Enhancing PHY Layer Security with Transmit and Receive Beamforming Diversity Schemes for MISO and SIMO System Models

Abeer A S Elhoula, Graduate Stud.
Libyan Academy
School of Applied Science and Engineering
Department of Electrical and Computer Engineering
abeer.elhoula@academy.edu.ly

Prof. Marai M. Abousetta
Libyan Academy
School of Applied Science and Engineering
Department of Electrical and Computer Engineering
m.abousetta@academy.edu.ly

Tarek Saleh M. Ghmati
Elemrgib University
Al-Graboulli Faculty of Engineering
Department of Electrical and Computer Engineering
t.ghmati@elmergib.edu.ly

ABSTRACT

The security of the communication channels has become a hot research topic for the 5G due to the tremendous advancements in wireless communications over the past two decades, including the recent emergence of the fifth generation (5G) in mobile wireless communications, which is anticipated to support extremely large user connections and exponentially increase the wireless services.

This paper describes a new approach to the problem of interception of wireless communication channels between the legitimate users. Physical Layer Security PLS is new topic enhancing the secrecy performance of a Single-input-multiple-output (SIMO) system for wireless communication from one base-station equipped by single transmitting antenna to many users equipped by multiple receiving antennas each. The receiving beamforming techniques "with a perfect channel CSI is assumed", such as Maximum Ratio Combining MRC and Equal Gain Combining EGC is utilized in order to achieve the perfect secure receiving for the legitimate users. A downlink transmission of Multiple-input-Single-output (MISO) has been designed 'Base-station' equipped by multiple transmitting antennas and users (legitimate and Eavesdropper) with single receiving antenna can focus the information signal in the direction of the intended/information user while minimizing the signal's quality as received by an eavesdropper. The technique of Artificial Noise AN is also researched in addition to beamforming.

The secrecy rate performance measured as Bit-error-ratio BER vs SNR in SIMO system model implemented with the receiving beamforming schemes MRC and EGC suggested that the MRC is considered as an optimal receive beamforming diversity technique in order to achieve a best secrecy rate of transmitted signal and as it was compared to secrecy rate performance resulted from MISO system model.

Keywords: Physical Layer Security PLS, Beamforming, Artificial Noise AN, Receive Beamforming, Eavesdropper, SIMO, MISO, Maximum ratio combining MRC, Equal gain combining EGC, Bit-error-ratio BER.

1. INTRODUCTION

Wireless communication technology may be a need for modern-day life since human creatures depend on this innovation for information transmission. In most cases, the information contains confidential data such as banking transactions, military applications, and interactive media. These networks are subject to various kinds of attacks. Usually, the upper layers of the open system interconnect model are utilized to handle any inconsistencies related to the security services, authenticity, confidentiality, integrity and privacy of transmitted information. These attributes are mostly dependent on cryptographic algorithms which include secret-key distribution, public-key, and symmetric encryption. All these techniques function independently from the physical layer [1].

Based on the assumption that the eavesdropper has limited computing power ability, the above-mentioned techniques are considered to be secure. Also, they rely on fundamental computational complexity for their robustness. Recent advances in quantum computing pose a serious threat to the currently used cryptographic schemes with their unlimited computational capacity [2]. Therefore, it is apparent that the traditional methods in secure wireless communication are becoming less reliable since its protecting data after the communication phase. Due to the broadcast nature of the physical medium, wireless multi-user communications are very susceptible to eavesdropping, and it is critical to protect the transmitted information. Security of wireless communications has been traditionally achieved at the network layer with cryptographic schemes. However, classical cryptography might not be suitable in large dynamic networks, since it requires key distribution and management, and complex encryption/decryption algorithms and it is more susceptible to deciphering using cryptosystems-analyst brute force and supercomputers available nowadays. A method that exploits the characteristics of wireless channels known as physical layer security PLS.

2. BACKGROUND

Traditionally, any conflicts relating to the attributes of authenticity, confidentiality, and privacy of data transmission are handled by the upper layers of the open system interconnect OSI model.

The computational security is conditioned on the limited computational capability of the adversary, such that the encryption is computationally infeasible to decrypt. With the rapid development of computational devices such as quantum computing poses a major threat in existing security techniques in wireless networks, the wireless security solely provided by cryptographic techniques is becoming vulnerable to attacks. Therefore, it is apparent that the traditional methods in secure wireless communication are becoming less reliable in the presence of the tremendous development in decoding algorithms and the great development in the speed of computer processors and supercomputers.

Cryptography techniques such as secret-key distribution, public-key, and symmetric encryption are mostly responsible for these characteristics. All of these methods are independent of the physical layer. These techniques are considered secure based on the assumption that the eavesdropper has limited processing capability. Moreover, they rely on underlying computational complexity for their robustness. Recent advances in quantum computing pose a serious threat to the currently used cryptographic schemes with their unlimited computational capacity [2]. As a result, it is clear that traditional secure wireless communication technologies are becoming less trustworthy.

2.1 Information-Theoretic

In Figure 1, *Claude Shannon* proposed it in 1949 [7] proposed a model of the secrecy system is illustrated. The main goal of this system is to reliably convey the message $\boldsymbol{M}$ (Plain message), which is also hidden from Eavesdropper's (Eve's) perspective. Alice (Transmitter) and Bob (Receiver) can do this because they have access to the random key $\boldsymbol{K}$, which is unknown to Eve and is used by Alice to encrypt the message into the Cipher test $\boldsymbol{C}$. Bob, on the receiving end, uses key $\boldsymbol{K}$ to decrypt the Cipher text $\boldsymbol{C}$ and determine the delivered message $\boldsymbol{M}$. For, $\boldsymbol{H(M)} \leq \boldsymbol{H(K)} \rightarrow Perfect\ Secrecy\ Condition - (One - time\ pad)$.

The entropy of the key $\boldsymbol{H(K)}$ should be higher than or equal the entropy of the message $\boldsymbol{H(M)}$, for an encryption scheme to be perfectly secured. In wireless network channels this is not going to work because we do need another channel in some way so it can transmit as much keys as we have messages due to one-time pad.

