(x_1+n_3)\times e_4+w \quad (7)$$

$$y_e = (x_1 + \frac{A}{h_1}) \times e_1 + (x_1 + \frac{B}{h_3}) \times e_3 + (x_1 + \frac{-(A+B)}{h_4}) \times e_4 + w \quad (8)$$

$$y_e = (x_1 \times e_1) + \frac{A}{h_1} \times e_1 + (x_1 \times e_3) + \frac{B}{h_3} \times e_3 + (x_1 \times e_4) - \frac{A+B}{h_4} \times e_4 + w \quad (9)$$

For transmission of second symbol of the main bits group, 0, it can be seen from the Fig. 2 that the regarding ANM bit mapper $N_2$ is 01, which means the activation of two antennas. This process is illustrated in Fig.3-b. In this case, the possible active antennas pattern is $\mathbf{v} = [0, 0, 1, 1]$ and the artificial interference signal vector is $\mathbf{n} = [\frac{A}{h_3}, \frac{-A}{h_4}, 0, 0]$. With this information, mathematical form of the transmission of 0 via two transmit antennas can be derived as follows for Bob's perspective.

$$y_b = (x_2 + n_1) \times h_3 + (x_2 + n_2) \times h_4 + w \quad (10)$$

$$y_b = (x_2 + \frac{A}{h_3}) \times h_3 + (x_2 + \frac{-A}{h_3}) \times h_4 + w \quad (11)$$

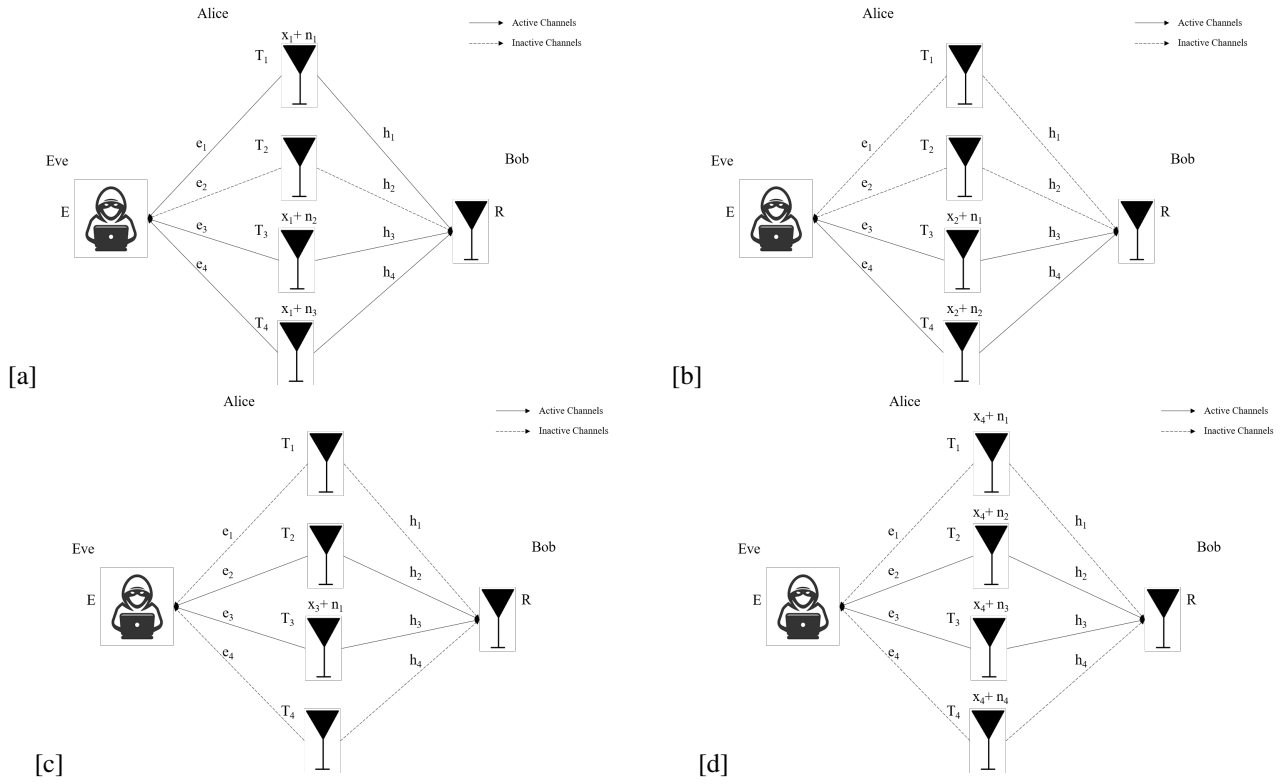


**FIGURE 3.** Simple Visualization of the Transmission of each Symbol in Main Bits Group for Different Antenna Activation Patterns

$$y_b = (x_2 \times h_3) + \frac{A}{h_3} \times h_3 + (x_2 \times h_4) - \frac{A}{h_4} \times h_4 + w \quad (12)$$

$$y_b = (x_2 \times h_3) + A + (x_2 \times h_4) - A + w \quad (13)$$

$$y_b = x_2 \times (h_3 + h_4) + w \quad (14)$$

The mathematical form of corrupted signal transmission of the regarding symbol from Eve's perspective is as follows.

