多播传输模式下的卫星通信安全波束成形算法

林 敏[1],张 健[1],林 志[2],王子宁[1],郭克锋[3],欧阳键[1]
(1. 南京邮电大学通信与信息工程学院,江苏南京 210003; 2. 国防科技大学电子对抗学院,安徽合肥 230037; 3. 航天工程大学航天信息学院,北京 101407)

摘 要: 与地面无线通信系统相比,卫星通信的广域覆盖特性使得信息安全传输问题成为该领域更具挑战性的研究课题. 为了提升多播传输模式下卫星通信系统的物理层安全性能,本文针对不同信道状态信息(Channel State Information,CSI)研究了两种安全波束成形(Beamforming,BF)算法. 在合法用户和窃听者CSI均准确已知的条件下,提出了基于半正定规划(Semidefinite Program,SDP)和惩罚函数相结合的安全BF算法;在合法用户CSI准确已知但窃听者CSI存在误差的条件下,提出了一种迭代的鲁棒安全BF算法. 最后,计算机仿真不仅验证了本文所提BF算法的正确性和有效性,而且展示了所提出的鲁棒算法能够有效地降低信道信息误差对系统安全性能的影响.

关键词: 卫星通信; 物理层安全; 波束成形; 多播传输
中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112(2022)01-0098-08
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20200622

Secure Beamforming Algorithm for Satellite Communication in Multicast Transmission Mode

LIN Min[1], ZHANG Jian[1], LIN Zhi[2], WANG Zi-ning[1], GUO Ke-feng[3], OUYANG Jian[1]
(1. *College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
2. *Institute of Electronic Countermeasure, National University of Defense Technology, Hefei, Anhui* 230037, *China*;
3. *College of Aerospace Information, Aerospace Engineering University, Beijing* 101407, *China*)

Abstract: Compared with the terrestrial wireless communication system, information secure transmission has become a more challenging research topic as a result of the wide coverage of satellite communication. In order to improve the physical layer security performance of multibeam satellite communication system in multicast transmission mode, two beamforming(BF) algorithms based on different channel state information(CSI) are studied in this paper. Under the condition that both legitimate user and eavesdropper CSI are known accurately, a secure BF algorithm based on semidefinite program(SDP) and penalty function is proposed. An iterative robust secure BF algorithm is proposed under the condition that the legitimate user CSI is known accurately but the eavesdropper CSI has errors. Finally, computer simulation not only verifies the correctness and effectiveness of the proposed BF algorithms in this paper, but also shows that the robust algorithm effectively reduce the influence of channel information errors on security performance of the system.

Key words: satellite communications; physical layer security; beamforming; multicast transmission

1 引言

卫星通信具有覆盖范围广、通信容量大、不受地理条件限制等优点,将在下一代移动通信系统中发挥重要的作用[1~4]. 然而,卫星通信的广域覆盖特性在为信息传递提供便利的同时,也为窃听者窃取私密信息提供了可乘之机,从而给卫星通信造成潜在的安全隐患. 传统的卫星通信网络安全协议主要是基于计算密码学方法的,破解密钥所需的计算复杂度决定了该加密算法的有效性. 但是随着云计算、量子计算等新技术的出现,这种基于计算复杂度的密钥安全体制面临着巨大

收稿日期:2020-06-24;修回日期:2020-08-30;责任编辑:孙瑶
基金项目:重点国际合作项目(No.61720106003);上海航天科技创新基金(No.SAST2019-095);国家自然科学基金(No.61901490);国防科技大学科研计划项目(No.ZK21-33);复杂电子系统仿真实验室基础研究课题(No.DXZT-JC-ZZ-2019-009)

的挑战. 在这种情况下,利用无线信道的差异性以及随机性来实现信息安全传输的物理层安全(Physical Layer Security,PLS)的技术在卫星通信领域显示了广阔的应用前景[5,6].

在地面无线网络中,对多天线技术的研究由来已久. 其中天线分集、空分复用、波束成形(Beamforming,BF)等技术已在3G和LTE网络中得到广泛应用[7,8]. 作为实现物理层安全的主要手段之一,BF技术通过调整天线的方向图,在增加合法用户接收信号功率的同时显著降低窃听者的接收信号质量,在空域维度上提升系统的安全性能. 由于卫星通信的广域覆盖和信道的开放性,近年来,基于BF的物理层安全技术在卫星通信领域受到了广泛的关注. 在发送端已知所有用户的信道状态信息(Channel State Information,CSI)的条件下,文献[9]针对多个窃听者的场景,建立以发射功率最小为准则的优化问题,并将该非凸问题转化为半正定规划(Semidefinite Program,SDP),在采用CVX包的基础上结合随机化算法得到BF权矢量. 文献[10]分别针对单个和多个窃听者的场景,提出了基于二阶锥规划的BF算法和基于梯度下降的双层迭代BF算法. 在实际的卫星通信系统中,量化误差和反馈时延等因素导致准确CSI往往难以获得,尤其是窃听者保持静默的情况下,系统甚至无法得到窃听信道的CSI[11]. 在这种情况下,针对系统准确已知合法用户的CSI,但仅已知窃听者统计CSI的场景,文献[12]建立了以窃听者接收信干噪比最小化为准则的优化问题,并且提出了一种基于二分法搜索的迭代算法求解最优BF权矢量. 在文献[12]模型的基础上,文献[13]假设窃听者CSI存在边界性的误差,研究了多个窃听者协作构成一个虚拟多天线的窃听者时多波束卫星通信中的安全速率最大化问题. 文献[14]在合法用户CSI存在角度估计误差而窃听者CSI未知条件下,提出了一种联合人工噪声和协同干扰BF方案,可以有效提高系统的安全性能. 上述文献主要对多波束卫星通信单播传输模式下的物理层安全问题进行了研究分析,但近几年来,随着卫星通信逐渐进入人们的日常生活,以内容为中心的各种数据业务如流媒体、数字视频广播等在卫星通信网络中得到了迅猛的发展,传统的单播传输在有限的频谱资源下已经无法满足日益增长的以内容为中心的通信需求. 在这种情况下,多播传输技术将在未来的卫星通信领域得到越来越广泛的应用[15,16]. 目前国内外学者对多播模式下的卫星通信物理层安全问题研究甚少,还面临着巨大的挑战.