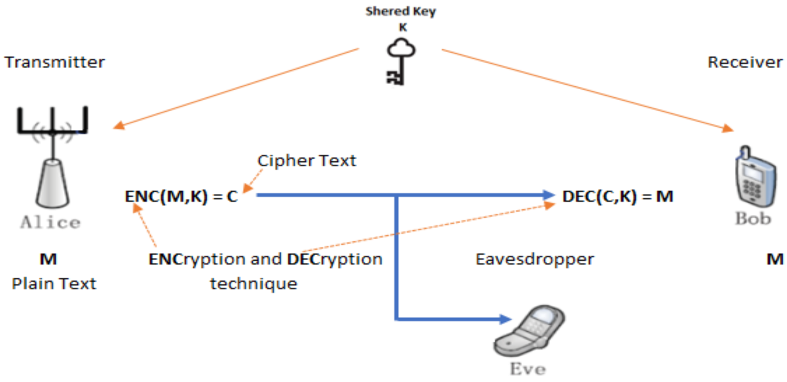

Fig. 1: Shannon Model for secure system

From the perspective of information-theoretic, this is the type of security that purely determines the fundamental limits of PLS measures. In an additive white Gaussian noise (AWGN) channel, the channel capacity is directly proportional to the power of the signal is given by:

$$\boldsymbol{C} = \boldsymbol{B}l \log_2(1 + \boldsymbol{SNR}) \tag{1}$$

where $\boldsymbol{B}$ represents the channel's bandwidth in Hertz (*Hz*), and $\boldsymbol{SNR}$ is the signal-to-noise ratio.

$$\boldsymbol{SNR} = \frac{\boldsymbol{P}}{\boldsymbol{\sigma^2}} \tag{2}$$

where $\boldsymbol{P}$ denotes the power of the signal and $\boldsymbol{\sigma^2}$ is the noise power.

Therefore, the difference between the capacities of Bob and Eve's channels gives the secrecy rate of the PLS system model given in Figure 2 by:

$$Secercy\ rate\ R = \boldsymbol{C}_{Bob} - \boldsymbol{C}_{Eve} \tag{3}$$

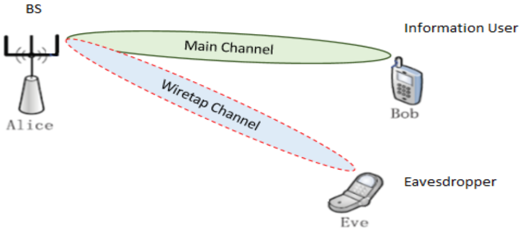

Fig. 2: PLS system model

In 1975, *Wyner* [11] proposed the concept of weak secrecy by expanding *Shannon's* information-theoretic secrecy theory Figure 3. In this model, the encoder operates on blocks of k source bits $\boldsymbol{S}^K = (S^1, S^2, S^3, \dots, S^k)$ and produces an encoded sequence $\boldsymbol{X}^n = (X^1, X^2, X^3, \dots, X^n)$ of length n.

An encoder receives a binary message from the source, $\boldsymbol{S}^K$, and turns it into a codeword, $\boldsymbol{X}^n$, with n bits. Before being recognized as $\boldsymbol{Y}^n$ at the targeted receiver (intended information user), the codeword travels through the main channel where it is subject to noise and other sources of error. However, the wiretap channel allows the eavesdropper to obtain an even larger degraded sample of $\boldsymbol{Y}^n$, which results in $\boldsymbol{E}^n$ being provided to the eavesdropper.

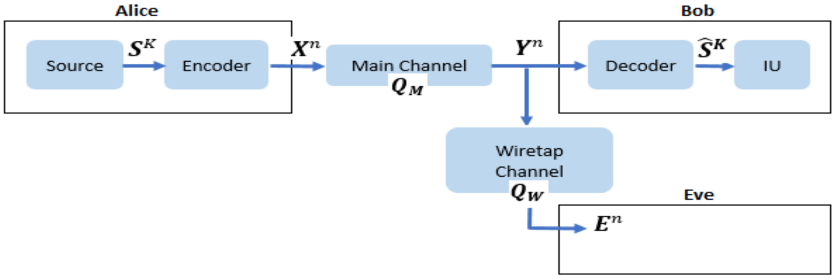

Fig. 3: *Wyner* wiretap channel model

With *Wyner's* model, it is assumed that the signal received by the eavesdropper is somewhat degraded and less reliable than the signal received by the legitimate receiver [11]. He proved that even in the presence of adversary Eve, a perfectly secure transmission to the IU is guaranteed if the information rate to the IU is greater than the leakage information rate obtained by the Eve [11,26-27].

3. PHYSICAL LAYER SECURITY

Due to the privacy issues brought on by the broadcast nature of wireless communications, PLS is best positioned to offer the greatest security benefits in this field. Through the use of the physical characteristics of wireless channels, researchers hope to gain a better understanding of the level of secrecy that may be achieved through PLS. The randomness of wireless channels produced on by noise, fading, and interference has historically been seen in wireless communications as having negative, deteriorating effects [21]. However, PLS can take advantage of these effects to guarantee a degraded, less desirable channel for a possible eavesdropper while offering a more favorable channel to the intended recipient [22].

The Secrecy coding at the physical layer has its basis in the well secrecy metrics from information-theoretic security. Secrecy rate, Secrecy Outage Probability (SOP), and Quality of Service (QoS) which is related to Signal-to-interference-plus-noise ratio (SINR): This metric may be described as the quantitative relationship between the power of the received signal and power of the interference plus noise.

In the recent, physical layer security (PLS) provides better signal quality at the information users IUs compared to that at the Eavesdropper Eve using signal beamforming and artificial noise AN technique through utilizing the knowledge of transmit channels.

3.1 Channel State Information CSI

The characteristics of a channel in a wireless communication link are defined by CSI. It’s is used to describe the propagation of the transmitted signal in relation to the corresponding effects such as scattering, fading, and power decay with distance. CSI can be classified into two classes, perfect and imperfect CSI. The perfect one involves the complete knowledge of the channel properties of a communication link. The imperfect CSI is concerned with characterization of the statistical information only. Such information includes the average channel gain, the type of fading distribution, the line-of-sight (LOS) component, and the spatial correlation [8].

4. BEAMFROMING

Beamforming is a method that concentrates a wireless signal on a single receiving device rather than having it spread out in all directions as it would typically from a broadcast antenna. It’s a signal processing technique that is used to transmit signals effectively in intended directions to give a maximum signal difference between the receiver in the intended direction and the one in the unintended direction. Beamforming forms a beam in the direction of the desired recipient to maximize the signal-to-noise power ratio while suppressing the reception or transmission in the direction of the unintended user, Figure 4. As a result, the system's energy efficiency is greatly increased. Instead of being dispersed evenly, the energy is conveyed or directed in a certain direction.

To achieve spatial selectivity, beamforming, can be utilized at both the sending and receiving ends, as known as transmit beamforming and receive beamforming.

4.1 Transmit Beamforming T-BF

Transmit beamforming steers the transmitted signal towards the intended receiver by finding the best possible channel among all the transmit antennas [8]. In terms of PLS, the goal of beamforming is to make sure that IU, the intended User, has a higher SNR than Eve, the eavesdropper.

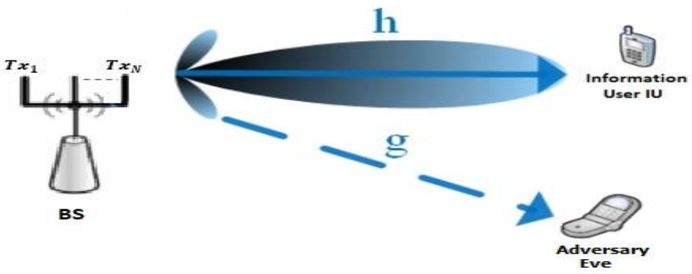

Fig. 4: Beamforming

Beamforming problem in PLS involves steering the transmitted signal towards the desired user while considering an interfering user trying to decode the transmitted information.

