基于半定规划方法的多个窃听用户认知网络物理层安全优化设计

谢显中 谢成静* 雷维嘉 战美慧
(重庆邮电大学宽带接入网络研究所 重庆 400065)

摘 要：针对具有多个多天线窃听者的认知无线电网络(CRN)，为了使系统保密速率达到最大，该文把对主用户的干扰设计成为一个约束条件，通过对次用户发送端传输协方差矩阵的优化设计来提高物理层安全性能。在已知信道状态信息(CSI)时利用矩阵性质和 Charnes-Cooper 变换，将该非凸函数转化为一个半定规划(SDP)，从而得到次用户发送端的优化方案。仿真结果表明，相对于现有二次优化传输策略，该方案能够使系统的保密速率更大，并在复杂度方面具有优势。

关键词：认知无线电网络；物理层安全；传输协方差矩阵； 多个窃听者；半定规划
中图分类号：TN915.01 **文献标识码**：A **文章编号**：1009-5896(2015)10-2424-07
DOI: 10.11999/JEIT150111

Improved Transmit Design for Physical Layer Security in Cognitive Radio Networks with Multiple Eavesdropper Base on Semi-definite Programming

Xie Xian-zhong Xie Cheng-jing Lei Wei-jia Zhan Mei-hui
(*Institute of Broadband Access Networks*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: In the Cognitive Radio Network (CRN) with multiple multi-antenna eavesdroppers, to make the system security rate maximum, secure communication over the physical layer that is subjected to the interference power constraints at the Primary Users (PU) is provided by designing the transmit covariance optimization of Secondary User Transmitter (SU-Tx).When the Channel State Information (CSI) is known, the properties of the matrices and Charnes-Cooper transformation are used, the non-convex function is converted to a Semi-Definite Programming (SDP) to get the optimization scheme of SU-Tx. Simulation results show that compared with the existing sub-optimal transmission designs, the proposed method improves the secrecy rate and has more advantages on the complexity.

Key words: Cognitive Radio Network(CRN); Physical-layer security; Transmission covariance matrix; Multiple eavesdroppers; Semi-Definite Programming(SDP)

1 引言

认知无线电网络(CRN)独有的特点使它比其他传统无线网络更容易受到攻击且对安全威胁更为敏感[1,2]。研究人员已提出了一些方法来提高认知无线电网络的物理层安全[3−9]。

相对于单输入单输出(SISO)方案，文献[3]说明多天线技术能从本质上提高认知传输网络的物理层安全。文献[4]研究了多输入单输出(MISO)认知无线电网络的物理层安全问题。文献[5]中，作者针对单天线窃听用户，研究了非完美信道状态信息下的系统设计。文献[6]将次用户的安全优化问题转化为一个半定规划问题，研究了噪声辅助下 MISO 认知无线电网络的物理层安全性能。而文献[7]以安全截断概率为约束条件最大化主用户的安全吞吐量，次用户通过设计预编码矩阵来消除次用户的信号对主用户接收机的干扰，以及次用户人工噪声对主用户接收机和次用户接收机的干扰。为了在物理层防止窃听用户窃听信息，文献[8,9]分别探讨了基于信道选择和多用户调度来提高认知无线电网络物理层安全的方案。

收稿日期：2015-01-21；改回日期：2015-06-02；网络出版：2015-07-06
*通信作者：谢成静 xiecheng_jing@163.com
基金项目：国家自然科学基金(61271259, 61471076)，重庆市自然科学基金(CTSC2011jjA40006)，重庆市教委科学技术研究项目(KJ120501, KJ120502, KJ130536)，长江学者和创新团队发展计划(IRT1299)和重庆市科委重点实验室专项经费(CSTC)
Foundation Items: The National Natural Science Foundation of China (61271259, 61471076); The Chongqing Natural Science Foundation (CTSC2011jjA40006); The Research Project of Chongqing Education Commission (KJ120501, KJ120502, KJ130536); The Program for Changjiang Scholars and Innovative Research Team in University (IRT1299); The Special Fund of Chongqing Key Laboratory (CSTC)

此外，文献[10~13]研究了一种防止被多天线窃听用户窃听的多输入多输出(MIMO)信道的保密容量问题，而文献[14]和文献[15]考虑了对应的 MISO 模型。从传输优化角度而言，MISO 和 MIMO 是不同的。在 MIMO 环境下，文献[16~18]通过全局优化算法来优化功率分配，即保密容量最大(SRM)的关键在于解决拟凸问题，而 MISO 环境下则主要采用封闭式的方式解决 SRM 问题。文献[19]中指出，发送端在不被窃听的情况下发送保密信息给合法接收端，用合法接收端信息速率与窃听端信息速率的差值作为安全性能指标，而影响差值的因素主要是窃听端的信息速率，窃听端的信息速率越小，差值越大，安全性就越高。因此，为了使系统获得的保密速率最大，设计传输信号的协方差矩阵显得非常重要[20]。

