Physical Layer Secrecy rate improvement in MIMO using Artificial Fast Fading

[1]Harsha Chauhan, [2]Vimal Nayak, [3]Rina Parikh

[1]PG Student, [2,3]Professor,

[1]Electronics and Communication,
[1]Silver Oak college of Engineering and Technology, Ahmedabad, Gujarat, India

Abstract : Wireless communication system has broad cast nature so it limits the security and privacy. Physical layer security provides secure communication and having legitimate user to successfully obtain secure information. In the physical layer security schemes, an AFF (artificial fast fading) scheme decreased the eavesdroppers' received signal quality by pseudo fast fading to the transmitters signals, for symbol interval transmitted signals are multiplied by random weights. So, the artificial fast fading scheme increased weighted signals' power. So in such a manner, before transmission the weighted signals must be equalized. Due to this energy loss is generated in the legitimate receiver. Therefore, we to intercept weight vector so that weighted signal's power does not reduced. So that, we propose and achieve Physical layer secrecy rate in MIMO system using artificial fast fading plus information theory with detecting eavesdropper first.

Index Terms **- Physical layer security, MIMO, Artificial Fast Fading, Information Theory**.

I. INTRODUCTION

The wireless air interface is open and accessible to both authorized and illegitimate users due to the broadcast nature of radio propagation [1]. It has reported that in [2] an increasing number of wireless devices are abused for malicious attacks, data forging, financial information theft, online bullying, and so on. Therefore, ensuring secrecy and privacy are of utmost concern for future wireless communication systems.

A. *Physical Layer Security (PLS):*

The history of physical layer security started when Wyner suggested a discrete memoryless wiretap channel [3] consisting of a source, a destination, and an eavesdropper.

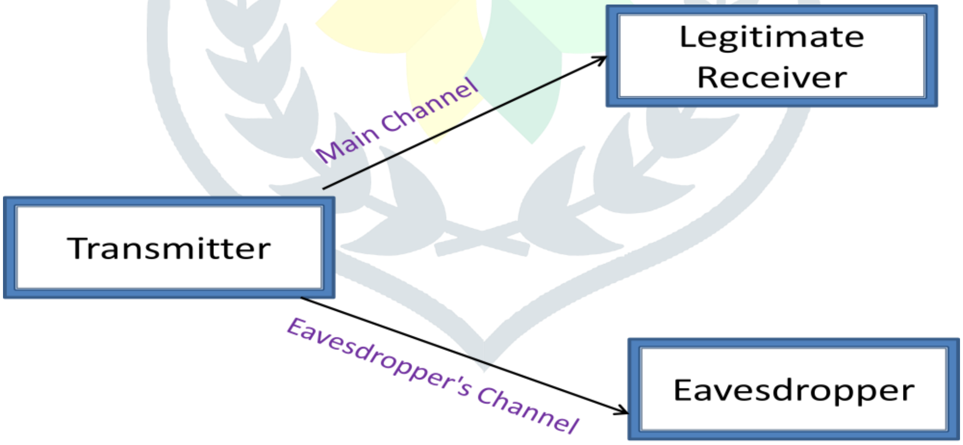


Figure 1 Basic System Model of physical layer security over wireless channels.[06]

It has been shown in figure 1 that secure transmission can be achieved, provided that the channel capacity in [4] of the main link from the source to the destination is higher than that of the wiretap link from the source to the eavesdropper. Wyner's results were extended from the discrete wiretap channel to the Gaussian wiretap channel, where the notation of secrecy capacity was developed, which was shown to be equal to the difference between the channel capacity of the main link and that of the wiretap link. In [5] author proved that for an arbitrary number of transmit/receive antennas, the perfect secrecy capacity is the difference of the two capacities, the one of the legitimate user minus the one of the eavesdropper, after a suitable optimization over the transmitter's input covariance matrix which was shown to be equal to the difference between the channel capacity of the main link and that of the wiretap link.
Basically, the objective of physical layer security is to minimize the amount of confidential information that can be obtained by the illegitimate users according to their received signals. To achieve secure communications over wireless channels, physical layer security explores time varying properties of the fading channel, smartly designs the channel code, and processes the transmitted signals, instead of relying on encryption. [6]. As an alternative, physical layer security (PLS), or information theoretic

security, is emerging as a promising paradigm to realize secure communication against eavesdropping attacks by exploiting the characteristics of wireless channels [7].

The existing physical layer security techniques can be classified into five major categories: theoretical secure capacity, and the power, code, channel, and signal detection approaches [8]. It was suggested that perfect secrecy is achievable using physical layer techniques subject to the condition that the channels are unknown to unauthorized users or the channel of the unauthorized users is noisier than that of the authorized users. Mainly there are two parts to do security on the physical layer 1) information theoretic 2) signal processing. Here we discuss on the base of information theoretic analysis [9].