Employing the base station's multiple transmit antennas will enhance downlink performance. Depending on whether channel state information CSI is available at the transmitter, this provides us two options: *Transmit diversity* and *Transmit beamforming*; The Transmit diversity approaches like the *Alamouti* scheme [37] can be utilized to create diversity gain if the channel state information CSI at transmitter is not available 'imperfect channel'.

In transmit beamforming scheme, illustrated in Figure 5, two users assumed (IU and Eve) with a Multiple Input Single Output (MISO) channel has assumed with $\boldsymbol{N}$ transmit antennas and single receive antenna for each user. Weighting the information symbols s with a transmit beamforming vector $\boldsymbol{w} = [w_1, w_2, \dots, w_N]^T$ that adheres to the sum-power restriction creates the transmitted signal vector $\boldsymbol{x}$.

$$\boldsymbol{x} = \boldsymbol{w}s \tag{4}$$

$$\begin{bmatrix} x_1 \\ \cdot \\ x_N \end{bmatrix} = \begin{bmatrix} sw_1 \\ \cdot \\ sw_N \end{bmatrix} \tag{5}$$

Since the beamforming phase shifts is as: $w_i = \frac{{h_i}^*}{|h_i|} = \ e^{-i(\theta(h_i))}$

The fading-channel responses for the $\boldsymbol{N}$ independent fading paths is given by the vector

$\boldsymbol{h} \ = \ [h_1 \, , h_2 \ \cdots , h_N \ ]^T$, Then, the $IU's$ received signal is gained as:

$$r = \sqrt{\boldsymbol{P}}\boldsymbol{h^T x} + n \quad \rightarrow \quad r = \sqrt{\boldsymbol{P}}\ [h_1 \, , h_2 \ \cdots , h_N \ ] \begin{bmatrix} sw_1 \\ \cdot \\ sw_N \end{bmatrix} + n \tag{6}$$

$$r = \sqrt{\boldsymbol{P}} \sum_{i=1}^{N} h_i \, w_i s + n \tag{7}$$

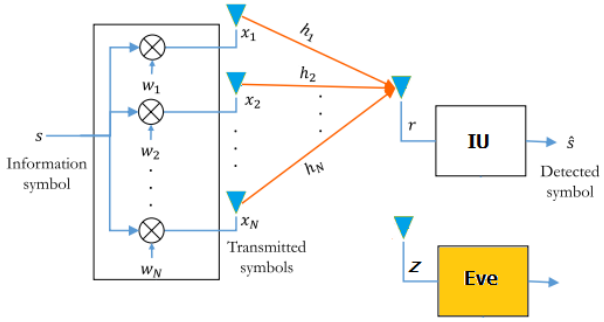

Fig. 5: Transmit Beamforming for MISO

$$r = \sqrt{\boldsymbol{P}}(h_1 w_1 s + h_2 w_2 s + \cdots + h_N w_N s) + n \tag{8}$$

$$r = \sqrt{\boldsymbol{P}}(h_1 \frac{{h_1}^*}{|h_1|} s + h_2 \frac{{h_2}^*}{|h_2|} s + \cdots + h_N \frac{{h_N}^*}{|h_N|} s) + n \tag{9}$$

$$r = \sqrt{\boldsymbol{P}}(|h_1| + |h_2| + \cdots + |h_N|)s + n \tag{10}$$

As a result, the receiver's SNR is increased by combining the many signals that are received at the intended Information User IU.

The estimation and detection of transmitted symbols $\hat{s}$ over flat-fading channel in additive Gaussian noise in a complex vector space can be measured by the following formula:

$$\hat{s} = r \frac{\mathbf{1}}{|\boldsymbol{h}|} = \frac{\mathbf{1}}{|\boldsymbol{h}|}(|h_1| + |h_2| + \cdots + |h_N|)s + \frac{\mathbf{1}}{|\boldsymbol{h}|} n = s + \frac{\mathbf{1}}{|\boldsymbol{h}|} n \tag{11}$$

Since the absolute value $|\boldsymbol{h}| = \sum_{i=1}^{N} |h_i|$ and the Frobenius norm $\|\boldsymbol{h}\|$ are related as $|h|^2 = hh^*$; $\|\boldsymbol{h}\| = \sqrt{\sum_{i=1} |hi|^2}$.

Where, the output of the received signal is scaled down by a factor $|\boldsymbol{h}| = \sum_{i=1}^{N} |h_i|$ which is the total-energy contained in the impulse response of the flat-fading channel.

4.2 Receive Diversity Beamforming R-BF

Here in this section a channel model of one transmitting antenna and several receiving antennas defines a SIMO channel configuration will be investigated. Since this configuration offer receive diversity, which allows the same information to be received across various fading channels.

The channels are randomly selected and assumed as independent and identically distributed $(i.i.d)$, so, the error event across those independent channels is also independent. The signal to noise ratios (SNR) of the channels are also $i.i.d$ and every channel path has the same average SNR. This forms the cornerstone of the SIMO model with receive diversity [16].

To improve the receiver's overall SNR, received signals are combined. When a receiver has multiple antennas, a signal processing method called Maximum Ratio Combining MRC and Equal

Gain Combing EGC will be employed [16]. Similar to how a matching filter MF, processes an incoming signal in the frequency domain, MRC processes the signal in the spatial domain. The inner product of the weights and the signal vector is maximized by MRC. Considering M-PSK transmission and $\boldsymbol{M}$ receive antennas are being used in the receiver, the signal that is being received is as follows:

$$r_k = h_k s + n_k \qquad for \quad 1 \le \ k \ \le \boldsymbol{M} \tag{12}$$

where $h_k = |h_k| e^{i(angle(h_k))}$ is the channel state response of the k^{th} channel path;

writing in the compact form as:

$$\boldsymbol{r} = \boldsymbol{h}s + \boldsymbol{n} \tag{13}$$

where, for each channel path, $\boldsymbol{r}$, $\boldsymbol{h}$, and $\boldsymbol{n}$ are vectors carrying samples of the received signal, channel state information, and noise component.

The receiver's combiner linearly combines $\boldsymbol{M}$ noisy received signals with weighting factors $\boldsymbol{w}$ and produces the combined signal as:

$$y = \boldsymbol{w}^H \boldsymbol{r} = \ \boldsymbol{w}^H \boldsymbol{h} s + \boldsymbol{w}^H \boldsymbol{n} \tag{14}$$

where $\boldsymbol{w}^H$ is *Hermitian vector = (conjugate transpose* of vector) $\boldsymbol{w}$.