本文考虑多波束卫星通信系统的下行链路场景,针对多播模式下潜在窃听和非法窃听两种情况,分别提出安全BF算法. 在潜在窃听的情况下,窃听者本身也是网内合法用户,但是没有接收特定多播信号的权限,所以系统已知其准确的CSI. 针对这种情况,将原NP-hard问题转化为SDP问题并且结合惩罚函数的方法求解. 在非法窃听的情况下,窃听者通常为非法用户,所以系统很难获得其准确的CSI. 针对这种情况,通过迭代的方法交替求解最优化和最差化问题并提出了鲁棒安全BF算法. 与大多数文献研究单播传输模式下的物理层安全问题不同,本文研究的是多播传输模式. 此外,与文献[9]和文献[10]理想地假设窃听者CSI准确已知相比,考虑了窃听者CSI非理想的情况. 因此,本文所提出的算法更具有一般性,可以为卫星通信多播传输系统的安全设计提供参考依据.

本文的符号说明如下:大写粗体字母表示矩阵,小写粗体字母表示矢量,$(\cdot)^{\mathrm{H}}$代表矩阵的共轭转置,E(·)表示数学期望运算,tr(·)表示矩阵的迹,rank(·)表示矩阵的秩,$\|\cdot\|_2$表示矩阵2范数,$\langle \boldsymbol{X},\boldsymbol{Y}\rangle$表示矩阵内积且$\langle \boldsymbol{X},\boldsymbol{Y}\rangle=\mathrm{tr}(\boldsymbol{X}^{\mathrm{H}}\boldsymbol{Y})$,$\boldsymbol{X}\succeq 0$表示矩阵$\boldsymbol{X}$是半正定矩阵,$\mathbb{C}^{m\times n}$表示$m\times n$复矩阵,$\mathrm{CN}(\mu,\sigma^2)$表示均值为$\mu$且方差为$\sigma^2$的复高斯随机分布,$\boldsymbol{A}\odot\boldsymbol{B}$表示矩阵$\boldsymbol{A}$和矩阵$\boldsymbol{B}$的Hadamard积,$[x,0]^+=\max\{x,0\}$,$\lambda_{\max}(\cdot)$表示矩阵的最大特征值.

2　系统模型

如图1所示,本文研究了多波束卫星通信系统下行链路的物理层安全问题. 该系统包含一个静止轨道(GEO)卫星、K个合法用户和L个窃听者. 多波束卫星采用多馈源单反射面形式的天线,并配置N个馈源. 与现有文献[12]和文献[13]不同的是,本文考虑了卫星通信系统多播传输模式,K个合法用户同时请求相同的信息内容.

在多播传输系统下,卫星采用BF技术同时向K个

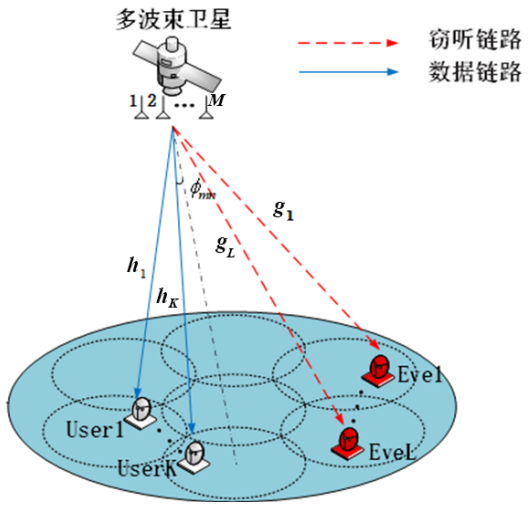


图1　存在窃听者的多波束卫星通信系统

合法用户发送信号$\boldsymbol{y}=\boldsymbol{w}s(t)$,其中卫星BF权矢量为$\boldsymbol{w}$,$s(t)$为卫星信号且满足$\mathrm{E}\left[\left|s(t)\right|^2\right]=1$. 由于卫星通信的广播特性,合法用户和窃听者接收到的信号分别表示为

$$z_k=\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{y}+n_k=\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}s(t)+n_k;\ k=1,2,\cdots,K \tag{1}$$

$$z_l=\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{y}+n_l=\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{w}s(t)+n_l;\ l=1,2,\cdots,L \tag{2}$$

其中,n_k和n_l表示均值为0且方差为σ^2的加性高斯白噪声(Additive White Gaussian Noise, AWGN),方差$\sigma^2=\kappa BT$,κ、B、T分别为玻尔兹曼常数、噪声带宽和用户处噪声温度[1];$\boldsymbol{h}_k$、$\boldsymbol{g}_l$分别表示卫星至第k个合法用户和第l个窃听者的信道矢量. 根据文献[9],卫星下行链路的信道矢量$\boldsymbol{h}_m\in\mathbb{C}^{N\times1}$通常表示为

$$\boldsymbol{h}_m=\sqrt{G_rC_m}\odot\boldsymbol{r}_m^{-\frac{1}{2}}\odot\boldsymbol{b}_m^{\frac{1}{2}}\odot\mathrm{e}^{\mathrm{j}\boldsymbol{\varphi}_m} \tag{3}$$

