TELKOMNIKA, Vol.13, No.2, June 2015, pp. 478 ~ 486
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v13i2.995

Integration of Signal and Artificial Noise in MIMO Wiretap Channel

Zhiliang Yang*[1,2], Aihua Wang[1], Xiqiang Qu[2]
[1] School of Information and Electronics, Beijing Institute of Technology, Beijing 100081,China
[2] School of Information and Communication Engineering, North University of China Taiyuan 030051, China
*Corresponding author, e-mail: sxtyyzl@sina.com

Abstract

In this paper, the integrated signal-to-artificial noise (ISAN) design is applied in MIMO wiretap channel to ensure wireless communication security. When the information of eavesdropper is unknown, the total power is divided into two parts: signal and artificial noise. The signal can secure certain quality at the legitimate receiver. The artificial noise which is in the null space of the receiver channel matrix can deteriorate eavesdropper channel by the method of beam forming. The artificial noise power is distributed evenly in other space, so that the eavesdropper channel is deteriorated in all directions. The signal to interface and noise ratio (SINR) is regarded as the efficient parameter on measuring reliability and security of information at the legitimate receiver. The simulations reveal that ISAN can deteriorate the eavesdropper channel and safeguard the information transmission on the premise of the given SINR of the legitimate receiver.

Keywords: *MIMO Wiretap Channel, ISAN, Average SINR*

1. Introduction

With the rapid development of wireless communication business, the security of information transmission has been paid widely attention. The traditional encryption methods are mostly based on cryptography [1]-[3], which built security mechanism above the network layer. In 1975, Wyner proposed the wiretap channel model (WTC), which provided the theoretic foundation for information transmission over physical layer from the angle of information theory. The WTC proved that there is a security capacity C_s ($C_s > 0$) when the channels of eavesdropper is inferior to the source. The information can be transmitted safely from the source to the destination if the data rate is less than C_s, in this situation the eavesdropper can receive the data, but he cannot obtain any useful information of source [4]. In this paper, the source is Alice, the legitimate receiver is Bob, and the eavesdropper is Eve. Eve can get part of the source information by wiretapping. The channel between Alice and Bob is main channel, and the channel between Alice and Eve is eavesdropper channel (see Figure 1).

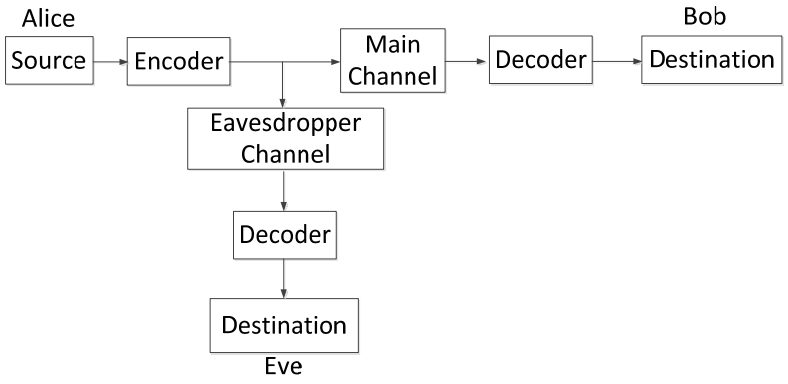


Figure 1. The wiretap channel

Received November 13, 2014; Revised February 21, 2015; Accepted March 12, 2015

The aim of integrated signal-to-artificial noise (ISAN) design is to improve C_s. There were many researches on the methods by which C_s can be improved. The security capacity of WTC is proposed based on the broadcasting channel. The main channel of the wiretap channel is noiseless channel, and the eavesdropper channel is recession channel of the main channel (Binary Symmetric Channel). S. Leung calculated under these conditions that main channel and eavesdropper channel are Gaussian channels [5], and proved that when the eavesdropper channel is the degraded channel of main channel, C_s is the difference between the main channel and the eavesdropper channel. To increase C_s significantly, Hero introduced the Multiple Input Multiple Output (MIMO) and space diversity technology into security communication [6], and gave the fundamental computing method of C_s. A. Khisti [7]-[9] studied the computing method of C_s in the MIMOME scenarios. In most cases, because the eavesdropper is passive, Alice cannot obtain anything about the channel state information (CSI) of Eve, Negi [10]-[13] proposed the scheme of artificial noise to maximum the security rate when the eavesdropper is passive. The basic idea of the scheme is: Alice splits the transmitting signal vector into two parts: the signal vector and the artificial noise vector. The artificial noise lies in the null space of the signal vector, deteriorates the eavesdropper channel and has no effect on the main channel. N. Romero studied the scheme of artificial noise to secure data transmission in the MISO system [14]-[15]. The receiver signal to interface and noise ratio (SINR) is applied as the measurement of C_s by A. Mukherjee, then he proposed an optimized method of power distribution [16].

