认知无线电网络的物理层安全研究及其鲁棒性设计

陈 涛 余 华* 韦 岗
(华南理工大学电子与信息学院 广州 510640)

摘 要：该文从用户服务质量(QoS)的角度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。通过在次用户的发送信号中加入适当功率的人为噪声，能够有效地提高网络的物理层安全性能。经过适当的变换，将次用户的安全优化问题转化为一个半定规划，从而可以有效地求得次用户的最优发射方案。另外，针对信道状态信息不确定性的问题，在假设已知信道状态信息误差范围的前提下，采用最差性能最优的方法对系统进行鲁棒性设计，以保证即使在信道状态信息误差最大的情况下，依然可以满足系统的约束条件。最后，通过仿真验证了算法的有效性。

关键词：认知无线电；物理层安全；服务质量；鲁棒优化；半定规划
中图分类号：TN915.01 **文献标识码**：A **文章编号**：1009-5896(2012)04-0770-06
DOI: 10.3724/SP.J.1146.2011.01002

Study on the Physical Layer Security of Cognitive Radio Networks and Its Robustness Design

Chen Tao Yu Hua Wei Gang
(*School of Electronic and Information Engineering*, *South China University of Technology*, *Guangzhou* 510640, *China*)

Abstract: This paper studies on the issue of physical layer security of MISO Cognitive Radio Networks (CRN) from the Quality of Service (QoS) perspective. By adding a suitable amount of artificial noise into the transmitting signal of the Secondary User Transmitter (SU-Tx), the security performance could be enhanced apparently. Through some appropriate transformations, the optimization problem is converted into a semi-definite programming, which can be easily solved. Furthermore, a robust optimal transmitter is designed by using the worst-case optimization approach on the premise of knowing the region of uncertainties of Channel State Information (CSI). Therefore, all the constraints can still be satisfied even with the maximal CSI errors. Simulation results verify the effectiveness of the proposed approach.

Key words: Cognitive Radio (CR); Physical layer security; Quality of Service (QoS); Robust optimization; Semi-Definite Program (SDP)

1 引言

认知无线电是解决当前频谱资源紧张的一种有效方法。认知无线电网络中，在保证对主用户的通信不造成严重干扰的情况下，允许次用户使用已分配给主用户的频段进行通信[1,2]。通常，次用户对主用户产生的干扰信号功率被称为干扰温度(interference temperature)[1]。另外，网络安全是认知无线电网络需要考虑的一个重要问题[3]。由于无线通信自身的广播特性，通信信号很容易被非法用户窃听。以前，无线网络的安全问题主要是通过对发射信号进行密钥加密的方法来实现[4]。然而，基于密钥加密技术的网络安全存在许多问题，比如对称密码系统的密钥分配问题、非对称密码系统的高复杂度问题，等等[4,5]。最近，物理层安全技术作为密钥加密技术的补充或替代，已经受到了越来越多的关注，研究人员提出了各种各样的方法来提高无线网络的物理层安全[6–10]。其中，作为未来无线通信的关键技术之一的多天线技术，可以用来有效地提高通信的安全速率[6]。另外，通过在发射信号中加入一定功率的人为噪声，用来对窃听用户的信号接收进行干扰，从而可以有效的提高用户的安全通信速率[7,8]。

相对于其他传统的无线网络，认知无线电网络由于其自身独有的特点，对安全威胁更为敏感[9,10]。文献[9]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，在发射功率和干扰温度的限制下，分析得到了最大安全速率(secrecy rate)目标下的最佳波束成形。文献[11]中，作者在前面工作的

2011-09-23 收到，2012-02-13 改回
国家自然科学基金(61071212, U1035003)和华南理工大学中央高校基本科研业务费(2011ZZ0004, 2012ZZ0028)资助课题
*通信作者：余华 yuhua@scut.edu.cn