其中,$\boldsymbol{\varphi}_m\in C^{N\times1}$中的各元素在$[0,2\pi)$均匀分布;$\boldsymbol{r}=\left[r_{m1},r_{m2},\cdots,r_{mN}\right]^{\mathrm{T}}$表示雨衰系数,以dB为单位表示的$r_{mn}^{\mathrm{dB}}=20\log_{10}\left(r_{mn}\right)$服从对数正态随机分布$\ln\left(r_{mn}^{\mathrm{dB}}\right)\sim\mathrm{CN}\left(\mu,\sigma_r^2\right)$,$1\leqslant n\leqslant N$,$\mu$和$\sigma_r$取决于卫星的通信频率、极化方式和用户的位置;$\boldsymbol{b}=\left[b_{m1},b_{m2},\cdots,b_{mN}\right]^{\mathrm{T}}$表示点波束增益,其中的元素可以表示为

$$b_{mn}=b_{\max}\left(\frac{J_1\left(u_{mn}\right)}{2u_{mn}}+36\frac{J_3\left(u_{mn}\right)}{u_{mn}^3}\right)^2 \tag{4}$$

其中,$b_{\max}$表示卫星天线的最大增益;$J_1(\cdot)$和$J_3(\cdot)$分别是1阶和3阶的第一类贝塞尔函数,并且$u_{mn}=2.07123\sin\phi_{mn}/\sin\phi_{3\mathrm{dB}}$,$\phi_{mn}$表示第$m$个用户相对于第$n$个波束的偏轴角,$\phi_{3\mathrm{dB}}$为单侧半功率波束宽度. C_m表示自由空间损耗,可表示为

$$C_m=\left(\frac{c}{4\pi f\sqrt{{d_m}^2+{d_h}^2}}\right)^2 \tag{5}$$

其中,c为光速;f是载频频率;$d_h\approx35786$ km表示卫星高度;d_m是第m个用户到卫星覆盖区域中心距离.

此外,式(3)中,G_r表示接收天线增益. 当系统工作在Ku及以上频段时,通常采用抛物面天线,其表达式为[17]

$$G_r[\mathrm{dB}]=\begin{cases}G_{\max}, & 0^\circ<\theta_m<1^\circ\\ 32-25\log\theta_m, & 1^\circ<\theta_m<48^\circ\\ -10, & 48^\circ<\theta_m<180^\circ\end{cases} \tag{6}$$

其中,$G_{\max}$为抛物面天线轴向的最大增益;θ_m为第m个地球站相对于卫星的离轴角.

根据式(1)和式(2),不难得到合法用户和窃听者信噪比为

$$\gamma_k=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_k\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}}{\sigma_k^2};\ k=1,2,\cdots,K \tag{7}$$

$$\gamma_l=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{g}_l\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{w}}{\sigma_l^2};\ l=1,2,\cdots,L \tag{8}$$

在卫星通信系统中,由于窃听者相隔较远,它们之间很难进行合作. 在这种情况下,根据文献[9],第k个合法用户接收端的可达安全速率可以表示为

$$R_k=\left[\left(\log_2\left(1+\gamma_k\right)-\max_{1\leqslant l\leqslant L}\log_2\left(1+\gamma_l\right)\right),0\right]^+;\ k=1,2,\cdots,K \tag{9}$$

一般来说窃听分为潜在窃听和非法窃听两种形式. 对于潜在窃听,窃听者本身也是网内合法用户,因此卫星发射端可以获得窃听者的准确CSI. 由于非法窃听的窃听者通常为非法用户,其准确CSI在卫星发射端难以得到. 因此,本文分别对窃听者CSI准确已知和窃听者CSI存在误差两种情况提出了基于不同CSI的安全BF算法.

3 准确已知CSI条件下的安全BF算法

本节针对合法用户和窃听者CSI均准确已知的情况,通过BF技术在保证合法用户安全速率满足需求的前提下,使得卫星总发射功率最小. 根据式(7)~(9),该优化问题在数学上可以表示为

$$\min_{\boldsymbol{w}}\ \|\boldsymbol{w}\|_2^2$$

$$\text{s.t. }\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_k\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}}{\sigma_k^2}\right)-\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{g}_l\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{w}}{\sigma_l^2}\right)\geqslant R_k^{\mathrm{th}};$$

$$k=1,2,\cdots,K;\ l=1,2,\cdots,L \tag{10}$$

其中,R_k^{th}表示第k个合法用户处的安全速率门限值.

由于优化问题(10)属于NP-hard问题,针对此非凸问题,本节提出了基于半正定规划和惩罚函数的BF算法. 首先令$\boldsymbol{W}=\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$、$\tilde{\boldsymbol{h}}_k=\frac{\boldsymbol{h}_k}{\sigma_k}$、$\tilde{\boldsymbol{g}}_l=\frac{\boldsymbol{g}_l}{\sigma_l}$,优化问题(10)进一步表示为

$$\min_{\boldsymbol{W}\succeq0}\ \mathrm{tr}\{\boldsymbol{W}\} \tag{11a}$$

$$\text{s.t. }\mathrm{tr}\left\{\tilde{\boldsymbol{h}}_k\tilde{\boldsymbol{h}}_k^{\mathrm{H}}\boldsymbol{W}\right\}-2^{R_k^{\mathrm{th}}}\mathrm{tr}\left\{\tilde{\boldsymbol{g}}_l\tilde{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{W}\right\}+1\geqslant2^{R_k^{\mathrm{th}}};\ k=1,2,\cdots,K;\ l=1,2,\cdots,L \tag{11b}$$