Furthermore, various physical-layer techniques were proposed to achieve secure communication even if the receiver's channel is worse than the eavesdropper's channel. One of the main techniques is the use of interference or artificial noise in [10] to confuse the eavesdropper. With two base stations connected by a high capacity backbone, one base station can simultaneously transmit an interfering signal to secure the uplink communication for the other base station. In the scenario where the transmitter has a helping interferer or a relay node, the secrecy level can also be increased by having the interferer or relay to send codewords independent of the source message at an appropriate rate. When multiple cooperative nodes are available to help the transmitter, the optimal weights of the signal transmitted from cooperative nodes, which maximize an achievable secrecy rate, were derived for both decode-and-forward and amplify and- forward protocols. The use of interference for secrecy is also extended to multiple-access and broadcast channels with user cooperation [12].

B. Artificial Fast Fading

The Artificial Fast Fading scheme causes the effect of pseudo fast fading to the received signal of an eavesdropper without affecting the received signal of a legitimate receiver. This can be achieved by multiplying the signal to be transmitted by an intentional random weight which is called the AFF weight. AFF weight is generated to be canceled out by the CSI between an Alice and a Bob while processing the random property. Since the signal detection under a fading channel generally results in a lower performance then that under a noise only channel, the AFF scheme is effective in improving the secrecy. In the AFF scheme is considered for single stream transmitter. For cancelling the AFF weight by the CSI between a transmitter and a legitimate receiver, it is required that the system has Multiple Input Single Output (MISO) architecture Thus the AFF scheme has been developed in a MISO system in[13].

II. AFF GENERATION SCHEME (FREQUENCY DOMAIN) FOR MISO-OFDM MODEL

Here, we discuss a AFF generation scheme (frequency-domain) for OFDM systems proposed in [14]. We assume that Alice (transmitter) communicates with a Bob (legitimate receiver). At the same time, eavesdropper which is passive is tries to receive the signal from transmitter. We also assume Alice transmits a single OFDM stream which has N subcarriers. To make the effect of pseudo fast fading to the transmitting signal, Alice(transmitter) multiplies a frequency-domain data symbol $\mathrm{s}\boldsymbol{l}$ on the l-th subcarrier ($l \in \{1, 2,\ldots N\}$) by a complex Gaussian random weight $\delta\boldsymbol{l} \sim CN(0,1)$. The weighted symbol $\mathrm{T}\boldsymbol{l}$ on the l-th subcarrier is expressed as

$$\mathrm{T}\boldsymbol{l} = \delta\boldsymbol{l}\, \mathrm{s}\boldsymbol{l} \qquad (1)$$

Here we create to make the effect of pseudo fast fading to the received signal to Eavesdropper without affecting the received signal of Bob. If Alice and Bob each have one antenna, this cannot be achieved because the frequency-domain received signal $\mathrm{R}^{\mathrm{B}}\boldsymbol{l}$ on the l-th subcarrier of Bob is expressed as,

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \mathrm{h}\boldsymbol{l}\, \mathrm{T}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}}$$
$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \mathrm{h}\boldsymbol{l}\, \delta\boldsymbol{l}\, \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}} \qquad (2)$$

Where $\mathrm{h}\boldsymbol{l}$ is the channel frequency response between Alice and Bob, and $\eta\boldsymbol{l}^{\mathrm{B}}$ is the frequency-domain additive white Gaussian noise (AWGN) at Bob. Since $\mathrm{h}\boldsymbol{l}$ and $\delta\boldsymbol{l}$ are independent, so $\mathrm{h}\boldsymbol{l}\delta\boldsymbol{l}$ also randomness. This implies that Bob cannot demodulate his received signal if he cannot estimate the value of $\delta\boldsymbol{l}$**.** To enable Bob to demodulate his received signal without estimating the value of $\delta\boldsymbol{l}$**.** So, Alice must have more than one antenna.
When Alice has N_{T} transmit antennas, the weighted symbol vector is expressed as

$$\begin{aligned} \mathrm{T}\boldsymbol{l} &= [\mathrm{T}\boldsymbol{l}^{(1)}\ \mathrm{T}\boldsymbol{l}^{(2)} \ldots\ldots \mathrm{T}\boldsymbol{l}^{(N\mathrm{T})}]^{\mathrm{T}} \\ &= [\delta\boldsymbol{l}^{(1)}\ \delta\boldsymbol{l}^{(2)} \ldots\ldots \delta\boldsymbol{l}^{(N\mathrm{T})}]^{\mathrm{T}}\, \mathrm{s}\boldsymbol{l} \\ &= \delta\boldsymbol{l}\, \mathrm{s}\boldsymbol{l} \end{aligned} \qquad (3)$$