$$y_e = (x_2 + n_1) \times e_3 + (x_2 + n_2) \times e_4 + w \quad (15)$$

$$y_e = (x_2 + \frac{A}{h_3}) \times e_3 + (x_2 - \frac{A}{h_3}) \times e_4 + w \quad (16)$$

$$y_e = (x_2 \times e_3) + \frac{A}{h_3} \times e_3 + (x_2 \times e_4) - \frac{A}{h_4} \times e_4 + w \quad (17)$$

The transmission process of the third symbol of main bits group is visually given in Fig.3-c. As it can be seen from Fig.2, third symbol of the main bits group is sent by activating only one antenna as the ANM bit mapper is 00. In this case, the possible active antennas pattern is $\mathbf{v} = [0, 0, 1, 0]$ and the artificial interference signal vector is $\mathbf{n} = [\frac{A}{h_3}, \frac{-A}{h_2}, 0, 0]$. Under these circumstances, the transmission of 0 can be presented as follows from Bob's perspective.

$$y_b = (x_3 + n_1) \times h_3 + n_2 \times h_2 + w \quad (18)$$

$$y_b = (x_3 + \frac{A}{h_3}) \times h_3 - \frac{A}{h_2} \times h_2 + w \quad (19)$$

$$y_b = (x_3 \times h_3) + \frac{A}{h_3} \times h_3 - \frac{A}{h_2} \times h_2 + w \quad (20)$$

$$y_b = (x_3 \times h_3) + A - A + w \quad (21)$$

$$y_b = x_3 \times (h_3) + w \quad (22)$$

The mathematical form of corrupted signal transmission of the regarding symbol from Eve's perspective is given as follows.

$$y_e = (x_3 + n_1) \times e_3 + n_2 \times e_2 + w \quad (23)$$

$$y_e = (x_3 + \frac{A}{h_3}) \times e_3 - \frac{A}{h_2} \times e_2 + w \quad (24)$$

$$y_e = (x_3 \times e_3) + \frac{A}{h_3} \times e_3 - \frac{A}{h_2} \times e_2 + w \quad (25)$$

As the last symbol of the main bits group 1, transmission must be operated by four antennas as the ANM bit mapper ($N_2$) is 11, which can be seen in Fig.2. The visual illustration of this transmission is given in Fig.3-d In this case, the possible active antennas pattern is $\mathbf{v} = [1, 1, 1, 1]$ and the artificial interference signal vector is $\mathbf{n} = [\frac{A}{h_1}, \frac{-A}{h_2}, \frac{B}{h_3}, \frac{-B}{h_4}]$. Under these circumstances, the transmission of 1 can be presented as follows from Bob's perspective.

$$y_b = (x_4 + n_1) \times h_1 + (x_4 + n_2) \times h_2 + (x_4 + n_3) \times h_3 + (x_4 + n_4) \times h_4 + w \quad (26)$$

$$y_b = (x_4 + \frac{A}{h_1}) \times h_1 + (x_4 + \frac{-A}{h_2}) \times h_2 + (x_4 + \frac{B}{h_3}) \times h_3 + (x_4 + \frac{-B}{h_4}) \times h_4 + w \quad (27)$$

$$y_b = (x_4 \times h_1) + \frac{A}{h_1} \times h_1 + (x_4 \times h_2) - \frac{A}{h_2} \times h_2 + (x_4 \times h_3) + \frac{B}{h_3} \times h_3 + (x_4 \times h_4) - \frac{B}{h_4} \times h_4 + w \quad (28)$$

$$y_b = (x_4 \times h_1) + A + (x_4 \times h_2) - A + (x_4 \times h_3) + B + (x_4 \times h_4) - B + w \quad (29)$$

$$y_b = x_4 \times (h_1 + h_2 + h_3 + h_4) + w \quad (30)$$

The mathematical form of corrupted signal transmission of the regarding symbol from Eve's perspective is given as follows.

$$y_e = (x_4 + n_1) \times e_1 + (x_4 + n_2) \times e_2 + (x_4 + n_3) \times e_3 + (x_4 + n_4) \times e_4 + w \quad (31)$$

$$y_e = (x_4 + \frac{A}{h_1}) \times e_1 + (x_4 + \frac{-A}{h_2}) \times e_2 + (x_4 + \frac{B}{h_3}) \times e_3 + (x_4 + \frac{-B}{h_4}) \times e_4 + w \quad (32)$$

$$y_e = (x_4 \times e_1) + \frac{A}{h_1} \times e_1 + (x_4 \times e_2) - \frac{A}{h_2} \times e_2 + (x_4 \times e_3) + \frac{B}{h_3} \times e_3 + (x_4 \times e_4) - \frac{B}{h_4} \times e_4 + w \quad (33)$$

### B. DESIGN OF THE RECEPTION END OF ISS-MIMO-ANM-AAS

The general structure of the proposed ISS-MIMO-ANM-AAS receiver is shown in Fig. 4.

