Research on the Vulnerability of MIMO Secrecy using AN Matrix Blind Space Elimination

Xiao Chen, Yan Zhu, Xinxing Yin, Fangbiao Li, Zhi Xue, Yongkai Zhou, Liang Pang
School of Electronic, Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China
E-mail: {chenxiao, topbestzy1983, yinxinxing, flyin2009, zxue, ssmailzyk, cyclone0000} @sjtu.edu.cn

***Abstract*—The security problem of Gaussian MIMO (multiple-inputs multiple-outputs) channel is considered where a transmitter is communicating to a receiver in the presence of an eavesdropper. All the nodes are equipped with multiple antennas. Through utilizing some of the available power to produce 'artificial noise' that only degrades the eavesdropper's channel, the transmitter ensures the security of communication. However, the artificial noise could be void possibly due to the inherent security weakness. In this paper, the vulnerability of the MIMO wireless channel with artificial noise (MIMOAN) through matrix analysis is researched. Then a Matrix Blind Space Elimination (MBSE) scheme is proposed and proved to fix the design flaw in order to strengthen the original one.**

Keywords-Security; wireless; secrecy capacity; artificial noise; MIMO; MBSE

I. INTRODUCTION

The inherent openness of wireless channel makes communication over this medium vulnerable to eavesdropping. In general, the security model of wireless communication involves three nodes: transmitter, receiver and eavesdropper. We consider the secret communication scenario where a transmitter sends some secure messages to an intended receiver while an eavesdropper is trying to overhear them. We need to constitute a security scheme to let the eavesdropper cannot decode any secure messages.

In this paper, secure communication is accomplished by information theoretic approach, which is more reliable than cryptographic technologies such as encryption. The notion of information theoretic security was introduced by Claude Shannon in [1] firstly. It is such strict that the received signal of the eavesdropper cannot provide even one bit information about the secret information. Shannon also defined the conception of 'secrecy capacity' in [1]. Wyner generalized the scenario where the eavesdropper's channel was a degraded version of the intended receiver's in [2]. It was possible to achieve a nonzero secrecy capacity in the wiretap channel. [3-13] extended their work. Nevertheless, the secrecy capacity will be zero, if the receiver's channel is not better than the eavesdropper's. But artificial noise is considered in [14-17] to guarantee secret communication even when the receiver's channel is not better.

In this paper, we concentrate on Multiple-inputs Multiple-outputs with artificial noise (MIMOAN) wireless channel model. In the scheme, all channel state information (CSI) is assumed to be publicly available. The transmitter, receiver and eavesdropper all have multiple antennas. The transmitter uses multiple antennas to transmit artificial noise, and utilizes the rest of antennas to send secret messages to the receiver. The noise is created such that it only degrades the eavesdropper's channel, but not the receiver's channel, thus achieving perfect secret communication.

However, there also is a weakness in MIMOAN. The function of artificial noise may become invalid by matrix operation. Currently, there is still not related research in detail about it. We analyze the failing and then present an improved approach—Matrix Blind Space Elimination (MBSE) to enhance the original scheme. The performance analysis demonstrates that the MBSE scheme can make up the weak point of MIMOAN effectively, through reselecting the artificial noise matrix out of the invalid space.

The remaining paper is organized as follows. Section II provides some notations for the paper, and describes MIMOAN. Section III points out the vulnerability of MIMOAN through matrix analysis and proposes a solution scheme—MBSE-MIMOAN. Section IV calculates and compares both of the schemes' secrecy capacities. Section V concludes the paper in the end.

II. THE REVIEW OF MIMOAN MODEL

In this paper, vectors and matrices are denoted by bold font. And the Hermitian operator is denoted by $\dagger$. It's assumed that all the wireless channels are slow fading and all the vectors and matrices are complex. The key idea of MIMOAN is that the transmitter with multiple antennas can utilize partial power to generate artificial noise to conceal the secret information which the transmitter make use of the rest of the power to transmit. In the MIMOAN model, only the eavesdropper's channel is degraded, and the receiver's channel can't be affected.