Based on former researches, ISAN design is proposed in the MIMO wiretap channel which can deteriorate the eavesdropper channel and safeguard the information transmission over the wireless channel, meanwhile, security rate is always positive and Bob can get the information successfully.

2. MIMOME system model

The number of transmitter antennas of Alice is $N_a (N_a \geq 2)$, the number of receiver antennas of Bob is $N_b (N_b \geq 1)$, the number of eavesdropper antennas of Eve is $N_e (N_e \geq 1)$ (see Figure 2). We suppose that the channel between Alice and Bob is Rayleigh flat fading channel($\mathbf{H}_b$) which is known by Alice and its covariance matrix is $\sigma_{h_b}^2 \mathbf{I}$; the channel between Alice and Eve is Rayleigh flat fading channel($\mathbf{H}_e$) which is unknown by Alice its covariance matrix is $\sigma_{h_e}^2 \mathbf{I}$. The channel between Alice and Bob and noise vector ($\mathbf{n}_b$) are superimposed; the channel between Alice and Eve and noise vector ($\mathbf{n}_e$) are superimposed. We suppose that the values of $\mathbf{n}_b$ at different times are independent of each other, the mean of $\mathbf{n}_b$ is zero, and the variance of $\mathbf{n}_b$ (σ_b^2)is complex Gaussian matrix. Vector $\mathbf{n}_e$ also has such a property. Respectively the variance matrix of $\mathbf{n}_b$ and $\mathbf{n}_e$ is:

$$\begin{aligned} E\{\mathbf{n}_b \mathbf{n}_b^H\} &= \sigma_b^2 \mathbf{I} \\ E\{\mathbf{n}_e \mathbf{n}_e^H\} &= \sigma_e^2 \mathbf{I} \end{aligned} \tag{1}$$

We suppose that the signals of Alice based on beam forming technology is $\mathbf{s}$, the signal received by Bob and Eve is as following:

$$\begin{aligned} \mathbf{y}_b &= \mathbf{H}_b \mathbf{s} + \mathbf{n}_b \\ \mathbf{y}_e &= \mathbf{H}_e \mathbf{s} + \mathbf{n}_e \end{aligned} \tag{2}$$

The covariance matrix of $\mathbf{s}$ is $\mathbf{Q}_s = E\{\mathbf{s}\mathbf{s}^H\}$, the total power of $\mathbf{s}$ is $P_0 = Tr\{\mathbf{Q}_\mathbf{s}\}$。

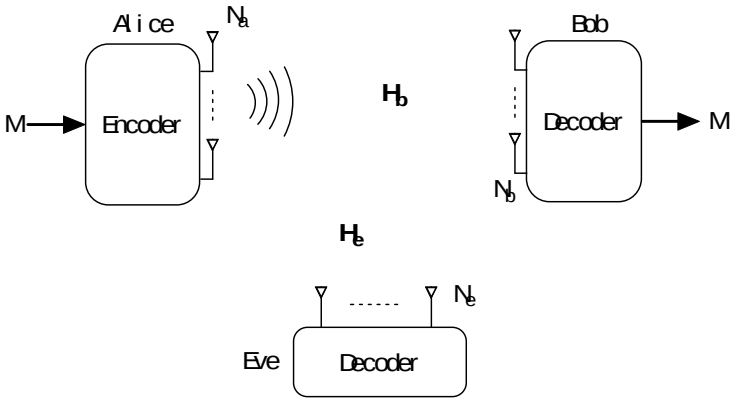


Figure 2. The MIMOME wiretap channel

3. Integrated signal-to-artificial noise design

3.1. The model of ISAN

The signal $\mathbf{s}$ can be split into two parts: signal vector and artificial noise vector. The total power of $\mathbf{s}$ is defined: $P_0 = a + b$, where a is the power that Alice wants to send and b is the artificial noise power. Then the signal $\mathbf{s}$ can be defined as