Where $\mathrm{T}\boldsymbol{l}^{(\mathrm{n})}$ ($\mathrm{n} \in \{1,2,\ldots \mathrm{N}_{\mathrm{T}}\}$) is the weighted symbol which is transmitted from the n-th antenna on the l-th subcarrier of Alice, and $\delta\boldsymbol{l}^{(\mathrm{n})}$ is the AFF weight of the n-th antenna on the l-th subcarrier of Alice. The superscript $[\cdot]^{\mathrm{T}}$ denotes the transpose. By increasing the number of transmit antennas of Alice, the single-input single-output (SISO) OFDM system becomes the MISO-OFDM system as shown in Fig. 2.

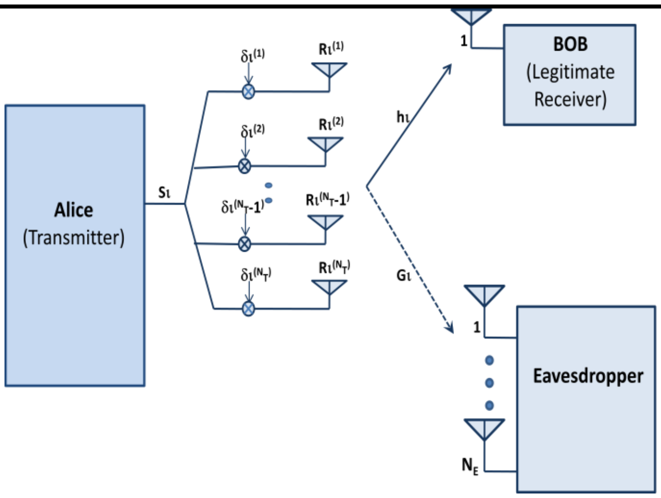


Figure 2 MISO-OFDM System with Eavesdropper

In this case, the frequency-domain received signal $\mathrm{R}^{\mathrm{B}}\boldsymbol{l}$ of Bob is expressed as

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \mathrm{h}\boldsymbol{l}\ \mathrm{T}\boldsymbol{l}\ + \eta\boldsymbol{l}^{\mathrm{B}}$$

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \mathrm{h}\boldsymbol{l}\ \delta\boldsymbol{l}\ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}} \tag{4}$$

Where hι is the channel frequency response vector between Alice and Bob on the *l*-th subcarrier, and is expressed as

$$\mathrm{h}\boldsymbol{l} = [\mathrm{h}\boldsymbol{l}^{(1)}\ \mathrm{h}\boldsymbol{l}^{(2)}\ \ldots..\ \mathrm{h}\boldsymbol{l}^{(NT)}] \tag{5}$$

In Eq. (5), h$\boldsymbol{l}$ is the channel frequency response between the *n*-th transmit antenna of Alice and the receive antenna of Bob. Here, Bob is possible to demodulate his received signal, if the AFF weight vector satisfies the following condition.

$$h\boldsymbol{l}\ \delta\boldsymbol{l}\ =\ 1 \tag{6}$$

This can be achieved by generating the AFF weight vector as

$$\delta\boldsymbol{l}^{(\mathrm{n})} = \begin{cases} \dfrac{1-\sum_{m=1,m\neq A}^{NT} \mathrm{h}\boldsymbol{l}^{(\mathrm{m})}\ \delta\boldsymbol{l}^{(\mathrm{m})}}{\mathrm{h}\boldsymbol{l}^{(\mathrm{A})}}, & n = A \\ z\boldsymbol{l}^{(\mathrm{n})}, & n \neq A \end{cases} \tag{7}$$

Where

$$\mathrm{A}\ =\ \mathrm{argmax}\ (||\ \mathrm{h}\boldsymbol{l}^{(\mathrm{n})}\ ||) \tag{8}$$

and $z\boldsymbol{l}^{(\mathrm{n})} \sim CN(0,1)$ is a complex Gaussian random variable. The reason of using Eq. (8) is that $\delta\boldsymbol{l}^{(\mathrm{n})}$ diverges if $||\ \mathrm{h}\boldsymbol{l}^{(\mathrm{n})}||$ is very small. In the AFF weight vector, the elements of the vector are categorized into two functions: random weights ($n \neq A$) and a canceling weight ($n = A$).The random weights cause the effect like pseudo fast fading. On the other hand, the canceling weight is used to cancel random weights out as well as the actual fading. Thus, the frequency-domain received signal on the l-th subcarrier of Bob becomes

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} =\ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}} \tag{9}$$

