基于非理想信道状态信息的鲁棒安全发送方法

张立健 金 梁* 刘 璐 罗文宇
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对协方差信道状态信息(Channel State Information, CSI)不理想导致的通信系统安全性能恶化问题，该文提出一种鲁棒的人工噪声辅助的物理层安全发送方法。该方法基于非理想的协方差信道信息，对发送者的波束成形向量及人工噪声协方差进行联合优化设计，从而最大化系统的最差情况安全速率(Worst-Case Secrecy Rate, WCSR)。该功率受限的安全速率最大化问题是非凸的，采用半定松弛(SemiDefinite Relaxation, SDR)技术和Lagrange对偶理论将其转化为一系列的半定规划(SemiDefinite Program, SDP)问题进行求解。仿真结果表明，与现有方案相比，所提方法的安全性能有了明显的提升。

关键词：无线通信；物理层安全；安全速率；非理想信道状态信息；人工噪声；鲁棒性
中图分类号： TN92 **文献标识码**： A **文章编号**：1009-5896(2015)05-1187-07
DOI: 10.11999/JEIT140994

Robust Secure Transmit Method with Imperfect Channel State Information

Zhang Li-jian Jin Liang Liu Lu Luo Wen-yu
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: The security performance of the communication system degrades dramatically when the covariance-based Channel State Information (CSI) is imperfect at the transmitter. To overcome this problem, a robust Artificial Noise (AN) aided transmit method is proposed. The objective is to jointly design the transmit beamforming vector and the AN covariance with the imperfect covariance-based CSI at the transmitter, such that the Worst-Case Secrecy Rate (WCSR) of the system is maximized. The secrecy rate maximization problem is non-convex. Due to the intractability, this problem is recast into a series of SemiDefinite Programs (SDPs) using the SemiDefinite Relaxation (SDR) technique and the Lagrange duality. Simulation results demonstrate that the proposed method provides substantial performance improvements over the existing method.

Key words: Wireless communication; Physical layer security; Secrecy rate; Imperfect Channel State Information (CSI); Artificial Noise (AN); Robustness

1 引言

传统的无线安全通信主要是在通信协议的上层采用基于密钥的加密算法对信息进行保护。然而，无线网络的动态拓扑及节点的移动性为密钥的分发与管理带来了更多的挑战。作为对传统加密算法的替代或者补充，无线物理层安全的研究得到了诸多研究机构和学者的重视，已成为无线通信领域的一个研究热点。在关于物理层安全的研究中，文献[1]证明了主信道优于窃听信道时，可实现信息传输的绝对安全。

目前，多数文献[2]都是假设发送者具有理想信道状态信息(Channel State Information, CSI)展开研究的。但是，在实际通信应用中，由于不可避免地受到估计误差、量化误差以及反馈时延等因素的影响，发送者所获得的CSI并不是理想的。针对这一问题，已有学者展开了关于鲁棒无线物理层安全发送方法的研究，在非理想CSI条件下，尽可能地保证系统的安全性能。一般来讲，信道误差模型可以分为两类：统计误差模型和确定误差模型。在统计误差模型下，通常将遍历安全容量[3,4]和安全中断概率[5]作为系统的安全性能指标。基于确定误差模型，文献[6–9]研究了基于最差情况的鲁棒发送问题。文献[6]假设合法信道和窃听信道均为非理想情况下，给出了最优波束成形向量的解析解；假设仅窃听信道是非理想的，文献[7]通过信号与噪声协方差的联合优化，研究了MISO信道多个多天线窃听者场景中的安全速率最大化问题；在所有信道均为非理想情况下，文献[8]提出了次优的人工噪声辅助的发送方法。文献[9]从用户服务质量(Quality of Service,

2014-07-25收到，2014-10-13改回
国家自然科学基金(61171108, 61401510, 61379006)资助课题
*信作者：金梁 liangjin@263.net

QoS)角度，研究了 MISO 认知无线电网络的物理层安全问题。需要指出的是以上提到的鲁棒性研究均基于非理想的信道向量或矩阵信息，并没有考虑非理想的协方差 CSI 情况。

在实际应用中，由于信道的二阶统计特性相对于瞬时的信道本身来讲变化较慢，因此基于前者的反馈需求相对较少，这在快衰落信道中更有实际意义[10]。基于非理想信道协方差信息，文献[10–12]研究了认知通信中的频谱共享问题，没有考虑安全通信的情况。文献[13]基于多中继协作解码转发(Decode and Forward, DF)协议，研究了第 2 个传输阶段的鲁棒安全发送问题，该模型可以对应到 MISO 窃听信道的场景中。然而，文献[13]的方法存在以下问题：(1)在信道协方差误差的建模中，没有考虑到信道协方差的正定性限制，是一种保守的估计方法；(2)仅适用于一个窃听者的情况；(3)没有充分利用多个中继节点协作构成的虚拟多天线这一有利条件，引入人工噪声，提高系统的安全容量。

针对上述不足，本文考虑多个单天线窃听者的情况，基于非理想信道协方差 CSI，提出了一种鲁棒的人工噪声辅助的安全发送方法。其目的是，通过对发送波束成形向量与噪声协方差的联合优化，在发送者总功率受限的情况下，最大化系统的最差情况安全速率(Worst-Case Secrecy Rate, WCSR)。采用半定松弛技术[14](SemiDefinite Relaxation, SDR)和拉格朗日对偶理论[15]，将原始的非凸优化问题转化为简单的单变量优化问题。通过求解一系列的半定规划问题[15](SemiDefinite Program, SDP)，完成对单变量的 1 维搜索。