基础上，分析了认知无线电网络物理层安全的鲁棒性问题，研究了非完美信道状态信息情况下的系统设计。

本文在文献[9]和文献[10]的基础上，引入噪声辅助的方法，研究 MISO 认知无线电网络的物理层安全问题及其鲁棒性设计。在噪声辅助的情况下，若以最大安全速率为目标，次用户的优化将是一个极其复杂难以求解的问题。所以本文从保证用户服务质量(QoS)的角度考虑，以接收端的信噪比为目标，分析次用户最佳发射波束成形及人为噪声协方差矩阵的联合设计。虽然对于物理层安全传输协议的设计来讲，最大安全速率(secrecy rate)是其通常关注的目标，但在一些实际的应用场景中，如下行单播、下行多播以及多组多播，从接收信噪比的角度考虑系统的设计也是很有意义的[11]。

2　系统模型及问题描述

本文考虑的认知无线电网络模型如图 1 所示。系统包括一个天线数为 N_t 的次用户发射端(SU-Tx)，一个单天线的次用户接收端(SU-Rx)，一个单天线的主用户(PU-Rx)和 K 个单天线的窃听用户(Eve)。

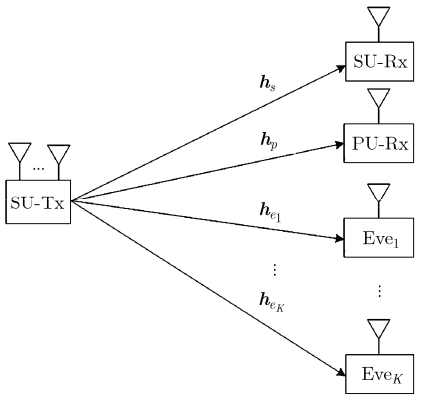

图 1 MISO 认知无线电网络

次用户 SU-Rx，主用户 PU-Rx 和窃听用户 Eve 的接收信号分别为

$$y_s = \boldsymbol{h}_s^{\mathrm{H}}\boldsymbol{x}+n_s \tag{1}$$

$$y_p = \boldsymbol{h}_p^{\mathrm{H}}\boldsymbol{x}+n_p \tag{2}$$

$$y_{e_k} = \boldsymbol{h}_{e_k}^{\mathrm{H}}\boldsymbol{x}+n_{e_k},\quad k=1,\cdots,K \tag{3}$$

其中 $\boldsymbol{x}\in\mathcal{C}^{N_t\times 1}$ 为次用户发送端的发射信号，$\boldsymbol{h}_s$，$\boldsymbol{h}_p$，$\boldsymbol{h}_{e_k}\in\mathcal{C}^{N_t\times 1}$ 分别为系统中次用户、主用户和窃听用户的信道向量。n_s，n_p 和 n_{e_k} 是各接收端的加性噪声，并且假设 n_s，n_p，$n_{e_k}\sim\mathcal{CN}(0,1)$。如前面所述，为了尽可能地扰乱窃听者的接收信号，本文采用噪声辅助的信号发射方法，在发送信号中加入一定功率的人为噪声信号。因此，发射信号 $\boldsymbol{x}$ 可以表示为

$$\boldsymbol{x} = \boldsymbol{w}s+\boldsymbol{z} \tag{4}$$

其中 $s\in\mathcal{C}$ 为发送数据，这里假设 $\mathrm{E}\{|s|^2\}=1$；$\boldsymbol{w}\in\mathcal{C}^{N_t\times 1}$ 是发射波束成形向量；人为噪声信号 $\boldsymbol{z}$ 服从零均值的高斯分布，即 $\boldsymbol{z}\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{\Sigma})$，$\boldsymbol{\Sigma}\succeq\boldsymbol{0}$ 是人为噪声信号 $\boldsymbol{z}$ 的协方差矩阵，$\boldsymbol{\Sigma}=\mathrm{E}\{[\boldsymbol{z}-\mathrm{E}(\boldsymbol{z})][\boldsymbol{z}-\mathrm{E}(\boldsymbol{z})]^{\mathrm{H}}\}=\mathrm{E}\{\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\}$，其中 $\boldsymbol{\Sigma}\succeq\boldsymbol{0}$ 表示 $\boldsymbol{\Sigma}$ 为厄密特半正定矩阵。因此，SU-Tx 的总发射功率为 $P_T=\mathrm{tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})+\mathrm{tr}(\boldsymbol{\Sigma})$，其中 $\mathrm{tr}(\bullet)$ 代表矩阵的迹运算。