Meanwhile, if we assume Eavesdropper has N_E receive antennas, the frequency-domain received signal $\mathrm{R}^{\mathrm{E}}\boldsymbol{l}$ on the *l*-th subcarrier of Eavesdropper is expressed as

$$\mathrm{R}^{\mathrm{E}}\boldsymbol{l} = \mathrm{G}\boldsymbol{l}\ \delta\boldsymbol{l}\ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{E}} \tag{10}$$

Where G$\boldsymbol{l}$ is the channel frequency response matrix between Alice and Eavesdropper on the *l*-th subcarrier, and $\eta\boldsymbol{l}^{\mathrm{E}}$ is the frequency domain AWGN vector on the *l*-th subcarrier at Eve. The channel frequency response between Alice and Eavesdropper on the *l*-th subcarrier is expressed as

$$\mathrm{G}l = \begin{bmatrix} gl^{(1,1)} & gl^{(1,2)} & \cdots & gl^{(1,N_T)} \\ gl^{(2,1)} & gl^{(2,2)} & \cdots & gl^{(2,N_T)} \\ \vdots & \vdots & & \vdots \\ gl^{(N_E,1)} & gl^{(N_E,2)} & \cdots & gl^{(N_E,N_T)} \end{bmatrix} \tag{11}$$

Where g$\boldsymbol{l}^{(k,n)}$,k ∈ {1,2,…N$_E$} and n ∈ {1,2,…N$_T$},is the channel frequency response between the *n*-th transmit antenna of Alice and the *k*-th receive antenna of Eavesdropper. Since Eavesdropper cannot estimate the value of δ*l*, she cannot eavesdrop on Alice. Thus, the AFF scheme attains secure wireless communications. However, this scheme is applicable only to MISO-OFDM systems that transmit a single OFDM stream. Since modern wireless communications systems usually employ MIMO architecture which can transmit multiple OFDM streams, an AFF generation scheme for MIMO-OFDM systems is indispensable. Therefore, we propose an AFF generation scheme for MIMO-OFDM systems in the next section.

III. PROPOSED AFF GENERATION SCHEME (FREQUENCY DOMAIN) FOR MIMO-OFDM MODEL

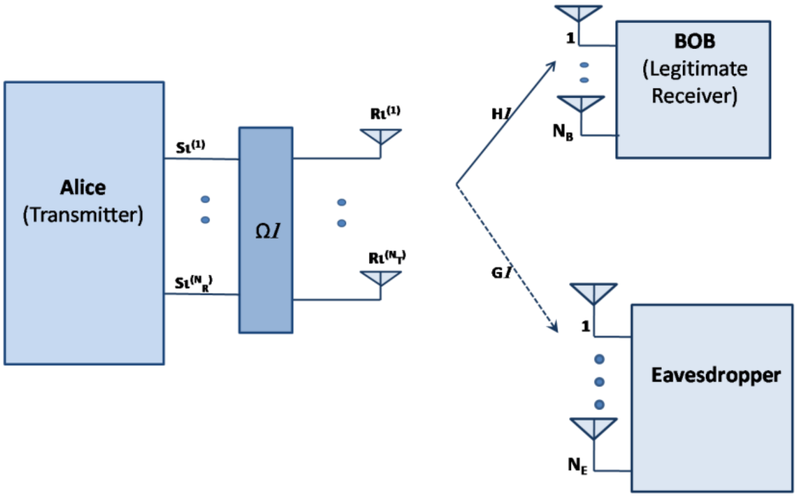


Figure 3 Proposed System Architecture for MIMO-OFDM System with Eavesdropper

In this section, we propose a frequency-domain AFF generation scheme especially for MIMO-OFDM systems that employ spatial multiplexing. In this system, Alice transmits multiple OFDM streams to Bob, while Eavesdropper tries to eavesdrop on Alice. We assume that Alice, Bob, and Eavesdropper have N_T, N_R, and N_E antennas, respectively. Therefore, the channel frequency response matrix between Alice and Bob on the l-th subcarrier is expressed as

$$\mathrm{H}l=\begin{bmatrix} hl^{(1,1)} & hl^{(1,2)} & \cdots & hl^{(1,N_T)} \\ hl^{(2,1)} & hl^{(2,2)} & \cdots & hl^{(2,N_T)} \\ \vdots & \vdots & & \vdots \\ hl^{(N_R,1)} & hl^{(N_R,2)} & \cdots & hl^{(N_R,N_T)} \end{bmatrix} \qquad (12)$$

Where $hl^{(i,n)}$ (i ∊ {1,2,…$\mathrm{N_R}$} and n ∊ {1,2,…$\mathrm{N_T}$}) is the channel frequency response between the n-th transmit antenna of Alice and the i-th receive antenna of Bob on the l-th subcarrier.