2 系统模型与问题描述

2.1 系统模型

本文考虑的无线通信系统模型如图 1 所示，包括一个具有 N 个天线的发送者(Alice)，一个单天线合法接收者(Bob)和 K 个单天线窃听者(Eve)。令 $\boldsymbol{h}\in\mathcal{C}^N$ 为 Alice 到 Bob 的信道向量；$\boldsymbol{g}_k\in\mathcal{C}^N$ 为 Alice 到第 k 个 Eve 的信道向量，$\forall k\in\mathcal{K}$，$\mathcal{K}\triangleq\{1,2,\cdots,K\}$。假设所有的信道相互独立，并服从瑞利平坦衰落。Bob 和第 k 个 Eve 的接收信号分别表示为

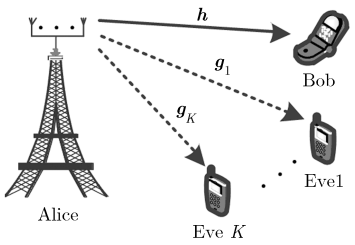


图 1 MISO 窃听信道模型

$$y_b=\boldsymbol{h}^{\mathrm{H}}\boldsymbol{x}+n_b,\quad y_{e,k}=\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{x}+n_{e,k},\ \forall k\in\mathcal{K}\tag{1}$$

式中，n_b 和 $n_{e,k}$ 分别为 Bob 和第 k 个 Eve 处的加性高斯噪声(AWGN)，且服从均值为 0，方差为 1 的复高斯分布，即 $n_b\sim\mathcal{CN}(0,1)$ 和 $n_{e,k}\sim\mathcal{CN}(0,1)$；$\boldsymbol{x}\in\mathcal{C}^N$ 为 Alice 所发送的信号，其表达式为

$$\boldsymbol{x}=\boldsymbol{w}s+\boldsymbol{z}\tag{2}$$

这里，$s\in\mathcal{C}$ 为 Alice 发送给 Bob 的保密信息，$\mathrm{E}\{s\}=0$，$\mathrm{E}\{|s|^2=1\}$；$\boldsymbol{w}\in\mathcal{C}^N$ 为波束成形向量；$\boldsymbol{z}\in\mathcal{C}^N$ 为 Alice 生成的用于干扰 Eve 接收的人工噪声向量，假设 $\boldsymbol{z}\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{\Sigma})$，其中 $\Sigma\succeq\boldsymbol{0}$ 为人工噪声协方差。

根据式(1)和式(2)，Bob 和第 k 个 Eve 的信干噪比(Signal-to-Interference-plus-Noise Ratio, SINR)分别为

$$\left.\begin{aligned}\mathrm{SINR}_b&=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Sigma})}\\ \mathrm{SINR}_{e,k}&=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{G}_k\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{G}_k\boldsymbol{\Sigma})},\ \forall k\in\mathcal{K}\end{aligned}\right\}\tag{3}$$

式中，$\boldsymbol{H}\triangleq\mathrm{E}\{\boldsymbol{h}\boldsymbol{h}^{\mathrm{H}}\}$ 为合法信道的协方差，$\boldsymbol{G}_k\triangleq\mathrm{E}\{\boldsymbol{g}_k\boldsymbol{g}_k^{\mathrm{H}}\}$ 为第 k 个窃听信道的协方差。根据上述信号模型，Alice 可以获得的安全速率为[7]

$$R_s=\min_{k\in\mathcal{K}}\{\log_2(1+\mathrm{SINR}_b)-\log_2(1+\mathrm{SINR}_{e,k})\}\tag{4}$$

2.2 问题描述

在实际应用中，由于估计误差、量化误差及反馈时延等因素的影响，Alice 无法获得理想的 CSI。相应地，系统的安全性能也会随之降低。因此，需要考虑在 CSI 存在误差的情况下，如何设计具有鲁棒性的发送方法，提升系统的安全性能。本文考虑信道协方差的误差，类似文献[12]和文献[13]，将合法信道与窃听信道的协方差分别表示为

$$\boldsymbol{H}=\boldsymbol{H}+\boldsymbol{\Delta}_b=\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}+\boldsymbol{\Delta}_b\tag{5a}$$

$$\boldsymbol{G}_k=\widehat{\boldsymbol{G}}_k+\boldsymbol{\Delta}_{e,k}=\hat{\boldsymbol{g}}_k\hat{\boldsymbol{g}}_k^{\mathrm{H}}+\boldsymbol{\Delta}_{e,k},\ \forall k\in\mathcal{K}\tag{5b}$$

式中，$\widehat{\boldsymbol{H}}=\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}$ 和 $\widehat{\boldsymbol{G}}_k=\hat{\boldsymbol{g}}_k\hat{\boldsymbol{g}}_k^{\mathrm{H}}$，$\forall k\in\mathcal{K}$，分别为 Alice 到 Bob 和到第 k 个 Eve 的信道协方差矩阵估计值；$\boldsymbol{\Delta}_b$ 和 $\boldsymbol{\Delta}_{e,k}$ 为相应的估计误差。本文考虑基于椭球界的确定性误差模型[10,12]，即

$$\left.\begin{aligned}\mathcal{H}&\triangleq\{\boldsymbol{\Delta}_b\mid\boldsymbol{\Delta}_b=\boldsymbol{\Delta}_b^{\mathrm{H}},\widehat{\boldsymbol{H}}+\boldsymbol{\Delta}_b\succeq\boldsymbol{0},\\&\qquad\mathrm{Tr}(\boldsymbol{\Delta}_b\boldsymbol{C}\boldsymbol{\Delta}_b)\le\varepsilon_b^2\}\\ \mathcal{G}_k&\triangleq\{\boldsymbol{\Delta}_{e,k}\mid\boldsymbol{\Delta}_{e,k}=\boldsymbol{\Delta}_{e,k}^{\mathrm{H}},\widehat{\boldsymbol{G}}_k+\boldsymbol{\Delta}_{e,k}\succeq\boldsymbol{0},\\&\qquad\mathrm{Tr}(\boldsymbol{\Delta}_{e,k}\boldsymbol{D}_k\boldsymbol{\Delta}_{e,k})\le\varepsilon_{e,k}^2\},\ \forall k\in\mathcal{K}\end{aligned}\right\}\tag{6}$$