As the main bits and artificial interference signal differentiation is operated at the transmission side, receiver side structure of ISS-MIMO-ANM-AAS is designed same as the conventional MIMO-ANM. In this manner, decoding of the

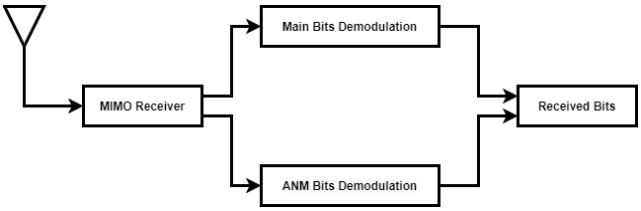


**FIGURE 4.** Receiver Structure of ISS-MIMO-ANM.

main bits and ANM bits are operated by using a Maximum Likelihood (ML) detector, that can separately predict the active antenna's pattern and signal constellation point. Mathematical implementations of the regarding ML detectors are given in the following formulas for the detection of ANM bits and main bits respectfully.

$$J_v = \min_{\hat{v}} \left( ||y - \left( \sum_{i=1}^{\hat{v}} h_{1i} \right) x||^2 \right), \quad (34)$$

$$J_x = \min_{\hat{x}} \left( ||y - \left( \sum_{i=1}^{v} h_{1i} \right) \hat{x}||^2 \right). \quad (35)$$

where $v \in 1, 2, 3, 4$ is the possible number of active transmit antennas, $y_i \in y_1, y_2, y_3, y_4$ is the received signal according to the possible antenna number usage, and $\hat{x_i}$ is the estimated BPSK symbol.

## III. 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 average BER.

### A. AVERAGE SYMBOL ERROR RATE OF BOB

Calculation of the symbol error rate (SER) of Bob is not as easy as the conventional MIMO 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 antennas 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 antennas, $p_1$, and the second portion of the data stream of Bob, $p_2$, that is modulated by one of the $M-$ary modulation orders to be sent over these active antennas 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 antennas 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 antennas 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 $P_{SNM}(E)$ as the error probability of $A1$ (i.e., the antenna pattern activity) and $P_{BPSK}(E)$ as the error probability for $A2$ (i.e., the BPSK symbol recovery) at the receiver side, the overall error probability $P_T(E)$ can be formulated as

$$P_T(E) = P_T(E|A_1)P(A_1) + P_T(E|A_2)P(A_2), \quad (36)$$

$$P_T(E) = \frac{2}{3}P_{SNM}(E) + \frac{1}{2}P_{BPSK}(E). \quad (37)$$

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

### B. SYMBOL ERROR RATE ANALYSIS OF THE ACTIVE ANTENNAS THAT TRANSMIT LEGITIMATE USER'S DATA

By formulating the PDF of the first portion of the Bob's data, $p_1$, the analytical error rate evaluation of the symbols that define the number of active antennas 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 antennas.

$$SER_{b_{p_1}} = \int_0^\infty P_{\gamma_{b\,p_1}}(\gamma_b)\, d_{\gamma_b}. \quad (38)$$

By substituting the value of $P_{\gamma_{b\,p_1}}(\gamma_b)$ in (38), the result turns into

$$SER_{b_{p_1}} = \int_0^\infty 2\frac{T-1}{T}Q_f(\sqrt{2Z\gamma_b})d_{\gamma_b}. \quad (39)$$

By integrating (39), the resulting formula can be presented as

$$SER_{b_{p_1}} = \frac{T-1}{T}\left(1 - \sqrt{\frac{Z\bar{\gamma}_b}{1+Z\bar{\gamma}_b}}\right), \quad (40)$$

where $Z = 3/(T^2-1)$, $\gamma_{b_s} = \gamma_b \log_2(M)$, $\gamma_b = \frac{||H_{b_i}||^2 \times P}{\sigma_b^2}$, and $Q_f(.)$ is the $Q$ function defined as

$$Q_f(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}dt, \quad (41)$$

### C. BIT ERROR RATE 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 BER evaluation of the conventionally transmitted data Bob under the proposed MIMO-ANM-ISS scheme. This evaluation is in analysed in both BPSK (i.e., $M = 2$).