Here, we use the notations, $\boldsymbol{s}\boldsymbol{l}$ and $\boldsymbol{\Omega}l$ which denote the transmit symbol vector and the AFF weight matrix, respectively. Then, the frequency-domain received signal of Bob is expressed as

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \mathrm{H}\boldsymbol{l}\ \boldsymbol{\Omega l}\ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}} \qquad (13)$$

$$\begin{bmatrix} \overbrace{\begin{pmatrix} \delta l^{(1,1)} & \delta l^{(1,2)} & \cdots & \delta l^{(1,N_R)} \\ \vdots & \vdots & \ddots & \vdots \\ \delta l^{(N_T-N_R,1)} & \delta l^{(N_T-N_R,2)} & \cdots & \delta l^{(N_T-N_R,N_R)} \end{pmatrix}}^{\boldsymbol{\Omega l}^{rand}\text{ (random weight)}} \\ \underbrace{\begin{pmatrix} \delta l^{(N_T-N_R+1,1)} & \delta l^{(N_T-N_R+1,2)} & \cdots & \delta l^{(N_T-N_R+1,N_R)} \\ \vdots & \vdots & \ddots & \vdots \\ \delta l^{(N_T,1)} & \delta l^{(N_T,2)} & \cdots & \delta l^{(N_T,N_R)} \end{pmatrix}}_{\boldsymbol{\Omega l}^{cancell}\text{ (cancelling weight)}} \end{bmatrix}$$

Figure 3 AFF Weight Compositions

Where $\eta\boldsymbol{l}^{\mathrm{B}}$ is the frequency-domain AWGN vector on the l-th subcarrier at Bob. Similar to the case of MISO-OFDM, to enable Bob to demodulate his received signal without estimating the value of $\boldsymbol{\Omega}l$, we should make the received signal of Bob become as follows:

$$\mathrm{R}^{\mathrm{B}}\boldsymbol{l} = \ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{B}} \qquad (14)$$

To realize this, the following condition is required:

$$\mathrm{H}\boldsymbol{l}\ \boldsymbol{\Omega l} = \mathbf{I} \qquad (15)$$

Where **I** is the identity matrix. That is, the AFF weight matrix is required to cancel the channel frequency response matrix out. This can be achieved by exploiting the spatial degrees of freedom; this requires $\mathrm{N_T} > N_\mathrm{R}$.

Based on the above conditions, we consider the structure of the AFF weight matrix. In a spatial multiplexing system, the maximum number of independent streams that can be transmitted reliably is $\mathrm{N_{st}} = \min(\mathrm{N_T}, N_\mathrm{R})$. That is, Alice is required to transmit $\mathrm{N_R}$ OFDM streams using $\mathrm{N_T}$ transmit antennas. Therefore, the symbol vector $\mathrm{s}\boldsymbol{l}$ and the AFF weight matrix Ωl must have the sizes of $\mathrm{N_R}$-by-one and $\mathrm{N_T}$-by-$\mathrm{N_R}$, respectively, and are expressed as

$$\mathrm{s}\boldsymbol{l} = [\mathrm{s}\boldsymbol{l}^{(1)}\ \mathrm{s}\boldsymbol{l}^{(2)} \ldots \mathrm{s}\boldsymbol{l}^{(\mathrm{N_R})}]^{\mathrm{T}} \qquad (16)$$

$$\mathbf{\Omega}l=\begin{bmatrix}\delta l^{(1,1)} & \delta l^{(1,2)} \cdots & \delta l^{(1,N_R)}\\ \delta l^{(2,1)} & \delta l^{(2,2)} \cdots & \delta l^{(2,N_R)}\\ \vdots & \vdots & \vdots\\ \delta l^{(N_T,1)} & \delta l^{(N_T,2)} \cdots & \delta l^{(N_T,N_R)}\end{bmatrix} \quad (17)$$

In Eq. (17), similar to the case of MISO-OFDM, the elements of the AFF weight matrix are categorized into two functions: random weights and canceling weights. Fig. 3 shows the composition of the AFF weight matrix. In Fig. 3, the first ($N_T - N_R$) rows of the matrix take on the role of generating the effect of pseudo fast fading. On the other hand, the bottom N_R rows of the matrix take on the role of canceling the AFF as well as actual channels. We call them the random weight matrix $\mathbf{\Omega}l^{\text{rand}}$ and the canceling matrix $\mathbf{\Omega}l^{\text{cancel}}$, respectively.