本文考虑 CR 网络中具有多个窃听者的 MISO 信道的保密容量问题，在文献[3]的多天线技术基础上，研究多个多天线窃听用户模型下的发送端传输协方差矩阵的设计。在实际 CR 网络中，窃听者为了获取更多的信息往往采用多根接收天线，所以本文将文献[4~6]的单天线窃听用户扩展为多个多天线窃听用户。相对于文献[7,8]采用相关预编码设计来消除主用户的干扰，本文把对主用户的干扰设计成为一个约束条件，研究频谱共享下次用户的保密容量问题。本文首先讨论了保密速率受限(SRC)的情况，然后，利用 SRC 情况得出的结论，采用半定规划(SDP)的方法解决保密速率最大化(SRM)的问题。进一步，得到了多个窃听用户的认知网络物理层安全优化方案，通过复杂度分析，相对文献[6,17]等，本文方案的复杂度更低。最后，将 SDP 算法与文献[4,6,8]等中的投影最大比例传输(projected-MRT)和平坦最大比例传输(plain-MRT)等二次优化传输策略进行比较，证实了采用 SDP 方法能够使系统的保密速率更大。

2　系统模型与优化思路

本文中，多个多天线窃听用户的认知无线电网络模型如图 1 所示。由一个具有 N_{t} 天线次用户发送机(SU-Tx)，一个单天线次用户接收机 SU-Rx，一个单天线主用户接收机 PU-Rx 和 K 个具有 N_{e} 天线窃听用户(ED-Rx)。SU-Tx 到 SU-Rx 和 PU-Rx 的信道均为 MISO 信道，SU-Tx 到 ED-Rx 的信道为 MIMO。我们主要分析 CR 网络下 MISO 信道的安全性，即 SU-Tx 在对 ED-Rx 保密的情况下，使用分配给 PU-Rx 的合法频段传输信息给 SU-Rx。

设 $\boldsymbol{x}(t)\in\mathcal{C}^{N_{\mathrm{t}}\times 1}$ 为次用户发送端的发送信号，根据图 1，次用户 SU-Rx、主用户 PU-Rx 和第 k 个窃听用户 ED-Rx 的接收信号分别为

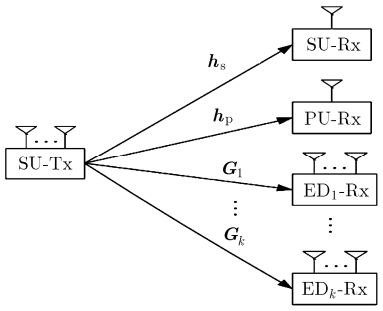

图 1 MISO 认知无线电网络模型

$$y_{\mathrm{s}}(t)=\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}x(t)+n_{\mathrm{s}}(t) \tag{1}$$

$$y_{\mathrm{p}}(t)=\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}x(t)+n_{\mathrm{p}}(t) \tag{2}$$

$$y_{\mathrm{e},k}(t)=\boldsymbol{G}_k^{\mathrm{H}}x(t)+\boldsymbol{V}_k(t),\ k=1,2,\cdots,K \tag{3}$$

其中，$\boldsymbol{h}_{\mathrm{s}},\boldsymbol{h}_{\mathrm{p}}\in\mathcal{C}^{N_{\mathrm{t}}\times 1}$，分别表示次用户发送端到次用户和主用户接收端的信道增益；$\boldsymbol{G}_k\in\mathcal{C}^{N_{\mathrm{t}}\times N_{\mathrm{t}}}$ 表示次用户发送端到窃听端的信道矩阵。$n_{\mathrm{s}}(t),n_{\mathrm{p}}(t)\in\mathcal{C},\boldsymbol{V}_k(t)\in\mathcal{C}^{N_{\mathrm{t}}}$ 分别为次用户接收端、主用户接收端和窃听用户接收端的加性高斯白噪声。本文假定所有噪声的均值为 0 方差为 1，即 $\mathrm{E}\left\{|n(t)|^2\right\}=1$，$\mathrm{E}\left\{\boldsymbol{V}_k(t)\boldsymbol{V}_k^{\mathrm{H}}(t)\right\}=\boldsymbol{I}$；$K$ 表示窃听者的数目。

发送信号 $\boldsymbol{x}(t)$ 的传输协方差为 $\boldsymbol{W}=\mathrm{E}\{\boldsymbol{x}(t)\boldsymbol{x}^{\mathrm{H}}(t)\}$，$\Gamma$ 为主用户 PU-Rx 的干扰温度约束，P 是次用户 SU-Tx 的平均发射功率约束。我们采用最大化次用户接收端获得的信息速率与第 k 个窃听用户获得的信息速率差值的思路，即在窃听用户获得最大的信息速率情况下，也可以得到最大的保密速率。

用 $\mathrm{f}_k(\boldsymbol{W})$ 表示次用户接收端获得信息速率与第 k 个窃听用户获得信息速率的差值：

$$\mathrm{f}_k(\boldsymbol{W})=\lg\left(1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}\right)-\lg\det\left(\boldsymbol{I}+\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k\right) \tag{4}$$

其中，$\boldsymbol{W}\succeq 0$ 表示 $\boldsymbol{W}$ 为半正定矩阵，$\mathrm{Tr}(\boldsymbol{W})$ 为矩阵的迹运算，$\det(X)$ 表示 X 的行列式。则保密速率最大(SRM)的传输协方差矩阵设计为

$$\left.\begin{aligned}&\mathbf{R}^{*}(\mathrm{P})=\max_{\boldsymbol{W}}\ \min_{k=1,2,\cdots,K}\mathrm{f}_k(\boldsymbol{W})\\&\text{s.t.}\quad\boldsymbol{W}\succeq 0\\&\qquad\mathrm{Tr}(\boldsymbol{W})\le\mathrm{P}\\&\qquad\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{p}}\le\Gamma\end{aligned}\right\} \tag{5}$$