$$\mathrm{rank}(\boldsymbol{W})=1 \tag{11c}$$

式(11)中约束(11c)是一个非凸约束,传统的半定松弛方法是将此非凸约束直接去除来简化优化问题,构成SDP问题并直接用数学工具包求解. 如果得到最优解$\boldsymbol{W}$的秩不等于1,则采用随机化算法从大量随机产生的秩为1的BF权矢量中选择其中的最优解[9]. 然而,半定松弛方法无法确保得到原优化问题(11)的最优解,该方法的解可能是次优的,甚至其性能远差于最优解性能[18]. 针对此问题,本文采用了一种惩罚函数方法,将非凸约束(11c)转化为

$$\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W})=0 \tag{12}$$

需要指出的是,任意的半正定矩阵 $\boldsymbol{W}$ 有 $\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W})\geqslant 0$,结合式(12)采用惩罚函数的方法可将优化问题(11)转化为

$$\begin{aligned}&\min_{\boldsymbol{W}\succeq 0}\ \mathrm{tr}\{\boldsymbol{W}\}+\rho\left[\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W})\right]\\&\text{s.t. }\mathrm{tr}\left\{\tilde{\boldsymbol{h}}_k\tilde{\boldsymbol{h}}_k^{\mathrm{H}}\boldsymbol{W}\right\}-2^{R_k^{\mathrm{th}}}\mathrm{tr}\left\{\tilde{\boldsymbol{g}}_l\tilde{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{W}\right\}+1\geqslant 2^{R_k^{\mathrm{th}}};\\&k=1,2,\cdots,K;\ l=1,2,\cdots,L\end{aligned} \tag{13}$$

其中,ρ 是惩罚因子,用于约束 $\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W})\approx 0$,优化问题(11)达到最优的前提条件为 $\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W})\approx 0$. 对 $\lambda_{\max}(\boldsymbol{X})$ 进行次梯度 $\partial\lambda_{\max}(\boldsymbol{X})=\boldsymbol{x}_{\max}\boldsymbol{x}_{\max}^{\mathrm{H}}$,由 $\lambda_{\max}(\boldsymbol{X})$ 对 $\boldsymbol{X}$ 的一阶泰勒展开式可以得到

$$\begin{aligned}&\lambda_{\max}(\boldsymbol{X})-\lambda_{\max}(\boldsymbol{W})\geqslant\left\langle\ \boldsymbol{w}_{\max}\boldsymbol{w}_{\max}^{\mathrm{H}},\boldsymbol{X}-\boldsymbol{W}\ \right\rangle;\\&\forall\boldsymbol{X}\succeq 0\end{aligned} \tag{14}$$

$\boldsymbol{W}^{(k)}$ 表示优化问题(13)第 k 次迭代得出的解,计算其最大特征值 $\lambda_{\max}(\boldsymbol{W}^{(k)})$ 和最大特征值对应的特征向量 $\boldsymbol{w}_{\max}^{(k)}$,构建以下SDP问题:

$$\begin{aligned}&\min_{\boldsymbol{W}\succeq 0}\ \mathrm{tr}\{\boldsymbol{W}\}+\rho\left[\mathrm{tr}(\boldsymbol{W})-\lambda_{\max}(\boldsymbol{W}^{(k)})-\left\langle\ \boldsymbol{w}_{\max}^{(k)}\boldsymbol{w}_{\max}^{(k)\mathrm{H}},\boldsymbol{W}-\boldsymbol{W}^{(k)}\ \right\rangle\right]\\&\text{s.t. }\mathrm{tr}\left\{\tilde{\boldsymbol{h}}_k\tilde{\boldsymbol{h}}_k^{\mathrm{H}}\boldsymbol{W}\right\}-2^{R_k^{\mathrm{th}}}\mathrm{tr}\left\{\tilde{\boldsymbol{g}}_l\tilde{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{W}\right\}+1\geqslant 2^{R_k^{\mathrm{th}}};\\&k=1,2,\cdots,K;\ l=1,2,\cdots,L\end{aligned} \tag{15}$$

获得最优解为 $\boldsymbol{W}^{(k+1)}$. 记优化问题(13)的目标函数为 $f(\boldsymbol{W})$,根据式(14)有

$$\begin{aligned}f(\boldsymbol{W}^{(k+1)})&=\mathrm{tr}\left\{\boldsymbol{W}^{(k+1)}\right\}+\rho\left[\mathrm{tr}(\boldsymbol{W}^{(k+1)})-\lambda_{\max}(\boldsymbol{W}^{(k+1)})\right]\\&\leqslant\mathrm{tr}\left\{\boldsymbol{W}^{(k+1)}\right\}+\rho\left[\mathrm{tr}(\boldsymbol{W}^{(k+1)})-\lambda_{\max}(\boldsymbol{W}^{(k)})\right.\\&\quad\left.-\left\langle\ \boldsymbol{w}_{\max}^{(k)}\boldsymbol{w}_{\max}^{(k)\mathrm{H}},\boldsymbol{W}^{(k+1)}-\boldsymbol{W}^{(k)}\ \right\rangle\right]\\&\leqslant\mathrm{tr}\left\{\boldsymbol{W}^{(k)}\right\}+\rho\left[Tr(\boldsymbol{W}^{(k)})-\lambda_{\max}(\boldsymbol{W}^{(k)})\right]\\&=f(\boldsymbol{W}^{(k)})\end{aligned} \tag{16}$$

由式(16)可知,迭代优化问题(15)是递减收敛的,本文所提的迭代算法如算法1所示.

通过以上迭代算法可以得到秩等于1的解 $\boldsymbol{W}$,再分解 $\boldsymbol{W}=\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$ 得到最优BF权矢量 $\boldsymbol{w}$. 该解满足所有合法用户安全速率在安全门限值以上同时使得发射功率最小.