式中，$\boldsymbol{C}\succ\boldsymbol{0}$ 和 $\boldsymbol{D}_k\succ\boldsymbol{0}$，$\forall k\in\mathcal{K}$，确定了椭球误差界的形状，并且存在矩阵分解 $\boldsymbol{C}=\widetilde{\boldsymbol{C}}^{\mathrm{H}}\widetilde{\boldsymbol{C}}$ 和 $\boldsymbol{D}_k=\widetilde{\boldsymbol{D}}_k^{\mathrm{H}}\widetilde{\boldsymbol{D}}_k$；$\varepsilon_b\ge0$，$\varepsilon_{e,k}\ge0$ 限制了误差界的大小。

研究目的为总发送功率受限时，通过联合设计波束成形向量 $\boldsymbol{w}$ 和人工噪声协方差 $\boldsymbol{\Sigma}$，最大化系统的 WCSR。根据文献[7]，该安全速率最大化问题可以描述为

$$\left.\begin{aligned}\max_{\boldsymbol{w},\boldsymbol{\Sigma}}\quad & \min_{k\in\mathcal{K}}\left\{\min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\log_2(1+\mathrm{SINR}_b)\right.\\ & \left.-\max_{\boldsymbol{\Delta}_{e,k}\in\mathcal{G}_k}\log_2(1+\mathrm{SINR}_{e,k})\right\}\\ \text{s.t.}\quad & \boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}+\mathrm{Tr}(\boldsymbol{\Sigma})\le P,\quad \boldsymbol{\Sigma}\succeq\boldsymbol{0}\end{aligned}\right\}\tag{7}$$

式中，P 为 Alice 的最大发送功率。文中均假设原始的优化问题式(7)是可行的。在理想信道条件下，即 $\varepsilon_b=\varepsilon_{e,k}=0,\forall k\in\mathcal{K}$，该问题的求解可以参考文献[7]。本文基于信道协方差误差模型，研究合法信道与窃听信道同时存在误差时，鲁棒的安全速率最大化设计问题。由于对 $\boldsymbol{w}$ 和 $\boldsymbol{\Sigma}$ 的联合优化问题式(7)是非凸的，在下一节我们将推导一种可行的方法，对问题式(7)进行求解。

3　鲁棒的人工噪声辅助发送方法

为了后续的推导，需要对原始的优化问题式(7)进行重新描述。将式(3)代入式(7)，同时考虑到所有信道之间的相互独立性，式(7)可以等价地表示为

$$\max_{\boldsymbol{w},\boldsymbol{\Sigma}}\quad \min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Sigma})}\right)-\log_2\frac{1}{\tau}\tag{8a}$$

$$\text{s.t.}\quad \max_{\boldsymbol{\Delta}_{e,k}\in\mathcal{G}_k}\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{G}_k\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{G}_k\boldsymbol{\Sigma})}\right)\le\log_2\frac{1}{\tau},\quad \forall k\in\mathcal{K}\tag{8b}$$

$$\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}+\mathrm{Tr}(\boldsymbol{\Sigma})\le P,\quad \boldsymbol{\Sigma}\succeq\boldsymbol{0}\tag{8c}$$

式中，τ 为辅助变量。从物理意义上来看，$\log_2(1/\tau)$ 表示所有 Eve 的最大互信息，变动该值也就变动了窃听信道的最大互信息，进而实现对整个系统安全速率的控制。

3.1 双层优化问题表述

根据文献[7]，问题式(8a)～式(8c)可以转化为一个双层优化问题，其外层优化为一个单变量优化问题，可以通过 1 维搜索进行求解；内层优化可以转化为一个凸的半定规划问题，采用内点法进行求解[15]。外层优化问题，即单变量优化问题，可以表述为

$$\left.\begin{aligned}R^{*}=\max_{\tau}\quad & \log_2(1+\varphi(\tau))+\log_2(\tau)\\ \text{s.t.}\quad & \tau_{\min}\le\tau\le\tau_{\max}\end{aligned}\right\}\tag{9}$$

式中，$\tau_{\min}$ 和 $\tau_{\max}$ 分别为变量 τ 的下界和上界；$\varphi(\tau)$ 为 τ 给定时，下面内层优化问题的最优目标值

$$\varphi(\tau)=\max_{\boldsymbol{w},\boldsymbol{\Sigma}}\quad \min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{w}}{(1+\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Sigma}))}\tag{10a}$$

$$\text{s.t.}\quad \max_{\boldsymbol{\Delta}_{e,k}\in\mathcal{G}_k}1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{G}_k\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{G}_k\boldsymbol{\Sigma})}\le\frac{1}{\tau},\quad \forall k\in\mathcal{K}\tag{10b}$$

$$\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}+\mathrm{Tr}(\boldsymbol{\Sigma})\le P,\quad \boldsymbol{\Sigma}\succeq\boldsymbol{0}\tag{10c}$$