Then for more simplifying of Eq. 14:

$$y = \sum_{k=1}^{M} w_k{}^* r_k = \ [w_1{}^*, w_2{}^*, \cdots, w_M{}^*] \begin{bmatrix} r_1 \\ \cdot \\ r_M \end{bmatrix} \tag{15}$$

The choice of weighting factors $\boldsymbol{w}$ depends on the type of combining technique used. Maximum Ratio Combining ***MRC*** and Equal Gain Combining ***EGC*** techniques are the well-known combining schemes.

4.2.1 Maximum Ratio Combining MRC

The maximum ratio combining method employs all $\boldsymbol{M}$ received signal components, weights them, and then combines the weighted signals to optimize the SNR at the combiner output. If the receiver is completely aware of the gains and phases of the channels, the SNR is maximized. To get the combined signals out of $\boldsymbol{M}$ receiving antennas and recalling to Eq. 14, Eq. 15 where the estimated channel gain and phase, the weights $\boldsymbol{w}$ is given as:

$$\boldsymbol{w_{MRC}}^k = \hat{h}_k{}^* = |\hat{h}_k| e^{-i\left(angle(\hat{h}_k)\right)} \qquad 1 \le \ k \le \boldsymbol{M}$$

where, $\hat{h}_k{}^*$ is estimated (gain and phase) CSI of k^{th} channel path

$$= \hat{\boldsymbol{h}} \ = \ [\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_M]^T \tag{16}$$

$$\therefore \quad (\boldsymbol{w_{MRC}}^k \ )^{\boldsymbol{H}} = \ [\hat{h}_1{}^*, \hat{h}_2{}^*, \cdots, \hat{h}_M{}^*] \tag{17}$$

Substitute $\boldsymbol{w_{MRC}}^k$ in Eq. 15 yields:

$$y = (\boldsymbol{w_{MRC}}^{k})^{H}\boldsymbol{r} = \sum_{k=1}^{M} \hat{h}_k{}^{*} r_k = \left(\hat{h}_1{}^{*} h_1 + \hat{h}_2{}^{*} h_2 + \cdots + \hat{h}_M{}^{*} h_M\right) s + noise \qquad (18)$$

Where $noise$ is summation of all $\boldsymbol{M}$ antennas noises ➔ $noise = \sum_{k=1}^{M} \hat{h}_k{}^{*} n_k$
As a perfect channel response CSI is assumed, the estimated channel gain and phase for the k^{th} channel $|\hat{h}_k|$, $angle(\hat{h}_k)$ respectively is almost equal to the complex impulse response of the k^{th} channel path$h_k = |h_k| e^{i(angle(h_k))}$.

$$|\hat{h}_k| \approx |h_k|, \quad angle(\hat{h}_k) = angle(h_k)$$

Then the output of MRC in Eq. 18 becomes as:

$$y = (|h_1|^2 + |h_2|^2 + \cdots + |h_M|^2)s + noise = \|\boldsymbol{h}\|^{\boldsymbol{2}} s + noise \qquad (19)$$

Here, a prove that the SNR will increase with an increase of channel response paths, i.e., receiving antennas $\boldsymbol{M}$. The estimation and detection of transmitted symbols $\hat{s}$ over flat-fading channel in additive Gaussian noise in a complex vector space can be measured by multiplying the output of MRC y yielded in Eq. 19 by $\frac{1}{\|\boldsymbol{h}\|^2}$ or, in other words, scaled down by a factor of $\|\boldsymbol{h}\|^{\boldsymbol{2}}$ which is the total-energy contained in the impulse response of the flat-fading channel, as following formula:

$$\hat{s} = y \quad \frac{\boldsymbol{1}}{\|\hat{\boldsymbol{h}}\|^{\boldsymbol{2}}} \approx \frac{\boldsymbol{1}}{\|\boldsymbol{h}\|^{\boldsymbol{2}}}(|h_1|^2 + |h_2|^2 + \cdots + |h_M|^2)s + \frac{\boldsymbol{1}}{\|\boldsymbol{h}\|^{\boldsymbol{2}}} noise$$

$$= \frac{\sum_{k=1}^{M} \hat{h}_k{}^{*} r_k}{\sum_{k=1}^{M} |\hat{h}_k|^2} = s + \frac{\boldsymbol{1}}{\|\boldsymbol{h}\|^{\boldsymbol{2}}} noise \qquad (20)$$

Since $\|\boldsymbol{h}\|^{\boldsymbol{2}} = \sum_{k=1}^{M} |h_k|^2$

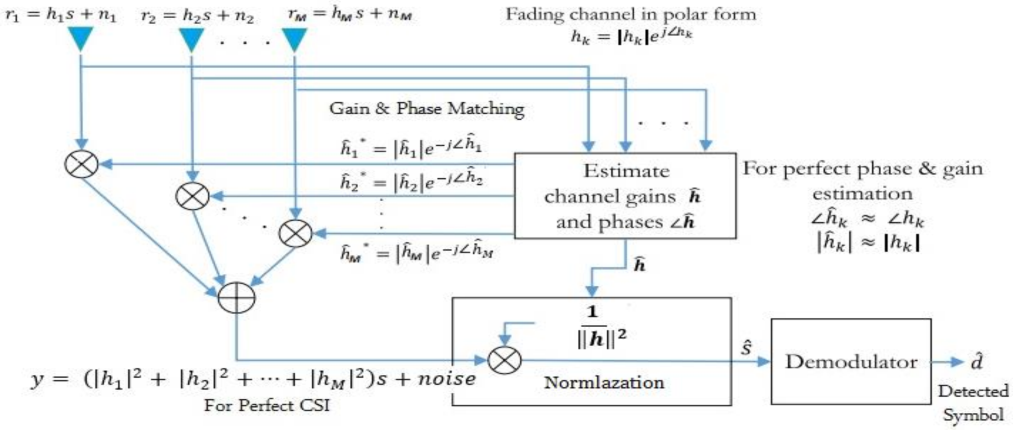
$r_1 = h_1 s + n_1$
$r_2 = h_2 s + n_2$
$r_M = h_M s + n_M$
Fading channel in polar form
$h_k = |h_k| e^{j\angle h_k}$
Gain & Phase Matching
$\hat{h}_1{}^* = |\hat{h}_1| e^{-j\angle \hat{h}_1}$
$\hat{h}_2{}^* = |\hat{h}_2| e^{-j\angle \hat{h}_2}$
$\hat{h}_M{}^* = |\hat{h}_M| e^{-j\angle \hat{h}_M}$
Estimate channel gains $\hat{\boldsymbol{h}}$ and phases $\angle\hat{\boldsymbol{h}}$
For perfect phase & gain estimation
$\angle\hat{h}_k \approx \angle h_k$
$|\hat{h}_k| \approx |h_k|$
$\hat{\boldsymbol{h}}$
$\frac{1}{\|\boldsymbol{h}\|^2}$
Normlazation
$\hat{s}$
Demodulator
$\hat{d}$
Detected Symbol
$y = (|h_1|^2 + |h_2|^2 + \cdots + |h_M|^2)s + noise$
For Perfect CSI

Fig. 6: Maximum Ratio Combining MRC with perfect CSI assumed [16].

