Jammer Optimization Design for Multi-Antenna Proactive Eavesdropping Systems (Postprint)

Authors: Tu Xiaolan, Guangchi Zhang, Wan Linqing, Cui Miao, Lin Fan

Date: 2018-05-20T00:00:00+00:00

Abstract

Unlike conventional passive eavesdropping techniques for physical layer security in wireless communications, this work investigates physical layer active eavesdropping techniques, which are primarily employed by legitimate authorities to monitor communications of suspicious users. Considering a system model where the suspicious transmitter and legitimate jammer are equipped with multiple antennas while the suspicious receiver and legitimate eavesdropper have single antennas, and under the condition that the suspicious communication link gain is stronger than the eavesdropping link gain, jamming signals are transmitted to control the communication rate of the suspicious user, thereby enabling the legitimate eavesdropper to correctly decode the eavesdropped information. Optimal jamming signal design and jamming power control are investigated for two scenarios: with and without interference from the legitimate jammer to the legitimate eavesdropper, with the objective of maximizing the eavesdropping rate. Simulation results demonstrate that reasonably positioning the jammer in different application scenarios can effectively improve the eavesdropping rate, and the proposed jammer design methods both achieve superior eavesdropping performance compared to two existing benchmark methods.

Full Text

Jammer Optimization for Multi-Antenna Proactive Eavesdropping Systems

Tu Xiaolan[1], Zhang Guangchi[1], Wan Linqing[1], Cui Miao[1], Lin Fan[2]
[1]School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China
[2]Guangzhou GCI Science & Technology Co., Ltd, Guangzhou 510310, China

Abstract: Unlike traditional passive eavesdropping techniques for physical layer security in wireless communications, this paper investigates proactive

eavesdropping technology at the physical layer, which is employed by legitimate authorities to monitor communications between suspicious users. Considering a system model where the suspicious transmitter and legitimate jammer are equipped with multiple antennas while the suspicious receiver and legitimate eavesdropper have single antennas, we control the communication rate of suspicious users by transmitting jamming signals when the suspicious communication link gain is stronger than the eavesdropping link gain, enabling the legitimate eavesdropper to correctly decode the intercepted information. We design optimal jamming signals and power control strategies to maximize the eavesdropping rate for two scenarios: with and without interference from the legitimate jammer to the legitimate eavesdropper. Simulation results demonstrate that reasonably positioning the jammer in different application scenarios can effectively improve the eavesdropping rate, and the proposed jammer design methods achieve superior eavesdropping performance compared to two existing benchmark approaches.

Keywords: proactive eavesdropping; jamming signal design; interference power control; eavesdropping rate performance

0 Introduction

The rapid development of wireless communication technology has brought convenience to people' s lives while simultaneously introducing risks of privacy and confidential information leakage. In wireless networks, the inherent broadcast nature of wireless transmission facilitates convenient information exchange among authorized users, but this characteristic is also exploited by malicious attackers who attempt to steal user identity information, passwords, and other sensitive data. Such malicious attacks are known as passive eavesdropping attacks, where eavesdroppers typically listen to user information without actively disrupting reception. Ensuring secure information transmission has always been a critical research topic in information security.

Traditional approaches to counter physical layer security threats include: (a) conventional cryptographic encryption techniques, which encrypt information through effective mechanisms to prevent interception. While this technology provides effective protection, the rapid expansion of eavesdropper populations presents significant challenges in terms of increasing key management complexity. (b) Physical layer security methods that exploit channel and noise characteristics to degrade the eavesdropper' s channel environment and enhance transmission security. This protection technology offers broad application prospects and value.

While eavesdropping is generally considered illegal, eavesdroppers can launch active attacks to enhance their eavesdropping performance, known as proactive eavesdropping. In special security domains, proactive eavesdropping is used to investigate criminal and terrorist communications to reduce unlawful activities, and such monitoring by government agencies is considered legitimate.

Currently, academic research has proposed two main physical layer proactive eavesdropping techniques: (a) jamming-based proactive eavesdropping, where a full-duplex legitimate eavesdropper transmits jamming signals to adjust the suspicious communication rate when located far from the suspicious transmitter, thereby strengthening eavesdropping effectiveness; and (b) proactive eavesdropping where the eavesdropper acts as a relay to forward interference signals. In this approach, the eavesdropper functions as a relay, amplifying and forwarding a beneficial signal to the receiver when the eavesdropping channel is favorable, and forwarding a destructive signal otherwise, thereby confusing the source transmitter and enabling successful decoding of intercepted information.

