非理想信道状态下多波束卫星通信的鲁棒安全传输设计

王 舒* 达新宇
(空军工程大学信息与导航学院 西安 710077)

摘 要：考虑多波束卫星通信中存在多天线窃听用户的场景以及非理想信道状态信息带来的系统安全性能恶化，针对合法信道与窃听信道均不理想的多用户 MISOME(Multi Input, Single Output, Multi Eavesdropper)系统，该文基于两种类型的信道误差提出了两种鲁棒安全传输方法。在确定误差模型下，利用发送波束成形以及人工噪声协方差的联合优化设计解决系统最差情况安全速率最大化问题(Worst-Case Secrecy Rate Maximization, WC-SRM)问题，通过推导分析将非凸的 WC-SRM 问题等价为一个 1 维搜索问题，而这个等价问题的最优解可通过一系列半定规划(SemiDefinite Program, SDP)问题的求解而得到。在统计误差模型下，为求解中断概率约束安全速率最大化(Outage Probability Constrained Secrecy Rate Maximization, OP-SRM)问题，该文提出一种基于 WC-SRM 的鲁棒安全设计的可靠近似方案。仿真分析验证了该文所提方法的鲁棒性与有效性。

关键词：多波束卫星通信系统；物理层安全；安全速率；鲁棒性
中图分类号：TN927 **文献标识码**：A **文章编号**：1009-5896(2017)02-0342-09
DOI: 10.11999/JEIT160429

Robust Secure Transmit Methods for Multibeam Satellite Communication with Imperfect Channel State Information

WANG Shu DA Xinyu
(*College of Information and Navigation, Air Force Engineering University, Xi'an* 710077, *China*)

Abstract: Considering a general eavesdropping case where the eavesdropper is equipped with multiple antennas and two uncertainty models for the imperfect Channel State Information (CSI) on the main and eavesdropper's channels at the transmitter. Two robust transmission methods are proposed for multiuser Multiple-In, Single-Out, Multiple-antenna Eavesdropper (MISOME) systems to provide SINR guarantee for the legitimate user by the optimization of beamforming and artificial noise covariance matrix. For the deterministic uncertainty model, the Worst-Case Secrecy Rate Maximization (WC-SRM) problem is derived an equivalent problem of the WC-SRM problem through analysis. The equivalent problem can be recast as a single-variable optimization problem, which can be handled by solving a sequence of convex SemiDefinite Programs (SDPs). For the stochastic uncertainty model, a suboptimal scheme to solve the Outage Probability constrained Secrecy Rate Maximization (OP-SRM) problem is proposed based on the robust design for the WC-SRM problem. Finally, the effectiveness and the robustness of the proposed algorithms are validated by the simulation results.

Key words: Multibeam satellite communication; Physical layer security; Secrecy rate; Robustness

1 引言

卫星通信信号由于其广播特性极易被第三方用户窃听，因此卫星通信的安全性与保密性受到了广泛关注。目前卫星通信网络的安全主要依赖传输上层的安全协议来保障，如验证、鉴权和记账(AAA)协议、IP 安全(IPSEC)协议以及互联网安全关联与密钥管理协议(ISAKMP)等。但这些协议的安全是通过设计复杂的加解密算法来实现，一旦密钥泄露或被破解，卫星通信的安全则无法保障。利用无线信道的随机性、互易性、差异性的物理层安全技术成为了近年来的研究热点[1,2]。Wyner[3]首先从信息论的角度描述信道的可加密程度，引入保密容量的概念并用来衡量系统的保密性能。文献[4]指出，在高斯广播信道下，当主信道容量大于窃听信道容量时，即保密容量大于零时，认为系统是绝对安全的。然而实际中，窃听者的信道状态一般未知，无法保证其信道容量低于合法用户。为解决这一问题，文

收稿日期：2016-04-29；改回日期：2016-09-23；网络出版：2016-11-16
*通信作者：王舒 xss_wang@163.com
基金项目：国家自然科学基金(61271250, 61571460)
Foundation Items: The National Natural Science Foundation of China (61271250, 61571460)

献[5]提出一种人工噪声辅助方法来保障系统的保密性。受文献[5]的启发，这种人工噪声辅助方法被广泛应用于 MISO[6]以及 MIMO[7]系统，通过合理分配有用信号功率与人工噪声功率以达到期望的保密容量。但是上述研究均假设为理想信道状态条件，在实际中这是不太可能的。假设仅窃听信道非理想状态下，文献[8]通过信号与噪声协方差的联合优化，研究了 MISO 信道多天线窃听者场景中的鲁棒性安全速率最大化问题。文献[9]又将其扩展到合法信道和窃听信道均为非理想情况下鲁棒性最优波束成形设计。目前国内外有关卫星通信物理层安全的文献较少。文献[10]首先将物理层安全技术引入了多波束卫星通信中，假设仅窃听信道非理想情况下，研究了多用户 MISOSE(Multiple-Input Single-Output Single-antenna Eavesdropper)窃听模型中保密速率最大化问题，提出了次优的完全迫零波束成形法。文献[11]考虑了一种更广泛的窃听模型，即存在多个窃听用户的多用户 MISOSE 模型，在已知部分窃听信道状态信息情况下，引入人工噪声联合设计信号与人工噪声功率，提出了最优的人工噪声辅助的发送方法。然而，文献[11]的方法存在以下问题：(1)在信道的建模中，仅考虑理想的信道状态信息(Channel State Information, CSI)，没有考虑信道状态信息误差可能带来的影响；(2)仅适用于单天线窃听者的情况，没有考虑到多个窃听者协作可构成一个虚拟多天线的窃听者这一不利因素。而文献[8,9]虽然考虑了非理想信道的情况，却只适用于单用户场景，并不能直接应用于多用户多波束卫星通信。

针对上述不足，本文在多用户 MISOME (Multiple-Input Single-Output Multiple-antenna Eavesdropper)系统中同时考虑合法CSI误差以及窃听 CSI 误差分别针对确定误差信道模型以及统计误差信道模型，提出了两种鲁棒的安全传输方法。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，分别最大化系统最差情况安全速率(Worst-Case Secrecy Rate, WC-SR)与中断概率约束安全速率 (Outage Probability Constrained Secrecy Rate, OPC-SR)。在非理想 CSI 条件下，由于 WC-SR 问题是非凸的，通过分析推导出与其等价的 1 维搜索问题，这一等价问题的最优解最终可通过一系列的半定规划问题的求解得到。而 OPC-SR 问题的求解通过推导分析可以转化为 WC-SR 问题的可靠近似，其求解过程可参考 WC-SR 问题。

2　系统模型与问题描述

考虑一个多波束卫星通信系统的下行链路，包括一个有 N_t 个发送天线的发送端(Alice), K 个单天线合法用户(Bob)和一个有 Ne 个接收天线的窃听用户(Eve)。系统共有 K 个波束分别为地面 K 个合法用户服务，采用时分复用(Time Division Multiplexing, TDM)和全频复用，每个波束内的用户间无干扰，不同波束之间产生不同程度的多用户干扰。为了能采用人工噪声对窃听用户加扰，下文中假设 $N_t > K$ 。