算法1　准确已知CSI条件下的安全BF算法

步骤1:设定合法用户和窃听者个数及位置

步骤2:设定合法用户安全速率门限 R_k^{th}

步骤3:初始化计算精度 δ、惩罚因子 ρ、迭代次数 k=0

步骤4:求解SDP问题(13)获得 $\boldsymbol{W}^{(k)}$

步骤5:计算 $\boldsymbol{W}^{(k)}$ 最大特征值 $\lambda_{\max}(\boldsymbol{W}^{(k)})$ 和对应的特征向量 $\boldsymbol{w}_{\max}^{(k)}$

步骤6:求解SDP问题(15)获得最优解 $\boldsymbol{W}^{(k+1)}$

步骤7:如果 $\boldsymbol{W}^{(k)}\approx\boldsymbol{W}^{(k+1)}$,则更新 $\rho=2\rho$;否则,$k=k+1$

步骤8:如果满足收敛条件 $\left|\mathrm{tr}(\boldsymbol{W}^{(k)})-\lambda_{\max}(\boldsymbol{W}^{(k)})\right|\leqslant\delta$,迭代算法结束,输出 $\boldsymbol{W}$;否则,返回步骤5,重新循环

4　窃听者CSI存在误差时的鲁棒安全BF算法

在上一节中,针对窃听者CSI准确已知的情况研究了卫星发射功率最小化问题,提出了基于半正定规划和惩罚函数的BF算法. 本节考虑到非理想窃听者CSI的场景,首先对窃听信道误差建模,然后提出了多波束卫星通信鲁棒安全BF算法.

采用确定性误差模型对窃听信道误差进行建模[13]. 卫星可以根据窃听者的大致位置通过信道估计得到窃听者CSI的估计值 $\bar{\boldsymbol{g}}_i$. 而实际的窃听者CSI的 $\boldsymbol{g}_i$ 位于椭球不确定集 G_i 中,计算如下

$$\begin{aligned}&\boldsymbol{g}_i\in G_i\\&G_i=\left\{\boldsymbol{g}_i\left|\ \|\boldsymbol{F}_i(\boldsymbol{g}_i-\bar{\boldsymbol{g}}_i)\|\leqslant 1\right.\right\}\end{aligned} \tag{17}$$

其中,$\boldsymbol{F}_i=\dfrac{1}{\varepsilon}\boldsymbol{I}$ 决定了信道误差的大小.

考虑到非理想的窃听者CSI,将窃听信道误差带入优化问题(10),此时优化问题(10)的鲁棒BF问题可以描述为

$$\begin{aligned}&\min_{\boldsymbol{w}}\ \|\boldsymbol{w}\|_2^2\\&\text{s.t. }\min_{\boldsymbol{g}_l\in G_l}\left(\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_k\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}}{\sigma_k^2}\right)-\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{g}_l\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{w}}{\sigma_l^2}\right)\right)\geqslant R_k^{\mathrm{th}};\\&k=1,2,\cdots,K;\ l=1,2,\cdots,L\end{aligned} \tag{18}$$

为了解决优化问题(18),首先求解优化问题(10)得到BF权矢量,然后建立了一个最差化问题在当前BF权矢量条件下求解最差信道. 而最差信道就是在假设的椭球不确定集 G_i 中查找一个信道向量 $\boldsymbol{g}_l$ 使得用户的安全速率达到最小. 最差化问题为

$$\begin{aligned}&\min_{\boldsymbol{g}_l}\ \left(\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_k\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}}{\sigma_k^2}\right)-\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{g}_l\boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{w}}{\sigma_l^2}\right)\right)\\&\text{s.t. }\ \boldsymbol{g}_l\in\boldsymbol{G}_l;\ k=1,2,\cdots,K;\ l=1,2,\cdots,L\end{aligned} \tag{19}$$

通过简单的化简,式(19)可等价为

$$\begin{aligned}&\min_{\boldsymbol{g}_l}\ -\tilde{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\tilde{\boldsymbol{g}}_l\\&\text{s.t. }\ \boldsymbol{g}_l\in\boldsymbol{G}_l;\ l=1,2,\cdots,L\end{aligned} \tag{20}$$

将式(17)代入式(20)化简得

$$\begin{aligned}&\min_{\boldsymbol{g}_l}\ -\tilde{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\tilde{\boldsymbol{g}}_l\\&\text{s.t. }\ \boldsymbol{g}_l^{\mathrm{H}}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l\boldsymbol{g}_l-2\mathrm{Re}(\bar{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l\boldsymbol{g}_l)+\bar{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l\bar{\boldsymbol{g}}_l\leqslant 1;\\&l=1,2,\cdots,L\end{aligned} \tag{21}$$

根据文献[19]中S程序将优化问题(21)转化为对偶问题,即

$$\begin{aligned}&\max_{\mu_l,\lambda_l}\ \mu_l\\&\text{s.t. }\lambda_l\geqslant 0;\\&\boldsymbol{A}_l\succeq 0;\ l=1,2,\cdots,L\end{aligned}\tag{22}$$

其中，$\boldsymbol{A}_l=\begin{bmatrix}-\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}+\lambda_l\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l & -\lambda_l\boldsymbol{F}_l\boldsymbol{F}_l^{\mathrm{H}}\bar{\boldsymbol{g}}_l\\ -\bar{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{F}_l\boldsymbol{F}_l^{\mathrm{H}}\lambda_l & \lambda_l\bar{\boldsymbol{g}}_l^{\mathrm{H}}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l-\lambda_l-\mu_l\end{bmatrix}$.