However, existing literature [7–10] only considers single-antenna scenarios. For practical applications, we propose adding a separate multi-antenna jammer that can adjust its transmit power within a movable range. System eavesdropping performance improves when the jammer is positioned closer to the suspicious receiver, making effective jammer placement crucial for enhancing legitimate eavesdropping performance. Building upon the jamming-based proactive eavesdropping technique proposed in literature [7], we consider a multiple-input single-output (MISO) multi-antenna model with an added multi-antenna jammer. By optimizing the jammer' s transmit power, we improve the system' s eavesdropping rate. Based on the definition of proactive eavesdropping from literature [7], a legitimate eavesdropper can successfully decode suspicious communications when the eavesdropping rate exceeds the suspicious communication rate in fading channels.

Notation: Bold lowercase and uppercase letters denote vectors and matrices, respectively. $(\cdot)^T$ and $(\cdot)^H$ denote transpose and conjugate transpose. $\mathrm{tr}(\cdot)$ denotes matrix trace. $\|\cdot\|$ denotes matrix norm, and $\|\cdot\|_2$ denotes Euclidean norm (2-norm) of a vector.

1 System Model

Consider a legitimate wireless monitoring scenario over a MISO Rayleigh fading channel [Figure 1: see original paper], where a legitimate eavesdropper monitors a point-to-point suspicious communication link. When the eavesdropping environment is weaker than the communication environment, a jammer transmits interference signals to disrupt communication between suspicious users. Let N_s and N_j denote the number of antennas at the suspicious transmitter (S) and jammer (J), respectively. The suspicious receiver (D) and legitimate eavesdropper (E) each have a single antenna. The channel gains between S-D, S-E, J-D, and J-E links are denoted by $\mathbf{h}_{sd}$, $\mathbf{h}_{se}$, $\mathbf{h}_{jd}$, and $\mathbf{h}_{je}$, respectively, which follow complex Gaussian distributions and remain constant during each transmission frame.

1.1 Communication Model Without Proactive Eavesdropping

Without proactive eavesdropping, the received signal at the suspicious receiver D is

$$y_d = \sqrt{P_s}\mathbf{h}_{sd}^H \mathbf{w}_s x_s + n_d \tag{1}$$

where P_s is the transmit power of the suspicious transmitter, $\mathbf{w}_s$ and x_s are the weighted transmission vector and transmitted signal, respectively, with $E\{|x_s|^2\} = 1$, and $n_d \sim \mathcal{CN}(0, \sigma_d^2)$ is the additive white Gaussian noise at D. From (1), the average output SNR at the suspicious receiver for a given channel is

$$\gamma_d = \frac{P_s |\mathbf{h}_{sd}^H \mathbf{w}_s|^2}{\sigma_d^2} \tag{2}$$

The transmit weight vector $\mathbf{w}_s$ should maximize (2). By the Schwartz inequality for inner product operations, when $\mathbf{w}_s = \frac{\mathbf{h}_{sd}}{\|\mathbf{h}_{sd}\|}$, (3) holds with equality. This conclusion follows from the maximum ratio transmission principle [15], where weighting values are designed at the transmitter to maximize the communication rate.

1.2 Proactive Eavesdropping Model

Assume the legitimate eavesdropper E monitors the transmitted signal from the suspicious transmitter S. During monitoring, the jammer J with N_j antennas transmits jamming signals to interfere with the suspicious link [16]. The jamming power is P_j and the autocorrelation matrix of the jamming signal is $\mathbf{V} = E\{\mathbf{v}\mathbf{v}^H\}$. The received signals at the legitimate eavesdropper E and suspicious receiver D are

$$y_e = \sqrt{P_s}\mathbf{h}_{se}^H \mathbf{w}_s x_s + \sqrt{a}\mathbf{h}_{je}^H \mathbf{v} + n_e \tag{4}$$

$$y_d = \sqrt{P_s}\mathbf{h}_{sd}^H \mathbf{w}_s x_s + \mathbf{h}_{jd}^H \mathbf{v} + n_d \tag{5}$$

where $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ is the additive white Gaussian noise at the legitimate eavesdropper E, and a is the interference coefficient. If $a = 0$, the eavesdropper can completely eliminate interference; if $a = 1$, the eavesdropper also suffers from interference. The eavesdropping decision condition is otherwise.