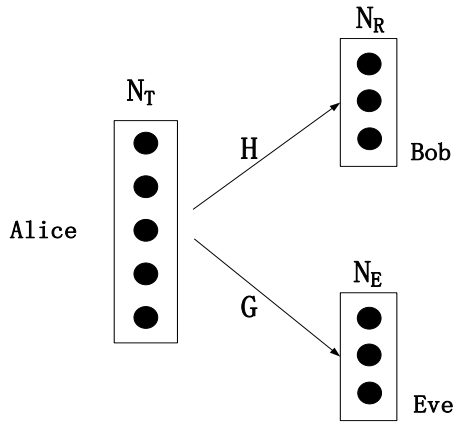

Figure.1 MIMOAN Model

In Fig.1, it shows that a transmitter Alice with N_T antennas, a receiver Bob with N_R antennas and an eavesdropper Eve with N_E antennas. It is assumed that multiple eavesdroppers (if they exist) cannot collude. This example is like a wireless LAN, with the base station as Alice. The channel gain vector of Bob and Eve is denoted by $\mathbf{H}_k$ and $\mathbf{G}_k$ respectively, at time k. The elements of $\mathbf{H}_k$ and $\mathbf{G}_k$ are denoted by $h_{i,j}$ and $g_{i,j}$ which are the channel gains from transmitting antenna i to receiving (wiretap) antenna j. Both of the channels are assumed to be i.i.d (independent and identically distributed) Rayleigh distributed and publicly available.

In this model, Alice uses a portion of its antennas to transmit artificial noise that lies in the null space of Bob's channel, and uses the remaining antennas to transmit information signal that lies in the range space of Bob's channel. Bob's channel is not affected by the artificial noise, because it can null out the noise. In general, the range space of Eve's channel may be different from that of Bob's channel, so the artificial noise will almost lie in the range space of Eve's channel. Apparently, only Eve's channel will be degraded, and the security object can be achieved in all probability.

Alice transmits $\mathbf{x}_k$ at time k. $\mathbf{a}_k$ and $\mathbf{b}_k$ are the information which Bob and Eve receive respectively,

$$\mathbf{a}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k \tag{1}$$

$$\mathbf{b}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k \tag{2}$$

Where $\mathbf{n}_k$ and $\mathbf{e}_k$ are i.i.d Additive White Gaussian Noise (AWGN) samples with variance σ_n^2 and σ_e^2 respectively.

Alice chooses $\mathbf{x}_k$ as the sum of information bearing signal $\mathbf{s}_k$ and the artificial noise signal $\mathbf{w}_k$:

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k \tag{3}$$

$$\mathbf{s}_k = \mathbf{p}_k \mathbf{u}_k \tag{4}$$

Where, $\mathbf{u}_k$ is the Gaussian distributed information signal. $\mathbf{w}_k$ is chosen to lie in the null space of $\mathbf{H}_k$, such that $\mathbf{H}_k \mathbf{w}_k = 0$. $\mathbf{p}_k$ is chosen such that $\mathbf{H}_k \mathbf{p}_k \neq 0$, and $\mathbf{p}_k$ is normalized, so that $\|\mathbf{p}_k\| = 1$, and the signals received by Bob and Eve are given by,

$$\mathbf{a}_k = \mathbf{H}_k \mathbf{p}_k \mathbf{u}_k + \mathbf{n}_k \tag{5}$$

$$\mathbf{b}_k = \mathbf{G}_k \mathbf{p}_k \mathbf{u}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k \tag{6}$$

Note that the artificial noise $\mathbf{w}_k$ nulls out $\mathbf{H}_k$ successfully, so $\mathbf{w}_k$ cannot affect Bob and only degrades Eve's channel in probability.

III. Vulnerability And Solution

A. Vulnerability Analysis

Apparently, MIMOAN model is safe enough because of the artificial noise $\mathbf{w}_k$, even when Bob's channel is not better than Eve's. But we still find a weakness in this model. Note that $\mathbf{G}_k$ is independent of $\mathbf{H}_k$, so it is also independent of $\mathbf{w}_k$, which can lie in the null space of $\mathbf{G}_k$ too. In other words, the null spaces of $\mathbf{H}_k$ and $\mathbf{G}_k$ may have intersection set. Evidently, $\mathbf{w}_k$ may be compensated by $\mathbf{G}_k$ in (6) if it belongs to the set.

$$\mathbf{G}_k \mathbf{w}_k = \mathbf{0} \tag{7}$$

Then the signal received by Eve is converted into

$$\mathbf{b}'_k = \mathbf{G}_k \mathbf{p}_k \mathbf{u}_k + \mathbf{e}_k \tag{8}$$

From (8) we can see that $\mathbf{w}_k$ is invalid. The eavesdropper Eve can remove the impact of the artificial noise to get the secret information through the vulnerability.

B. Solution

To make up for the deficiency, we present a solution scheme— Matrix Blind Space Elimination (MBSE).

