© 2019 IJSRSET | Volume 6 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196187

Physical Layer Secrecy rate improvement in MISO using Artificial Fast Fading

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

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

[2,3]Assistant Professor, Electronics and Communication Silver Oak college of Engineering and Technology, Ahmedabad, Gujarat, India

ABSTRACT

Wireless communication system limits the security and privacy because of its broad cast nature. Physical layer security gives secure correspondence and having legitimate user to effectively get secure data. Among the physical layer security techniques, an artificial fast fading (AFF) technique dtrait's the received signal quality of eavesdroppers by causing pseudo fast fading to the transmitting signals. This is realized by multiplying the signals to be transmitted by random weights every symbol interval. However, the AFF technique often increases the power of the weighted signals. In such cases, the weighted signals must be normalized before transmission. This causes energy loss in the legitimate receiver. Therefore, we consider minimizing the norm of the weight vector to prevent the power of the weighted signals from being increased. In this, we propose and achieve Physical layer secrecy rate in MISO system using artificial fading plus information theory.

Keywords: Physical layer security, secrecy rate, MISO, AFF.

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.

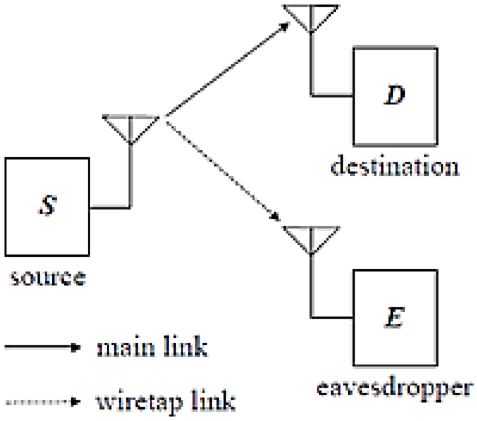

Figure 1. A wireless communication scenario consisting of one source and one destination in the presence of eavesdropping attack [3]

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 amplifyand- 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 SYSTEMS

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 **sl** on the l-th subcarrier ($l \in \{1, 2, \ldots N\}$) by a complex Gaussian random weight **δl ~**CN(0,1). The weighted symbol Tl on the l-th subcarrier is expressed as

$$Tl = \delta l \; sl \qquad (1)$$

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 R^Bl on the l-th subcarrier of Bob is expressed as,

$$R^Bl = hl \; Tl + \eta l^B$$

$$R^Bl = hl \; \delta l \; sl + \eta l^B \qquad (2)$$

Where **hl** is the channel frequency response between Alice and Bob, and ηl^B is the frequency-domain additive white Gaussian noise (AWGN) at Bob. Since **hl** and **δl** are independent, so **hlδl** also randomness. This implies that Bob cannot demodulate his received signal if he cannot estimate the value of **δl**. To enable Bob to demodulate his received signal without estimating the value of **δl.** So, Alice must have more than one antenna.

When Alice has N_T transmit antennas, the weighted symbol vector is expressed as

$$Tl = [Tl^{(1)} \; Tl^{(2)} \ldots\ldots Tl^{(NT)}]^T$$

$$= [\delta l^{(1)} \; \delta l^{(2)} \ldots\ldots \delta l^{(NT)}]^T \, sl \qquad (3)$$

$$= \delta l \; sl$$

Where $Tl^{(n)}$ ($n \in \{1,2,\ldots N_T\}$) is the weighted symbol which is transmitted from the n-th antenna on the l-th subcarrier of Alice, and $\delta_\iota^{(n)}$ is the AFF weight of the n-th antenna on the l-th subcarrier of Alice. The superscript $[\cdot]^T$ 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

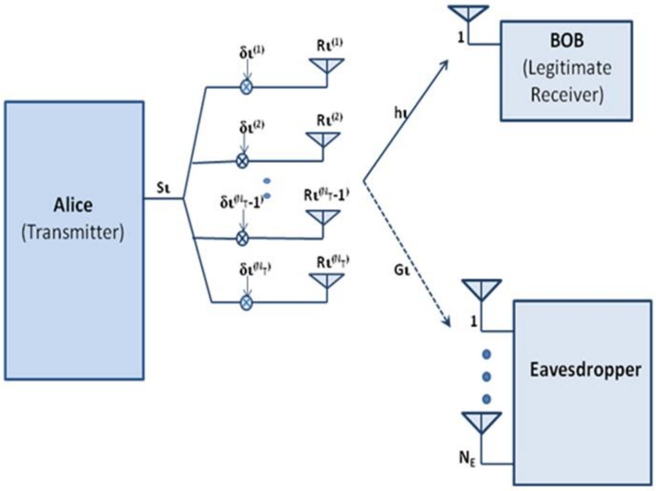

Figure 2. MISO-OFDM System with Eavesdropper

In this case, the frequency-domain received signal R^B_ι of

Bob is expressed as

$$R^Bl = hl \; Tl + \eta l^B$$

$$R^Bl = hl \; \delta l \; sl + \eta l^B \qquad (4)$$

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

$$hl = [hl^{(1)} \; hl^{(2)} \ldots\ldots hl^{(NT)}] \qquad (5)$$

In Eq. (5), **hl** 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.