To satisfy Eq. (15), the elements of $\mathbf{\Omega}l^{\text{rand}}$ **and** $\mathbf{\Omega}l^{\text{cancel}}$ are determined as follows. First, the elements of $\mathbf{\Omega}l^{\text{rand}}$ are the complex Gaussian random variables. Next, $\mathbf{\Omega}l^{\text{cancel}}$ is determined using the following equation.

$$\mathbf{\Omega}l^{\text{cancel}} =(\mathrm{H}\boldsymbol{l}^{cancel})^{-1} (\ \mathbf{I} - \mathrm{H}l^{\text{rand}}\ \mathbf{\Omega}l^{\text{rand}}) \quad (18)$$

Where $\mathrm{H}\boldsymbol{l}^{cancel}$ is the right $\mathrm{N_R}$ columns of $\mathrm{H}l$ in Eq. (12), and $\mathrm{H}\boldsymbol{l}^{cancel}$ is the left ($\mathrm{N_T} - \mathrm{N_R}$) columns of $\mathrm{H}l$. By using this AFF weight matrix, the received signal of Bob becomes Eq. (14). The MIMO-OFDM system using the proposed AFF weight is described in Fig. 3. Finally, the received signal of Eve $\mathrm{R^E}\boldsymbol{l}$ is expressed as

$$\mathrm{R^E}\boldsymbol{l} = \mathrm{G}\boldsymbol{l}\ \mathbf{\Omega}l\ \mathrm{s}\boldsymbol{l} + \eta\boldsymbol{l}^{\mathrm{E}} \quad (19)$$

Since $\mathrm{G}\boldsymbol{l}\ \mathbf{\Omega}l$ does not become the identity matrix, Eve must estimate $\mathbf{\Omega}l$ blindly to demodulate her received signal. However, the blind estimation of random weights is impractical. Thus, Eve cannot demodulate her received signal.

IV. RESULTS AND SIMULATION PERFORMANCE

Here, we evaluate the effectiveness of the proposed frequency-domain AFF + IT scheme for MIMO-OFDM systems. In physical layer security, the performance of a scheme is often measured by the secrecy rate. The secrecy rate $R_{MISO/MIMO}$ is expressed as

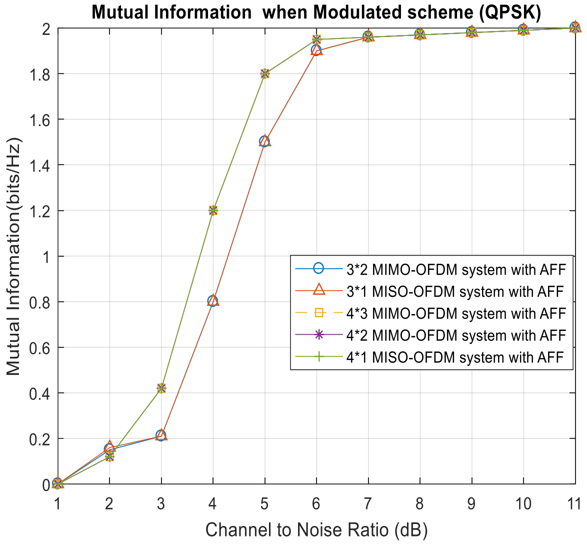
$$\boldsymbol{R_{system}} = I(\mathrm{s}\boldsymbol{l}\ ;\ \mathrm{R^B}\boldsymbol{l}\ ) - I(\mathrm{s}\boldsymbol{l}\ ;\ \mathrm{R^E}\boldsymbol{l}\ ) \quad (20)$$

$I(\mathrm{s}\boldsymbol{l}\ ;\ \mathrm{R^B}\boldsymbol{l}\ )$ is the mutual information between the Alice and the Bob(legitimate receiver) , while $I(\mathrm{s}\boldsymbol{l}\ ;\ \mathrm{R^E}\boldsymbol{l}\ )$ is the mutual information between the Alice and the Eavesdropper. In general, since the blind estimation of $\mathbf{\Omega}l$ is unrealizable, the AFF scheme reduces $I(\mathrm{s}\boldsymbol{l}\ ;\ \mathrm{R^E}\boldsymbol{l}\ )$ to nearly zero by causing the effect of fast fading to the received signal of Eve [10]. Thus, we use the mutual information between Alice and Bob instead of the secrecy rate $\boldsymbol{R_{system}}$ as a measure of performance. The mutual information is calculated through computer simulation. Moreover, to compare the systems of different antenna configurations, we evaluate the mutual information per stream. In our simulation, $\mathrm{N_T}$ pilot OFDM symbols are placed at the head of each packet followed by thirty data OFDM symbols, and the channel matrix $\mathrm{H}\boldsymbol{l}$ is estimated using the pilot OFDM symbols. The simulation parameters are listed in Table I.