注意，由于对数函数具有单调性，为了计算方便，约束条件式(10b)中去掉了对数函数 $\log_2(\bullet)$，仅保留其内部的子函数。

确定外层优化问题式(9)的单变量变化范围。根据约束条件式(8b)，可知 $\tau\le1$。τ 的下界确定为

$$\begin{aligned}\tau&\overset{(a)}{\ge}\left(1+\min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{w}}{1+\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Sigma})}\right)^{-1}\\ &\ge\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\widehat{\boldsymbol{H}}\boldsymbol{w})}{1+\mathrm{Tr}(\widehat{\boldsymbol{H}}\boldsymbol{\Sigma})}\right)^{-1}\overset{(b)}{\ge}\left(1+P\mathrm{Tr}(\widehat{\boldsymbol{H}})\right)^{-1}\end{aligned}\tag{11}$$

式中，步骤(a)是根据安全速率非负确定的，见目标函数式(8a)；步骤(b)是因为 $\widehat{\boldsymbol{H}}=\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}$，且由式(8c)可知 $\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}\le P$，当 $\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}=P\widehat{\boldsymbol{H}}/\mathrm{Tr}(\widehat{\boldsymbol{H}}),\boldsymbol{\Sigma}=\boldsymbol{0}$ 时等式成立。因此，可以确定 $\tau_{\max}=1$，$\tau_{\min}=(1+P\mathrm{Tr}(\widehat{\boldsymbol{H}}))^{-1}$。

如前所述，外层优化问题式(9)和内层优化问题式(10)所构成的双层优化问题为原始问题式(7)的等价形式。如果对于给定的 τ，可以确定相应的 $\varphi(\tau)$，则可以通过在区间 $\tau_{\min}\le\tau\le\tau_{\max}$ 内进行 1 维搜索求得问题式(9)的最优值，也是原始问题式(7)的最优值。因此，问题求解的关键在于确定 $\varphi(\tau)$ 的值，即对内层优化问题式(10)求解。

3.2 内层优化问题的求解

本小节将专注于内层优化问题式(10)的求解。可以看到，当 τ 给定时，问题式(10)是一个非凸的二次分数规划问题，直接求解非常困难。因此需要对问题式(10)进行适当的转化，而后对其进行求解。定义 $\boldsymbol{W}=\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w}$，可见存在非凸的约束条件 $\mathrm{Rank}(\boldsymbol{W})=1$。采用半定松弛的思想[15]，去掉 $\mathrm{Rank}(\boldsymbol{W})=1$ 的约束，则式(10)的松弛问题可表示为

$$\phi(\alpha)=\max_{\boldsymbol{W},\boldsymbol{\Sigma}}\ \beta\tag{12a}$$

$$\text{s.t.}\quad \max_{\boldsymbol{\Sigma}_{e,k}\in\mathcal{G}_k}\mathrm{Tr}(\boldsymbol{G}_k\boldsymbol{\psi})\le\alpha,\ \forall k\in\mathcal{K}\tag{12b}$$

$$\mathrm{Tr}(\boldsymbol{W})+\mathrm{Tr}(\boldsymbol{\Sigma})\le P\tag{12c}$$

$$\min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Phi})\ge\beta\tag{12d}$$

$$\boldsymbol{W}\succeq\boldsymbol{0},\ \boldsymbol{\Sigma}\succeq\boldsymbol{0}\tag{12e}$$

式中，$\alpha=(1/\tau-1),\boldsymbol{\psi}=\boldsymbol{W}-\alpha\boldsymbol{\Sigma},\boldsymbol{\Phi}=\boldsymbol{W}-\beta\boldsymbol{\Sigma}$，$\beta$ 为引入的辅助变量。上述转化过程采用了问题式(10)的上镜图形式[15]，得到 $\min_{\boldsymbol{\Delta}_b\in\mathcal{H}}\dfrac{\mathrm{Tr}(\boldsymbol{H}\boldsymbol{W})}{(1+\mathrm{Tr}(\boldsymbol{H}\boldsymbol{\Sigma}))}\ge\beta$，进而得到约束条件式(12d)。可以看到问题式(12b)和式(12d)中包含有无限多的约束条件，无法直接求

解。为此，需要引入下面的引理。

引理 1 对于任一厄密特(Hermit)矩阵 $\boldsymbol{R}$, $\boldsymbol{A}$, $\boldsymbol{C}$, $\boldsymbol{\Delta}\in\mathbb{H}^N$, 并且 $\boldsymbol{C}\succ\boldsymbol{0}$, $\boldsymbol{C}=\widetilde{\boldsymbol{C}}^{\mathrm{H}}\widetilde{\boldsymbol{C}}$, 下面两个优化问题

$$\max_{\boldsymbol{\Delta}}\ \mathrm{Tr}((\boldsymbol{R}+\boldsymbol{\Delta})\boldsymbol{A}),\ \text{s.t.}\ \ \mathrm{Tr}(\boldsymbol{\Delta}\boldsymbol{C}\boldsymbol{\Delta})\le\varepsilon^2,\quad \boldsymbol{R}+\boldsymbol{\Delta}\succeq\boldsymbol{0} \tag{13}$$

与

$$\min_{\boldsymbol{Z}}\ \mathrm{Tr}(\boldsymbol{R}(\boldsymbol{A}+\boldsymbol{Z}))+2\varepsilon\Upsilon(\boldsymbol{A}+\boldsymbol{Z},\boldsymbol{C}),\ \text{s.t.}\ \boldsymbol{Z}\succeq\boldsymbol{0} \tag{14}$$