From (4) and (5), the SNRs at the suspicious receiver D and legitimate eavesdropper E are

$$\gamma_d = \frac{P_s |\mathbf{h}_{sd}^H \mathbf{w}_s|^2}{\mathbf{h}_{jd}^H \mathbf{V} \mathbf{h}_{jd} + \sigma_d^2} \tag{6}$$

$$\gamma_e = \frac{P_s|\mathbf{h}_{se}^H \mathbf{w}_s|^2}{a\mathbf{h}_{je}^H \mathbf{V}\mathbf{h}_{je} + \sigma_e^2} \tag{7}$$

2 Optimal Jamming Design

According to literature [4], when the eavesdropping channel gain exceeds the suspicious communication channel gain ($\|\mathbf{h}_{se}\|^2 > \|\mathbf{h}_{sd}\|^2$), the eavesdropper can decode the transmitted signal from S, and the information leakage rate equals the receiver' s communication rate R_d. Otherwise, the eavesdropper cannot decode the intercepted signal, and the eavesdropping rate is zero. Therefore, the eavesdropping rate is defined as

$$R_e = \begin{cases} R_d, & \|\mathbf{h}_{se}\|^2 \geq \|\mathbf{h}_{sd}\|^2 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

To improve overall system performance, we optimize the jamming signal' s autocorrelation matrix $\mathbf{V}$ to maximize the eavesdropping rate under jamming power constraints. Based on the definition of proactive eavesdropping in (9), the optimal jamming design problem can be formulated as

$$\begin{aligned} \max_{\mathbf{V}} \quad & R_e && \text{(9a)} \\ \text{s.t.} \quad & R_e \geq R_d && \text{(9b)} \\ & \mathbf{V} \succeq 0 && \text{(9c)} \\ & \text{tr}(\mathbf{V}) \leq P_j && \text{(9d)} \end{aligned}$$

Constraints (9b)-(9d) represent system limitations: (9c) ensures $\mathbf{V}$ is positive semidefinite, (9d) is the jamming power constraint, and (9b) corresponds to the condition where the eavesdropping channel gain is relatively strong, meaning no jamming is transmitted. According to the definition from literature [7], when the legitimate eavesdropper' s channel condition is stronger than the suspicious receiver' s, the legitimate eavesdropper E can successfully decode the suspicious transmission. The ultimate goal is to optimize the jamming transmit power to maximize the eavesdropping rate.

2.1 No Self-Interference: Optimal Jamming Signal Design Based on Semidefinite Programming

Assuming complete channel state information and that the legitimate eavesdropper E can avoid jamming signal interference through advanced analog and digital self-interference cancellation, the eavesdropper' s objective is to optimize the jamming transmit power to maximize the eavesdropping rate and improve performance.

Based on literature [8], the problem is solvable when constraint (9b) is satisfied. The jammer employs an adaptive power adjustment strategy: when the eavesdropping channel gain is better than the communication channel gain ($\|\mathbf{h}_{se}\|^2 > \|\mathbf{h}_{sd}\|^2$), there exists a feasible jamming power solution that satisfies the constraint (eavesdropping rate greater than suspicious communication rate). Otherwise, the jammer adjusts its power according to the decision conditions for self-interference and no-self-interference scenarios.

According to literature [11-13], the semidefinite programming (SDP) method can transform the problem into an SDP formulation:

$$\begin{aligned} \max_{\mathbf{V}} \quad & \mathrm{tr}(\mathbf{H}_{se}\mathbf{V}) && \text{(10a)} \\ \text{s.t.} \quad & \mathrm{tr}(\mathbf{H}_{sd}\mathbf{V}) \geq \beta && \text{(10b)} \\ & \mathbf{V} \succeq 0 && \text{(10c)} \\ & \mathrm{tr}(\mathbf{V}) \leq P_j && \text{(10d)} \end{aligned}$$

where $\beta = \frac{\sigma_e^2}{\sigma_d^2}\|\mathbf{h}_{se}\|^2 - \|\mathbf{h}_{sd}\|^2$. Since constraints (14) and (15) are convex, the optimal solution can be obtained directly using interior-point methods. The SDP method optimizes the autocorrelation matrix $\mathbf{V}$ to achieve the maximum eavesdropping rate.

The optimal jamming power design is:

$$P_j^* = \begin{cases} 0, & \|\mathbf{h}_{se}\|^2 > \|\mathbf{h}_{sd}\|^2 \\ P_j^{\mathrm{SDP}}, & \text{otherwise} \end{cases}$$

where P_j^{SDP} is the optimal power obtained from the SDP solution.