对于 $l=1,2,\cdots,L$，优化问题(21)是一个强对偶问题．因此，对偶问题(22)的最优解与原问题最优解相同，μ_l为优化问题(22)最优解．由KKT条件和拉格朗日乘子法可以得到对应的最差信道为

$$\begin{aligned}&\boldsymbol{g}_{wc,l}^{*}=(-\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}+\lambda_l^{*}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l)^{-1}\lambda_l^{*}\boldsymbol{F}_l^{\mathrm{H}}\boldsymbol{F}_l\bar{\boldsymbol{g}}_l;\\&l=1,2,\cdots,L\end{aligned}\tag{23}$$

通过求解最差化问题(21)，判断最差情况下合法用户的安全速率是否满足安全速率门限值约束．如果满足，此时的$\boldsymbol{w}$即为鲁棒BF最优权矢量．反之，将式(23)中最差信道代入优化问题(10)重新求解．具体的鲁棒安全BF算法如算法2所示．

算法2 窃听者CSI存在误差时的鲁棒安全BF算法

步骤1：设定合法用户和窃听者个数、合法用户位置、窃听者大致位置

步骤2：设定窃听者信道存在的误差大小ε

步骤3：根据窃听者大致位置初始化L个窃听者的CSI，即$\bar{G}=\left\{\bar{\boldsymbol{g}}_1,\bar{\boldsymbol{g}}_2,\cdots,\bar{\boldsymbol{g}}_L\right\}$

步骤4：根据算法1求解最优化问题(10)，得到权矢量$\boldsymbol{w}$

步骤5：将$\boldsymbol{w}$带入最差化问题(21)，解出此时的最差信道$\boldsymbol{g}_{wc,l}^{*}$，$l=1,2,\cdots,L$

步骤6：更新窃听者的CSI，即$\bar{G}=\left\{\boldsymbol{g}_{wc,1}^{*},\boldsymbol{g}_{wc,2}^{*},\cdots,\boldsymbol{g}_{wc,L}^{*}\right\}$

步骤7：如果$\log_2\left(1+\dfrac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_k\boldsymbol{h}_k^{\mathrm{H}}\boldsymbol{w}}{\sigma_k^2}\right)-\log_2\left(1+\dfrac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{g}_{wc,l}^{*}\boldsymbol{g}_{wc,l}^{*\mathrm{H}}\boldsymbol{w}}{\sigma_l^2}\right)\geqslant R_k^{\mathrm{th}}$，$\forall k,l$，即最差情况下所有合法用户安全速率满足需求，则优化算法结束；否则，返回步骤4，重新循环求解波束成形权矢量$\boldsymbol{w}$

在以上优化算法中，交替求解最优化问题(10)和最差化问题(21)．根据文献[20]该鲁棒优化方法是收敛的．在仿真中发现该算法经过4~8次迭代可以跳出循环条件得到一个稳定的鲁棒安全BF权矢量，该解满足在最差窃听信道情况下所有合法用户安全速率在安全门限以上同时使得发射功率最小．

5 数值仿真

本节对所提出的两种BF算法进行性能仿真，系统参数设置如表1所示[10]．仿真中以3个合法用户和3个窃听者为例，假设3个合法用户的位置分别为$(3.75\times10^5\ \mathrm{m},2.16\times10^5\ \mathrm{m})$、$(-3.75\times10^5\ \mathrm{m},2.16\times10^5\ \mathrm{m})$、$(0\ \mathrm{m},-4.33\times10^5\ \mathrm{m})$．在准确已知CSI条件下的仿真中，假设3个窃听者位置分别在$(-3.75\times10^5\ \mathrm{m},-2.16\times10^5\ \mathrm{m})$、$(3.75\times10^5\ \mathrm{m},-2.16\times10^5\ \mathrm{m})$、$(0\ \mathrm{m},4.33\times10^5\ \mathrm{m})$．而在窃听者CSI存在误差条件下的仿真中以上窃听者位置作为窃听信道矢量估计值对应的位置．本节将所提的准确已知CSI条件下的安全BF算法与现有的SDP与主特征向量相结合的方案[21]、SDP与随机化算法相结合的方案[9]进行安全性能对比．而对于窃听者CSI存在误差时的鲁棒安全BF算法，将其与非鲁棒方案进行了对比．

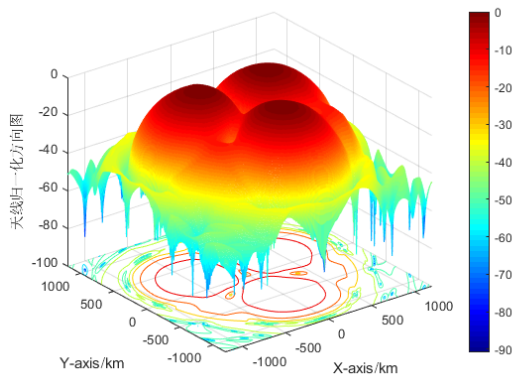
表1 系统参数设置

参数	数值
卫星轨道	GEO
卫星馈源数M	7
卫星高度d_0	35786 km
载频f	20 GHz
噪声带宽B	50 MHz
噪声温度T	300 K
3 dB角度$\theta_{3\mathrm{dB}}$	0.4°
卫星天线增益$b_{\max}$	52 dBi
雨衰系数	$\mu=-3.125,\sigma_r=1.591$
用户安全速率门限值R^{th}	2 bit/s/Hz

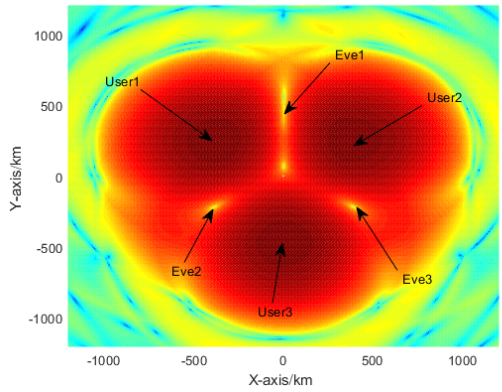
图2给出了窃听信道存在3%估计误差时归一化BF权矢量$\boldsymbol{w}$的方向图及其俯视图．从图中可以看出天线辐射方向图最大振幅方向指向合法用户且在窃听者方向上产生零陷．由此可见，所提BF算法能够增强合法用户接收信号质量，同时抑制窃听者接收信号质量，从而验证了所提BF算法的正确性．