具有相同的目标值，问题式(14)中，$\Upsilon(\boldsymbol{Z}+\boldsymbol{A},\boldsymbol{C})=||(\boldsymbol{I}\otimes\widetilde{\boldsymbol{C}})(\boldsymbol{I}\otimes\boldsymbol{C}+\boldsymbol{C}^{\mathrm{T}}\otimes\boldsymbol{I})^{-1}\mathrm{vec}(\boldsymbol{Z}+\boldsymbol{A})||$, $\otimes$ 表示矩阵直积(Kronecker 积)运算。

引理 2 对于任一厄密特(Hermit)矩阵 $\boldsymbol{R}$, $\boldsymbol{A}$, $\boldsymbol{C}$, $\boldsymbol{\Delta}\in\mathbb{H}^N$, 并且 $\boldsymbol{C}\succ\boldsymbol{0}$, $\boldsymbol{C}=\widetilde{\boldsymbol{C}}^{\mathrm{H}}\widetilde{\boldsymbol{C}}$, 下面两个优化问题

$$\min_{\boldsymbol{\Delta}}\ \mathrm{Tr}((\boldsymbol{R}+\boldsymbol{\Delta})\boldsymbol{A}),\ \text{s.t.}\ \ \mathrm{Tr}(\boldsymbol{\Delta}\boldsymbol{C}\boldsymbol{\Delta})\le\varepsilon^2,\quad \boldsymbol{R}+\boldsymbol{\Delta}\succeq\boldsymbol{0} \tag{15}$$

与

$$\max_{\boldsymbol{Z}}\ \mathrm{Tr}(\boldsymbol{R}(\boldsymbol{A}-\boldsymbol{Z}))-2\varepsilon\Upsilon(\boldsymbol{Z}-\boldsymbol{A},\boldsymbol{C}),\ \text{s.t.}\ \boldsymbol{Z}\succeq\boldsymbol{0} \tag{16}$$

具有相同的目标值，问题式(16)中，$\Upsilon(\boldsymbol{Z}-\boldsymbol{A},\boldsymbol{C})=||(\boldsymbol{I}\otimes\widetilde{\boldsymbol{C}})(\boldsymbol{I}\otimes\boldsymbol{C}+\boldsymbol{C}^{\mathrm{T}}\otimes\boldsymbol{I})^{-1}\mathrm{vec}(\boldsymbol{Z}-\boldsymbol{A})||$。

引理 1 和引理 2 将具有无限多约束条件的优化问题等价地转化为凸的半定规划问题，为问题式(12)的求解提供了思路。下面将应用这两个引理，对问题式(12)中的约束条件式(12b)和式(12d)进行处理，将其转化为线性约束条件，进而对整个优化问题进行求解。

首先，对约束条件式(12b)进行转化。将式(4b)代入式(12b)，并应用引理 1，则式(12b)中的约束条件可以等价表示为

$$\min_{\boldsymbol{Z}_{e,k}\succeq\boldsymbol{0}}\ \mathrm{Tr}(\widehat{\boldsymbol{G}}(\boldsymbol{\psi}+\boldsymbol{Z}_{e,k}))+2\varepsilon_{e,k}\Upsilon(\boldsymbol{Z}_{e,k}+\boldsymbol{\psi},\boldsymbol{D}_k)\le\alpha,\quad \forall k\in\mathcal{K} \tag{17}$$

显然，如果存在矩阵 $\boldsymbol{Z}_{e,k}\succeq\boldsymbol{0}$，满足

$$\mathrm{Tr}(\widehat{\boldsymbol{G}}(\boldsymbol{\psi}+\boldsymbol{Z}_{e,k}))+2\varepsilon_{e,k}\Upsilon(\boldsymbol{Z}_{e,k}+\boldsymbol{\psi},\boldsymbol{D}_k)\le\alpha,\quad \forall k\in\mathcal{K} \tag{18}$$

则式(12b)与式(17)中的不等式均成立。因此约束条件式(12b)可以等价地替换为式(18)，其中，$\boldsymbol{Z}_{e,k}\succeq\boldsymbol{0}$。

其次，对约束条件式(12d)进行转化。将式(4a)代入式(12d)，并应用引理 2，则式(12d)中的约束条件可以等价地表示为

$$\max_{\boldsymbol{Z}_b\succeq\boldsymbol{0}}\ \mathrm{Tr}(\widehat{\boldsymbol{H}}(\boldsymbol{\Phi}-\boldsymbol{Z}_b))-2\varepsilon_b\Upsilon(\boldsymbol{Z}_b-\boldsymbol{\Phi},\boldsymbol{C})\ge\beta \tag{19}$$

显然，如果存在矩阵 $\boldsymbol{Z}_b\succeq\boldsymbol{0}$，满足

$$\mathrm{Tr}(\widehat{\boldsymbol{H}}(\boldsymbol{\Phi}-\boldsymbol{Z}_b))-2\varepsilon_b\Upsilon(\boldsymbol{Z}_b-\boldsymbol{\Phi},\boldsymbol{C})\ge\beta \tag{20}$$

则式(12d)与式(19)中的不等式均成立。因此，约束条件式(12d)可以等价地替换为式(20)，其中，$\boldsymbol{Z}_b\succeq\boldsymbol{0}$。