一般地，SRM 问题主要采用次优化方法，即采用投影最大比例传输(projected-MRT)[18]算法来求解。该算法使用所有窃听用户联合信道的零空间来设计 $\boldsymbol{W}$，满足 $\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}=0$，窃听用户总的联合信道矩阵为 $\boldsymbol{G}=[\boldsymbol{G}_1,\boldsymbol{G}_2,\cdots,\boldsymbol{G}_K]$，而 $\boldsymbol{G}$ 的正交补投影为 $\prod_{\boldsymbol{G}}^{\perp}=\boldsymbol{I}-\boldsymbol{G}\left(\boldsymbol{G}^{\mathrm{H}}\boldsymbol{G}\right)^{\dagger}\boldsymbol{G}^{\mathrm{H}}$，则采用 projected-MRT 传输预编码的权值为

$$\mu = \frac{\sqrt{\mathrm{P}}}{\left\| \prod_G^{\perp} \boldsymbol{h}_{\mathrm{s}} \right\|_2} \prod_G^{\perp} \boldsymbol{h}_{\mathrm{s}} \tag{6}$$

于是取 $\boldsymbol{W} = \alpha \boldsymbol{\mu} \boldsymbol{\mu}^{\mathrm{H}}$，$\alpha$ 的具体取值为

$$\alpha = \begin{cases} \Gamma \Big/ \left(\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{h}_{\mathrm{p}} \right), & \left(\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} * \boldsymbol{W} * \boldsymbol{h}_{\mathrm{p}} \right) < \Gamma \\ 1, & \left(\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} * \boldsymbol{W} * \boldsymbol{h}_{\mathrm{p}} \right) \geq \Gamma \end{cases}$$

此外，在采用 plain-MRT[18]时，如果联合保密速率为正，则设定权值为 $\alpha \boldsymbol{W}$，其中，

$$\boldsymbol{W} = \left(\frac{\mathrm{P}}{\left\| \boldsymbol{h}_{\mathrm{s}} \right\|^2} \right) \boldsymbol{h}_{\mathrm{s}} \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}, \ \alpha = \begin{cases} 1, & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} \leq \Gamma \\ \dfrac{\Gamma}{\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}}}, & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} > \Gamma \end{cases}$$

其他情况则设定权值 $\boldsymbol{W} = 0$。

3 基于 SDP 方法的保密速率最大化问题求解

针对式(5)保密速率最大化(SRM)问题，由于式(5)是一个非凸函数，直接求解非常困难，而保密速率受限(SRC)问题相对于保密速率最大(SRM)问题更容易分析，因此，我们首先将 SRM 问题重新表述为 SRC 问题，然后将其等价为一个半定规划问题，最后根据 SRC 的结论，采用 SDP 算法解决 SRM 问题。

为此，将式(5)重新表述为保密速率受限(SRC)的情况，即给定 P 的优化保密速率设计为

$$\left.\begin{aligned} \mathrm{P}^*(\mathrm{R}) = \min_{\boldsymbol{W} \succeq 0} \ & \mathrm{Tr}(\boldsymbol{W}) \\ \text{s.t.} \quad & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} \leq \Gamma \\ & \min_{k=1,\cdots,K} \mathrm{f}_k(\boldsymbol{W}) \geq \mathrm{R} \end{aligned}\right\} \tag{7}$$

3.1 保密速率受限(SRC)的情况

利用式(4)，可以将式(7)改写为

$$\left.\begin{aligned} \mathrm{P}^*(\mathrm{R}) = \min_{\boldsymbol{W} \succeq 0} \ & \mathrm{Tr}(\boldsymbol{W}) \\ \text{s.t.} \quad & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} \leq \Gamma \\ & 2^{-\mathrm{R}} \geq \max_{k=1,\cdots,K} \frac{\det\left(\boldsymbol{I} + \boldsymbol{G}_k^{\mathrm{H}} \boldsymbol{W} \boldsymbol{G}_k \right)}{1 + \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{s}}} \end{aligned}\right\} \tag{8}$$

由于式(8)的目标函数为非凸函数，因此可用下面的引理将其近似为凸函数。

利用矩阵行列式性质，将式(8)进行放松得到：

$$\left.\begin{aligned} \mathrm{P}^*(\mathrm{R}) \geq \mathrm{P}_2^*(\mathrm{R}) = \min_{\boldsymbol{W} \succeq 0} \ & \mathrm{Tr}(\boldsymbol{W}) \\ \text{s.t.} \quad & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} \leq \Gamma \\ & 2^{-\mathrm{R}} \geq \max_{k=1,\cdots,K} \frac{1 + \mathrm{Tr}\left(\boldsymbol{G}_k^{\mathrm{H}} \boldsymbol{W} \boldsymbol{G}_k \right)}{1 + \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{s}}} \end{aligned}\right\} \tag{9}$$