由此，次用户接收端 SU-Rx 和窃听用户 ED-Rx 的接收信噪比分别表示为

$$\mathrm{SNR}_s(\boldsymbol{w},\boldsymbol{\Sigma}) = \frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}}\boldsymbol{w}}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2} \tag{5}$$

$$\mathrm{SNR}_{e_k}(\boldsymbol{w},\boldsymbol{\Sigma}) = \frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}}\boldsymbol{w}}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+\sigma_{e_k}^2},\quad k=1,\cdots,K \tag{6}$$

另外，主用户 PU-Rx 处的干扰温度为

$$P_{it} = \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}}\boldsymbol{w}+\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}}) \tag{7}$$

我们感兴趣的问题是，在限制窃听用户的接收信噪比 SNR_{e_k} 及主用户 PU-Rx 处的干扰温度 P_{it} 不超过预先设定值的条件下，通过联合优化波束成形向量 $\boldsymbol{w}$ 和噪声的协方差矩阵 $\boldsymbol{\Sigma}$，使得 SU-Rx 的接收信噪比最大。因此，问题的数学模型可以表示为

$$\left.\begin{aligned}\max_{\boldsymbol{w},\,\boldsymbol{\Sigma}}\ & \frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}}\boldsymbol{w}}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2}\\ \text{s.t.}\ & \frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}}\boldsymbol{w}}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+\sigma_{e_k}^2}\le\gamma_{e_k},\ k=1,\cdots,K\\ & \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}}\boldsymbol{w}+\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})\le\Gamma\\ & \mathrm{tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})+\mathrm{tr}(\boldsymbol{\Sigma})\le P_T,\ \boldsymbol{\Sigma}\succeq\boldsymbol{0}\end{aligned}\right\} \tag{8}$$

其中 $\gamma_{e_k}>0$ 是第 k 个窃听用户允许的信噪比 SNR 门限；Γ 是主用户的干扰温度限制；P_T 为 SU-Tx 的最大发射功率。

3　发射端的优化设计

在前面的系统模型和问题的数学描述基础上，这节开始联合优化设计发射波束成形向量 $\boldsymbol{w}$ 和噪声的协方差矩阵 $\boldsymbol{\Sigma}$。

3.1 完美信道状态信息的情况

首先，假设发射端能够获得全部的信道状态信息。优化问题式(8)的目标函数是一个复杂的二次商函数的形式，难以根据其 Hessian 矩阵来判断它是否是凸函数[12]，因而无法直接对其进行求解。但从下面的分析可以看到，通过适当的变化，我们可以把优化问题式(8)转化成一个半定规划，从而能够对其有效的求解。

首先，令 $\boldsymbol{X}=\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$，优化问题式(8)等价于

$$\left.\begin{aligned}&\max_{\boldsymbol{X},\boldsymbol{\Sigma}}\ \frac{\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2}\\ &\text{s.t.}\ \ \frac{\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+\sigma_{e_k}^2}\le\gamma_{e_k},\ k=1,\cdots,K\\ &\qquad\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})+\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})\le\Gamma\\ &\qquad\mathrm{tr}(\boldsymbol{X})+\mathrm{tr}(\boldsymbol{\Sigma})\le P_T\\ &\qquad\boldsymbol{\Sigma}\succeq\boldsymbol{0},\ \ \boldsymbol{X}\succeq\boldsymbol{0},\ \mathrm{rank}(\boldsymbol{X})=1\end{aligned}\right\}\tag{9}$$