First of all we describe null space as follow conveniently,

$$\mathrm{Null}(\mathbf{m}) = \{\mathbf{v} \in \mathbf{V} : \mathbf{M}\mathbf{v} = \mathbf{0}\} \tag{9}$$

As mentioned above, when

$$\mathbf{w}_k \in \mathrm{Null}(\mathbf{G}_k) \tag{10}$$

The eavesdropper's channel cannot be degraded by the artificial noise. Thus we need to optimize the parameters to make $\mathbf{G}_k \mathbf{w}_k \neq 0$. We note that all of the channel gain matrix cannot be changed at will, while $\mathbf{w}_k$ is optional, so we should restructure $\mathbf{w}_k$ through a new approach which is called MBSE. It is described as follows,

Firstly, define

$$\mathbf{R} = \left\{ \mathrm{Null}\left(\mathbf{H}_k\right) \cap \mathrm{Null}\left(\mathbf{G}_k\right) \right\} \tag{11}$$

$$\mathbf{Q} = \mathrm{Null}\left(\mathbf{H}_k\right) \tag{12}$$

$$\mathbf{C_Q R} = \mathbf{Q} - \mathbf{R} \tag{13}$$

Then choose

$$\tilde{\mathbf{w}}_k \in \mathbf{C_Q R} \tag{14}$$

$$\Leftrightarrow \begin{cases} \mathbf{G}_k \tilde{\mathbf{w}}_k \neq 0 & (15) \\ \mathbf{H}_k \tilde{\mathbf{w}}_k = 0 & (16) \end{cases}$$

IV. Performance Analisis

We call $\mathbf{R}$ security blind space in MIMOAN. Once $\mathbf{w}_k \in \mathbf{R}$, MIMOAN will lose its security. Obviously, MBSE-MIMOAN can avoid the security blind space effectively. The artificial noise can always be valid in MBSE-MIMOAN, which guarantees security.

We will compare MIMOAN with MBSE-MIMOAN through computing the secrecy capacities. Secrecy capacity is bounded below by the difference in mutual information between the transmitter and the receiver versus the transmitter and the eavesdropper.

If $\mathbf{w}_k \in \mathbf{r}$, the secrecy capacity of MIMOAN is given by

$$\begin{aligned} &Secrecy\,Capacity \geq C_{\sec}^{a} \\ &= I\left(\mathbf{A};\mathbf{S}\right) - I\left(\mathbf{B};\mathbf{S}\right) \\ &= \log\left(\left|\mathbf{I}\sigma_n^2 + \mathbf{H}_k \mathbf{J}_s \mathbf{H}_k^{\dagger}\right| / \left|\mathbf{I}\sigma_n^2\right|\right) \\ &- \log\left(\left|\mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| / \left|\mathbf{I}\sigma_e^2\right|\right) \end{aligned} \tag{17}$$

Optimization after ($\tilde{\mathbf{w}}_k \in \mathbf{C_q r}$), the eavesdropper Eve observes colored Gaussian noise with covariance $\mathbf{K} = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^{\dagger} \mathbf{G}_k^{\dagger})\sigma_v^2 + \mathbf{I}\sigma_e^2$. The secrecy capacity of MBSE-MIMOAN is given by

$$\begin{aligned} &\tilde{C}_{\sec}^{a} = I\left(\mathbf{A};\mathbf{S}\right) - I\left(\mathbf{B};\mathbf{S}\right) \\ &= \log\left(\left|\mathbf{I}\sigma_n^2 + \mathbf{H}_k \mathbf{J}_s \mathbf{H}_k^{\dagger}\right| / \left|\mathbf{I}\sigma_n^2\right|\right) \\ &- \log\left(\left|\mathbf{K} + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| / \left|\mathbf{K}\right|\right) \end{aligned} \tag{18}$$

Where $\mathbf{J}_s = \mathbf{E}\left[\mathbf{s}_k \mathbf{s}_k^{\dagger}\right]$. The secrecy capacity is maximized by choosing

$$\mathbf{p}_k = \mathbf{h}_k / \left\|\mathbf{h}_k\right\| \tag{19}$$

Distinctly, $\mathbf{p}_k \mathbf{u}_k$ lies in the range space of $\mathbf{H}_k$, and yet the artificial noise is transmitted in the null space of $\mathbf{H}_k$. Therefore, the two spaces are well separated.