根据以上处理结果，用式(18)和式(20)分别代替式(12b)和式(12d)，优化问题式(12)可等价地表述为

$$\phi(\alpha)=\max_{\boldsymbol{W},\boldsymbol{\Sigma}}\ \beta \tag{21a}$$

$$\text{s.t.}\ \ \mathrm{Tr}(\widehat{\boldsymbol{G}}(\boldsymbol{\psi}+\boldsymbol{Z}_{e,k}))+2\varepsilon_{e,k}\Upsilon(\boldsymbol{Z}_{e,k}+\boldsymbol{\psi},\boldsymbol{D}_k)\le\alpha,\quad \forall k\in\mathcal{K} \tag{21b}$$

$$\mathrm{Tr}(\boldsymbol{W})+\mathrm{Tr}(\boldsymbol{\Sigma})\le P \tag{21c}$$

$$\mathrm{Tr}(\widehat{\boldsymbol{H}}(\boldsymbol{\Phi}-\boldsymbol{Z}_b))-2\varepsilon_b\Upsilon(\boldsymbol{Z}_b-\boldsymbol{\Phi},\boldsymbol{C})\ge\beta \tag{21d}$$

$$\boldsymbol{W}\succeq\boldsymbol{0},\quad \boldsymbol{\Sigma}\succeq\boldsymbol{0} \tag{21e}$$

问题式(21a)和式(21b)中的 α 是给定的，然而由于变量 β 的存在，约束式(21d)仍然是非凸的。通过观察，我们发现，如果 β 确定，则问题式(21a)为一个凸的半定规划问题。因此，可以采用二分法对其进行有效求解[15]。

3.3 求解算法描述

可以看到，外层单变量优化问题式(9)的变量的区间长度小于 1，因此存在许多无需求导的 1 维优化方法[16,17]用于搜索问题式(9)的最优解。例如，均匀采样法(uniform sampling)可以在计算精度与计算复杂度之间进行折中处理，而复杂度较低的黄金分割法(golden-section search)至少可以保证一个局部最优解。在进行 1 维搜索的过程中，需要对内层优化问题，即问题式(21)，进行求解。可利用现有的优化工具包，如 CVX[18]，采用二分法求解问题式(21)。本文采用黄金分割法对双层优化问题进行求解，整个算法的描述见表 1。

如果得到的最优解 $(\boldsymbol{W}^*,\boldsymbol{\Sigma}^*)$ 满足 $\mathrm{Rank}(\boldsymbol{W}^*)=1$，则 $\boldsymbol{W}^*$ 的主特征向量作为波束成形向量。如果 $\mathrm{Rank}(\boldsymbol{W}^*)\ge2$，可以采用高斯随机化的方法获得次优的波束成形向量[14,19]。非常有趣的是，在仿真中我们发现，所有信道实现所获得的最优解 $(\boldsymbol{W}^*,\boldsymbol{\Sigma}^*)$ 均满足 $\mathrm{Rank}(\boldsymbol{W}^*)=1$ 的条件。

4 仿真分析

4.1 仿真参数设置

所有的仿真中，设置 $N=4$。合法信道的估计协方差为 $\widehat{\boldsymbol{H}}=\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}$，其中，$\hat{\boldsymbol{h}}$ 随机生成，并服从瑞利衰落，即，$\hat{\boldsymbol{h}}\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{I})$；类似地，窃听信道的估计协方差为 $\widehat{\boldsymbol{G}}_k=\hat{\boldsymbol{g}}_k\hat{\boldsymbol{g}}_k^{\mathrm{H}}$, $\hat{\boldsymbol{g}}_k\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{I})$。不失一般性，考虑 $\boldsymbol{C}=\boldsymbol{I}$, $\boldsymbol{D}_k=\boldsymbol{I}$, $\forall k$，也就是简单的范数界情况。令 $\alpha_b=\varepsilon_b/||\widehat{\boldsymbol{H}}||_F$ 和 $\alpha_e=\varepsilon_{e,k}/||\widehat{\boldsymbol{G}}_k||_F$, $\forall k\in\mathcal{K}$，分别表示合法信道与窃听信道的误差比。该值越大，表示对应信道质量越差。所得的最终数据是对 1000 次独立信道实现所得结果的平均。仿真中，

表 1 双层优化问题的求解算法

初始化：	$a=\tau_{\min}=(1+P\mathrm{Tr}(\hat{\boldsymbol{H}}))^{-1}, b=\tau_{\max}=1$，最优目标值求解精度 ξ。
步骤 1	$l=a+0.382(b-a), u=a+0.618(b-a)$，对优化问题式(21)进行求解，得到 $\phi_l=\phi(1/l-1)$，$\phi_u=\phi(1/u-1)$，用 ϕ_l 和 ϕ_u 代替 $\varphi(\tau)$，计算问题式(9)的目标函数值，分别得到 $R(l)$ 和 $R(u)$；
步骤 2	**while** $(b-a)>\xi$
步骤 3	**if** ($R(l)<R(u)$) $a=l, l=u, \phi_l=\phi_u, u=a+0.618(b-a)$，对优化问题式(21)进行求解，得到 $\phi_u=\phi(1/u-1)$，用 ϕ_u 代替 $\varphi(\tau)$，计算问题式(9)的目标函数值，得到 $R(u)$；
步骤 4	**else**
步骤 5	$b=u, u=l, \phi_u=\phi_l, l=a+0.382(b-a)$，对优化问题式(21)进行求解，得到 $\phi_l=\phi(1/l-1)$，用 ϕ_l 代替 $\varphi(\tau)$，计算问题式(9)的目标函数值，得到 $R(l)$；
步骤 6	**end if**
步骤 7	**end while**
步骤 8	$\tau=(a+b)/2$，将 $\alpha=(1/\tau-1)$ 代入问题式(21)，求得最优目标值 $\phi(\alpha)$ 和最优解 $(\boldsymbol{W}^*,\boldsymbol{\Sigma}^*)$，用 $\phi(\alpha)$ 代替 $\varphi(\tau)$，计算问题式(9)的目标函数值 R_s^*；
输出：	局部最优解 $(\boldsymbol{W}^*,\boldsymbol{\Sigma}^*)$，最优目标值 R_s^*。