$$\mathbf{s} = \sqrt{a}\mathbf{t}d + \sqrt{b}\boldsymbol{\eta} \tag{3}$$

Where $\mathbf{t}$ is the $(N_a \times 1)$ normalized beam forming vector and $\|\mathbf{t}\| = 1$. d is the scalar complex information symbol which Alice wants to send, and the mean of d is $E\{|d|\} = 1$. $\boldsymbol{\eta}$ is the $(N_a \times 1)$ artificial noise vector, its covariance matrix is $\mathbf{Q}_\eta = E\{\boldsymbol{\eta}\boldsymbol{\eta}^H\}$, and its trace is $Tr\{\mathbf{Q}_\eta\}$ $(Tr\{\mathbf{Q}_\eta\} = 1)$.

The signals that Bob and Eve receive are

$$\begin{aligned} \mathbf{y}_b &= \sqrt{a}\mathbf{H}_b\mathbf{t}d + \sqrt{b}\mathbf{H}_b\boldsymbol{\eta} + \mathbf{n}_b \\ \mathbf{y}_e &= \sqrt{a}\mathbf{H}_e\mathbf{t}d + \sqrt{b}\mathbf{H}_e\boldsymbol{\eta} + \mathbf{n}_e \end{aligned} \tag{4}$$

Because Eve is a passive receiver, Alice cannot get the CSI about Eve. In this case, we should not regard C_s as the security measurement of the system. The receiver signal to interference and noise ratio (SINR) reflects the receiver quality, so the SINR is used to indicate the quality of receiver signals.

Assume $\mathbf{w}_b$ denotes the $N_b \times 1$ beam forming vector of Bob. Similarly, $\mathbf{w}_e$ denotes the $N_e \times 1$ beam forming vector of Eve, the receiver vector of Bob and Eve can be denoted separately as:

$$\begin{aligned} \hat{z}_b &= \mathbf{w}_b^H\mathbf{y}_b = \mathbf{w}_b^H(\sqrt{a}\mathbf{H}_b\mathbf{t}d + \sqrt{b}\mathbf{H}_b\boldsymbol{\eta} + \mathbf{n}_b) \\ \hat{z}_e &= \mathbf{w}_e^H\mathbf{y}_e = \mathbf{w}_e^H(\sqrt{a}\mathbf{H}_e\mathbf{t}d + \sqrt{b}\mathbf{H}_e\boldsymbol{\eta} + \mathbf{n}_e) \end{aligned} \tag{5}$$

And the receiver SINR of Bob and Eve can be denoted separately as:

$$SINR_b = \frac{a\left|\mathbf{w}_b^H \mathbf{H}_b \mathbf{t}\right|^2}{\mathbf{w}_b^H (\mathbf{H}_b \mathbf{Q}_\eta \mathbf{H}_\mathbf{b}^\mathbf{H} + \sigma_b^2 \mathbf{I})\mathbf{w}_b}$$
$$SINR_e = \frac{\rho P\left|\mathbf{w}_e^H \mathbf{H}_e \mathbf{t}\right|^2}{\mathbf{w}_e^H (\mathbf{H}_e \mathbf{Q}_\eta \mathbf{H}_e^\mathbf{H} + \sigma_e^2 \mathbf{I})\mathbf{w}_e} \quad (6)$$

If $SINR_b > SINR_e$, there is the scheme of modulation and coding to ensure that Bob can decode the message d successfully, at the same time, Eve cannot get anything about d.

The MIMO wiretap channel based on integrated signal-to-artificial noise design can be described as:

$$\begin{aligned} &\min_{\mathbf{t}} \quad SINR_e \\ &s.t. \quad P_0 = a + b \\ &\qquad SINR_b = \gamma_b \\ &\qquad a > 0,\ b \geq 0 \end{aligned} \quad (7)$$

Where γ_b is the given target value of Bob's SINR.

3.2. Integrated signal-to-artificial noise design

The aim of integrated signal-to-artificial noise design is to cause Alice to send the noise in all directions, to influence the eavesdropper as much as possible, and to influence the legitimate receiver as little as possible.