由于式(9)是一个凸函数。则可利用 SDP 方法将上述问题转变为

$$\left.\begin{aligned} \mathrm{P}_2^*(\mathrm{R}) = \min_{\boldsymbol{W}} \ & \mathrm{Tr}(\boldsymbol{W}) \\ \text{s.t.} \quad & \boldsymbol{W} \succeq 0 \\ & \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{p}} \leq \Gamma \\ & 1 + \mathrm{Tr}\left(\boldsymbol{h}_{\mathrm{s}} \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}} \boldsymbol{W} \right) \geq 2^{\mathrm{R}} \left(1 + \mathrm{Tr}\left(\boldsymbol{G}_k \boldsymbol{G}_k^{\mathrm{H}} \boldsymbol{W} \right) \right), \\ & k = 1, 2, \cdots, K \end{aligned}\right\} \tag{10}$$

引理 1[21]：考虑保密速率 $\mathrm{R} > 0$，对于放松保密速率受限(SRC)问题，假定式(9)是可行的，则当且仅当 $\mathrm{rank}(\boldsymbol{W}) = 1$ 为其优化结果。

由此可知，当矩阵 $\boldsymbol{W}$ 的秩为 1 时，$\mathrm{P}^*(\mathrm{R}) = \mathrm{P}_2^*(\mathrm{R})$。用引理 1 可得到以下结论。

定理 1 对于 $\mathrm{R} > 0$ 时的 SRC 问题，假定式(8)成立，则放松后的式(9)恰好能解决 SRC 问题。此时，式(8)的优化解决方式和式(9)的相同，即 SRC 优化解决方案是 $\boldsymbol{W}$ 的秩为 1 的情况。

证明 用 $\widehat{\boldsymbol{W}}$ 优化解决式(9)，通过引理 1 和矩阵行列式性质可知当且仅当其秩为 1 时为其优化结果。

令 $r = \mathrm{rank}(\widehat{\boldsymbol{W}})$，忽略 $r = 0$ 的情况。当 $r \geq 1$，用 $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$ 表示矩阵 $\widehat{\boldsymbol{W}}$ 的 r 个非零特征值。当且仅当 $r = 1$ 时，取等号。则

$$\begin{aligned} \det\left(\boldsymbol{I} + \widehat{\boldsymbol{W}} \right) &= \prod_{i=1}^{r} (1 + \lambda_i) \\ &= 1 + \sum_{i=1}^{r} \lambda_i + \sum_{i \neq k} \lambda_i \lambda_k + \cdots \geq 1 + \sum_{i=1}^{r} \lambda_i \\ &= 1 + \mathrm{Tr}\left(\widehat{\boldsymbol{W}} \right) \end{aligned} \tag{11}$$

于是，式(9)的 $\widehat{\boldsymbol{W}}$ 可行，即 $\mathrm{P}_2^*(\mathrm{R}) = \mathrm{Tr}(\widehat{\boldsymbol{W}}) \geq \mathrm{P}^*(\mathrm{R})$。又因为 $\mathrm{P}^*(\mathrm{R}) \geq \mathrm{P}_2^*(\mathrm{R})$，则可得到 $\mathrm{P}_2^*(\mathrm{R}) = \mathrm{P}^*(\mathrm{R})$；所以我们可以利用 $\widehat{\boldsymbol{W}}$ 来优化式(8)。另外，若 $\boldsymbol{W}^*$ 是式(8)的一个优化结果，同理可知，式(9)的 $\boldsymbol{W}^*$ 是可行的，即 $\mathrm{P}_2^*(\mathrm{R}) = \mathrm{P}^*(\mathrm{R}) = \mathrm{Tr}(\boldsymbol{W}^*)$，因此能够说明 $\boldsymbol{W}^*$ 是式(9)的优化结果。根据引理 1 可知 $\boldsymbol{W}^*$ 的秩只能为 1。 证毕

由此可知，可以采用 SDP 算法得到 SRC 问题的预编码设计方案，即为优化传输策略。

3.2 保密速率最大(SRM)的情况

现在我们讨论保密速率最大的情况。为了方便，我们将式(5)进行以下变换：

$$\begin{aligned} \mathrm{R}^*(\mathrm{P}) &= \max_{\boldsymbol{W}} \ \min_{k=1,\cdots,K} \mathrm{f}_k(\boldsymbol{W}) \\ &= \max_{\boldsymbol{W}} \ \min_{k=1,\cdots,K} \lg \frac{1 + \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{s}}}{\det\left(\boldsymbol{I} + \boldsymbol{G}_k^{\mathrm{H}} \boldsymbol{W} \boldsymbol{G}_k \right)} \end{aligned} \tag{12}$$

为了最小化 $\lg \dfrac{1 + \boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{s}}}{\det\left(\boldsymbol{I} + \boldsymbol{G}_k^{\mathrm{H}} \boldsymbol{W} \boldsymbol{G}_k \right)}$，即可以最大化

$\dfrac{\det\left(\boldsymbol{I}+\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k\right)}{1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}}$，则式(5)重写为

$$\gamma^{*}(\mathrm{P})=\min_{\substack{\boldsymbol{W}\succeq 0\\ \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{p}}\le\Gamma\\ \mathrm{Tr}(\boldsymbol{W})\le\mathrm{P}}}\ \max_{k=1,\cdots,K}\frac{\det(\boldsymbol{I}+\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k)}{1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}}\tag{13}$$