Bit error rate (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.

$$BER_{b_{p_2}} = \frac{1}{2}\int_0^\infty \text{erfc}\left(\sqrt{\gamma_b}\right) P_{\gamma_{b\,p_2}}(\gamma_b)\, d_{\gamma_b}, \quad (42)$$

where erfc(.) is the error function. By substituting the corresponding value of $P_{\gamma_{b\,p_2}}(\gamma_b)$ into (42), the obtained integration becomes

$$BER_{b_{p_2}} = \frac{1}{2}\int_0^\infty \text{erfc}\left(\sqrt{\gamma_b}\right)\frac{1}{2u^2}\frac{1}{\Gamma(\mu)} \frac{\Omega_b^{\frac{3}{2}}\sqrt{\gamma_b}}{\frac{1}{u}\bar{\gamma}_b^{\frac{3}{2}}} \times \exp\left(-\frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\bar{\gamma}_b}\right) d\gamma_b, \quad (43)$$

$$BER_{b_{p_2}} = \frac{1}{2}\frac{1}{2u^2}\frac{1}{\Gamma(\mu)}\frac{\Omega_b^{\frac{3}{2}}}{\frac{1}{u}\bar{\gamma}_b^{\frac{3}{2}}}\int_0^\infty \text{erfc}\left(\sqrt{\gamma_b}\right)\sqrt{\gamma_b} \times \exp\left(-\frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\bar{\gamma}_b}\right) d\gamma_b. \quad (44)$$

The integral in (44) can be solved by introducing the variables $G = \frac{1}{2}\frac{1}{2u^2}\frac{1}{\Gamma(\mu)}\frac{\Omega_b^{\frac{3}{2}}}{\frac{1}{u}\bar{\gamma}_b^{\frac{3}{2}}}$ and $\rho = \frac{1}{2u^2}\frac{\Omega_b\gamma_b}{\bar{\gamma}_b}$ for simplicity. The resulting solution of the integral is given as

$$BER_{b_{p_2}} \approx \frac{G}{2\sqrt{\pi}}\left(\frac{\arctan(\sqrt{\rho})}{2\rho^{\frac{3}{2}}} - \frac{1}{2\rho(1+\rho)}\right), \quad (45)$$

where $\arctan(.)$ is the inverse of tangent.

### D. BIT ERROR RATE ANALYSIS OF THE TRANSMITTED SYMBOL OF EAVESDROPPER'S DATA

Antenna activations in the proposed scheme are dependent on the Bob's data, and these activations are made in a descending order (i.e., from the antennas that have higher channel amplitude to lower channel amplitude). For this reason, antenna 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 MIMO. Under these circumstances, the BER performance of Eve under BPSK modulation ($M = 2$) where $\gamma_e = \frac{||H_{e_i}||^2 \times P}{\sigma_e^2}$, $\gamma_{e_s} = \gamma_e \log_2 2 = \gamma_e$ can be given as

$$BER_e = \frac{1}{2}\int_0^\infty \text{erfc}(\sqrt{\gamma_e})P_{\gamma_e}(\gamma_e)d\gamma_e. \quad (46)$$

$$BER_e = \frac{1}{2}\int_0^\infty \text{erfc}(\sqrt{\gamma_e})\left(\frac{1}{\Omega_e\bar{\gamma}_e}\right)\exp\left(\frac{\gamma_e}{\Omega_e\bar{\gamma}_e}\right)d\gamma_e. \quad (47)$$

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

$$BER_e = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_e}{1+\bar{\gamma}_e}}\right). \quad (48)$$

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

$$SER_e = 2\left(\frac{\sqrt{M}-1}{\sqrt{M}}\right)\left(1-\sqrt{\frac{1.5\bar{\gamma}_{e_s}}{M-1+1.5\bar{\gamma}_{e_s}}}\right) - \left(\frac{\sqrt{M}-}{\sqrt{M}}\right.$$
$$\times\left[1-\sqrt{\frac{1.5\bar{\gamma}_{e_s}}{M-1+1.5\bar{\gamma}_{e_s}}}\left(\frac{4}{\pi}\arctan\left(\sqrt{\frac{M-1+1.5\bar{\gamma}_{e_s}}{1.5\bar{\gamma}_{e_s}}}\right)\right)\right. \tag{49}$$

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 created according to Bob's channel, and the adaptive interleaver that activates the antennas that transmit Bob's data cannot be reached by Eve, her performance will not be the same as (48) and (49). 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.

## IV. SIMULATION RESULTS

In this section, simulated results will be illustrated in terms of the secrecy level of the data at the reception end of the legitimate user and the eavesdropper, as the BER, spectral efficiency, power efficiency of the proposed system are same as the conventional MIMO-ANM in both simulation and theoretical bases. In this manner, simulation results are obtained by conducting Monte-Carlo simulations over a Rayleigh fading channel to obtain the BER of the proposed ISS-MIMO-ANM-AAS from both legitimate user's and eavesdropper's perspective. In this simulation scenario, the number of transmit antennas is considered to be four ($T = 4$), whereas number of receive antennas at the legitimate receiver side and eavesdropper side is considered to be singular ($R = 1$, $E = 1$).