非鲁棒方法是指将带有估计误差的 CSI 看作为理想的 CSI，进行安全速率最大化设计。理想信道条件和非鲁棒方法的安全性能求解参考文献[7]。

4.2 性能分析

4.2.1 单个窃听者情况的安全性能对比　首先验证单个窃听者($K=1$)的情况，将本文所提的安全发送方法与文献[13]设计的方法进行对比。图 2(a)给出了 $\alpha_b=0.02$ 和 $\alpha_e=0.05$，不同发送功率时系统的 WCSR。图 2(a)中，随着发送功率的增加，参考方法的 WCSR 趋于恒定。说明在发送者天线个数给定时，单纯地增大发送功率并不能有效提升系统的安全性能。本文所提的鲁棒的人工噪声辅助发送方法获得的安全速率随着发送功率的增加而逐渐增加，且安全性能明显优于参考方法及非鲁棒性方法。这是因为所提的发送方法中，引入的人工噪声可以有区别地对窃听者进行干扰。尽管非鲁棒方法采用了人工噪声，但发送者 Alice 将存在误差的估计信道当作是理想信道，在优化设计过程中没有考虑信道的误差问题，所以其安全性能相对较差。此外，可以看到理想 CSI 条件下，两种方法的安全性能是一样的，也就是说，在理想信道条件下，Alice 的最优发送策略是将所有的功率均用于发送信号，并不采用人工噪声。验证了文献[20]的结论：理想信道条件下，单个窃听者时，不采用人工噪声就可以达到系统的安全容量。

图 2(b)给出了 $\alpha_b=0.01$, Alice 的最大发送功率 $P=20$ dB 时，系统安全速率与窃听信道误差比 α_e 的关系。随着 α_e 的增加，系统的 WCSR 逐渐降低。相对于理想 CSI 条件下的安全性能，本文所提鲁棒方法的安全性能损耗明显小于参考方法和非鲁棒方法。而且可以看到，窃听信道误差比 α_e 越大，所提方法的优越性更加明显。在 $\alpha_e=0.01$ 时，所提方法优于其它方法大概 0.2 bit/(s·Hz)；而在 $\alpha_e=0.1$ 时，所提方法的 WCSR 要比参考方法和非鲁棒方法的安全性能分别高出约 3.4 bit/(s·Hz) 和 1.4 bit/(s·Hz)。

4.2.2 多个窃听者情况的安全性能验证　文献[13]的参考方法不适用于多个窃听者的情况。这里单独对本文方法在多窃听者情况下的安全性能进行评估。图 3(a)给出了不同窃听者数目时，系统的 WCSR 变化情况，其中，Alice 的最大发送功率 $P=20$ dB。可以看到，系统安全速率随着窃听者数目的增加而降低。由于考虑了信道误差，鲁棒方法的安全性能损耗(相对于理想 CSI 条件)要比非鲁棒方法少，即安全性能更优。同时，可以看到信道误差比越大，系统的安全速率越低。

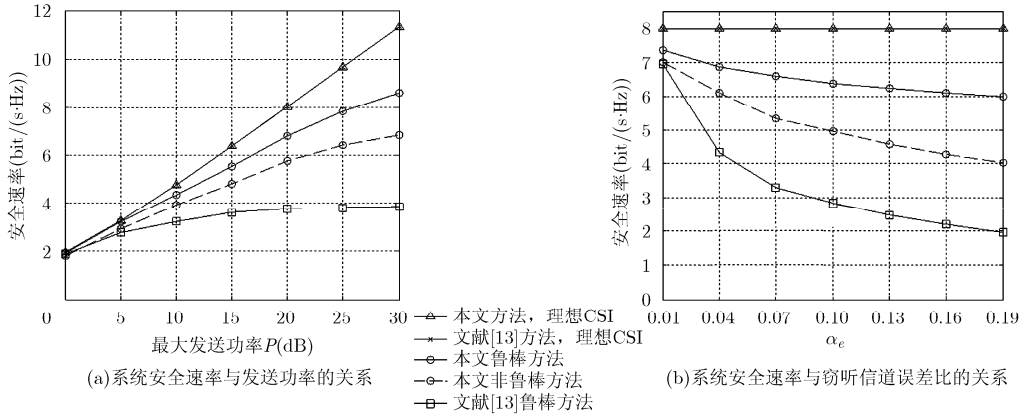
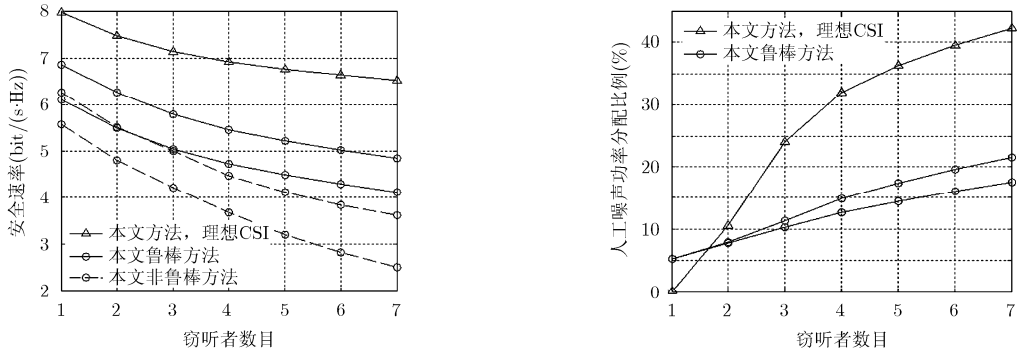