2.1 信道模型

假设卫星工作频率为 Ka 波段，卫星信号在空中传播时会受到大气内各种物理介质影响，从而引起较大的信号衰减，其中降雨衰减影响最为严重[12]。定义雨衰系数矩阵为 $\boldsymbol{\Lambda} = \mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_K)$，其中 α_k 表示为

$$\alpha_k = \beta_k^{-1/2} \mathrm{e}^{-\mathrm{j}\varphi_k} \tag{1}$$

其中，β_k 为雨衰因子，φ_k 为均匀分布在 $(0, 2\pi]$ 区间内的相位。

波束增益矩阵 $\boldsymbol{G}$ 中的元素可表示为

$$g_{ij}(\theta_{ij}) = G_{\max}\left(\frac{J_1(u)}{2u} + 36\frac{J_3(u)}{u^3}\right)^2 \tag{2}$$

其中 $u = 2.07123\sin\theta_{ij} / \sin\theta_{3\,\mathrm{dB}}$，$G_{\max}$ 表示为最大的天线增益，θ_{ij} 表示为波束中心与接收点之间的夹角，$\theta_{3\,\mathrm{dB}}$ 为 3 dB 功率损耗对应的角度，J_1 与 J_3 分别为第 1 类一阶和三阶贝塞尔函数。于是，信道矩阵可以表示为

$$\boldsymbol{H} = \boldsymbol{\Lambda G} \tag{3}$$

2.2 人工噪声加扰的信号模型

定义 s_k 为 Alice 发送给第 k 个 Bob 的保密信息符号，且有 $\mathbb{E}\{s_k\}=0$，$\mathbb{E}\{|s_k|^2\}=1$，在发送前，所有符号都需要乘以波束成形向量 $\boldsymbol{w}_k \in \mathbb{C}^{N_t \times 1}$，在发送保密信息的同时，为干扰 Eve 的接收，Alice 还发送人工噪声向量 $\boldsymbol{s}' \in \mathbb{C}^{N_t \times (N_t - K)}$，且 $\boldsymbol{s}' \sim \mathcal{CN}(0, \boldsymbol{\Sigma})$，其中 $\boldsymbol{\Sigma} \succeq \boldsymbol{0}$ 为人工噪声协方差。于是，总发送信号 $\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$ 表示为

$$\boldsymbol{x} = \sum_{k=1}^{K} \boldsymbol{w}_k s_k + \boldsymbol{s}' \tag{4}$$

令 $\boldsymbol{h}_k \in \mathbb{C}^{N_t \times 1}$ 为 Alice 到第 k 个 Bob 的信道向量；$\boldsymbol{g} \in \mathbb{C}^{N_t \times N_e}$ 为 Alice 到 Eve 的信道向量，$\forall k \in \kappa$，$\kappa \triangleq \{1, 2, \cdots, K\}$。假设所有的信道相互独立，并服从瑞利平坦衰落。第 k 个 Bob 和 Eve 的接收信号分别表示为

$$\boldsymbol{y}_k = \boldsymbol{h}_k^{\mathrm{H}} \boldsymbol{w}_k s_k + \sum_{j=1, j\neq k}^{K} \boldsymbol{h}_j^{\mathrm{H}} \boldsymbol{w}_j s_j + \boldsymbol{h}_k^{\mathrm{H}} \boldsymbol{s}' + \boldsymbol{n}_k \tag{5}$$

$$\boldsymbol{y}_e = \boldsymbol{g}^{\mathrm{H}}\sum_{k=1}^{K}\boldsymbol{w}_k s_k + \boldsymbol{g}^{\mathrm{H}}\boldsymbol{s}' + \boldsymbol{n}_e \tag{6}$$

式中，$\boldsymbol{n}_k$ and $\boldsymbol{n}_e$ 分别为第 k 个 Bob 和 Eve 处的加性高斯噪声(AWGN)，且服从零均值单位方差的复高斯分布，即 $\boldsymbol{n}_k \sim \mathcal{CN}(0,1)$ 和 $\boldsymbol{n}_e \sim \mathcal{CN}(0,\boldsymbol{I})$。

2.3 问题描述

根据上述信号模型，用户 k 可以获得的安全速率为

$$R_s = \min_{k\in\kappa}\{R_{b,k} - R_e\}^{+} \tag{7}$$

其中，$R_{b,k}$ 和 R_e 分别为第 k 个 Bob 和 Eve 的互信息[13]。

$$R_{b,k} = \log_2\left(1 + \frac{\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{w}_k\boldsymbol{h}_k}{\sum\limits_{j=1,j\neq k}^{K}\boldsymbol{h}_j^{\mathrm{H}}\boldsymbol{w}_j^{\mathrm{H}}\boldsymbol{w}_j\boldsymbol{h}_j + \mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right) + 1}\right) \tag{8}$$

$$R_e = \log_2\det\left(\boldsymbol{I} + \frac{\boldsymbol{g}\boldsymbol{w}_k\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{g}^{\mathrm{H}}}{\sum\limits_{j=1,j\neq k}^{K}\boldsymbol{g}\boldsymbol{w}_j\boldsymbol{w}_j^{\mathrm{H}}\boldsymbol{g}^{\mathrm{H}} + \mathrm{Tr}\left(\boldsymbol{g}\boldsymbol{\Sigma}\boldsymbol{g}^{\mathrm{H}}\right) + \boldsymbol{I}}\right) \tag{9}$$

在卫星总发送功率受限时，通过联合设计波束成形向量 $\boldsymbol{W}_k$ 和人工噪声协方差 $\boldsymbol{\Sigma}$，第 k 个 Bob 的保密速率最大化问题可以描述为

$$\left.\begin{aligned}&\max_{\boldsymbol{w},\boldsymbol{\Sigma}} \quad R_s\\ &\text{s.t.} \quad \sum_{k=1}^{K}\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{w}_k + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P,\ \ \boldsymbol{\Sigma}\succeq\boldsymbol{0}\end{aligned}\right\} \tag{10}$$

式中，P 为 Alice 的最大发送功率。在 Alice 已知理想合法信道以及窃听信道的条件下，该问题为非凸的，其求解方法可以参考文献[11]。但由于量化误差、反馈延迟、多普勒频移等影响，Alice 不可能获得完整的信道状态信息，因此建立非理想的信道状态信息的模型，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问题是非常必要的。

3 非理想信道状态下鲁棒的安全传输方法

本节中，根据文献[14]，当地球站的位置已知时，即已知下行链路的信道特征，这样其信道雨衰系数矩阵就可以估计得到。因此当 Alice 已知所有 Bob 和 Eve 的位置时，由式(3)可分别估计出合法信道 $\tilde{\boldsymbol{h}}_k$ 与窃听信道 $\tilde{\boldsymbol{g}}$，考虑存在信道估计误差时，将合法信道与窃听信道分别表示为

$$\boldsymbol{h}_k = \tilde{\boldsymbol{h}}_k + \Delta\boldsymbol{h}_k,\ \boldsymbol{g} = \tilde{\boldsymbol{g}} + \Delta\boldsymbol{g} \tag{11}$$