This purposefully selected setup is considered as so in order to concentrate the attention on the fundamental concepts of the proposed schemes, and to simplify the comparison with the other competitive schemes available in the literature. The parameters used in the simulations are shown and summarized in Table 2.

**TABLE 2.** Simulation Parameters

| | |
|---|---|
| Modulation Type | BPSK ($M$=2) |
| Number of Symbols | $10^6$ per iteration |
| Number of Transmit Antennas | 4 |
| Number of Receive Antennas | 1 |
| Number of Eavesdropping Antennas | 1 |
| Number of available antennas for ANM | 4 |
| Number of ANM mapping bits | 2 |
| Wireless channel | Block Rayleigh fading |

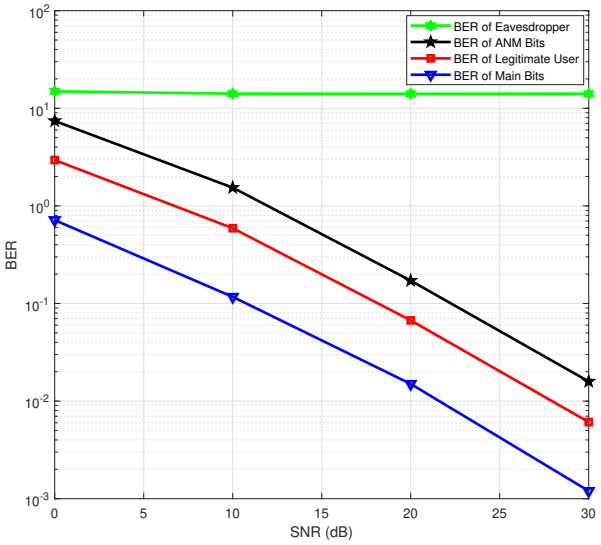


**FIGURE 5.** BER of ISS-MIMO-ANM-AAS of legitimate receiver and eavesdropper vs. SNR (Eb/N0).

The numerically simulated BER performance of proposed ISS-MIMO-ANM-AAS is shown in Fig. 5. In this figure, the error rates of the main bits, which are modulated by BPSK to serve legitimate receiver, ANM bits, which are modulated by number of active antennas, and their average, which is the BER of legitimate receiver is presented with the error rate of the eavesdropper who tries to infiltrate the communication system. It can be observed from the figure that, as the SNR value is varied from 0 to 30, the BER's of the main bits, ANM bits, and dependently their average ISS-MIMO-ANM-AAS rapidly falls, whereas the BER of the eavesdropper exhibits a poor performance, thanks to the artificial interference noise, which is specifically designed according to the legitimate receiver's CSI, and added into the main bits signal to create a confusion at the eavesdropper's receiver.

Fig. 6 shows the simulation and analytical BER performances of the proposed ISS algorithm under BPSK the legitimate receiver. In this figure while the straight lines represent the simulation outputs, dashed lines represent the theoretically analysed results. It can be inferred from Fig.6 that the BER results of the main bits, ANM bits, and overall BER results of legitimate receiver get better values in each increment of the SNR value, $E_b/N_{o,T}$. This is due to the fact that while the additive artificial interference signal that is specifically created for legitimate receiver's effective channels can be successfully differentiated at the transmitter for the transmission of legitimate user'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.