图3描绘了理想CSI条件下本文所提算法与文献[9]和文献[21]的性能对比曲线．从图中可以看出，SDP与主特征向量相结合的方案用户安全速率有20%的概率在门限值以下甚至有可能出现性能极差的情况，因此不能保证满足用户需求．而其余两种方案均能满足用户安全速率需求．特别地，本文所提SDP与罚函数相结合的方案能够保证用户安全速率刚好达到安全速率门限值，避免了功率的浪费．图4描绘了理想CSI条件下3种BF算法卫星发射功率与安全速率门限关系图，该图展示了用户安全速率门限值的设置对3种BF算法卫星发射功率的影响．从图中可以看出，随着安全速率门限增加，三种算法最小发射功率随之增加．此外，SDP与随机化算法相结合的方案消耗功率始终高于另外两种．综合图3和图4的结果，本文所提准确已知CSI条件下的安全BF算法在安全性能和功率消耗上均取得优势．

图5绘制了非理想CSI条件下所提两种BF算法用户可达安全速率分布直方图，图中考虑了3%窃听信道估计误差对所提方案性能的影响．从图中可知，当窃听者CSI存在误差时第2节中安全BF算法有50%的概率不满足用户需求，而第3节中提出的鲁棒安全BF算法在窃听者CSI存在误差时仍能满足用户需求，证明了本



(*a*)　天线归一化辐射方向图



(*b*)　天线归一化辐射方向图(俯视图)

图2　天线归一化辐射方向图

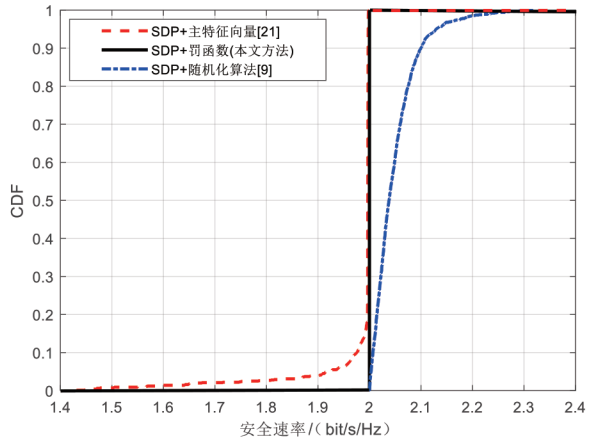


图3　理想CSI条件下3种BF算法可达安全速率累计分布曲线

文所提非理想CSI条件下安全BF算法对于信道误差具有较好的鲁棒性. 图6给出了非理想CSI条件下安全速率门限值和信道估计误差ε对天线最小发射功率的影响. 由图中可以看出,随着安全速率门限值的增加,最小发射功率也随之增加,与此同时,信道估计误差ε的增大也会增加卫星最小发射功率.

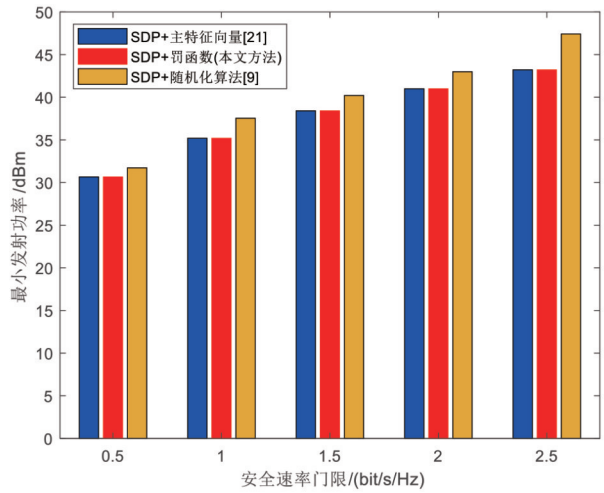


图4　理想CSI条件下3种BF算法卫星发射功率与安全速率门限关系图

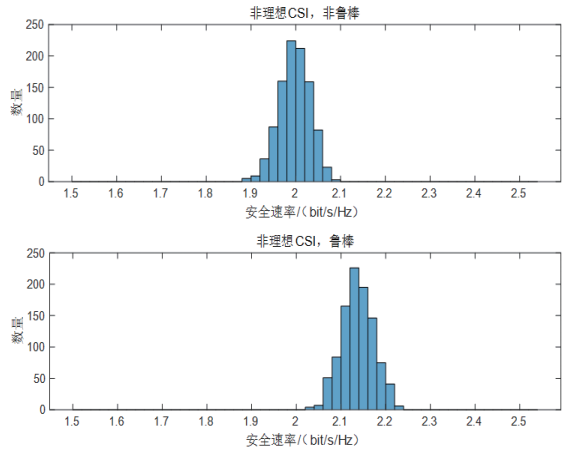


图5　非理想CSI条件下用户可达安全速率分布直方图

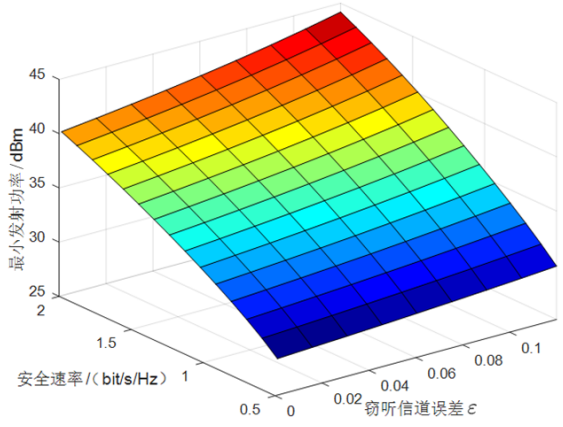


图6　最小发射功率与安全速率门限和信道误差的关系图

6　结束语

本文研究了多播传输模式下卫星通信安全BF算法. 针对存在多个窃听者的多播传输系统,推导出安全速率表达式,并构建了安全速率约束下的发射功率最

小化问题. 针对潜在窃听场景,在假设合法用户和窃听者CSI均已知的条件下,将原NP-hard优化问题转化为SDP问题,并运用惩罚函数的方法求解出BF权矢量. 接着,针对非法窃听场景中窃听者CSI存在误差的条件,提出了一种迭代的鲁棒安全BF算法,并得到最优的BF权矢量. 最后,仿真结果表明,两种安全BF算法能够有效提升多波束卫星通信下行链路多播传输系统的物理层安全性能.