其中，$\Delta\boldsymbol{h}_k$ 与 $\Delta\boldsymbol{g}$ 分别为合法信道与窃听信道相应的估计误差，一般来讲，信道误差模型可以分为两类：确定误差模型和统计误差模型。在确定误差模型中，误差在确定的范围内，即 $\|\Delta\boldsymbol{h}_k\| \le \varepsilon_{h,k}$，$\|\Delta\boldsymbol{g}\| \le \varepsilon_g$ 这种模型广泛存在于CSI在接收端量化后反馈给发送端的通信系统[15]。在统计误差模型中，误差都为零均值方差分别为 $\sigma_{b,k}^2$ 和 σ_e^2 的高斯分布变量，即 $\Delta\boldsymbol{h}_k \sim \mathcal{CN}(0,\sigma_{b,k}^2\boldsymbol{I})$，$\Delta\boldsymbol{g} \sim \mathcal{CN}(0,\sigma_e^2\boldsymbol{I})$ 这种模型用于研究非理想 CSI 如信道估计误差，反馈延迟等影响。一般来说，$\sigma_{b,k}^2$ 和 σ_e^2 的值不同。

3.1 基于确定误差信道模型下的鲁棒安全传输方法

在确定信道误差模型下，定义误差范围集合为 $\mathcal{A} \triangleq \{\boldsymbol{h}_k \mid \boldsymbol{h}_k = \tilde{\boldsymbol{h}}_k + \Delta\boldsymbol{h}_k, \|\Delta\boldsymbol{h}_k\| \le \varepsilon_{h,k}\}, \forall k \in \kappa$，$\mathcal{B} \triangleq \{\boldsymbol{g} \mid \boldsymbol{g} = \tilde{\boldsymbol{g}} + \Delta\boldsymbol{g}, \|\Delta\boldsymbol{g}\| \le \varepsilon_e\}$，定义变量 $\boldsymbol{T}_k \triangleq \boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{w}_k$，可见存在非凸的约束条件 $\mathrm{Rank}(\boldsymbol{W}_k) = 1$，系统的最差情况鲁棒安全速率最大化(Worst-Case Robust Secrecy Rate Maximization, WCR-SRM)问题可描述为

$$\left.\begin{aligned}&\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma}} \quad \min\{R_{b,k} - R_e\}\\ &\text{s.t.} \quad \sum_{k=1}^{K}\boldsymbol{W}_k + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P\\ &\qquad \mathrm{Rank}(\boldsymbol{W}_k) = 1,\ \ \boldsymbol{\Sigma}\succeq\boldsymbol{0}, \forall k\in\kappa, \boldsymbol{h}_k\in\mathcal{A}, \boldsymbol{g}\in\mathcal{B}\end{aligned}\right\} \tag{12}$$

由于 $\Delta\boldsymbol{h}_k$ 与 $\Delta\boldsymbol{g}$ 相互独立，引入松弛变量 $\boldsymbol{\tau} \triangleq \{\tau_1,\tau_2,\cdots,\tau_K\}$，问题式(12)转化为

$$\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma},\tau_k} \quad \min\log_2\left(1 + \frac{\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{h}_k}{\sum\limits_{j=1,j\neq k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k + \mathrm{Tr}(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k) + 1}\right) - \log_2\frac{1}{\tau_k},\ \ \forall k\in\kappa,\ \boldsymbol{h}_k\in\mathcal{A} \tag{13a}$$

$$\text{s.t.} \quad \max\log_2\det\left(\boldsymbol{I} + \frac{\boldsymbol{g}\boldsymbol{W}_k\boldsymbol{g}^{\mathrm{H}}}{\sum\limits_{j=1,j\neq k}^{K}\boldsymbol{g}\boldsymbol{W}_j\boldsymbol{g}^{\mathrm{H}} + \mathrm{Tr}\left(\boldsymbol{g}\boldsymbol{\Sigma}\boldsymbol{g}^{\mathrm{H}}\right) + \boldsymbol{I}}\right) \le \log_2\frac{1}{\tau_k},\ \ \forall\boldsymbol{g}\in\mathcal{B} \tag{13b}$$

$$\sum_{k=1}^{K}\boldsymbol{W}_k + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P,\ \ \boldsymbol{\Sigma}\succeq\boldsymbol{0} \tag{13c}$$

$$\mathrm{Rank}(\boldsymbol{W}_k) = 1 \tag{13d}$$

上述问题式(13)是非凸的，首先，将目标函数化简，定义变量 $\boldsymbol{W} \triangleq \sum_{k=1}^{K}\boldsymbol{W}_k$，由于对数函数是递增的，因此去掉对数函数 $\log_2(\cdot)$ 后

$$\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma},\tau_k} \quad \min\frac{\tau_k\left[\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_k + \mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right) + 1\right]}{\sum\limits_{j=1,j\neq k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k + \mathrm{Tr}(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k) + 1},\quad \forall k\in\kappa,\ \boldsymbol{h}_k\in\mathcal{A} \tag{14}$$

而由于问题式(13)其中的约束条件式(13b)是非凸的且难以计算，需对其进行转化，由 $\det(\boldsymbol{I}+\boldsymbol{AB})=\det(\boldsymbol{I}+\boldsymbol{BA})$，得到

$$\log_2\det\left[\boldsymbol{I}+\left(\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{g}\right)+\boldsymbol{I}\right)^{-1}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g}\right]\leq\log_2\frac{1}{\tau_k}\Leftrightarrow\det\left(\boldsymbol{I}+\boldsymbol{V}^{\frac{-1}{2}}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g}\boldsymbol{V}^{\frac{-1}{2}}\right)\leq\frac{1}{\tau_k}\quad(15)$$

式中 $\boldsymbol{V}=\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{Z}\boldsymbol{g})+\eta\boldsymbol{I}$，但此时约束条件式(15)仍然是非凸的，因此，需要引入下面引理：

引理 1[16]　对于任一厄密特(Hermit)矩阵 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in\mathbb{H}^n$，令 $\boldsymbol{A}\geq 0$，当且仅当 $\mathrm{Rank}(\boldsymbol{A})\leq 1$ 时，有

$$\det(\boldsymbol{I}+\boldsymbol{A})\geq 1+\mathrm{Tr}(\boldsymbol{A})\quad(16)$$

将其应用于式(15)，则约束条件式(13b)可转化为一个凸不等式。

$$\log_2\det\left(\boldsymbol{I}+\frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g}}{\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{g}\right)+\boldsymbol{I}}\right)\leq\log_2\frac{1}{\tau_k}\Rightarrow\left(\frac{1}{\tau_k}-1\right)\cdot\left(\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{g}\right)+\boldsymbol{I}\right)\geq\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g}\quad(17)$$