Fig. 7 and Fig. 8 shows the simulated throughput and

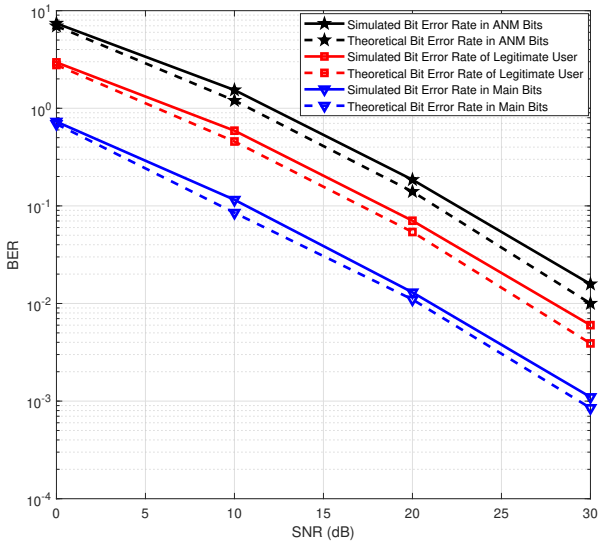


**FIGURE 6.** Theoretical Results of the Proposed ISS-MIMO-ANM-AAS for the legitimate receiver.

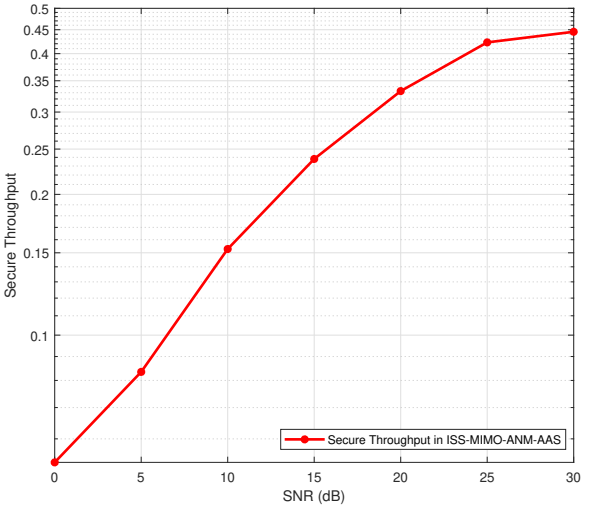


**FIGURE 8.** Secure Throughput vs SNR for the proposed ISS-MIMO-ANM-AAS.

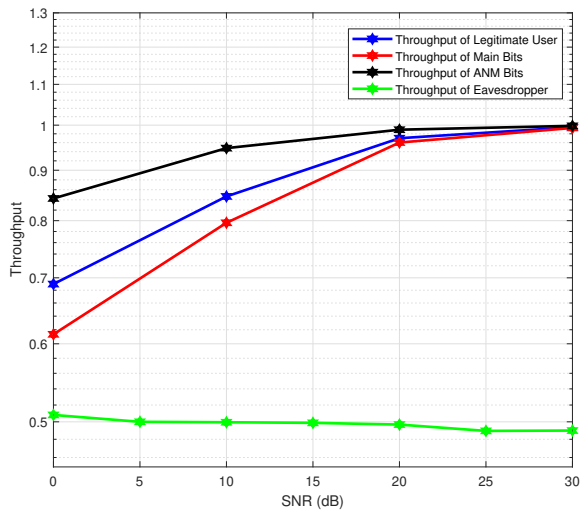


**FIGURE 7.** Simulation Results of the Throughput of the Proposed ISS-MIMO-ANM-AAS for the legitimate receiver and eavesdropper.

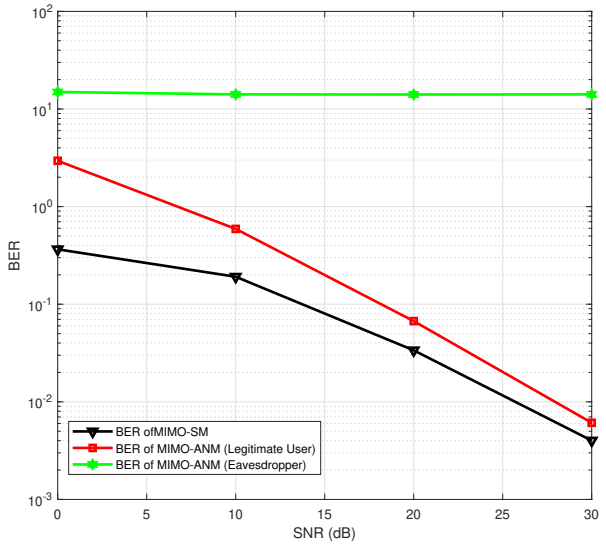


**FIGURE 9.** BER Comparison of the proposed ISS Algorithm Supported MIMO-ANM with Spatial Modulation.

secure throughput performances of Bob and Eve under BPSK modulation order. As it can be observed from the Figure 7, while the throughput performance of Bob under BPSK, as shown in blue line ($M = 2$), gets better values for each increment of SNR, the throughput performance of Eve for BPSK does not change and follows a low path at $0.2$ level for any SNR value, as shown in green line for BPSK ($M = 2$).

It is also important to compare the BER performance of the proposed scheme with its other competitor spatial modulation 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 legitimate user's data. In order to make this comparison, the BER vs. $E_b/N_{o,T}$ performance for ANM and SM is shown in Fig.9. As it can be observed from Fig.9, the performance of the proposed ISS algorithm supported ANM has shown similar performance as the plain spatial modulation. With a simple interpretation from Fig.9, it can be inferred that the ISS algorithm that is applied on the ANM scheme does not bring any disadvantage in terms of BER along with the secrecy.

## V. CONCLUSION

In this paper, a novel technique called ISS-MIMO-ANM-ASS is proposed for reliable and secure communication. The fundamental principle of ISS-MIMO-ANM-ASS is to utilize the number of activated antennas in MIMO-ANM modulation method as another degree of freedom that can be used for conveying extra data bits besides those transmitted by conventional M-ary PSK/QAM symbols, while an artificial interference signal is embedded in those active antennas to create a confusion for any eavesdropping activities by exploiting the uniqueness of the legitimate receiver's CSI. The simulation results prove that the proposed method is a good candidate for providing secure communication at the receiver side, and it can offer a resilient solution for the future applications that require joint high spectral efficiency, ultra-reliability, and perfect secrecy.