根据定理 1，式(13)可变为

$$\gamma^{*}(\mathrm{P})\ge\gamma_2^{*}=\min_{\substack{\boldsymbol{W}\succeq 0\\ \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{p}}\le\Gamma\\ \mathrm{Tr}(\boldsymbol{W})\le\mathrm{P}}}\ \max_{k=1,\cdots,K}\frac{1+\mathrm{Tr}\left(\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k\right)}{1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}}\tag{14}$$

通过引理 1 和验证优化问题的 KKT 条件[12]可知式(14)是紧的，由此就可以通过缩放后的式(14)来解决式(13) SRM 问题，即下面的定理 2。

定理 2　考虑到(13)式 $0<\gamma^{*}(\mathrm{P})<1$ 的情况，在式(13)中进行缩放后，其优化结果可以解决式(13) SRM 问题。

为此，利用 Charnes-Cooper 变换，令传输协方差 $\boldsymbol{W}=\boldsymbol{Z}/\xi$，其中，$\boldsymbol{Z}\succeq 0,\ \xi>0$，则式(14)可转变为

$$\min_{\boldsymbol{Z},\xi}\ \max_{k=1,2,\cdots,K}\frac{\xi+\mathrm{Tr}(\boldsymbol{G}_k\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{Z})}{\xi+\mathrm{Tr}(\boldsymbol{h}_{\mathrm{s}}\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{Z})}\tag{15a}$$

$$\text{s.t.}\quad \mathrm{Tr}(\boldsymbol{Z})\le\xi\mathrm{P}\tag{15b}$$

$$\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{p}}\boldsymbol{Z}\le\Gamma\xi\tag{15c}$$

$$\boldsymbol{Z}\succeq 0,\ \xi>0\tag{15d}$$

$$\min_{\boldsymbol{Z},\xi,\tau}\ \tau\tag{16a}$$

$$\text{s.t.}\quad \xi+\mathrm{Tr}\left(\boldsymbol{G}_k\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{Z}\right)\le\tau,\ k=1,\cdots,K\tag{16b}$$

$$\xi+\mathrm{Tr}(\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}}\boldsymbol{Z})=1\tag{16c}$$

$$\mathrm{Tr}(\boldsymbol{Z})\le\xi\mathrm{P}\tag{16d}$$

$$\boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{p}}\boldsymbol{Z}\le\Gamma\xi\tag{16e}$$

$$\boldsymbol{Z}\succeq 0,\quad \xi>0\tag{16f}$$

不失一般性地，固定式(15a)中的分母，则式(15)可以进一步改写成式(16)。

定理 3　问题式(16)等价于式(15)，这样，式(16)通过 $\boldsymbol{W}=\boldsymbol{Z}/\xi$ 等价于式(12)的 SRM 问题。

证明　假定 $\xi=0$，则通过式(16d)和 $\boldsymbol{Z}\succeq 0$，就可以得到 $\boldsymbol{Z}=0$，与式(16c)矛盾，所以式(16)中一定不会有 $\xi=0$。这就证明了式(16)和式(15)等价。根据上面的讨论和引理 1，通过 $\boldsymbol{W}=\boldsymbol{Z}/\xi$，可知式(15)和式(12)的解具有等价性。

由此可知，当满足条件 $\mathrm{rank}(\boldsymbol{W})=1$ 时可以利用 SDP 算法来解决 SRM 问题。

3.3 基于 SDP 的保密速率最大化问题求解算法

根据上面第 3.1 节和第 3.2 节的讨论结果，基于 SDP 的保密速率最大化问题求解算法和流程可以总结如下：

首先，利用矩阵行列式性质，将保密速率最大化问题(非凸函数)

$$\gamma^{*}(\mathrm{P})=\min_{\substack{\boldsymbol{W}\succeq 0\\ \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{p}}\le\Gamma\\ \mathrm{Tr}(\boldsymbol{W})\le\mathrm{P}}}\ \max_{k=1,\cdots,K}\frac{\det(\boldsymbol{I}+\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k)}{1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}}$$

进行缩放(定理 1 和定理 2)，转化为

$$\gamma_{\mathrm{relax}}^{*}=\min_{\substack{\boldsymbol{W}\succeq 0\\ \boldsymbol{h}_{\mathrm{p}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{p}}\le\Gamma\\ \mathrm{Tr}(\boldsymbol{W})\le\mathrm{P}}}\ \max_{k=1,\cdots,K}\frac{1+\mathrm{Tr}\left(\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k\right)}{1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}}}$$

其次，缩放后的式子中令 $\boldsymbol{W}=\boldsymbol{Z}/\xi$，转化为半定规划(SDP)问题(定理 3)。

进一步，利用 Charnes-Cooper 变换成标准式。

接下来，利用 CVX 工具箱求解得到传输协方差矩阵 $\boldsymbol{W}$。

最后，判断 $\boldsymbol{W}$ 的秩是否为 1；如果为 1，则利用式子 $\mathrm{f}_k(\boldsymbol{W})=\lg(1+\boldsymbol{h}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{s}})-\lg\det(\boldsymbol{I}+\boldsymbol{G}_k^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_k)$ 求出信道保密速率；如果不为 1，则不能进行特征值分解。