Alice's beam forming vector is $\mathbf{t}$ which is the eigenvectors corresponding to the maximum eigenvalue of $\mathbf{H_b}$. Artificial noise vector ($\boldsymbol{\eta}$) is the linear combination of other $N_a - 1$ characteristic vectors of $\mathbf{H}_b$. As a result, the signal vectors and artificial noise vectors are orthogonal. Other $N_a - 1$ characteristic vectors of $\mathbf{H}_b$ are distributed equally, in this principle, $\boldsymbol{\eta}$ is defined as:

$$\boldsymbol{\eta} = \frac{1}{\sqrt{N_a - 1}} \sum_{i=2}^{N_a} \mathbf{t}_i \eta_i \quad (8)$$

Where, $\mathbf{t_i}$ is the ith eigenvector of $\mathbf{H}_b$, and η_i is a random complex scalar which has unit amplitude and random phase. η_i is defined as: $\eta_i = e^{j\phi_i}$.

The phase of η_i is ϕ_i which follows uniform distribution, and $\phi_i \in [0, 2\pi]$. $\mathbf{Q}_\eta$ is defined as:

$$\mathbf{Q}_\eta = \frac{1}{N_a - 1} \sum_{i=2}^{N_a} \mathbf{t}_i \mathbf{t}_i^H \quad (9)$$

$\mathbf{w}_b$ is Bob's receive beam forming vector($\mathbf{w}_b = \mathbf{H}_b \mathbf{t}$). Eve's SINR will be maximized when his beam forming vector is $\mathbf{w}_e = (\mathbf{H}_e \mathbf{Q}_\eta \mathbf{H}_e^H + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_e \mathbf{t}$.

At this moment, the SINRs of Bob and Eve are $SINR_b$ and $SINR_e$ respectively.

$$\begin{aligned} SINR_b &= \frac{a\mathbf{t}_1^H \mathbf{H}_b^H \mathbf{H}_\mathbf{b} \mathbf{t}_1}{\sigma_b^2} = \frac{a\sigma_1^2}{\sigma_b^2} \\ SINR_e &= a\mathbf{t}_1^H \mathbf{H}_e^H (\mathbf{H}_e \mathbf{Q}_\eta \mathbf{H}_e^H + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_e \mathbf{t}_1 \end{aligned} \quad (10)$$

where, σ_1 is the maximum eigenvalue of $\mathbf{H}_b$.

The information of eavesdropper cannot be sure, and we cannot ensure that the eavesdropper is influenced by manual noise, so we can deteriorate eavesdropper channel as far as possible statistically. SINR can describe the extent how the eavesdropper channel is influenced by manual noise. Under the conditions that the total transmit power and Bob's SINR are constant, all these problems come down to find Eve's minimum SINR with $SINR_b$ constraints:

$$\begin{aligned} \min AV_e &= \min E[a\mathbf{t}_1^H \mathbf{H}_e^H (\mathbf{H}_e \mathbf{Q}_\eta \mathbf{H}_e^H + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_e \mathbf{t}_1] \\ s.t. \quad & a+b \le P_0 \\ & SINR_b = \frac{a\sigma_1^2}{\sigma_b^2} = \gamma_b \\ & a > 0, b \ge 0 \end{aligned} \tag{11}$$

4. Results and Analysis

Because the eavesdropper channel is unknown, the Monte Carlo method is applied to examine how the integrated signal-to-artificial noise design affects the eavesdropper channel. All the simulations in the paper set the times of Monte Carlo experiment to be 5000, and the signal-to-interference-and-noise-ratio (SINR) of the legitimate receiver (Bob) is $\gamma_b = 5dB$. Once Alice know Eve's average SINR in CSI, and the situation of Bob's SINR is proper, Alice could put artificial noise in Eve's channel space easily in order to deteriorate the eavesdropper channel.