## REFERENCES

[1] Claude E Shannon. Communication theory of secrecy systems. The Bell system technical journal, 28(4):656–715, 1949.
[2] Vinay Uday Prabhu and Miguel RD Rodrigues. On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and $\varepsilon$-outage secrecy capacity. IEEE Transactions on Information Forensics and Security, 6(3):853–860, 2011.
[3] Matthieu Bloch, João Barros, Miguel RD Rodrigues, and Steven W McLaughlin. Wireless information-theoretic security. IEEE Transactions on Information Theory, 54(6):2515–2534, 2008.
[4] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In 2006 IEEE international symposium on information theory, pages 356–360. IEEE, 2006.
[5] Haji M Furqan, Jehad M Hamamreh, and Huseyin Arslan. Adaptive ofdm-im for enhancing physical layer security and spectral efficiency of future wireless networks. Wireless Commun. Mobile Comput, 2018:1–16, 2018.
[6] Haji M Furqan, Muhammad Sohaib J Solaija, Jehad M Hamamreh, and Huseyin Arslan. Intelligent physical layer security approach for v2x communication. arXiv preprint arXiv:1905.05075, 2019.
[7] Jehad M Hamamreh. Improving the physical layer security of iot-5g systems. In Artificial Intelligence in IoT, pages 25–44. Springer, 2019.
[8] Aaron D Wyner. The wire-tap channel. Bell system technical journal, 54(8):1355–1387, 1975.
[9] Praveen Kumar Gopala, Lifeng Lai, and Hesham El Gamal. On the secrecy capacity of fading channels. IEEE Transactions on Information Theory, 54(10):4687–4698, 2008.
[10] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. IEEE transactions on information theory, 24(3):339–348, 1978.
[11] Ender Tekin and Aylin Yener. The gaussian multiple access wire-tap channel. IEEE Transactions on Information Theory, 54(12):5747–5755, 2008.
[12] Amitav Mukherjee, S Ali A Fakoorian, Jing Huang, and A Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3):1550–1573, 2014.
[13] Ertuğrul Güvenkaya, Jehad M Hamamreh, and Hüseyin Arslan. On physical-layer concepts and metrics in secure signal transmission. Physical Communication, 25:14–25, 2017.
[14] Jehad M Hamamreh, Ertugrul Basar, and Huseyin Arslan. Ofdm-subcarrier index selection for enhancing security and reliability of 5g urllc services. IEEE Access, 5:25863–25875, 2017.
[15] Jehad M Hamamreh, Ertugrul Guvenkaya, Tuncer Baykas, and Huseyin Arslan. A practical physical-layer security method for precoded ostbc-based systems. In 2016 IEEE Wireless Communications and Networking Conference, pages 1–6. IEEE, 2016.
[16] Li Sun and Qinghe Du. Physical layer security with its applications in 5g networks: A review. China Communications, 14(12):1–14, 2017.
[17] Jehad M Hamamreh, Haji M Furqan, Zain Ali, and Guftaar Ahmad Sardar Sidhu. Enhancing the security performance of ostbc using pre-equalicodization. In 2017 International Conference on Frontiers of Information Technology (FIT), pages 294–298. IEEE, 2017.
[18] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. Safeguarding 5g wireless communication networks using physical layer security. IEEE Communications Magazine, 53(4):20–27, 2015.
[19] Muhammad Farhan Khan, Farrukh Aziz Bhatti, Aamir Habib, Sobia Jangsher, Muhammad Imran Khan, Irfan Zafar, Syed Muslim Shah, Muhammad Ali Jamshed, and Javed Iqbal. Analysis of macro user offloading to femto cells for 5g cellular networks. In 2017 International Symposium on Wireless Systems and Networks (ISWSN), pages 1–6. IEEE, 2017.
[20] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek. Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks. IEEE Communications Magazine, 53(6):21–27, 2015.
[21] Raed Y Mesleh, Harald Haas, Sinan Sinanovic, Chang Wook Ahn, and Sangboh Yun. Spatial modulation. IEEE Transactions on vehicular technology, 57(4):2228–2241, 2008.
[22] Read Mesleh, Harald Haas, Chang Wook Ahn, and Sangboh Yun. Spatial modulation-a new low complexity spectral efficiency enhancing technique. In 2006 First International Conference on Communications and Networking in China, pages 1–5. IEEE, 2006.
[23] Ertugrul Basar. Index modulation techniques for 5g wireless networks. IEEE Communications Magazine, 54(7):168–175, 2016.
[24] Ertugrul Basar, Miaowen Wen, Raed Mesleh, Marco Di Renzo, Yue Xiao, and Harald Haas. Index modulation techniques for next-generation wireless networks. IEEE access, 5:16693–16746, 2017.
[25] Jehad M Hamamreh, Muhammet Kirik, Mehmet O. Sagman, and Naoki Ishikawa. Multiple input multiple output with antenna number modulation and adaptive antenna selection. RS Open Journal on Innovative Communication Technologies, 2020.
[26] Muhammet Kirik and Jehad M Hamamreh. Multiple mimo with antenna number modulation. In 2020 International Conference on UK-China Emerging Technologies (UCET), pages 1–4. IEEE, 2020.
[27] Seyit Karatepe, Muhammet Kirik, and Jehad M Hamamreh. Novel nonorthogonal multi-access method for multi-user mimo with antenna number modulation. RS Open Journal on Innovative Communication Technologies, 2(3):1–11, 2021.
[28] Muhammet Kirik and Jehad M Hamamreh. Multiple mimo with joint block antenna number modulation and adaptive antenna selection for future wireless systems. RS Open Journal on Innovative Communication Technologies, 1(2):12, 2020.
[29] Zhijie Huang, Zhenzhen Gao, and Li Sun. Anti-eavesdropping scheme based on quadrature spatial modulation. IEEE Communications Letters, 21(3):532–535, 2016.
[30] Xin Wang, Xia Wang, and Li Sun. Spatial modulation aided physical layer security enhancement for fading wiretap channels. In 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), pages 1–5. IEEE, 2016.
[31] Yuli Yang and Mohsen Guizani. Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate. IEEE Journal on Selected Areas in Communications, 36(4):877–889, 2018.
[32] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C-H Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: A tutorial. IEEE wireless Communications, 18(2):66–74, 2011.
[33] Matthieu Bloch and Joao Barros. Physical-layer security: from information theory to security engineering. Cambridge University Press, 2011.
[34] Haji M Furqan, Jehad Hamamreh, Huseyin Arslan, et al. Physical layer security for noma: Requirements, merits, challenges, and recommendations. arXiv preprint arXiv:1905.05064, 2019.
[35] Ashish Khisti, Gregory Wornell, Ami Wiesel, and Yonina Eldar. On the gaussian mimo wiretap channel. In 2007 IEEE International Symposium on Information Theory, pages 2471–2475. IEEE, 2007.
[36] Frédérique Oggier and Babak Hassibi. The secrecy capacity of the mimo wiretap channel. IEEE Transactions on Information Theory, 57(8):4961–4972, 2011.
[37] Jehad M Hamamreh and Huseyin Arslan. Joint phy/mac layer security design using arq with mrc and null-space independent papr-aware artificial noise in siso systems. IEEE Transactions on Wireless Communications, 17(9):6190–6204, 2018.
[38] Naoki Ishikawa, Jehad M Hamamreh, Eiji Okamoto, Chao Xu, and Lixia Xiao. Artificially time-varying differential mimo for achieving practical physical layer security. IEEE Open Journal of the Communications Society, 2:2180–2194, 2021.
[39] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Using the physical layer for wireless authentication in time-variant chan-