3.4 复杂度分析

这里对本文算法进行复杂度分析。因为实际操作中很难精确计算出各种算法的操作步数，为了方便对比各种算法的运算复杂度，我们只计算浮点运算操作的次数。在式(16)给出的优化模型中，限定条件中既包括等式约束式(16c)，也包括不等式约束式(16b)，式(16d)，式(16e)，还包括矩阵半正定约束式(16f)。等式限定条件的个数为 1 个，而 SDP 限定条件的维数为 M (假设天线数 $N_{\mathrm{t}}=M$)，很明显 SDP 限定条件维数远远大于等式限定条件维数，因此解决式(16)最差情况下的复杂度取决于 SDP 的限定条件。

一般来说，假设一个半正定规划中等式限定的维数为 n，SDP 限定条件的阶数为 m，则解这个凸优化模型的复杂度为 $O(\max\{m,n\}^4n^4)$。由此，解出式(16)中的凸优化模型的整体计算复杂度可以表示为 $O(M^4)$。同理，分析得到文献[6]的时间复杂度为 $O(M^4)$。而文献[16]提出的全局优化算法则涉及到多次搜索查找，而它的复杂度为 $O(M^6)$。因本文和文献[6]的时间复杂度都为 $O(M^4)$，为了能够更清楚地比较本文算法和文献[6]的复杂度，我们假定窃听用户数为 1，$\Gamma=0$ dB，$P=10$ dB，合法接收者、目标接收端和窃听用户的接收天线数均为 1，发射端的天线数从 5 到 10，然后仿真算出 100 次蒙特卡洛估计得到的平均时间如表 1。

表 1 算法时间复杂度对比(ms)

算法	天线数					
	5	6	7	8	9	10
plain-MRT 算法	0.3220	0.3206	0.3203	0.3230	0.3011	0.3224
project-MRT 算法	0.4352	0.4379	0.4380	0.4410	0.4534	0.4455
SDP 算法	209.6561	219.0635	220.0975	222.1636	232.0505	234.3234
文献[6]算法	243.0635	244.0975	246.1636	256.0505	258.3234	233.9634

综上所述，虽然文献[18]中 projected-MRT 和 plain-MRT 算法的时间复杂度相比 SDP 算法较低，但这两种算法的保密速率相比 SDP 算法却相差甚远。而文献[6]和文献[17]算法的时间复杂度则相比于 SDP 算法偏高。

4 仿真及性能分析

本节将本文算法(SDP 算法)与文献[4]，文献[6]以及 projected-MRT[18], plain-MRT[18]进行仿真比较并分析其结果。假定信道状态信息(CSI)完全已知，合法信道服从均值为 0，方差为 1 的复高斯分布，而窃听信道服从均值为 0，方差为 ρ_e^2 的实高斯分布。其中，主用户的干扰温度门限值 $\Gamma = 0$ dB，次用户的发射天线数 $N_{\mathrm{t}} = 10$，主用户的接收天线数为 $N_{\mathrm{Pr}} = 1$，次用户的接收天线数为 $N_{\mathrm{Sr}} = 1$，在多窃听用户 MIMO 场景中，窃听者的数目和天线数量分别设置为 10 和 3。而在单窃听用户 MISO 场景中，窃听者的数目和天线数量分别设置为 10 和 1。

利用 Matlab 进行 5000～10000 次蒙特卡洛仿真，包括：不同优化方法下，窃听用户数目对保密速率的影响，窃听信道方差对保密速率的影响，发射功率对保密速率的影响，主用户干扰温度门限对保密速率的影响，以及不同传输天线对于不同算法时间复杂度的影响等，具体仿真结果如图 2～图 6。

图 2 为窃听用户数对系统保密性能的影响。这里，窃听信道方差 $\rho_e^2 = 1$，主用户干扰温度 $\Gamma = 0$ dB，次用户发射功率 $P = 10$ dB，窃听天线数 $N_{\mathrm{e}} = 3$。图中可知 SDP 算法相比其他两种算法性能更优异。当 $K \le 2$ 时，projected-MRT 的保密速率接近于 SDP，但当 $K \ge 4$ 时，因其所构成的自由度大于次用户发送端的自由度，所以次用户的保密速率变成 0，通过对比，即使在 $K = 10$ 时，SDP 算法也能够提供 1.3 bps/Hz 左右的速率。

图 3 为窃听信道方差对系统保密性能的影响(包括多窃听用户和单个窃听用户)。这里，窃听信道方差为 ρ_e^2，主用户干扰温度 $\Gamma = 0$ dB，发射功率 $P = 10$ dB。

在多窃听用户 MIMO 场景中，从图 3 中可以看到，当 $\rho_e^2 > 1$ 时，窃听端接收信号强度比合法端接收信号更大，而当 $\rho_e^2 < 1$ 时，则相反。由于 project-MRT 考虑了联合窃听信道，并采用了迫零(nulling)处理，因此它不随 ρ_e^2 变化，这就意味着其能够适应不同窃听信道质量强度的场景，所以当 ρ_e^2 不断增加时，project-MRT 的性能较 plain-MRT 好。此外，可以看出 SDP 方法比文中提到的两种次优化算法 plain-MRT、project-MRT 的性能更好，特别是当 $\rho_e^2 \ge 1$。