The secrecy capacity difference between the two schemes is given by

$$\begin{aligned} &\tilde{C}_{\sec}^{a} - C_{\sec}^{a} \\ &= \log\left(\left|\mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| / \left|\mathbf{I}\sigma_e^2\right|\right) \\ &- \log\left(\left|\mathbf{K} + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| / \left|\mathbf{K}\right|\right) \\ &= \log\left(\frac{\left|\mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| \left|(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^{\dagger} \mathbf{G}_k^{\dagger})\sigma_v^2 + \mathbf{I}\sigma_e^2\right|}{\left|(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^{\dagger} \mathbf{G}_k^{\dagger})\sigma_v^2 + \mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| \left|\mathbf{I}\sigma_e^2\right|}\right) \\ &= \log\left(1 + \frac{\left|(\mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger})(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^{\dagger} \mathbf{G}_k^{\dagger})\sigma_v^2\right|}{\left|(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^{\dagger} \mathbf{G}_k^{\dagger})\sigma_v^2 + \mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{J}_s \mathbf{G}_k^{\dagger}\right| \left|\mathbf{I}\sigma_e^2\right|}\right) \\ &> 0 \end{aligned} \tag{20}$$

Note that the secrecy capacity of MBSE-MIMOAN is larger than MIMOAN's.

V. Conclusion

In this paper, the security problem of MIMO wireless channel with a multiple antennas eavesdropper is considered. In MIMOAN model, artificial noise is used to guarantee security effectively, even when the receiver's channel is not better than the eavesdropper's. However, MIMOAN also has vulnerability because the artificial noise may be invalid.

The weakness is analyzed in detail, then a solution scheme—MBSE is presented. The weakness can be made up by the advanced scheme. Finally, the secrecy capacities of both schemes are compared. It is proved that MBSE-MIMOAN is superior. Future work will concentrate on MIMO wireless channel with multiple colluding eavesdroppers. In addition, more accurate results will need to be obtained.

Acknowledgment

This work was supported in part by the National Science Foundation of China under Grant No. 60932003 and No. 61271220.

References

[1] C. E. Shannon, "Communication theory of secrecy systems." Bell Syst. Tech. J., 28:656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," Bell Sys. Tech. Journal, vol. 54, no. 8, pp. 1355– 1387, Oct 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inform. Theory, pp. 339-348, May 1978.

[4] A. E. Hero, "Secure space-time communication," IEEE Trans. Info. Theory, pp. 3235-3249, December 2003.

[5] G. J. Foschini, M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," Wireless Personal Commun: Kluwer Academic Press, no. 6, pp. 311-335, 1998.

[6] P. Y. Wang, G Yu, Z. Y. Zhang. "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," ISIT, Nice, France, pp. 1301-1305, 2007.

[7] Y. Liang and H. V. Poor, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2470-2492, June 2008.

[8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy capacity region of gaussian broadcast channel," CISS, March 2009.

[9] P. K. Gopala , L. F. Lai, H. E. Gamal, "On the capacity of fading channels, " IEEE Transaction on Information Theory, vol.54, no. 10, 2008.

[10] J. Zhu, J. Mo, M. Tao, "Cooperative Secret Communication with Artificial Noise in Symmetric Interference Channel," IEEE Communication letters, vol. 14, no. 10, pp. 885-887, Oct. 2010.

[11] Y. Zhu, X. Chen, Z. Xue, F. B. Li, et.al. "Research on the Multiple-inputs Single-output Channel Under Attack," ICCIS, Aug 17-19, China, pp. 973-976, 2012.

[12] Ersen Ekrem and S.Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel",IEEE Trans.Inform. Theory,vol.57, no.4, April 2011.

[13] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, "Analysis and performance of some basic space-time architectures," IEEE J. Select. Areas Comm, vol. 21, no. 3, pp. 303-320, April 2003.

[14] S. Goel, R. Negi, "Guaranteeing secrecy using artificial Noise," IEEE Trans. Wireless Communications, vol 7, no.6, pp:2180-2189, June 2008.

[15] R. Negi, S. Goel, "Secret communication using artificial noise," To appear in Proc. VTC Fall'05, vol.3, pp:1906-1910, Sept. 2005.

[16] X. Chen, Y. Zhu, Z. Xue, F. B. Li, et.al. "Security in Single-Input Single-Output Multiple-helpers Wireless Channel," ICCIS, Aug 17-19, China, pp. 969-972, 2012.

[17] X. Chen, F. B. Li, Z. Xue, Y.Zhu, et.al. "Research on the Security of MISO Wireless Channel with Artificial Noise," ICCIS, Jun 21-23, China, pp. 1534-1537, 2013.