2.2 Self-Interference: Jamming Signal Design Under Self-Interference Conditions

In self-interference scenarios, the eavesdropping decision condition requires satisfying $\|\mathbf{h}_{se}\|^2 \geq \|\mathbf{h}_{sd}\|^2$ for the Lagrangian method to be applicable. To obtain the global optimal solution for problem (9) under self-interference, we employ the Lagrangian method from literature [11, 14].

The Lagrangian primal problem for (9) is:

$$\mathcal{L}(\mathbf{V}, \lambda) = \mathrm{tr}(\mathbf{A}_1\mathbf{V}) + \lambda(\mathrm{tr}(\mathbf{A}_2\mathbf{V}) - \sigma_d^2)$$

where $\mathbf{A}_1$ and $\mathbf{A}_2$ are defined matrices. Introducing Lagrangian dual variables $\lambda \geq 0$, the dual function is $g(\lambda) = \min_{\mathbf{V}\succeq 0} \mathcal{L}(\mathbf{V}, \lambda)$. The dual problem becomes:

$$\max_{\lambda \geq 0} \quad g(\lambda) \quad \text{s.t.} \quad \mathbf{A}_1 + \lambda \mathbf{A}_2 \succeq 0$$

Since problem (9) is a convex SDP problem, its optimal solution can be obtained via interior-point methods [11]. The optimal jamming power design under self-interference is:

$$P_j^* = \begin{cases} 0, & \|\mathbf{h}_{se}\|^2 > \|\mathbf{h}_{sd}\|^2 \\ P_j^{\text{Lag}}, & \text{otherwise} \end{cases}$$

where P_j^{Lag} is the optimal power from the Lagrangian solution.

Algorithm 1: Optimization of Autocorrelation Matrix V Under Self-Interference/No-Self-Interference

Step 1: Compare eavesdropping channel gain with suspicious communication channel gain. If $\|\mathbf{h}_{se}\|^2 > \|\mathbf{h}_{sd}\|^2$, proceed to Step 3. Otherwise, proceed to Step 2 to optimize $\mathbf{V}$ under no-self-interference or self-interference conditions.

Step 2: - **No-self-interference** ($a = 0$)**:** When $\|\mathbf{h}_{se}\|^2 \leq \|\mathbf{h}_{sd}\|^2$, solve using the SDP method. The optimal jamming power is $P_j^* = P_j^{\text{SDP}}$. - **Self-interference** ($a = 1$)**:** When $\|\mathbf{h}_{se}\|^2 \leq \|\mathbf{h}_{sd}\|^2$, solve using the Lagrangian method. The optimal jamming power is $P_j^* = P_j^{\text{Lag}}$.

Step 3: Set jamming power $P_j = 0$.

Step 4: Compute the system eavesdropping rate R_e.

3 Simulation Results

This section presents computer simulations to validate the proposed proactive eavesdropping schemes under both self-interference and no-self-interference conditions. We compare the adaptive power adjustment scheme with two existing baseline methods: (a) proactive eavesdropping without a jammer, and (b) proactive eavesdropping with a jammer using fixed power $P_j = P_{\max}$ and maximum ratio transmission (MRT) beamforming. In the MRT approach, the multi-antenna jammer applies beamforming weights $\mathbf{w}_j = \frac{\mathbf{h}_{jd}^*}{\|\mathbf{h}_{jd}\|}$ to direct energy toward the target receiver, maximizing the interference power at the receiver.

In the path loss model, channel gains are modeled as $h_{ik} = g_{ik} d_{ik}^{-\alpha/2}$, where $g_{ik} \sim \mathcal{CN}(0,1)$ are i.i.d. complex Gaussian random variables, d_{ik} is the distance between nodes, and α is the path loss exponent. The noise power is $\sigma^2 = -80$ dBm and the maximum jamming power is $P_{\max} = 30$ dBm. The distances between suspicious transmitter S, legitimate eavesdropper E, and suspicious receiver D are fixed at 500 m, with coordinates (0,0) m, (500,0) m, and (0,500) m, respectively. The jammer' s initial position is (250,250) m.

Fixed Position Performance: With the jammer at (250,250) m, Figures 2 and 3 compare the three methods across transmit powers from 20 dBm to 30 dBm. The eavesdropping rate increases with transmit power P_s. Under the adaptive power adjustment method, when the eavesdropping channel gain is stronger, there exists a feasible jamming power solution satisfying the constraints. The MRT method increases jamming transmit power, raising the receiver' s noise power and reducing demodulation SNR, resulting in inferior performance compared to adaptive power adjustment. The no-jammer method yields zero eavesdropping rate when the eavesdropping channel gain is stronger, and $R_e = R_d$ when the suspicious channel gain is stronger, resulting in lower average eavesdropping rates than the MRT method.