也就是说，式(17)是式(13b)的一个松弛形式，用式(17)代替式(13b)构成 WCR-SRM 问题的可行解更多。而当 $\mathrm{Rank}(\boldsymbol{W}_k)\leq 1$，则上式是等价的。将式(14)和式(17)代入问题式(13)，得到松弛后问题：

$$\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma},\tau_k}\quad\min\frac{\tau_k\left[\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1\right]}{\sum_{j=1,j\neq k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1},\quad\forall k\in\kappa,\boldsymbol{h}_k\in\mathcal{A}$$

$$\text{s.t.}\quad\begin{cases}\max\left(\frac{1}{\tau_k}-1\right)\left(\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{g}\right)+\boldsymbol{I}\right)\\ \quad\geq\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g},\ \forall\boldsymbol{g}\in\mathcal{B}\\ \sum_{k=1}^{K}\boldsymbol{W}_k+\mathrm{Tr}(\boldsymbol{\Sigma})\leq P,\ \boldsymbol{\Sigma}\succeq\boldsymbol{0}\text{和}\mathrm{Rank}(\boldsymbol{W}_k)=1\end{cases}\quad(18)$$

由于存在非凸的约束条件式(13d)，即 $\mathrm{Rank}(\boldsymbol{W}_k)=1$，文献[17]中提到，QCQP 问题秩松弛形式的 Lagrange 对偶问题可以得到和原问题同样的最优值。对于本问题来说，同样采用秩松弛方法，忽略秩为 1 的这个约束条件，得到简化后模型

$$\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma},\tau_k}\quad\alpha$$

$$\text{s.t.}\quad\begin{cases}\dfrac{\tau_k\left[\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1\right]}{\sum_{j=1,j\neq k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1}\geq\alpha,\\ \quad\forall k\in\kappa,\ \boldsymbol{h}_k\in\mathcal{A}\\ \max\left(\frac{1}{\tau_k}-1\right)\left(\sum_{j=1,j\neq k}^{K}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{g}+\mathrm{Tr}\left(\boldsymbol{g}^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{g}\right)+\boldsymbol{I}\right)\\ \quad\geq\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}_k\boldsymbol{g},\ \forall\boldsymbol{g}\in\mathcal{B}\\ \sum_{k=1}^{K}\boldsymbol{W}_k+\mathrm{Tr}(\boldsymbol{\Sigma})\leq P,\ \boldsymbol{\Sigma}\succeq\boldsymbol{0}\end{cases}\quad(19)$$

式中，$\alpha>0$ 为辅助变量，从式(19)可以看出前两个约束条件中都含有一个波动变量，这就相当于有无限个约束条件，其中第 1 个约束条件可引入 S-procedure 定理[18]转化为

$$\begin{bmatrix}\lambda_h\boldsymbol{I}+\boldsymbol{Q} & \boldsymbol{Q}\tilde{\boldsymbol{h}}_k\\ \tilde{\boldsymbol{h}}_k^{\mathrm{H}}\boldsymbol{Q}^{\mathrm{H}} & -\lambda_h\varepsilon_{h,k}^2+\tilde{\boldsymbol{h}}_k^{\mathrm{H}}\boldsymbol{Q}^{\mathrm{H}}\tilde{\boldsymbol{h}}_k+(\tau_k-\alpha)\end{bmatrix}\geq 0\quad(20)$$

其中，$\overline{\boldsymbol{W}}=\sum_{j=1,j\neq k}^{K}\boldsymbol{W}_k$，$\tau_k\boldsymbol{W}-\alpha\overline{\boldsymbol{W}}+(\tau_k-\alpha)\mathrm{Tr}(\boldsymbol{\Sigma})=\boldsymbol{Q}$，而对于第 2 个约束条件，则需要引入引理 2。

引理 2[19]　对于任一厄密特(Hermit)矩阵 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in\mathbb{H}^n$，令 $f(\boldsymbol{X})=\boldsymbol{X}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{X}+\boldsymbol{X}^{\mathrm{H}}\boldsymbol{B}+\boldsymbol{B}^{\mathrm{H}}\boldsymbol{X}+\boldsymbol{C}$ 且 $\boldsymbol{D}\geq 0$，则式(21)是等价的。

$$\left.\begin{aligned}&f(\boldsymbol{X})\geq 0,\forall\boldsymbol{X}\in\left\{\boldsymbol{X}\middle|\mathrm{trace}\left(\boldsymbol{D}\boldsymbol{X}^{\mathrm{H}}\boldsymbol{X}\right)\leq 1\right\}\\ &\Leftrightarrow\begin{bmatrix}\boldsymbol{C} & \boldsymbol{B}^{\mathrm{H}}\\ \boldsymbol{B} & \boldsymbol{A}\end{bmatrix}-t\begin{bmatrix}\boldsymbol{I} & \boldsymbol{0}\\ \boldsymbol{0} & -\boldsymbol{D}\end{bmatrix}\geq 0,\ \text{且}t\geq 0\end{aligned}\right\}\quad(21)$$

利用引理将问题式(19)中的约束条件 3 进行转化，于是约束条件等价表示为

$$\begin{bmatrix}\left(\frac{\eta}{\tau_k}-\eta-t_{\mathrm{g}}\right)\boldsymbol{I}+\tilde{\boldsymbol{g}}^{\mathrm{H}}\left[\left(\frac{1}{\tau_k}-1\right)\left(\overline{\boldsymbol{W}}+\boldsymbol{Z}\right)-\boldsymbol{W}_k\right]\tilde{\boldsymbol{g}} & \tilde{\boldsymbol{g}}^{\mathrm{H}}\left[\left(\frac{1}{\tau_k}-1\right)\left(\overline{\boldsymbol{W}}+\boldsymbol{Z}\right)-\boldsymbol{W}_k\right]\\ \left[\left(\frac{1}{\tau_k}-1\right)\left(\overline{\boldsymbol{W}}+\boldsymbol{Z}\right)-\boldsymbol{W}_k\right]\tilde{\boldsymbol{g}} & \left[\left(\frac{1}{\tau_k}-1\right)\left(\overline{\boldsymbol{W}}+\boldsymbol{Z}\right)-\boldsymbol{W}_k\right]+t_{\mathrm{g}}\varepsilon_e^{-2}\boldsymbol{I}\end{bmatrix}\geq 0\quad(22)$$

最终，用式(20)和式(22)分别替换问题式(19)中的约束条件 1 和约束条件 2，得到表述式：

$$f(\tau_k)=\max_{\boldsymbol{W}_k,\boldsymbol{\Sigma}} \quad \alpha \\ \text{s.t.} \quad \left\{\begin{array}{l}\text{式(20)和式(22)}\\ \text{式(13c)}\end{array}\right\} \tag{23}$$