4.2.2 Equal Gain Combining EGC

In equal gain combining (EGC), the detection process is carried out on a linear combination of equally weighted co-phased signals. Because it doesn't need to estimate the fading channels' gain, it has a reasonably simple implementation. EGC provides comparable performance with respect to MRC scheme.

$$\boldsymbol{w_{EGC}}^{k} = \frac{\hat{h}_k^{\,*}}{\left|\hat{h}_k\right|} = e^{-i\left(angle\left(\hat{h}_k\right)\right)} \qquad 1 \le \ k \le \boldsymbol{M}$$

$$\therefore \qquad (\boldsymbol{w_{EGC}}^{k}\ )^{\boldsymbol{H}} = \ [\frac{\hat{h}_1^{\,*}}{\left|\hat{h}_1\right|}, \frac{\hat{h}_2^{\,*}}{\left|\hat{h}_2\right|}, \cdot \cdot \cdot, \frac{\hat{h}_{\boldsymbol{M}}^{\,*}}{\left|\hat{h}_{\boldsymbol{M}}\right|}] \qquad (21)$$

Substitute $\boldsymbol{w_{EGC}}^{k}$ in Eq. 15, the output of EGC becomes as:

$$\begin{aligned} y = (\boldsymbol{w_{EGC}}^{k})^{H}\boldsymbol{r} &= \sum_{k=1}^{M} e^{-i\left(angle\left(\hat{h}_k\right)\right)}\ \ h_k \ + \ \sum_{k=1}^{M} e^{-i\left(angle\left(\hat{h}_k\right)\right)}\ \ n_k \\ &= (|h_1| + |h_2| + \cdots + |h_M|)s + noise \qquad (22) \end{aligned}$$

Also, the estimation and detection of transmitted symbols $\hat{s}$ over flat-fading channel in additive Gaussian noise in a complex vector space can be measured by:

$$\hat{s} = \frac{y}{\sum_{k=1}^{M}|h_k|} = \ \frac{\boldsymbol{1}}{\sum_{k=1}^{M}|h_k|}(|h_1| + |h_2| + \cdots + |h_M|)s + \frac{\boldsymbol{1}}{\sum_{k=1}^{M}|h_k|}noise \qquad (23)$$

4.3 Artificial Noise AN

The notion of using artificial noise to enhance security in the physical layer was first proposed in [32]. They identified AN-based transmission as an effective technique that can be deployed in PLS to ensure secure communication in wireless networks. The procedure involves sending an interference signal to intentionally decrease the Eve eavesdropper's channel quality in order to interfere with their ability to listen in.

The transmitter BS creates an artificial noise and transmits it in all directions besides the direction of the intended user IU. This is the artificial noise technique. As assumed that, the channel is perfect channel, so the transmitter is aware of the Eve's CSI, transmitter can enhance the total impact of the AN on Eve.

Since the beamforming technique is used to concentrate the information signal power on the IU(s) while artificial noise (AN) signaling the information-unintended users Eve(s), consequently degrading the quality of the information signal at those users but not impacting the quality of the channel of the information-intended users IU [32]. In the AN precoding scheme, the transmitter-BS divides the transmission power between transmitting the information to the intended user or recipient, IU, and transmitting the noise signal towards the eavesdropper, Eve. Generating AN depends on the transmitter 's knowledge of the Eve eavesdroppers' channel state information. In a case where the IU 's CSI is known and the Eve 's CSI is unknown, the isotropic AN is generated.

The generated AN is designed such that it lies in the null-space (the orthogonal signal) of the intended IU and directed in the range space of the unintended receiver, eavesdropper Eve [8,33].

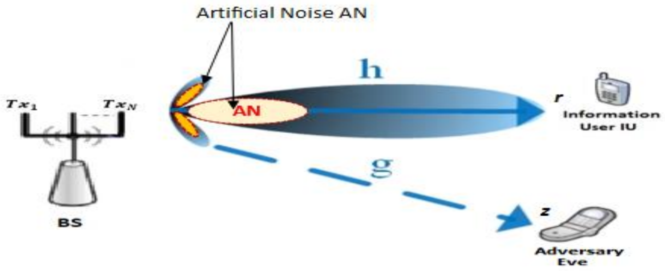

Fig. 7: MISO Model: Transmit Beamforming with Artificial Noise

The information signal is represented by the transmitted signal divided by the entire transmission power allocated to the generation of AN by:

$$\boldsymbol{x} \;=\; \sqrt{(1-\alpha)\boldsymbol{P}}\boldsymbol{w}s_k + \sqrt{\alpha\boldsymbol{P}}\,\boldsymbol{v}s_z \tag{24}$$

where $\boldsymbol{x}$ is the signal transmitted by a multi-antenna transmitter base-station; α denoted as fraction of power allocated for information signal power; s_k is the information signal, s_z denotes the AN signal, which is chosen to be separate from the source information symbols, i.e., $s_k \neq s_z$, and the beamforming complex Gaussian weight vector for the information and generated AN signal vector 'the signal lies in the null-space of $IU's$ CSI' are represented by $\boldsymbol{w}$ and $\boldsymbol{v}$ components, respectively. And $\mathrm{s}_k, \mathrm{E}\{|s_{k=1}|^2\} = 1 * P$, is the information source symbol intended for IU_k. s_z, $\mathrm{E}\{|s_z|^2\} = 1$, is a zero mean unit variance Gaussian random variable representing the AN used to jam the Eve.

Additionally, the requirement is met by the transmitter selecting $\boldsymbol{v}$ to lie within the $\boldsymbol{h^T}$ null-space, as:

$$\boldsymbol{h^T v} = \boldsymbol{0} \tag{25}$$

Thus, the signals received by IU will disappear the generated AN related component since its meet the above condition, the received signal at IU is:

$$\begin{aligned} r_{IU} &= \boldsymbol{h^T x} + n_{IU} \\ &= \boldsymbol{h^T}\left(\sqrt{(\boldsymbol{1}-\boldsymbol{\alpha})\boldsymbol{P}}\boldsymbol{w}s_k + \sqrt{\boldsymbol{\alpha P}}\boldsymbol{v}s_z\right) + n_{IU} \\ &= \boldsymbol{h^T}\sqrt{(\boldsymbol{1}-\boldsymbol{\alpha})\boldsymbol{P}}\boldsymbol{w}s_k + n_{IU} \end{aligned} \tag{26}$$

In contrast, the received signal by $\boldsymbol{Eve}$ via well-known *base-station -Eve* CSI channel response $\boldsymbol{g}$ is as:

$$\begin{aligned} z_{Eve} &= \boldsymbol{g^T x} + n_{Eve} \\ &= \boldsymbol{g^T}\left(\sqrt{(\boldsymbol{1}-\boldsymbol{\alpha})\boldsymbol{P}}ws_k + \sqrt{\boldsymbol{\alpha P}}\boldsymbol{v}s_z\right) + n_{Eve} \end{aligned}$$

$$= \boldsymbol{g^T}\sqrt{(\mathbf{1}-\boldsymbol{\alpha})\boldsymbol{P}}\boldsymbol{w}s_k + \boldsymbol{g^T}\sqrt{\boldsymbol{\alpha P}}\boldsymbol{v}s_z + n_{Eve} \qquad (27)$$

The related AN component $\{\boldsymbol{g^T v}\}$ of the observed signal by Eve is remains in the received signal in which will degrade the quality of received signal and by conditioning in Eq. 25 by configuring the AN to affect Eve and all possible Eavesdroppers in all subspaces besides $IU's$.