参考文献

[1] LIN Z, LIN M, CHAMPAGNE B, et al. Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks[J]. IEEE Wireless Communications Letters, 2020, 10(2): 251-255.

[2] HUANG Q Q, LIN M, WANG J B, et al. Energy efficient beamforming schemes for satellite-aerial-terrestrial networks[J]. IEEE Transactions on Communications, 2020, 68(6): 3863-3875.

[3] HUANG Q Q, LIN M, ZHU W P, et al. Performance analysis of integrated satellite-terrestrial multiantenna relay networks with multiuser scheduling[J]. IEEE Transactions on Aerospace and Electronic Systems, 2020, 56(4): 2718-2731.

[4] LIN Z, LIN M, WANG J B, et al. Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access[J]. IEEE Journal of Selected Topics in Signal Processing, 2019, 13(3): 657-670.

[5] FRITSCHEK R, WUNDER G. On the Gaussian multiple access wiretap channel and the Gaussian wiretap channel with a helper: Achievable schemes and upper bounds[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(5): 1224-1239.

[6] ALLEN T, TAJER A, AL-DHAHIR N. Secure alamouti multiple access channel transmissions: Multiuser transmission and multi-antenna eavesdroppers[J]. IEEE Wireless Communications Letters, 2019, 8(5): 1510-1513.

[7] CHAABAN A, REZKI Z, ALOUINI M S. Capacity bounds and high-SNR capacity of MIMO intensity-modulation optical channels[J]. IEEE Transactions on Wireless Communications, 2018, 17(5): 3003-3017.

[8] KUMAR S, PIVARO G, FRAIDENRAICH G. Comments on "cutset bounds on the capacity of MIMO relay channels"[J]. IEEE Access, 2018, 6: 35129-35131.

[9] CUMANAN K, DING Z G, XU M, et al. Secrecy rate optimization for secure multicast communications[J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10(8): 1417-1432.

[10] LIN M, LIN Z, ZHU W P, et al. Joint beamforming for secure communication in cognitive satellite terrestrial networks[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(5): 1017-1029.

[11] 宋高俊, 曹寿国. 基于部分信道信息的卫星多波束联合预编码优化方法[J]. 电子学报, 2015, 43(11): 2232-2236.
SONG G J, CAO S G. Joint precoding optimization of multibeam satellite system based on partial channel information[J]. Acta Electronica Sinica, 2015, 43(11): 2232-2236. (in Chinese)

[12] ZHENG G, ARAPOGLOU P D, OTTERSTEN B. Physical layer security in multibeam satellite systems[J]. IEEE Transactions on Wireless Communications, 2012, 11(2): 852-863.

[13] 王舒, 达新宇. 非理想信道状态下多波束卫星通信的鲁棒安全传输设计[J]. 电子与信息学报, 2017, 39(2): 342-350.
WANG S, DA X Y. Robust secure transmit methods for multibeam satellite communication with imperfect channel state information[J]. Journal of Electronics & Information Technology, 2017, 39(2): 342-350. (in Chinese)

[14] LIN Z, LIN M, CHAMPAGNE B, et al. Secure beamforming for cognitive satellite terrestrial networks with unknown eavesdroppers[J]. IEEE Systems Journal, 2021, 15(2): 2186-2189.

[15] ZHU X M, JIANG C X, YIN L G, et al. Cooperative multigroup multicast transmission in integrated terrestrial-satellite networks[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(5): 981-992.

[16] CHRISTOPOULOS D, CHATZINOTAS S, OTTERSTEN B. Multicast multigroup precoding and user scheduling for frame-based satellite communications[J]. IEEE Transactions on Wireless Communications, 2015, 14(9): 4695-4707.

[17] LIN Z, LIN M, DE COLA T, et al. Supporting IoT with rate-splitting multiple access in satellite and aerial integrated networks[J]. IEEE Internet of Things Journal, 2021, 8(14): 11123-11134.

[18] LIN Z, LIN M, WANG J B, et al. Robust secure beamforming for 5G cellular networks coexisting with satellite networks[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 932-945.

[19] BOYD S, VANDENBERGHE L. Convex Optimization [M]. Cambridge: Cambridge University Press, 2004.

[20] MUTAPCIC A, BOYD S. Cutting-set methods for robust convex optimization with pessimizing oracles[J]. Optimization Methods and Software, 2009, 24(3): 381-406.

[21] LI Q, LI C, LIN J R. Constant modulus secure beamforming for multicast massive MIMO wiretap channels[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 264-275.

作者简介

林　敏　男,1972年生. 博士、教授、博士生导师. 主要研究方向为无线通信系统、智能信号处理、天线新技术等.
E-mail:linmin@njupt.edu.cn

张　健　男,1997年生. 硕士研究生. 研究方向为无线通信、智能信号处理.
E-mail:13675119007@163.com

林　志　男,1992年生. 博士、讲师. 主要研究方向为无线通信系统、阵列信号处理、可重构智能反射面等.
E-mail:linzhi@nudt.edu.cn