式(23)的可行解为 $\{\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_K,\boldsymbol{Z},\tau_1,\tau_2,\cdots,\tau_K\}$，但问题式(23)仍然是非凸的，然而，若式(23)中 $\boldsymbol{\tau}$ 为确定值，问题式(19)就是一个半定规划(Semi Definite Programming, SDP)问题，可采用多种方法有效求解。因此将问题式(23)看作 τ_k 的一个函数 $f(\tau_k)$，考虑如何得到最优的 τ_k，从而得到问题式(23)的最优解。由于本文只考虑保密速率为正的情况，根据式(13a)可知 $\tau_k\le 1$，根据问题式(13)中的目标函数以及约束条件 1，得到

$$\begin{aligned}\frac{1}{\tau_k}-1 &\le \min_{\|\Delta\boldsymbol{h}_k\|\le\varepsilon_{h,k}} \frac{\boldsymbol{h}_k T_k \boldsymbol{h}_k^{\mathrm{H}}}{\sum\limits_{j=1,j\ne k}^{K}\boldsymbol{h}_k T_k \boldsymbol{h}_k^{\mathrm{H}}+\mathrm{Tr}(\boldsymbol{h}_k\boldsymbol{\Sigma}\boldsymbol{h}_k^{\mathrm{H}})+1}\\ &\le \frac{\tilde{\boldsymbol{h}}_k T_k \tilde{\boldsymbol{h}}_k^{\mathrm{H}}}{\sum\limits_{j=1,j\ne k}^{K}\tilde{\boldsymbol{h}}_k T_k \tilde{\boldsymbol{h}}_k^{\mathrm{H}}+\mathrm{Tr}\left(\tilde{\boldsymbol{h}}_k\boldsymbol{\Sigma}\tilde{\boldsymbol{h}}_k^{\mathrm{H}}\right)+1}\le P\left\|\tilde{\boldsymbol{h}}_k\right\|^2\end{aligned} \tag{24}$$

其中，最后一步等号在 $T_k=P$，$\boldsymbol{\Sigma}=\boldsymbol{0}$，$\sum_{j=1,j\ne k}^{K}T_j=0$ 时成立，于是有 $1\Big/\left(P\left\|\tilde{\boldsymbol{h}}_k\right\|^2+1\right)\le\tau_k$。有关 τ_k 的优化问题可以描述为

$$\max_{\tau_k} \quad f(\tau_k) \\ \text{s.t.} \quad 1\Big/\left(P\left\|\tilde{\boldsymbol{h}}_k\right\|^2+1\right)\le\tau_k\le 1,\forall k\in\kappa \tag{25}$$

其中，$f(\tau_k)$ 表示为优化问题式(24)在确定的 τ_k 下的最优值。通过求解问题式(24)和式(25)，可以得到 WCR-SRM 问题的最优解，注意到优化问题式(25)是一个单变量的优化问题，可以利用 1 维搜索方法求得 τ_k 的最优值，另外，当 τ_k 为确定值时，可以使用 SeDuMi 或者 CVX 有效求解 SDP 问题式(23)。

3.2 算法描述

容易看出，很多的 1 维搜索方法[16,20]可用于搜索问题式(25)的最优解。本文采用无需求导的黄金分割法进行求解，一方面其计算复杂度较低，另一方面至少可以保证一个局部最优解。同时，在进行 1 维搜索的过程中，本文利用现有的优化工具包 CVX 对优化问题式(23)进行求解。具体来说，优化问题式(23)的最优解可以通过二分法在包含其最优值 α^* 的区间 $[0,\overline{\alpha}]$ 内搜索得到。下面讨论两个比较重要的问题：一个是 $\overline{\alpha}$ 如何选取；另一个是优化问题式(23)的最优解与原优化问题式(25)的最优解的关系。

首先讨论如何选取迭代区间的上限 $\overline{\alpha}$，根据式(19)中第 1 个约束条件可知

$$\begin{aligned}\alpha &\le \frac{\tau_k\left[\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1\right]}{\sum\limits_{j=1,j\ne k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1}\\ &\le \frac{\tau_k\left(\boldsymbol{W}+\mathrm{Tr}(\boldsymbol{\Sigma})\right)\left\|\tilde{\boldsymbol{h}}_k+\Delta\boldsymbol{h}_k\right\|^2}{\sum\limits_{j=1,j\ne k}^{K}\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{W}_j\boldsymbol{h}_k+\mathrm{Tr}\left(\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{\Sigma}\boldsymbol{h}_k\right)+1}\\ &\le \tau_k P\left(\left\|\tilde{\boldsymbol{h}}_k\right\|+\varepsilon_{h,k}\right)^2\end{aligned} \tag{26}$$

因此，$\overline{\alpha}$ 可选为

$$\overline{\alpha}=\arg\min_{k=1,2,\cdots,K}\tau_k P\left(\left\|\tilde{\boldsymbol{h}}_k\right\|+\varepsilon_{h,k}\right)^2 \tag{27}$$

然后讨论优化问题式(23)的最优解与原优化问题式(13)的最优解的关系，采用秩松弛去掉秩 1 约束必将导致优化问题式(13)的可行解空间变大。因此，优化问题式(23)的最优值并不一定为秩 1 的解。如果问题式(23)的最优解 $\boldsymbol{W}_k^*,\forall k\in\kappa$ 的秩均为 1，即满足 $\mathrm{Rank}(\boldsymbol{W}_k^*)=1,\forall k\in\kappa$，也就说明采用秩松弛没有损失原优化问题的最优性，同时保证了式(17)等价于式(13b)，此时最优解可以通过对 $\boldsymbol{W}_k^*,\forall k\in\kappa$ 进行特征值分解，其主特征向量 $\boldsymbol{w}_k^*=\sqrt{\lambda_{\max}(\boldsymbol{W}_k^*)}q_{\max}$ 作为最优波束成形向量。另一方面，如果优化问题式(23)的最优解 $\mathrm{Rank}(\boldsymbol{W}_k^*)$ 不全为 1(即存在大于 1 的解)，则可以利用文献[19]提出的高斯随机化方法来获得优化问题式(23)的近似解。

根据上述分析，优化问题式(13)的最优解，即发送端最优波束成形矢量可以通过表 1 获得。

3.3 基于统计误差信道模型下的鲁棒安全传输方法

上一节的 WCR-SRM 问题是一个在确定信道误差范围内的绝对安全传输设计问题。在本节中，在统计信道误差模型下，信道误差是一个满足一定概率分布的随机的值，即误差范围是不确定的，因此很难对其进行绝对的安全传输设计。然而，可以采用中断概率准则对其进行安全传输设计，系统的中断约束鲁棒安全速率最大化(Outage-Constrained Robust Secrecy Rate Maximization, OCR-SRM)问题可描述为

$$\max_{\boldsymbol{w}_k,\boldsymbol{\Sigma}} \quad R_s \\ \text{s.t.} \quad \Pr_{\{\Delta\boldsymbol{h}_k\}_{k=1}^K,\{\Delta\boldsymbol{g}\}}\{\min_{\forall k\in\kappa}R_{b,k}-R_e\ge R_s\}\ge 1-\lambda \\ \sum_{k=1}^{K}\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{w}_k+\mathrm{Tr}(\boldsymbol{\Sigma})\le P,\ \ \boldsymbol{\Sigma}\succeq\boldsymbol{0} \\ \Delta\boldsymbol{h}_k\sim\mathcal{CN}(0,\sigma_{b,k}^2\boldsymbol{I}),\Delta\boldsymbol{g}\sim\mathcal{CN}(0,\sigma_e^2\boldsymbol{I}) \tag{28}$$