The method applied when Alice knows the exact Eve's location is used for reference.The ISAN and Ref are applied separately when the number of the antennas is $N_a = 8, N_b = 4, N_e = 4$. The Figure 3 shows the average SINR of eavesdropper in all situations. The results reveal that the SINR of legitimate receiver must be proper, in this situation, Eve's SINR gets smaller and allocated power of artificial noise becomes higher with the gradually increasing transmit power, and the security performance is better. If Alice knows that the Eve's CSI, more targeted actions have been taken by Alice to interfere with Eve. The result shows that Eve's SINR would be kept below $-13dB$ if the transmit power of Alice is big enough. The above method is supposed as a Ref. For ISAN, the artificial noise is distributed evenly from every direction, and the simulation results reveal that such a method can deteriorate eavesdropper channel effectively though its SINR is worse than the Ref. For example, if the transmit power $P_0 = 15dB$, reception SINR would below $-13dB$ (which is approximates to zero).

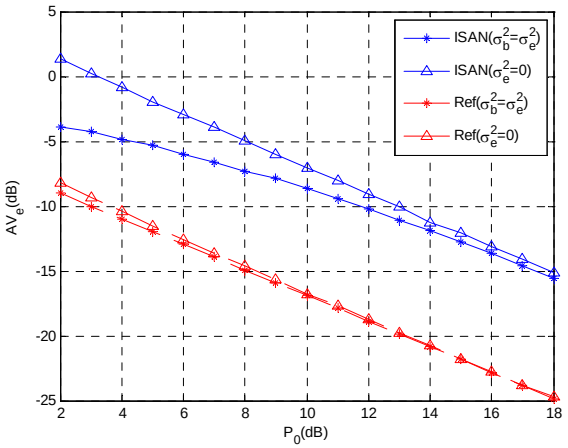


Figure 3. The average $SINR_e$ with respect to different transmit power

4.1. How does the number of antenna influences SINR of eavesdropper

The numbers of transmitting antennas and receiving antennas will affect the SINR of the receiver. The performance of eavesdropper's SINR is analyzed when the numbers of transmitting antennas and receiving antennas change on the premise that the SINR of legitimate receiver is constant($\gamma_b = 5dB$).In the method of ISAN, the performance of Eve's average SINR corresponding to the number of the antennas ($N_b = 4, N_e = 4$) is different (see Figure 4). The simulations reveal that the increase of the numbers of transmitting antennas and transmit power will reduce $SINR_e$ dramatically, especially $N_a \geq N_e$ .For example, $SINR_e$ will reach the level of $10^{-13} dB$ when $N_a = 8, P_0 = 10dB$. It is found that the gain of legitimate receiver channel and the dimension of artificial noise vector will increase when the number of transmitting antennas increases. As a result, the eavesdropper will be interfered seriously.

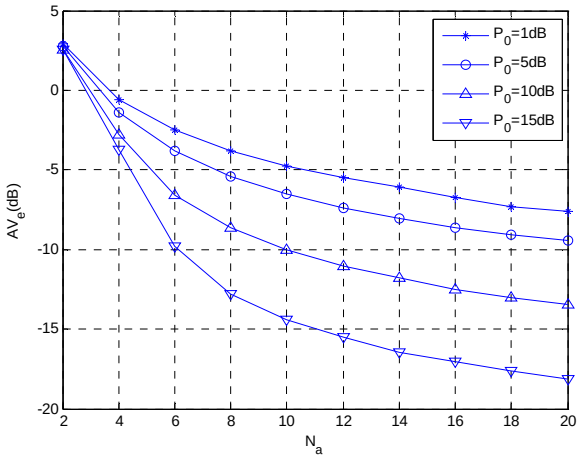


Figure 4. The average $SINR_e$ with respect to different transmitting antennas of Alice