5. SIMULATION MODELS AND RESULTS

5.1 Transmit Beamforming (MSO System Model) Simulation

To implement the beamforming transmission using a multiantenna system as derived in section 4.1. Based on whether the availability of beamforming technique at the transmitter, this provides us to implement two scenarios: firstly, the transmitter with multiple antennas transmits the data symbols in all directions isotropic ‘No beamforming’, secondly, transmit beamforming, it sends the data symbols directed to the intended information user IU with the condition of the CSI of the $transmitter - IU$ is known. A simulation MATLAB of MISO system model has been implemented in order to prove theoretical results. The proposed system model that was assumed is that the transmitter is equipped with a different $\boldsymbol{N} = 2, 4$ ... transmit antennas, and the legitimate information user IU and the eavesdropper Eve each have a single receiving antenna as illustrated in Figure 5.

5.1.1 BER Performance vs. SNR with / without Transmit Beamforming Result Discussion

This simulation, which employs 4-PSK modulation, shows how transmit beamforming based on $IU's$ CSI can give legitimate IU an improved BER over SNR range while $Eve's$ BER remains the same as the theoretical transmit No-beamforming performance.

Figure 8, shows the semiology plot of BER at legitimate IU and unintended user Eve and shows as the number of transmit antennas rises, so does the BER rate is hugely decreases ‘hugely improves’ at IU for the range of SNR. This clarifies the effectiveness of transmit beamforming and antenna diversity.

The idea of utilizing transmit-beamforming to offer a measurable amount of secrecy of the $transmitter - IU$ channel as opposed to that $transmitter - Eve$ is shown clearly in the plotted curve of SNR and BER difference values ‘gap’ between IU and Eve. This SNR and BER gap are increased as number of transmitting antennas increases.

5.1.2 BER Performance vs. SNR Transmit Beamforming with AN Result Discussion

A simulation MATLAB of MISO system model with power allocation in order to generate AN Artificial Noise with a different given value of transmit power has been implemented and investigated. The previous system model configurations and assumptions was kept the same except that, the base-station-Eve CSI is assumed unknown. N of transmit antennas, and the legitimate information user IU and single eavesdropper Eve each have a single receiving antenna as illustrated in Figure 7.

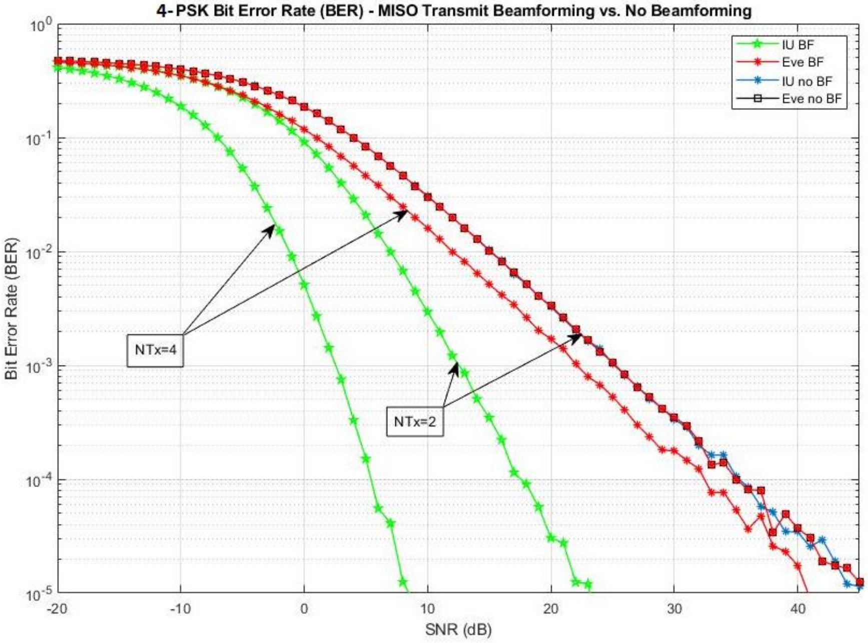

Fig. 8: MISO Semiology plot for BER vs. SNR with different NTx

This simulation, which employs 4-PSK modulation. Figure 9, shows the semiology plot of BER with range of SNR at legitimate IU and unintended user Eve. It's clear that when transmit beamforming based on IU's CSI with an artificial noise AN generated at the transmitter and transmitted along with source information signal with allocated power of 20% of total transmit power, i.e., 80% of transmit power is allocated for the useful source information with a variation of assumed power value $\boldsymbol{P} = 1{,}2$. It shows that legitimate IU improves the BER over SNR range while Eve's BER degraded with a clear curve reading with an increase in SNR. The reason of BER at Eve degraded and affected hugely is that the AN added to observed signal that makes the signal quality at Eve is very poor and the observed useful signal is not clear any more since it corrupted by AN plus channel noise.

An improve in BER of at IU is increasingly rises with a rising in value of transmitting power as it shown in the Figure 9 where the curve of IU BER colored yellow is increased with an increase in $\boldsymbol{P} = 2$ and that is very noticeable with respect to curve of IU BER colored green with $\boldsymbol{P} = 1$.

5.2 Receive Beamforming (SIMO System Model) Simulation

The proposed system model is a simple SIMO model consists of a single transmitting antenna at the base-station and single information user IU equipped by multiple receiving antennas. the maximum ratio combining MRC technique implemented as it is the most famous optimal beamforming receiving diversity technique beside to equal gain combining EGC in order to achieve better performance BER at the multiple receive antennas M at information user IU.