表 1 确定误差模型下鲁棒安全传输算法

初始化参数：$\tilde{\boldsymbol{h}}_k$, $\tilde{\boldsymbol{g}}$, P , $\varepsilon_{h,k}$, ε_g ，最优目标求解精度 ξ , γ ；

步骤 1　计算上下界 $\tau_{\min}=1\Big/\left(P\left\|\tilde{\boldsymbol{h}}_k\right\|^2+1\right)$, $\tau_{\max}=1$, $\overline{\alpha}=\arg\min\limits_{k=1,2,\cdots,K}\tau_k P\left(\left\|\tilde{\boldsymbol{h}}_k\right\|+\varepsilon_{h,k}\right)^2$, 令 $a=\tau_{\min}+0.382(\tau_{\max}-\tau_{\min})$, $b=\tau_{\min}+0.618(\tau_{\max}-\tau_{\min})$ ；

步骤 2　将 a 和 b 分别代入问题式(23)，求解 $f_a=f(a)$ and $f_b=f(b)$ ；

步骤 3　令 $\alpha_{\max}=\overline{\alpha}$, $\alpha_{\min}=0$ ；

步骤 4　令 $\alpha=(\alpha_{\max}+\alpha_{\min})/2$ ，利用 CVX 求解半定规划问题式(23)，如果式(23)可解，则令 $\alpha_{\min}=\alpha$ ，否则令 $\alpha_{\max}=\alpha$ ；

步骤 5　如果 $\alpha_{\max}-\alpha_{\min}<\gamma$ ，则表明二分法已收敛，执行下一步；否则返回步骤 4 继续迭代；

步骤 6　得到 $f_a=f(a)$ and $f_b=f(b)$ ；

步骤 7　如果 $f_a<f_b$ ，令 $\tau_{\min}\Leftarrow a$, $a\Leftarrow b$, $f_a\Leftarrow f_b$, $b\Leftarrow\tau_{\min}+0.618(\tau_{\max}-\tau_{\min})$ ，将 b 代入问题式(23)，重复步骤 3–步骤 5 得到 f_a ；否则令 $\tau_{\max}\Leftarrow b$, $b\Leftarrow a$, $f_b\Leftarrow f_a$, $a\Leftarrow\tau_{\min}+0.382(\tau_{\max}-\tau_{\min})$ ，将 a 代入问题式(23)，重复步骤 3–步骤 5 得到 f_b ；

步骤 8　如果 $(\tau_{\max}-\tau_{\min})>\xi$ ，则表明黄金分割法已收敛，执行下一步；否则返回步骤 7 继续迭代；

步骤 9　令 $\tau_k=(a+b)/2$ ，将其代入式(23)得到 $\phi(\alpha)$ and $\left(\boldsymbol{W}_k^*,\boldsymbol{\Sigma}^*\right)$ ；

步骤 10　如果 $\mathrm{Rank}(\boldsymbol{W}_k^*)=1$ ，则对优化问题式(13)的最优解 $\boldsymbol{W}_k^*$ 进行特征值分解，其主特征向量作为最终波束成形向量；否则，根据已知的 $\boldsymbol{W}_k^*$ 并利用高斯随机化技术获取优化问题式(23)的近似最优解；

输出：最优解 $\boldsymbol{W}_k^*$ 及最优值 R_s^* 。

其中，$0<\lambda<0.5$ 是给定的最大容忍安全中断概率，即安全速率低于 R_s 的概率，问题的目标就是最大化 $\lambda\%$ 的中断概率。由于约束条件 1 的存在使得这个 OCR-SRM 问题很难得到闭合表达式，除了一些特殊情况，例如只有一个单天线 Eve 或者 AN 严格存在于合法信道的零空间内。于是，考虑一种基于 WCR-SRM 问题的近似解，首先，由于不同用户的合法信道相互独立，得到约束条件 1 的等价约束条件

$$\begin{aligned}&\Pr_{\{\Delta\boldsymbol{h}_k\}_{k=1}^K,\{\Delta\boldsymbol{g}\}}\left\{\min_{\forall k\in\kappa}R_{b,k}-R_e\ge R_s\right\}\ge 1-\lambda\\&\Leftrightarrow\prod_{k=1}^K\Pr_{\{\Delta\boldsymbol{h}_k\},\{\Delta\boldsymbol{g}\}}\left\{R_{b,k}-R_e\ge R_s\right\}\ge 1-\lambda\\&\Leftarrow\Pr_{\{\Delta\boldsymbol{h}_k\},\{\Delta\boldsymbol{g}\}}\left\{R_{b,k}-R_e\ge R_s\right\}\ge 1-\overline{\lambda}\end{aligned}\tag{29}$$

其中，$\overline{\lambda}=1-(1-\lambda)^{1/K}$ ，由于误差是高斯分布的，根据文献[21]，其误差范围所在集合定义为

$$\left.\begin{aligned}\Re_h&=\left\{\Delta\boldsymbol{h}_k:\left\|\Delta\boldsymbol{h}_k\right\|\le r_{h,k},\forall k\in\kappa\right\}\\\Re_g&=\left\{\Delta\boldsymbol{g}:\left\|\Delta\boldsymbol{g}\right\|\le r_g\right\}\end{aligned}\right\}\tag{30}$$

其中，$r_{h,k}$ 与 r_g 用来表示误差范围的半径。于是有

$$\left.\begin{aligned}r_{h,k}&=\sqrt{\frac{\sigma_{b,k}^2}{2}\psi^{-1}_{\chi^2_{2N_tN_e}}\left((1-\lambda)^{1/K}\right)}\\r_g&=\sqrt{\frac{\sigma_e^2}{2}\psi^{-1}_{\chi^2_{2N_t}}(1-\lambda)}\end{aligned}\right\}\tag{31}$$

其中，$\psi^{-1}_{\chi^2_{2N_tN_e}}$ 表示自由度为 $2N_tN_e$ 卡方分布的逆累计分布函数，$\psi^{-1}_{\chi^2_{2N_t}}$ 表示自由度为 $2N_t$ 卡方分布的逆累计分布函数，由此得到式(29)的可靠近似：

$$\begin{aligned}&\min_{k\in\kappa}\{R_b-R_e\}\ge R_s,\ \left\|\Delta\boldsymbol{h}_k\right\|\le r_{h,k},\ \ \left\|\Delta\boldsymbol{g}\right\|\le r_g\\&\quad\Rightarrow\Pr_{\{\Delta\boldsymbol{h}_k\},\{\Delta\boldsymbol{g}\}}\{R_b-R_e\}\ge R_s\ge 1-\overline{\lambda}\end{aligned}\tag{32}$$

于是，得到问题式(28)的可靠近似

$$\left.\begin{aligned}\max_{\boldsymbol{w}_k,\boldsymbol{\Sigma}}\quad&R_s\\\text{s.t.}\quad&\min\{R_b-R_e\}\ge R_s,\left\|\Delta\boldsymbol{h}_k\right\|\le r_{h,k},\left\|\Delta\boldsymbol{g}\right\|\le r_g\\&\sum_{k=1}^K\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{w}_k+\mathrm{Tr}(\boldsymbol{\Sigma})\le P,\ \ \boldsymbol{\Sigma}\succeq 0\end{aligned}\right\}\tag{33}$$