Parameter	**Value**
Number of receivers to find out the eavesdropper	10-100
data length	64 bits (can be extended to 124)
# of subcarriers	16
length of CP	16 [samples]
modulation scheme	QPSK
# of transmit antenna ($\mathrm{N_T}$)	3 or 4
# of legitimate antenna($\mathrm{N_R}$)	1 or 2
# of eavesdropper antenna($\mathrm{N_E}$)	4
CSI feedback	Perfect

Table 1 Experimental Parameter

In Figs. 4, we compare the MIMO-OFDM systems using our proposed AFF generation scheme with the MISO-OFDM systems using the frequency-domain AFF generation scheme of Eq. (7) in terms of the mutual information. While in figs. 5, we compare the MIMO-OFDM systems using our proposed AFF generation scheme with the MISO-OFDM systems using the frequency-domain AFF generation scheme of Eq. (24) in terms of the secrecy rate. In general, the mutual information becomes large when the number of transmitted streams becomes large. For fair comparison, we evaluate the mutual information per stream in MIMO-OFDM systems because the MIMO-OFDM systems transmit more than one stream. Every system in Fig. 4 employs QPSK as a modulation scheme. In addition, the MIMO-OFDM system uses four, three, or two transmit antennas, and the MISO-OFDM system uses three or two transmit antennas.



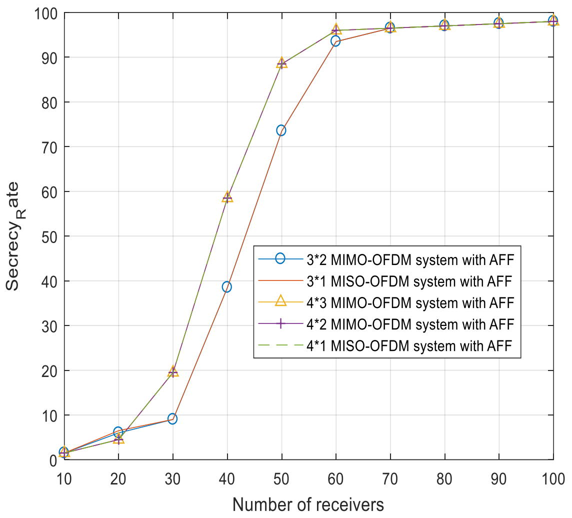


Figure 4 Mutual information when the modulation scheme is QPSK Figure 5 Secrecy rate of MISO as well as of MIMO system

Finally, in Fig. 4, we show the mutual information of MIMO-OFDM and MISO-OFDM systems using QPSK in the case of various antenna configurations. In the MIMO-OFDM system, since two or three streams are transmitted, the maximum mutual information of the system becomes double or triple as compared with that of MISO-OFDM system. Also in Figs. 5, we show that as the numbers of receivers are increased than the secrecy rate of MISO-OFDM as well as MIMO-OFDM systems are also increased.

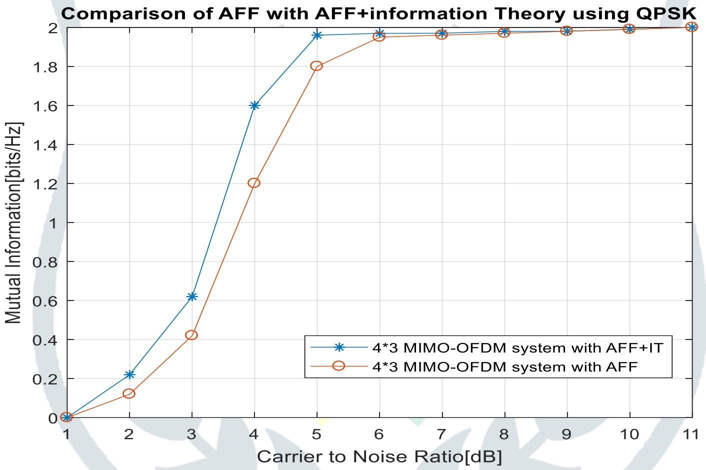


Figure 6 Comparison of AFF with AFF + Information Theory using QPSK

Finally, in Fig. 6, we show the Comparison of AFF with AFF + Information Theory using QPSK. Comparatively in MIMO-OFDM system, mutual information (bits/Hz) is high with respect to the carrier to noise ratio than the MISO-OFDM system. So, the proposed AFF matrix is composed by stacking the random weight matrix and the canceling weight matrix. The AFF produced by our AFF + IT generation scheme is successfully canceled out at the legitimate receiver, while causing the pseudo-fading effect at the eavesdropper. So, This AFF + IT generation scheme improves physical layer secrecy rate of MISO-OFDM system.

V. Conclusion

Modern wireless communication system demands for improved physical layer security due to its broadcasting nature. Here, we show that the proposed AFF matrix is composed by stacking the random weight matrix and the canceling weight matrix. The AFF produced by our AFF + IT generation scheme is successfully canceled out at the legitimate receiver, while causing the pseudo-fading effect at the eavesdropper. So, This AFF + IT generation scheme improves physical layer secrecy rate of MISO-OFDM system.