Variable Position Performance: With fixed transmit power $P_s = 25$ dBm and the jammer moving horizontally from 100 m to 900 m, Figures 4 and 5 show performance comparisons. The no-jammer method shows little variation since it depends only on channel gains. As the jammer moves closer to the receiver, the channel gain $\|\mathbf{h}_{jd}\|^2$ strengthens, increasing interference power and reducing the receiver' s demodulation SNR. Consequently, the eavesdropping rate increases when the jammer approaches the suspicious receiver and decreases when it moves away. Therefore, practical applications must carefully position the jammer to achieve optimal eavesdropping performance.

Performance Ranking: The eavesdropping rate comparison across the three methods is: (No-jammer proactive eavesdropping) $<$ (MRT-based proactive eavesdropping) $<$ (Adaptive power adjustment proactive eavesdropping). The proposed jammer design methods thus achieve superior eavesdropping rate performance compared to the two baseline approaches.

4 Conclusion

This paper addresses legitimate eavesdropping technology by considering both self-interference and no-self-interference environments. By reasonably positioning the jammer and designing optimal jamming transmission signals, we improve system eavesdropping performance. In different application scenarios, the jammer adaptively adjusts its power based on power judgment criteria to interfere with suspicious wireless links. Simulation results demonstrate that the proposed jammer design methods achieve better eavesdropping rate performance than existing benchmark approaches.

References

[1] Liang Y, Poor H V, Shamai S. Information theoretic security, foundations and trends in communications and information theory[M]. Now Publishers Inc, 2009.

[2] Massey J L. An introduction to contemporary cryptology[J]. Proceedings of the IEEE, 1988, 76(5): 533-549.

[3] Shannon C E. Communications theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[4] Zhang Guangchi, Li Xueyi, Cui Miao, et al. Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple-output relaying systems power minimization in multiuser downlink CoMP[J]. IEEE Trans on Communications, 2016, 10(7): 796-804.

[5] Zappone A, Lin P H, Jorswieck E. Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI[J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10(8): 1462-1477.

[6] Goel S, Negi R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans on Wireless Communication, 2008, 7(6): 2180-2189.

[7] Xu Jie, Duan Lingjie, Zhang Rui. Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels[J]. IEEE Wireless Communications letters, 2016, 5(1): 80-83.

[8] Zheng Yong, Zhang Rui. Active eavesdropping via spoofing relay attack[C]//Proc of IEEE International Conference on Acoustics, Speech and Signal Processing. 2016: 2159-2163.

[9] Zeng Yong, Zhang Rui. Wireless Information Surveillance via proactive eavesdropping with spoofing relay[J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10(8): 1449-1461.

[10] Kapetanovic D, Zheng Gan, Rusek F. Physical layer security for massive MIMO: an overview on passive eaves-dropping and active attacks[J]. IEEE Communication Magzine, 2015, 53(6): 21-27.

[11] Chi C Y, Li W C, Lin C H. Convex optimization for signal processing and communications from fundamentals to application[M]. CRC Press, [S. l.], 2016.

[12] Huang Jianli, Li Quanzhong, Zhang Qi, et al. Relay beamforming for amplify-and-forward multi-antenna relay networks with energy harvesting constraint[J]. IEEE Wireless Communication Letters, 2014, 21(4): 454-458.

[13] Li Quanzhong, Zhang Qi, Feng Renhai, et al. Optimal relay selection and beamforming in MIMO cognitive multirelay networks[J]. Communications Letters, 2013, 17(6): 1188-1191.

[14] Nguyen D H N, Le L B, Le-Ngoc T. Optimal dynamic point selection for power minimization in multiuser downlink CoMP[J]. IEEE Trans on Wireless Communications, 2017, 16(1): 619-633.

[15] 耿国桐. MIMO 系统中最大比发射和天线选择技术研究 [D]. 北京: 北京邮电大学, 2005.

[16] Liu Qian, Li Ming, Kong Xiangwei, et al. Disrupting MIMO communication with optimal jamming signal design[J]. IEEE Trans on Wireless Communications, 2015, 14(10): 5313-5325.

[17] Zheng Gan, Krikidis I, Li J S, et al. Improving physical layer security using full-duplex jamming receivers[J]. IEEE Trans on Signal Processing, 2015, 63(13): 3623-3634.

Note: Figure translations are in progress. See original paper for figures.