也就是说，问题式(33)的可行解同样适用于问题式(27)，同时，观察发现，当 $r_{h,k}=\varepsilon_{h,k}$ ， $r_g=\varepsilon_g$ 时，问题式(33)等价于确定误差模型下的 WCR-SRM 问题式(13)，所以问题式(33)的求解方法可以参照 3.1 节，不再赘述。

4　仿真实验

为了验证本文方法的保密性能，下面通过与文献[11]方法的比较，其主要区别在于本文同时考虑了主信道与非法信道的误差，而文献[11]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。仿真参数设置如下：发送天线 $N_t=5$ ，合法用户数 $K=3$ ，窃听天线 $N_e=3$ 。地球站与卫星仰角为 30°，波束直径 $D=500$ km ，其中合法用户地球站在 $0.15D$ 以内随机分布。在 Ka 频段内，第 k 个合法用户信道估计 $\tilde{\boldsymbol{h}}_k$ 与窃听信道估计 $\tilde{\boldsymbol{g}}$ 均由式(3)计算得到，其中 3 dB 功率损耗角 $\theta_{3\text{ dB}}=0.4°$ ，雨衰因子 $\ln\beta_k(\text{dB})\sim\mathcal{CN}(-3.125,1.591)$ 。定义合法信道与窃听信道误差比分别为 $\alpha_{h,k}=\varepsilon_{h,k}\Big/\left\|\tilde{\boldsymbol{h}}_k\right\|$ ， $\alpha_g=\varepsilon_g\Big/\left\|\tilde{\boldsymbol{g}}\right\|$ ，该值越大说明对应的信道估计偏差越大。

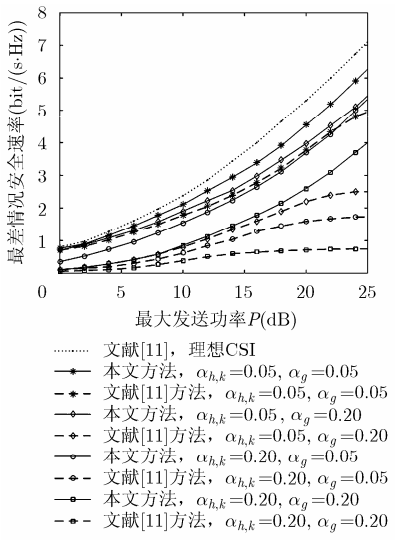
首先，在确定误差模型下比较文献[11]与本文方法的最差情况安全速率。如图 1(a)所示，无论是文献[11]方法还是本文方法，固定 $\alpha_{h,k}$ (或者 α_g)，随着 α_g (或者 $\alpha_{h,k}$)的增大，系统安全速率逐渐降低。但在相同误差比下，本文方法安全速率均高于文献[11]方法，这也验证了本文方法对于合法信道误差和窃听信道误差的鲁棒性，且发送功率越大，越能体现本文方法的有效性。同时观察发现，无论是文献[11]

方法还是本文方法，$\alpha_{h,k}=0.20$,$\alpha_g=0.05$ 时的系统安全速率低于 $\alpha_{h,k}=0.05$ ， $\alpha_g=0.20$ 时的系统安全速率，也就是说合法信道的误差比对于系统安全速率的影响大于窃听信道对于系统安全速率的影响，这是由于式(24)中有关合法信道的约束条件共有 $2K$ 个，而窃听信道的约束条件只有一个。当 $\alpha_{h,k}=0.05$, $\alpha_g=0.05$ ， $P=20$ dBW 时本文方法的系统安全速率优于文献[11]方法 0.7 bit/(s·Hz)，而当 $\alpha_{h,k}=0.20$, $\alpha_g=0.20$ ， $P=20$ dBW 时本文方法则比文献[11]方法高出 2 bit/(s·Hz)，说明信道误差越大本文方法的优越性越明显。图 1(b)中给出了确定误差模型下，发送功率 $P=20$ dBW 时文献[11]方法与本文方法的最差情况安全速率与信道误差比 $\alpha_{h,k}$ 或 α_g 的关系。观察发现，随误差比 $\alpha_{h,k}$ 或 α_g 的增大，本文方法系统 WCSR 都高于文献[11]方法的 WCSR，这也进一步验证了本文方法对于信道误差鲁棒性。同时发现，当 $\alpha_{h,k}$ 或 α_g 大于 0.25 时，本文方法的 WCSR 趋于一个稳定值，而文献[11]方法的 WCSR 仍随误差比的增大不断降低。而窃听信道误差比 $\alpha_g=0$ 时，本文所提方法与文献[11]方法之间安全速率的差距大于窃听信道误差比 $\alpha_{h,k}=0$ 时的差距，这也验证了图 1(a)中合法信道的误差比对于系统安全速率的影响大于窃听信道对于系统安全速率的影响。

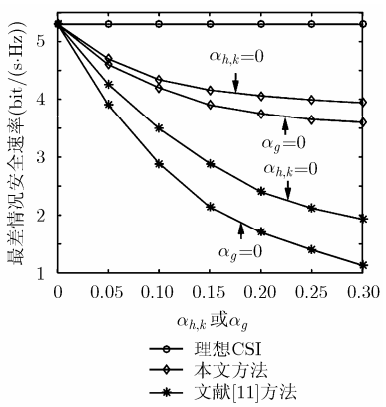
下面分析在统计误差模型下本文所提方法的中断安全速率。图 2(a)为不同中断安全速率与最大发送功率之间的关系，如图所示，系统中断安全速率随着 λ 的增大而增大，随误差变量方差 $\sigma_{b,k}^2$ 或 σ_e^2 的增大而减小，但同时观察发现，误差变量方差 $\sigma_{b,k}^2$ 或 σ_e^2 变化对系统安全速率的影响大于 λ 的变化的影响，这与计算误差半径的式(30)有直接关系。当 $\sigma_{b,k}^2=0.05$, $\sigma_e^2=0.01$ 时的系统安全速率低于 $\sigma_{b,k}^2=0.01$, $\sigma_e^2=0.05$ 时的系统安全速率，也就是说合法信道的误差比对于系统安全速率的影响大于窃听信道对于系统安全速率的影响，这是由于中断安全速率的计算为最差情况安全速率的近似。图 2(b)中给出了统计误差模型下，发送功率 $P=20$ dB 时不同 λ 情况下本文方法的中断安全速率与信道误差变量方差 $\sigma_{b,k}^2$ 或 σ_e^2 的关系。无论 λ 为何值， $\sigma_{b,k}^2=0$ 时的系统中断安全速率均大于 $\sigma_e^2=0$ 时的，这也与图 2(a)中的结果相一致。