nels. IEEE Transactions on Wireless Communications, 7(7):2571–2579, 2008.
[40] Wade Trappe. The challenges facing physical layer security. IEEE Communications Magazine, 53(6):16–20, 2015.

MUHAMMET KIRIK received the B.Sc. degree in electrical and electronics engineering from Antalya Bilim University, Turkey in 2020. He is currently pursuing his M.Sc degree in Antalya Bilim University in the electrical and computer engineering department. His current research interests include orthogonal frequency division multiplexing multiple input multiple output systems, multi-dimensional modulation techniques, and orthogonal/non-orthogonal multiple access schemes for future wireless systems.

JEHAD M. HAMAMREH Jehad M. HAMAMREH is the Founder and Director of WISLAB (wislabi.com), and A. Professor with the Electrical and Electronics Engineering Department, Antalya Bilim University. He received his Ph.D. degree in telecommunication engineering and cyber systems from Istanbul Medipol University, Turkey, in 2018. Previously, he worked as a Researcher at the Department of Electrical and Computer Engineering at Texas AM University. He is the inventor of more than 20+ Patents and an author of more than 75+ peer-reviewed scientific papers along with several book chapters. His innovative patented works won the gold, silver, and bronze medals by numerous international invention contests and fairs.

His current research interests include wireless physical and MAC layers security, orthogonal frequency-division multiplexing and multiple-input multiple-output systems, advanced waveforms design, multidimensional modulation techniques, and orthogonal/non-orthogonal multiple access schemes for future wireless systems. He is a serial referee for various scientific journals as well as a TPC member for several international conferences. He is an Editor at Researcherstore, RS-OJICT journal, and Frontiers in Communications and Networks. Email: jehad.hamamreh@gmail.com.