问题(9)的目标函数为拟凸(Quasi-convex)函数，且约束条件 $\mathrm{rank}(\boldsymbol{X})=1$ 为非凸[13]，其中 $\mathrm{rank}(\bullet)$ 代表矩阵的秩。

为了把式(9)转化为凸优化的问题，我们采用半定松弛技术[13]，忽略非凸的约束条件 $\mathrm{rank}(\boldsymbol{X})=1$。同时根据 Charnes-Cooper 变换[9,14]，令

$$t=\frac{1}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2}\tag{10}$$

并且 $\widehat{\boldsymbol{X}}=t\boldsymbol{X}$，$\widehat{\boldsymbol{\Sigma}}=t\boldsymbol{\Sigma}$，从而式(9)中的优化问题等价于：

$$\left.\begin{aligned}&\max_{\widehat{\boldsymbol{X}},\widehat{\boldsymbol{\Sigma}},t}\ \ \mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})\\ &\text{s.t.}\ \ \mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+t\sigma_s^2=1\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})\le\gamma_{e_k}(\mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+t\sigma_{e_k}^2),\ \ k=1,\cdots,K\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})+\mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})\le t\Gamma\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}})+\mathrm{tr}(\widehat{\boldsymbol{\Sigma}})\le tP_T,\ \widehat{\boldsymbol{\Sigma}}\succeq\boldsymbol{0},\widehat{\boldsymbol{X}}\succeq\boldsymbol{0},t\ge0\end{aligned}\right\}\tag{11}$$

容易看出，式(11)中的目标函数为线性函数，且其约束条件均为线性矩阵不等式(linear matrix inequality)[15]，从而该优化问题是一个半定规划[12]，可以利用已有的内点算法工具箱 CVX[16]对其进行有效的求解。需要注意的是，由于使用了半定松弛技术，在问题转化过程中忽略了非凸的约束条件 $\mathrm{rank}(\boldsymbol{X})=1$。但是通过验证优化问题的 KKT 条件[12]，我们可以证明式(11)的最优解 $\boldsymbol{X}^*$ 一定满足 $\mathrm{rank}(\boldsymbol{X}^*)=1$，从而它是式(9)的最优解，其证明可以参照文献[8]。

3.2 信道状态信息存在误差的情况

实际情况下，发射端可能无法获取完美的信道状态信息。很多因素都会影响信道状态信息的准确性，比如估计误差、量化误差、多普勒扩展及反馈延时，等等[10]。在前面的基础上，假设发射端已知信道状态信息的不确定性范围，使用最差性能最优[17]的方法，以使在信道状态信息误差最大的情况下，系统依然可以满足已知的约束条件。类似文献[10]和文献[17]，本文假设信道状态信息误差在一个椭球范围内，因而信道模型可以表示为

$$\left.\begin{aligned}&\boldsymbol{H}_s=\{\boldsymbol{h}_s\,|\,\boldsymbol{h}_s=\hat{\boldsymbol{h}}_s+\Delta\boldsymbol{h}_s,\Delta\boldsymbol{h}_s^{\mathrm{H}}\boldsymbol{W}_s\Delta\boldsymbol{h}_s\le1\}\\ &\boldsymbol{H}_p=\{\boldsymbol{h}_p\,|\,\boldsymbol{h}_p=\hat{\boldsymbol{h}}_p+\Delta\boldsymbol{h}_p,\Delta\boldsymbol{h}_p^{\mathrm{H}}\boldsymbol{W}_p\Delta\boldsymbol{h}_p\le1\}\\ &\boldsymbol{H}_{e_k}=\{\boldsymbol{h}_{e_k}\,|\,\boldsymbol{h}_{e_k}=\hat{\boldsymbol{h}}_{e_k}+\Delta\boldsymbol{h}_{e_k},\Delta\boldsymbol{h}_{e_k}^{\mathrm{H}}\boldsymbol{W}_{e_k}\Delta\boldsymbol{h}_{e_k}\le1\},\\ &\qquad\qquad k=1,\cdots,K\end{aligned}\right\}\tag{12}$$