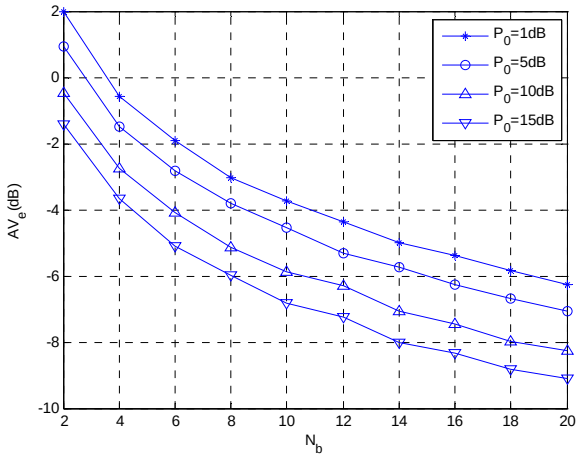


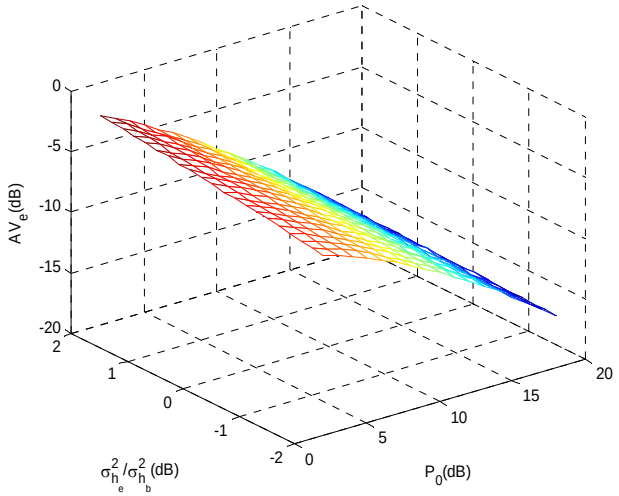
Figure 5. The average $SINR_e$ with respect to different RX antennas of Bob

In the method of ISAN, Eve's $SINR_e$ varies according to the changing N_b when N_a and N_e are constant ($N_a = 4, N_e = 4$) (see Figure5). The simulations reveal that the increasing of N_b will decrease $SINR_e$. As a result, the interference is greater within this context . It can not

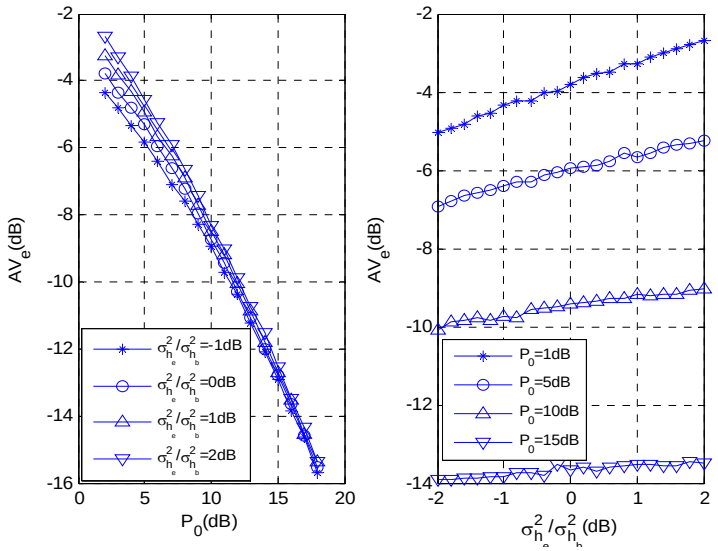
be ignored that $SINR_e$ is affected by N_a as well as N_b ,and the changing N_b has less influence than changing N_a because the increasing N_b only raise the diversity gain of legitimate receiver.

4.2. How does the channel variance influences SINR of eavesdropper

In the MIMO Wiretap channel, the important conclusion of information transmission security is the quality of legitimate receiver channel is superior to eavesdropper channel. The significant advantage of ISAN is that the information can be transferred security even if the quality of legitimate receiver channel is inferior to eavesdropper channel. In the section, we analyze the impacts of the quality of legitimate receiver channel and eavesdropper channel on the $SINR_e$ of eavesdropper (see Figure 6).



(a).



(b).

Figure 6. The average $SINR_e$; a) with respect to different P_0 and $\sigma_{h_e}^2 / \sigma_{h_b}^2$ holistically; b) with respect to different P_0 and $\sigma_{h_e}^2 / \sigma_{h_b}^2$