The work has been implemented under the assumption that the transmitter has the knowledge of channel and legitimate receiver prior to broadcasting the data. The result of the work has achieved a secrecy rate of 96% for MISO-OFDM model under the simulation condition as described in chapter 5. Same as we achieved nearer to 100% secrecy rate in MIMO-OFDM system.

REFERENCES

[01] Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang, A. Lee Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", IEEE Communications Surveys & Tutorials Volume: 16 , Issue: 3 , Third Quarter 2014.

[02] Zou, Y., Zhu, J., Wang, X., & Leung, V., "Improving Physical-Layer Security In Wireless Communications Using Diversity Techniques", IEEE Network, VOL.: 29, Issue: 1 , Jan.-Feb. 2015.

[03] 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 April 2015.

[04] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong and Xiqi Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", IEEE Journal on Selected Areas in Communications (Volume: 36 , Issue: 4 , April 2018).

[05] Binh Van Nguyen, Hyoyoung Jung, and Kiseon Kim, "Physical Layer Security Schemes for Full-Duplex Cooperative Systems: State of the Art and Beyond",IEEE Communications Magazine Volume : 56, Issue: 11 , November 2018.

[06] Biao He, Xiangyun Zhou, and Thushara D. Abhayapala, "Wireless Physical Layer Security with Imperfect Channel State Information: A Survey", arXiv:1307.4146v2 [cs.IT] 19 Jul 2013

[07] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, Hsiao-Hwa Chen, "Physical layer security in wireless networks: a tutorial", IEEE Wireless Communications (Volume: 18, Issue: 2, April 2011).

[08] Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trend", Proceedings of the IEEE Vol. 104, No. 9, September 2016.

[09] JONGYEOP KIM, JINWOONG KIM, JEMIN LEE AND JIHWAN P. CHOI, "Physical-Layer Security against Smart Eavesdroppers: Exploiting Full-Duplex Receivers", IEEE Access, Volume 6, June 2018

[10] Krishna Zalavadiya, Dimple Agrawal, "Investigation of Physical Layer Security Method in Cooperative Communication", 2018 IJSRSET | Volume 4 | Issue 1 | January-February-2018

[11] Xiangyun Zhou, Student Member, IEEE, and Matthew R. McKay, Member, IEEE, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation", IEEE Transaction on Vehicular Technology, Vol. 59, No. 8, October 2010.

[12] Hui-Ming Wang, Tongxing Zheng, and Xiang-Gen Xia, "Secure MISO Wiretap Channels with Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading", IEEE Transactions on Wireless Communications, VOL. 14, NO. 1, JANUARY 2015

[13] Changick Song, "Achievable Secrecy Rate of Artificial Fast-fading Techniques and Secret-key Assisted Design for MIMO Wiretap Channels with Multi-antenna Passive Eavesdropper", IEEE Transactions on Vehicular Technology (Volume: 67 , Issue: 10 , Oct. 2018

[14] Changick Song, "Achievable Secrecy Rate of Artificial Fast-fading Techniques and Secret-key Assisted Design for MIMO Wiretap Channels with Multi-antenna Passive Eavesdropper", IEEE Transactions on Vehicular Technology (Volume: 67 , Issue: 10 , Oct. 2018

[15] Ting Wang and Yaling Yang, "Enhancing Wireless Communication Privacy with Artificial Fading", IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012).

[16] Fr´ed´erique Oggier and Babak Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel", IEEE International Symposium on Information Theory 2008, Toronto, Canada, July 6 - 11, 2008

[17] Tie Liu, Member, IEEE, And Shlomo Shamai (Shitz), Fellow, IEEE, "A Note On The Secrecy Capacity Of The Multiple-Antenna Wiretap Channel", IEEE Transactions On Information Theory, Vol. 55, No. 6, June 2009

[18] Mukherjee, A., & Swindlehurst, A. L. (2012, March). "Detecting passive eavesdroppers in the MIMO wiretap channel". In 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2809-2812). IEEE.

[19] Bash, B. A., Goeckel, D., & Towsley, D. (2013). "Limits of reliable communication with low probability of detection on AWGN channels". IEEE journal on selected areas in communications, 31(9), 1921-1930.

[20] Yu Kozai and Takahiko Saba, "An Artificial Fast Fading Generation Scheme for Physical Layer Security of MIMO-OFDM System", 2015 9th International Conference on Signal Processing and Communication Systems (ICSPCS).

[21] Akitaya, Tomoki, and Takahiko Saba. "Energy efficient artificial fast fading for MISO-OFDM systems." 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, 2015.

[22] Ali, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.