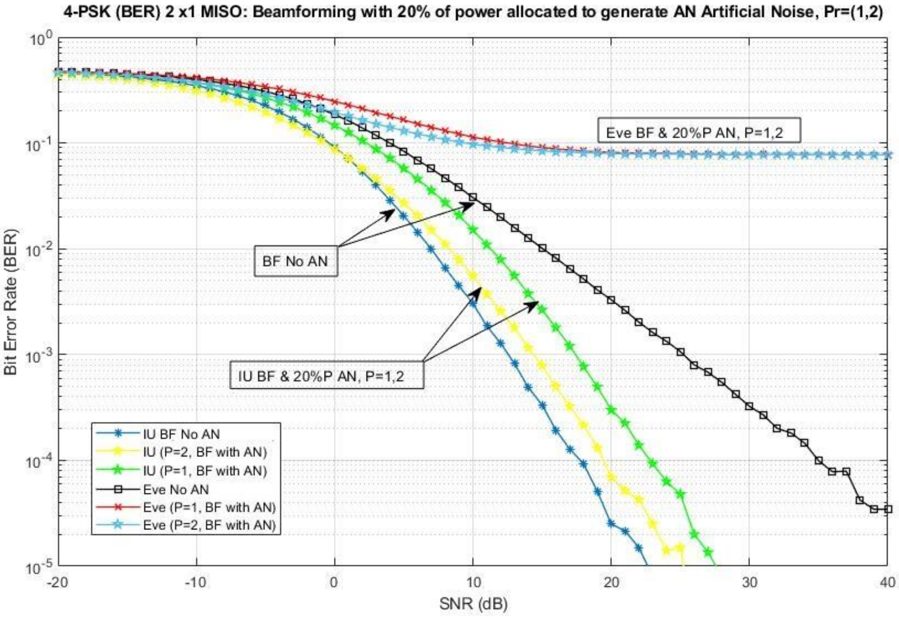

Fig. 9: BER vs. SNR 2x1 MISO of pair users (IU and Eve) BF with AN

5.2.1 BER Performance vs. SNR of MRC/EGC Receive Beamforming Result Discussion

The same system configuration is assumed as mentioned in the previous sections, perfect CSI, and a different number of receiving antennas at IU. In a $1x2, 1x4$ SIMO systems with MRC, the IU's BER performance is compared to the other system Model, i.e., MISO system of multiple transmit antennas at base-station and single receive antenna at IU, i.e., $2x1, 4x1$ MISO transmits beamforming, respectively. According to the simulation's results, a receiver can use this receiving technique to simplify the transmitter by reducing its complexity. A SNR increases the BER rate decreases.

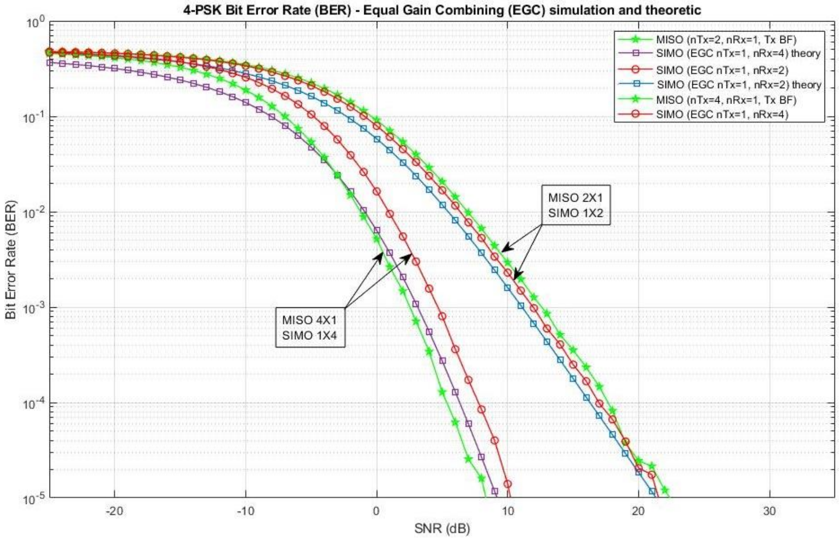

Fig. 10: BER vs. SNR for MRC SIMO compared to MISO, NTx=2,4 and MRx=2,4

As the number of transmit antennas rises in MISO, SNR improves at the IU. This clarifies the effectiveness of antenna diversity. In other words, the power of a system with several antennas is contrasted with a system with a single antenna. On the other hand, in SIMO MRC or EGC, the SNR gets increase as the number of receiving antennas at IU increases. This was proven clearly from the Eq. 19 and as it shown in plotted BER in Figure 10.

Since EGC is relatively less complexity in implementation and provides a comparable performance with respect to MRC scheme, here in Figure 11, a comparison of BER for both techniques EGC and MRC. We conclude that the MRC is achieving a better BER performance with respect to EGP, difference of the BER plot improves as number or receiving antennas increases.

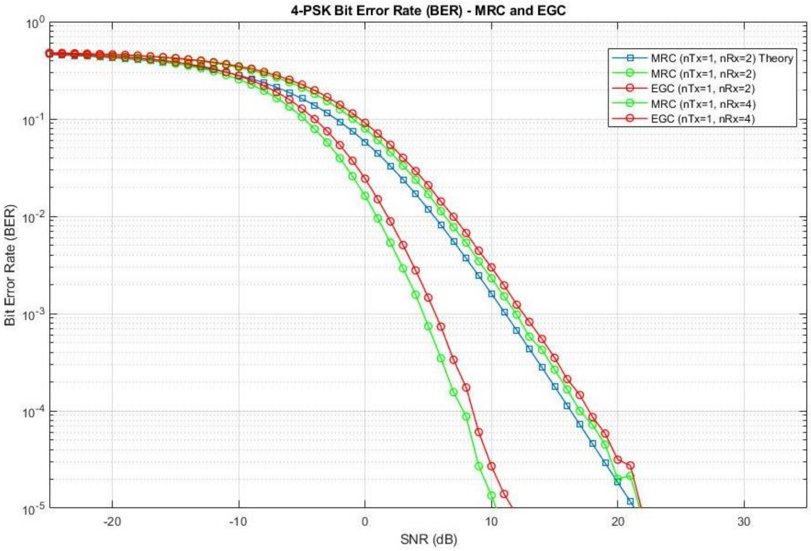

Fig. 11: MRC and EGC BER – SNR Comparison

6. CONCLUSIONS

In this paper, a beamforming, is highly recommended technique in the transmission and receiving signal, and used in the first place in order to achieve secure transmission of information signal via physical layer and enhances the upper layer security mechanisms. In terms of PLS, the goal of beamforming has been proved and assured that the intended User (IU) has a higher SNR than the eavesdropper (Eve). On the other hand, it was proved as well the BER at the IU is getting improved clearly compared to degraded BER at eavesdropper.

The illustrated results were demonstrated is clarified how beamforming transmission is used despite making it more challenging for an eavesdropper to intercept, beamforming can greatly increase the amount of secrecy of information being transmitted between a transmitter and an intended receiver. Moreover, the probability of intercept resulted of enhanced BER observed by an eavesdropper can be reduced even further by generating and utilizing isotropic AN by assuming eavesdropper CSI is unknown. Although the insertion of AN reduces the intended receiver's performance slightly, the impact on the eavesdropper is significantly greater, making AN is important component of a PLS security strategy. In SIMO system, as observed results out of simulating the two receive beamforming techniques, MRC and EGC; we concluded that the MRC is achieving a better BER performance with respect to EGC. The BER improves as a number of receiving antennas increases as well as with an increase of transmitting power.

REFERENCES

[1]. Zorgui, M. Wireless Physical Layer Security: On the Performance Limits of Secret-Key Agreement. Masters's Thesis, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, 2015.