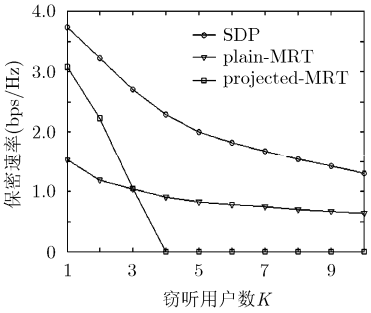

图 2 不同优化方法下窃听用户数目对保密速率的影响

在单窃听用户 MISO 场景中，从图 3 中可以看到，本文的 3 种算法的性能都有所提高，这是由于一个单天线窃听用户的自由度远远低于此用户发送端的自由度，导致其窃听能力大幅度降低，所以，窃听信道方差对 SDP 的影响基本可以忽略。从图 3 中还可以看出，对于不同的 ρ_e^2，本文的 SDP 算法与文献[4]的 SDP 算法具有相同的性能，但是本文的 SDP 算法可以应用到多窃听用户 MISO 的场景。

图 4 为发射功率对系统保密性能的影响(包括多窃听用户和单个窃听用户)。这里，窃听信道方差 ρ_e^2=1，主用户干扰温度 $\Gamma = 0$ dB。在多窃听用户 MIMO 场景中，当发送功率 P 较小时，plain-MRT 方法接近 SDP 算法，而当传输功率 P 较大的时候，project-MRT 算法更接近 SDP 算法。当发送功率进一步增加时，由于受到干扰温度 Γ 的约束，导致这 3 种方法的性能趋于饱和。而在单窃听用户 MISO 场景中，对于不同的发送功率，同样可以看到本文的 SDP 算法与文献[4]的 SDP 算法有相同的性能。此外，在这种场景中，需要更高的发送功率才能使其性能趋于饱和。

图 5 为主用户干扰温度门限 Γ 对系统保密性能

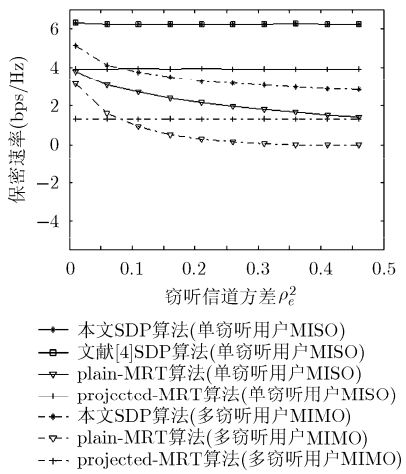

图 3 不同优化方法下窃听信道方差(ρ_e^2)对保密速率的影响

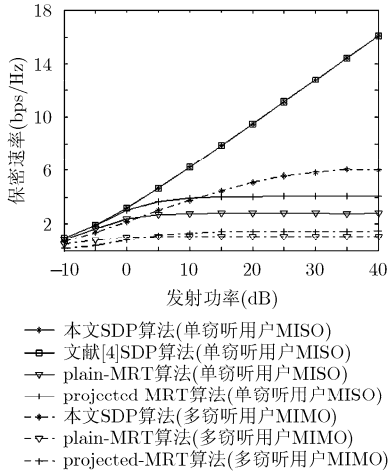

图 4 不同优化方法下发射功率 P 对保密速率的影响

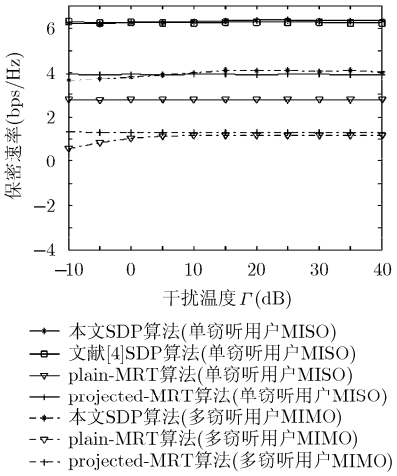

图 5 不同优化方法下主用户干扰温度门限 Γ 对保密速率的影响

的影响(包括多窃听用户和单个窃听用户)。这里，窃听信道方差 ρ_e^2=1，发送功率 $P=10$ dB 。从图 5 中可以看出，当发射天线数目一定且干扰温度 Γ 较低时，3 种算法保密速率随着 Γ 的增加而增大，而当干扰温度 Γ 较高时，因受限于功率 P 的约束，3 种算法的保密速率趋于平稳，这也符合第 1 节中 project-MRT，plain-MRT 算法及 2.2 节 SDP 算法的解释。在单窃听用户 MISO 场景中，对于 project-MRT 算法而言，当发射天线 N_{t} 数目一定，该算法能够很好地将干扰限制在零空间；而在多窃听用户 MIMO 场景中，由于发射天线的维度一定，project-MRT 算法则很难将干扰限制在较小的区域，所以，在多窃听用户 MIMO 场景中，本文 SDP 算法的性能明显优于另外两种次优化算法。通过对图 3，图 4，图 5 中 SDP 算法和文献[4]中 SDP 算法的对比分析，证实了本文的 SDP 算法具有很好的稳定性和实用性。

图 6 为次用户发送端(SU-Tx)天线数增加对于不同算法时间复杂度的影响。我们假定窃听用户数为 1，主用户干扰温度 $\Gamma=0$ dB，发送端发送功率 $P=10$ dB，合法接收者、目标接收端和窃听用户的接收天线数均为 1，发射端的天线数从 5 到 10，然后仿真算出 100 次蒙特卡洛估计得到的平均时间。从图 6 中可以看到，随着发送天线数增加，算法的时间复杂度也随之增加，但是文献[6]的时间复杂度始终都比本文 SDP 算法的时间复杂度要高。