$$hl \; \delta l = 1 \qquad (6)$$

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

$$R^{B}l = sl + \eta l^{B} \quad (7)$$

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

$$R^{E}l = Gl\,\delta l\,sl + \eta l^{E} \quad (8)$$

Where Gl is the channel frequency response matrix between Alice and Eavesdropper on the l-th subcarrier, and ηl^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

$$Gl = \begin{bmatrix} gl^{(1,1)} & gl^{(1,2)} & \cdots & gl^{(1,N_T)} \\ gl^{(2,1)} & gl^{(2,2)} & \cdots & gl^{(2,N_T)} \\ \vdots & \vdots & & \vdots \\ gl^{(N_E,1)} & gl^{(N_E,2)} & \cdots & gl^{(N_E,N_T)} \end{bmatrix} \quad (9)$$

Where $gl^{(k,n)}$, $k \in \{1,2,\ldots N_E\}$ and $n \in \{1,2,\ldots N_T\}$, 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 δl, she cannot eavesdrop on Alice.

Now, the channel capacity of the Bob is the mutual information between the Alice and Bob, while channel capacity of the Eavesdropper is the mutual information between the Alice and Eavesdropper. So this MISO-OFDM system's channel capacity (CS_{system}) is the differences of channel capacity of Bob to the eavesdropper.

$$CS_{system} = I(T;R) - I(T:E) \quad (10)$$

Thus, the AFF scheme attains secure wireless communications. However, this scheme is applicable only to MISO-OFDM systems that transmit a single OFDM stream.

III. SIMULATION RESULT

We have implemented MISO-OFDM model as per figure-2. The simulation parameters are as per table-1.

Table 1

Simulation Parameter

Parameter	**Value**
data length	64 bits
# of subcarriers	16
length of CP	16 [samples]
modulation scheme	QPSK
# of transmit antenna	3 or 4
# of legitimate antenna	1 or 2

The original serial data of length 64 bits are converted in parallel after performing QPSK modulation. The data is divided in 16 subcarriers which will be then multiplied with AFF weights (δι). The output of AFF module is then transmitted via antenna.

On other side, the legitimate receiver receives the data after due convolution with the channel matrix. The data is first demodulated and converted into serial form. It is assumed that the channel matrix between transmitter and legitimate receiver follows the criteria as per equation-7.

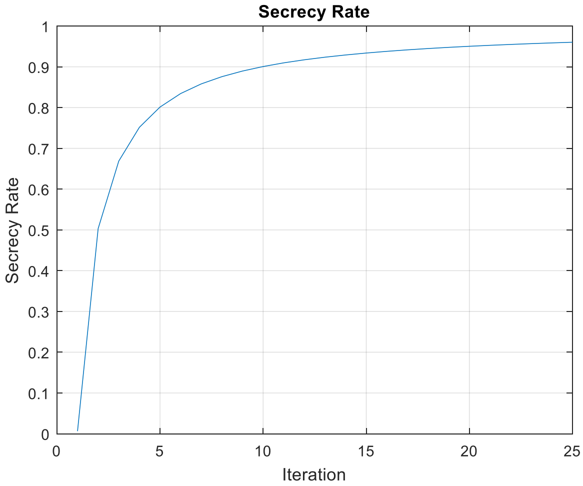

Figure 3. Secrecy rate of MISO-OFDM system

Figure-3 shows the plot of secrecy rate derived as per equation-10. It is evident from the figure that as the number of iteration increases the AFF fading in the path between transmitter and eavesdropper increases which reduces the channel capacity between them.

IV. CONCLUSION

Modern wireless communication system demands for improved physical layer security due to its broadcasting nature. The author in his present work shows the implementation of MISO-OFDM system using artificial fast fading. The channel between transmitter and eavesdropper is faded which makes it incapable to decode and demodulate the taped data. 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 98% for MISO-OFDM model under the simulation condition as described in section-IV.

The future work involves the implementation of AFF scheme for MIMO-OFDM model. The work can also be extended by applying prediction algorithms to detect the eavesdropper.

V. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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).

[5] 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.

[6] 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.

[7] 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.

[8] 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).

[9] 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.

[10] 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.

[11] Changick Song, “Achievable Secrecy Rate of Artificial Fast-fading Techniques and Secret-key Assisted Design for MIMO Wiretap Channels with Multi-antenna Passive”, IEEE Transactions

on Vehicular Technology (Volume: 67, Issue: 10, Oct. 2018).

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

[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] 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).

Cite this article as :

Harsha Chauhan, Vimal Nayak, Rina Parikh, "Physical Layer Secrecy rate improvement in MISO using Artificial Fast Fading", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN : 2456-3307, Volume 6 Issue 1, pp. 402-407, January-February 2019.
Available at doi :
https://doi.org/10.32628/IJSRSET196187
Journal URL : http://ijsrset.com/IJSRSET196187