[2]. Campagna, M.; Chen, A.L.; Dagdelen, Ö.; Darmstadt, T.U.; Ding, J.; Fernick, J.K.; Hayford, D.; Jennewein, T.; Lütkenhaus, N.; Mosca, M.; et al. Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges Quantum Safe Cryptography and Security Authors & contributors Quantum Safe Cryptography and Security 2. Technical Report. 2015. Available online: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[3]. Genço ˘glu, M.T. Importance of Cryptography in Information Security. IOSR J. Comput. Eng. 2019. 21, 65–68.

[4]. William Stallings, Book: 'Cryptography and Network Security Principles and Practices', Fourth Edition.

[5]. Djordjevic IB (2012) Quantum information processing and quantum error correction: an engineering approach. Elsevier/Academic Press, Amsterdam-Boston

[6]. Siddiqi.; Yu.; Joung. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices. Electronics 2019, 8, 981.

[7]. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715

[8]. An Overview of Key Technologies in Physical Layer Security. by: Abraham Sanenga, Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli, and Joseph Monamati Chuma.

[9]. Wei, Y.; Zeng, K.; Mohapatra, P. Adaptive wireless channel probing for shared key generation. In Proceedings of the IEEE INFOCOM, Shanghai, China, 30 Jule 2011; pp. 2165–2173.

[10]. Bassily, R.; Ekrem, E.; He, fX.; Tekin, E.; Xie, J.; Bloch, M.R.; Ulukus, S.; Yener, A. Cooperative security at the physical layer: A summary of recent advances. IEEE Signal Process. Mag. 2013, 30, 16–28.

[11]. Wyner A.D. The Wire-Tap Channel. Bell Syst. Tech. J. 1975. 54, 1355–1387.

[12]. Bloch, M.; Barros, J. Physical-layer Security: From Information Theory to Security Engineering; Cambridge University Press: Cambridge, UK,2011; p. 329.

[13]. A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned from Information Theory," Proceedings of the IEEE, vol. 103, no. 10, pp. 1814-1825, 2015.

[14]. What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing? WLAN Troubleshooting Guide—Huawei. Available online: https://support.huawei.com/enterprise/en/doc/EDOC1000060368/d9adbe5a/what-are-mimo-mrc-beamforming-stbc-and-spatial-multiplexing (accessed on 25 January 2020).

[15]. Mohaisen, M.; Wang, Y.; Chang, K. Multiple Antenna Technologies. Technical Report. Available online: https://arxiv.org/ftp/arxiv/papers/0909/0909.3342.pdf (accessed on 8 November 2019).

[16]. Mathuranathan Viswanathan, Wireless Communication Systems in Matlab, Second Edition, June 2020

[17]. S. M. Alamouti, A simple transmit diversity technique for wireless communications, IEEE Journal on Selected Areas in Communications pp. 1451-8, vol.16, no. 8, October 1998.

[18]. V. Tarokh, N. Seshadri, A. C alderbank, Space-Time codes for high data rate wireless communication: performance criterion and code construction, IEEE Trans. on. Information Theory, Vol. 44, No.2, pp.744-765, March 1998.

[19]. A. K. Sarangi, and A. Datta, “Capacity comparison of SISO, SIMO, MISO & MIMO systems,” 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), pp. 798-801, Erode, 2018, doi: 10.1109/ICCMC.2018.8488147

[20]. K. Sengar, and N. Rani, “Study and capacity evaluation of SISO, MISO and MIMO RF wireless communication systems,” International Journal of Engineering Trends and Technology, vol. 9, no. 9, March 2014.

[21]. M. Baldi and S. Tomasin, Physical and Data-Link Security Techniques for Future Communication Systems, Cham: Springer International Publishing Switzerland, 2016.

[22]. Wang, L. Physical Layer Security in Wireless Cooperative Networks; Wireless Networks; Springer International Publishing: Cham, Switzerland, 2018.

[23]. Björnson, E.; Bengtsson, M.; Ottersten, B. Optimal Multiuser Transmit Beamforming: A Difficult Problem with a Simple Solution Structure. IEEE Signal Process. Mag. 2014, 31, 142–148.

[24]. Sidiropoulos, N.D.; Member, S.; Davidson, T.N.; Luo, Z.Q. Transmit Beamforming for Physical-Layer Multicasting. IEEE Trans. SIGNAL Process. 2006, 54.

[25]. Huang, Y.; Palomar, D.P. Rank-constrained separable semidefinite programming with applications to optimal beamforming. IEEE Trans. Signal Process. 2010, 58, 664–678.

[26]. X. Liu, “Outage probability of secrecy capacity over correlated log-normal fading channels”, IEEE Commun. Lett., vol. 17, no. 2, pp. 289–292, Feb. 2013.

[27]. S. Jia, J. Zhang, H. Zhao, and Y. Xu, “Performance analysis of physical layer security over α-η-κ-μ fading channels”, China Commun., vol. 15, no. 11, pp. 138–148, Nov. 2018.

[28]. G. Chen and J. P. Coon, “Secrecy outage analysis in random wireless networks with antenna selection and user ordering”, IEEE Wireless Commun. Lett., vol. 6, no. 3, pp. 334–337, Jun 2017.

[29]. Weidong Fang, Fengrong Li,Yanzan Sun,Lianhai Shan, Shanji Chen, Chao Chen,and Meiju Li: 'Information Security of PHY Layer in Wireless Networks'

[30]. D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks”, IEEE Commun. Mag., vol. 53, no. 6, pp. 21–27, Jun. 2015.

[31]. Y. Zeng and R. Zhang, “Active eavesdropping via spoofing relay attack”, in 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, Mar. 2016, pp. 2159–2163.

[32]. Negi, R.; Goel, S. Secret communication using artificial noise. In Proceedings of the VTC-2005-Fall, 2005 IEEE 62nd Vehicular Technology Conference, Dallas, TX, USA, 28 September 2005; Volume 3, pp. 1906–1910.

[33]. Liao, W.C.; Chang, T.H.; Ma, W.K.; Chi, C.Y. QoS-based transmit beamforming in the presence of

[34]. eavesdroppers: An optimized artificial-aoise-aided approach. IEEE Trans. Signal Process. 2011, 59, 1202–1216.

[35]. S. Rohilla, D. K. Patidar and N. K. Soni, "Comparative Analysis of Maximum Ratio Combining and Equal Gain Combining Diversity Technique for WCDMA: A Survey," Internation Journal of Engineering Inventions, vol. 3, no. 1, pp. 72-77, 2013.

[36]. Beam-forming and matched filter techniques for the underwater acoustic detection of UHE neutrino; Online: https://www.sciencedirect.com/science/article/abs/pii/S0168900209005130?via%3Dihub

[37]. Jia Tang; Xi Zhang and Qinghe Du: "Alamouti scheme with joint antenna selection and power allocation over Rayleigh fading channels in wireless networks", GLOBECOM '05. IEEE Global Telecommunications Conference, 2005.