5 结束语

本文主要考虑 CR 网络中被多个多天线窃听用户窃听时物理层安全优化问题，这是对文献[3~8]，文献[17,18]等文献的综合改进。通过优化次用户发送端(SU-Tx)传输协方差矩阵，可以有效地提高信道安全性能。考虑到保密速率最大化(SRM)问题是一个非凸函数，本文将其等价为半定规划(SDP)问题解决，进而得到多个窃听用户认知网络物理层安全的优化方案。我们将在下一步工作中重点考虑不完美信道状态信息即部分信道状态信息已知的情况，进而分析的重点放在系统的中断概率约束上。

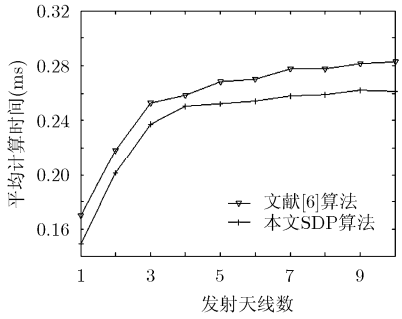

图 6 不同传输天线对于不同算法时间复杂度的影响

参 考 文 献

[1] Simon H. Cognitive radio: brain-empowered wireless communication[J]. *IEEE Journal on Selected Areas in Communications*, 2005, 23(2): 201–220.

[2] Shu Zhi-hui, Qian Yi, and Song Ci. On physical layer security for cognitive radio networks[J]. *IEEE Network*, 2013, 27(3): 28–33.

[3] Zhang Rui and Liang Ying-chang. Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks[J]. *IEEE Journal of Selected Topics in Signal Process*, 2008, 2(1): 88–102.

[4] Pei Yi-yang, Liang Ying-chang, Zhang Lan, *et al*.. Secure communication over MISO cognitive radio channel[J]. *IEEE*

Transactions on Wireless Communications, 2010, 9(4): 1494–1502.

[5] Pei Yi-yang, Liang Ying-chang, Zhang Lan, *et al*.. Secure communication in multi-antenna cognitive radio networks with imperfect channel state information[J]. *IEEE Transactions on Signal Processing*, 2011, 59(4): 1683–1693.

[6] 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.

[7] Wang Chao and Wang Hui-ming. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channel[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(11): 1814–1827.

[8] Houjeij A, Saad W, and Basar T. A game-theoretic view on the physical layer security of cognitive radio networks[C]. Proceedings of IEEE International Conference on Communications (ICC), Budapest, 2013: 2095–2099.

[9] Zou Yu-long, Wang Xian-bin, and Shen Wei-ming. Physical-layer security with multiuser scheduling in cognitive radio network[J]. *IEEE Transactions on Communications*, 2013, 61(12): 5103–5113.

[10] Yang Nan, Yeoh P l, and Elkashlan M T. Transmit antenna selection for security enhancement in MIMO wiretap channel[J]. *IEEE Transactions on Communications*, 2013, 61(1): 144–154.

[11] Khisti A and Wornell G. Secure transmission with multiple antennas Part II: the MIMOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(11): 5515–5532.

[12] He Xiang and Yener A. MIMO wiretap channels with unknown and varying eavesdropper channel states[J]. *IEEE Transactions on Information Theory*, 2014, 60(11): 6844–6869.

[13] Liu T and Shamai (Shitz) S. A note on the secrecy capacity of the multiple-antenna wiretap channel[J]. *IEEE Transactions on Information Theory*, 2009, 55(6): 2547–2553.

[14] Khisti A and Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(7): 3088–3104.

[15] Shafiee S and Ulukus S. Achievable rates in Gaussian MISO channels with secrecy constraints[C]. Proceedings of IEEE International of Information Theory(ISIT), Nice, 2007: 2466–2470.

[16] Gerbracht S, Wolf A, and Jorswieck E A. Beamforming for fading_wiretap channels with partial channel information[C]. Proceedings of ITG Workshop on Smart Antennas (WSA), Bremen, 2010: 394–401.

[17] Liu Jia, Hou Y, and Sherali H D. Optimal power allocation for achieving perfect secrecy capacity in MIMO wire-tap channels[C]. Proceedings of Information Sciences and Systems, Baltimore, MD, 2009: 606–611.

[18] Zang Li, Trappe W, and Yates R. Secret communication via multi-antenna transmission[C]. IEEE 41st Annual Conference on Information Sciences and Systems(CISS2007), Baltimore, MD, 2007: 905–910.

[19] Schaefer R F and Boche H. Physical layer service integration in wireless network: signal processing challenges [J]. *IEEE Signal Processing Magazine,* 2013, 31(3): 147–156.

[20] Li J and Petropulu A P. Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels[C]. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP) Dallas, TX, 2010: 3362–3365.

[21] Boyd S and Vandenbei'ghe L. Convex Optimization [M]. UK: Cambridge University Press, 2004: 69–71, 168–169, 655.

谢显中： 男，1966 年生，博士，教授，博士生导师，研究方向为移动通信网络、认知无线电技术等.

谢成静： 女，1990 年生，硕士生，研究方向为认知无线网络、物理层安全.

雷维嘉： 男，1969 年生，博士，教授，硕士生导师，研究方向为无线移动通信技术.

战美慧： 女，1991 年生，硕士生，研究方向为无线网络下的物理层安全.