图 2 系统安全速率与发送功率和窃听信道误差比的关系



(a)系统安全速率与窃听者数目的关系　　(b)窃听者数目变化时人工噪声分配比例

图 3 窃听者数目变化时性能比较

图 3(b)给出了窃听者数目变化时，人工噪声功率的分配比例情况。其中，最大发送功率 P=20 dB。图 3(b)表明多个窃听者($K \geq 2$)时，窃听者数目越多，分配给人工噪声的功率越多。用于降低窃听信道质量，提高系统安全速率。当信道误差比越大时，所分配的人工噪声功率越小。这说明在信道质量越差时，应将更多的功率分配给有用信号，用于提高合法信道容量，保证合法用户的安全可靠接收。

5 结束语

本文考虑了 MISO 通信系统中存在多个单天线窃听者的场景。针对发送者获得的基于协方差的信道状态信息不理想，造成安全性能恶化的问题，以最大化系统 WCSR 为目标，提出了一种鲁棒的人工噪声辅助的安全发送方法。 通过半定松弛技术及 Lagrange 对偶理论，将非凸优化问题转化为一个单位区间内的 1 维搜索问题。通过对一系列的 SDP 问题进行求解，完成整个 1 维搜索过程。仿真结果和性能分析验证了所提安全发送方法的鲁棒性和有效性。

参 考 文 献

[1] Wyner A D. The wire-tap channel[J]. *Bell System Technical Journal*, 1975, 54(8): 1355–1387.

[2] 赵家杰, 彭建华, 黄开枝, 等. 基于人工噪声的多用户 MIMO 系统加密算法[J]. 电子与信息学报, 2012, 34(8): 1939–1943.
Zhao Jia-jie, Peng Jian-hua, Huang Kai-zhi, *et al.*. A multi-user MIMO system encryption algorithm based on artificial noise[J]. *Journal of Electronics & Information Technology*, 2012, 34(8): 1939–1943.

[3] Lin S C and Lin P H. On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(2): 414–419.

[4] Lin P H, Lai S H, Lin S C, *et al.*. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1728–1740.

[5] Li Q, Ma W K, and So A M C. A safe approximation approach to secrecy outage design for MIMO wiretap channels[J]. *IEEE Signal Processing Letters*, 2014, 21(1): 118–121.

[6] Li J Y and Petropulu A P. Explicit solution of worst-case secrecy rate for MISO wiretap channels with spherical uncertainty[J]. *IEEE Transactions on Signal Processing*, 2012, 60(7): 3892–3895.

[7] Li Q and Ma W K. Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization[J]. *IEEE Transactions on Signal Processing*, 2013, 61(10): 2704–2717.

[8] Tang Y Q, Xiong J, Ma D T, *et al.*. Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty[J]. *IEEE Communications Letters*, 2013, 17(11): 2096–2099.

[9] 陈涛, 余华, 韦岗. 认知无线电网络的物理层安全研究及其鲁棒性设计[J]. 电子与信息学报, 2012, 34(4): 770–775.
Chen Tao, Yu Hua, and Wei Gang. Study on the physical layer security of cognitive radio networks and its robustness design[J]. *Journal of Electronics & Information Technology*, 2012, 34(4): 770–775.

[10] Wajid I, Pesavento M, Eldar Y C, *et al.*. Robust downlink beamforming with partial channel state information for conventional and cognitive radio networks[J]. *IEEE Transactions on Signal Processing*, 2013, 61(14): 3656–3670.

[11] Wajid I, Pesavento M, Eldar Y C, *et al.*. Robust downlink beamforming for cognitive radio networks[C]. IEEE Global Communications Conference (GLOBECOM), Miami, FL, USA, 2010: 1–5.

[12] Zheng G, Wong K K, and Ottersten B E. Robust cognitive beamforming with bounded channel uncertainties[J]. *IEEE Transactions on Signal Processing*, 2009, 57(12): 4871–4881.

[13] Zhang J W and Gursoy M C. Relay beamforming strategies

for physical-layer security[C]. The 44th Annual Conference on Information Sciences and Systems, Princeton, New Jersey, USA, 2010: 1–6.

[14] Luo Z Q, Ma W K, So A C, *et al*.. Semidefinite relaxation of quadratic optimization problems[J]. *IEEE Signal Processing Magazine*, 2010, 27(3): 20–34.

[15] Boyd S and Vandenberghe L. Convex Optimization[M]. Cambridge, UK New York: Cambridge University Press, 2004, Ch.4.

[16] Li Q and Ma W K. Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming[J]. *IEEE Transactions on Signal Processing*, 2011, 59(8): 3799–3812.

[17] Kolda T, Lewis R, and Torczon V. Optimization by direct search: new perspectives on some classical and modern methods[J]. *SIAM Review*, 2003, 45(3): 385–482.

[18] Boyd S P and Grant M C. CVX: Matlab software for disciplined convex programming, version 2.0. [OL]. http://cvxr.com/cvx, 2012.

[19] Liao W C, Chang T H, Ma W K, *et al*.. QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach[J]. *IEEE Transactions on Signal Processing*, 2011, 59(3): 1202–1216.

[20] Xiong Q, Gong Y, and Liang Y C. Achieving secrecy capacity of miso fading wiretap channels with artificial noise[C]. IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 2013: 2452–2456.

张立健：　男，1980 年生，博士生，研究方向为无线物理层安全.

金　梁：　男，1969 年生，教授，博士生导师，主要研究方向为移动通信技术、阵列信号处理、无线物理层安全等.

刘　璐：　男，1988 年生，博士生，研究方向为无线物理层安全.