In MIMOME, if the number of antennas are fixed ($N_a = 8, N_b = 4, N_e = 4$), Eve's average $SINR_e$ changes with the ratio of eavesdropper channel variance and the receivers channel variance ($\sigma_{h_e}^2 / \sigma_{h_b}^2$). Fig 6a shows how the $SINR_e$ changes with the change of $\sigma_{h_e}^2 / \sigma_{h_b}^2$ and P_0 holistically. Fig 6b shows how the $SINR_e$ changes with the change of $\sigma_{h_e}^2 / \sigma_{h_b}^2$ and P_0 respectively. The simulations reveal that ISAN can solve the influence caused by the difference between legitimate receiver channel and eavesdropper channel efficiently. For example, when $P_0 = 10dB$, $\sigma_{h_e}^2 / \sigma_{h_b}^2 = 2dB$,the varience of eavesdropper channel is 100 times the varience of legitimate receiver channel, and the method of ISAN can reduce $SINR_e$ to the level of $10^{-9} dB$. The higher the transmit power is, the more effective the ISAN deal with the difference between legitimate receiver channel and eavesdropper channel. The simulations reveal that when the eavesdropper channel is superior to the receiver channel, ISAN can ensure the quality of Bob's receiver $SINR_b$ and reduce Eve's average $SINR_e$. As a result, the channel capacity of eavesdropper will be reduced markedly and information's security can be ensured effectively.

5. Conclusion

In this paper, the method of integrated signal-to-artificial noise is applied in MIMO to improve the security of signals transmission. We design the specific steps to implement the algorithm. The method in which the transmitter knows the information of eavesdropper is used as a reference method, and we compare the interruptions of eavesdropper from different methods. The influences with eavesdropper are analyzed from the perspectives of the number of the antennas and channel variance. The simulations reveal that ISAN can reduce the average SINR of eavesdropper effectively and the security of information transmission will be improved on the condition of fixed SINR at the legitimate receiver.

Acknowledgments

This work was supported in part by NSF of China with grants 61271258, the Research Fund for the Doctoral Program of Higher Education with grants 20131101110027 ,National 863 Program with grants 2014AA01A707.

References

[1] JA Thomas,TM Cover. *Elements of Information Theory*. Wiley-Interscience. 2006.
[2] Suryadi MT, Sukirman E, Agus MM. The implementation of henon map algorithm for digital image encryption. *Telkomnika (Telecommunication Computing Electronics and Control)*. 2014; 12(3): 651-656.
[3] Nurpeti E, Suryadi MT, Widya D. Performance of chaos-based encryption algorithm for digital image. *Telkomnika (Telecommunication Computing Electronics and Control).* 2014; 12(3): 675-682.
[4] AD Wyner. The Wire-Tap Channel . *The bell system technical journal.* 1975; 54(8): 1355-1387.
[5] S Leung YC, Hellman ME. The Gaussian wire-tap channel. *Information Theory, IEEE Transactions on*. 1978; 24(4): 451-456.
[6] AO Hero. Secure space-time communication. *Information Theory, IEEE Transactions on*. 2003; 49(12): 3235-3249.
[7] A Khisti, Wornell, Gregory, Wiesel, Ami, Eldar, Yonina. *On the Gaussian MIMO Wiretap Channel*.Information Theory, 2007. ISIT 2007. IEEE International Symposium. 2007: 2471-2475.
[8] A Khisti, Wornell, Gregory W. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *Information Theory, IEEE Transactions on*. 2010; 56(7): 3088-3104.
[9] A Khisti, Wornell, Gregory W. Secure Transmission With Multiple Antennas-Part II: The MIMOME Wiretap Channel. *Information Theory, IEEE Transactions on*. 2010; 56(11): 5515-5532.
[10] R Negi, S Goel. Guaranteeing Secrecy using Artificial Noise. *IEEE Trnsactions on Wireless Communications.* 2008; 7(06): 2180-2189.
[11] S Goel, Negi R. Guaranteeing Secrecy using Artificial Noise. *Wireless Communications, IEEE Transactions on*. 2008; 7(6): 2180-2189.
[12] R Negi, Goel S. *Secret communication using artificial noise*. Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd. 2005: 1906-1910.

[13] S Goel, R Negi. *Secret communication in presence of colluding eavesdroppers*. Proc. MILCOM:1501-1506.
[14] N Romero Z, Ghogho M, Mclernon D. Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security. *Signal Processing Letters, IEEE.* 2012; 19(2): 71-74.
[15] Li J, Petropulu AP. On Ergodic Secrecy Rate for Gaussian MISO Wiretap Channels. *Wireless Communications, IEEE Transactions on*. 2011; 10(4): 1176-1187.
[16] A Mukherjee, Swindlehurst AL. Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI. *Signal Processing, IEEE Transactions on.* 2011; 59(1): 351-361.