5 结束语

针对合法用户 CSI 与窃听用户 CSI 均不理想导致多波束卫星通信系统安全性能恶化，基于两种信道误差模型本文分别提出了两种多用户 MISOME 系统的鲁棒安全传输方法。在确定误差模型下，通过发送波束成形以及人工噪声协方差的联合优化设计解决系统 WC-SRM 问题，由于该问题为非凸的，通过将非凸的约束条件替换为确定的凸约束条件，最终转化为一个半定规划(SemiDefinite Program, SDP)问题和一系列 1 维搜索问题对其进行求解。仿真结果表明，相较已有方案，本文方法的安全性能得到明显的提升，同时发现合法用户的信道误差比窃听用户的信道误差对系统安全性能的影响更大。在统计误差模型下，为求解 OP-SRM 问题，本文提出一种基于 WC-SRM 的鲁棒设计的可靠近似方案。仿真结果表明，所提方案为 OP-SRM 问题的次优解。

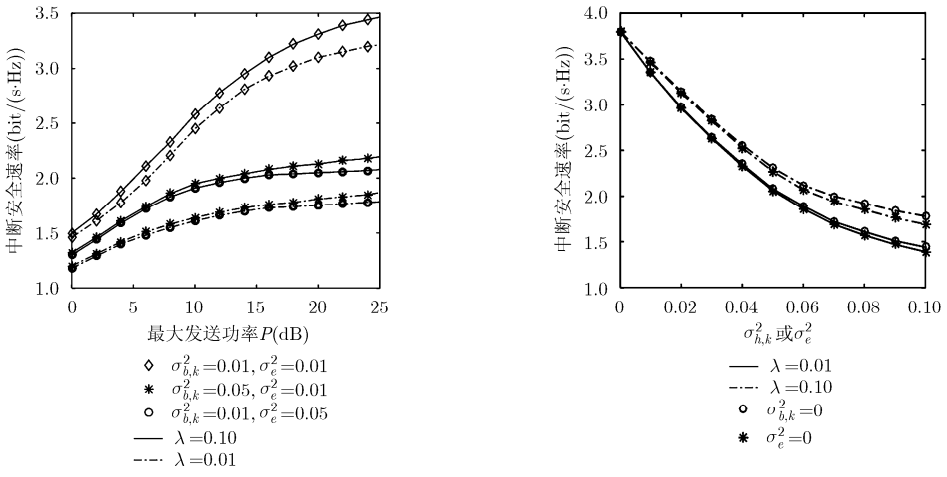


(a)最差情况安全速率与误差比的关系



(b)最差情况安全速率与发送功率的关系

图 1 确定误差模型系统安全性能比较



(a)中断安全速率与发送功率的关系　　(b)中断安全速率与误差变量方差的关系

图 2 统计误差模型系统安全性能比较

参 考 文 献

[1] ZHANG Xi, MCKAY M R , ZHOU Xiangyun, *et al*. Artificial-noise-aided secure multi-antenna transmission with limited feedback[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(5): 2742–2754. doi: 10.1109/TWC.2015.2391261.

[2] LI Na, TAO Xiaofeng, and XU Jin. Artificial noise assisted communication in the multiuser downlink: optimal power allocation[J]. *IEEE Wireless Communations Letters*, 2015, 19(2): 295–298. doi: 10.1109/LCOMM.2014.2385779.

[3] WYNER A D. The wire-tap channel[J]. *Bell System Technical Journal*, 1975, 54(8): 1355–1387. doi: 10.1002/j.1538-7305.1975.tb02040.x.

[4] CSISZAR I and KOMER J. Broadcast channels with confidential messages[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 339–348. doi: 10.1109/TIT.1978.1055892.

[5] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189. doi: 10.1109/TWC.2008.060848.

[6] WANG Huiming, ZHENG Tongxin, and XIA Xianggen. Secure MISO wiretap channels with multiantenna passive eavesdropper artificial noise vs. artificial fast fading[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(1): 94–106. doi: 10.1109/TWC.2014.2332164.

[7] LIU Shuiyin, HONG Yi, and VITERBO Emanuele. Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2015, 14(8): 4193–4203. doi: 10.1109/ TWC.2015.2417886.

[8] TANG Yanqun, XIONG Jun, MA Dongtang, *et al*. Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty[J]. *IEEE Communications Letters*, 2013, 17(11): 2096–2099. doi: 10.1109/LCOMM.2013.100713.131673.

[9] LI Qiang and MA Wingkin. 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. doi: 10.1109/TSP.2013. 2253771.

[10] JIANG Lei, ZHU Han, María Ángeles Vazquez-Castro, *et al*. Secure satellite communication systems design with individual secrecy rate constraints[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 661–671. doi: 10.1109/TIFS.2011.2148716.

[11] GAN Zheng, ATHANASIOS D, and OTTERSTEN Bjorn. Physical layer security in multibeam satellite systems[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(2): 852–863. doi: 10.1109/TWC.2011.120911.111460.

[12] DESTOUNIS A and ATHANASIOS D. Dynamic power allocation for broadband multi-beam satellite communication networks[J]. *IEEE Communications Letters*, 2011, 15(4): 380–382. doi: 10.1109/LCOMM.2011.020111.102201.

[13] 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. doi: 10.3724/SP.J.1146.2011.01068.
ZHAO Jiajie, PENG Jianhua, HUANG Kaizhi, *et al*. A multi-user MIMO system encryption algorithm based on artificial noise[J]. *Journal of Electronics & Information Technology*, 2012, 34(8): 1939–1943. doi: 10.3724/SP.J.1146.2011.01068.

[14] ZHU Jun, SCHOBER Robert, and BHARGAVA V K. Linear precoding of data and artificial noise in secure massive MIMO systems[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(3): 2245–2261. doi: 10.1109/TWC.2015.2500578.

[15] LI Qiang, MA Wingkin, and SO Anthony Mancho. A safe approximation approach to secrecy outage design for MIMO wiretap channels[J]. *IEEE Signal Processing Letters*, 2014,

21(1): 118–121. doi: 10.1109/LSP.2013.2293884.

[16] LI Qiang and MA Wingkin. Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming[J]. *IEEE Transactions on Signal Processing*, 2011, 59(8): 3799–3812. doi: 10.1109/TSP.2011.2146775.

[17] LUO Zhiquan, MA Wingkin, SO Anthony Mancho, *et al*. Semidefinite relaxation of quadratic optimization problems [J]. *IEEE Signal Processing Magazine*, 2010, 27(3): 20–34. doi: 10.1109/MSP.2010.936019.

[18] DATTORRO J. Convex Optimization and Euclidean Distance Geometry[M]. Meboo Publishing USA, 2005: 404–410.

[19] LUO Zhiquan, STURM F, and ZHANG Shuzhong. Multivariate nonnegative quadratic mappings[J]. *SIAM Journal on Control and Optimization*, 2004, 14(4): 1140–1162. doi: 10.2139/ssrn.545582.

[20] 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. doi: 10.1137/S003614450242889.

[21] XIONG Jun, MA Dongtang, WONG Kaikit, *et al*. Robust masked beamforming for MISO cognitive radio networks with unknown eavesdroppers[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(2): 744–755. doi: 10.1109/TVT.2015.2400452.

王 舒： 女，1987 年生，博士生，研究方向为物理层安全和卫星通信.

达新宇： 男，1961 年生，博士生导师，研究方向为卫星通信和通信信号处理.