其中 $\hat{\boldsymbol{h}}_s$，$\hat{\boldsymbol{h}}_p$ 和 $\{\hat{\boldsymbol{h}}_{e_k}\}$ 为次用户发射端 SU-Tx 获得的信道状态信息的估计值；$\Delta\boldsymbol{h}_s$，$\Delta\boldsymbol{h}_p$ 和 $\{\Delta\boldsymbol{h}_{e_k}\}$ 为各信道的信道状态信息误差；$\boldsymbol{W}_s$，$\boldsymbol{W}_p$ 和 $\{\boldsymbol{W}_{e_k}\}$ 均为正定的 $N_t\times N_t$ 阶矩阵，它们分别决定了相应的信道状态信息的不确定性范围。

当系统获得的信道状态信息为式(12)时，式(9)中的优化问题等价于：

$$\left.\begin{aligned}&\max_{\boldsymbol{X},\boldsymbol{\Sigma}}\ \min_{\boldsymbol{h}_s\in\boldsymbol{H}_s}\ \frac{\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2}\\ &\text{s.t.}\ \ \frac{\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+\sigma_{e_k}^2}\le\gamma_{e_k},\ \forall\boldsymbol{h}_{e_k}\in\boldsymbol{H}_{e_k},\ k=1,\cdots,K\\ &\qquad\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})+\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})\le\Gamma,\ \forall\boldsymbol{h}_p\in\boldsymbol{H}_p\\ &\qquad\mathrm{tr}(\boldsymbol{X})+\mathrm{tr}(\boldsymbol{\Sigma})\le P_T\\ &\qquad\boldsymbol{\Sigma}\succeq\boldsymbol{0},\ \ \boldsymbol{X}\succeq\boldsymbol{0},\ \ \mathrm{rank}(\boldsymbol{X})=1\end{aligned}\right\}\tag{13}$$

类似上一节的方法，我们可以通过使用 Charnes-Cooper 变换，同时采用半定松弛技术，忽略非凸约束条件 $\mathrm{rank}(\boldsymbol{X})=1$，同时令

$$\tau=\min_{\boldsymbol{h}_s\in\boldsymbol{H}_s}\frac{\mathrm{tr}(\boldsymbol{X}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})}{\mathrm{tr}(\boldsymbol{\Sigma}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+\sigma_s^2}$$

式(13)可以转化为

$$\left.\begin{aligned}&\max_{\widehat{\boldsymbol{X}},\widehat{\boldsymbol{\Sigma}},\tau,t}\ \ \tau\\ &\text{s.t.}\ \ \mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})+t\sigma_s^2\le1,\quad\forall\boldsymbol{h}_s\in\boldsymbol{H}_s\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_s\boldsymbol{h}_s^{\mathrm{H}})\ge\tau,\quad\forall\boldsymbol{h}_s\in\boldsymbol{H}_s\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})\le\gamma_{e_k}\mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_{e_k}\boldsymbol{h}_{e_k}^{\mathrm{H}})+\gamma_{e_k}t\sigma_{e_k}^2,\\ &\qquad\quad\forall\boldsymbol{h}_{e_k}\in\boldsymbol{H}_{e_k},\ k=1,\cdots,K\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})+\mathrm{tr}(\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_p\boldsymbol{h}_p^{\mathrm{H}})\le t\Gamma,\quad\forall\boldsymbol{h}_p\in\boldsymbol{H}_p\\ &\qquad\mathrm{tr}(\widehat{\boldsymbol{X}})+\mathrm{tr}(\widehat{\boldsymbol{\Sigma}})\le tP_T,\ \widehat{\boldsymbol{\Sigma}}\succeq\boldsymbol{0},\widehat{\boldsymbol{X}}\succeq\boldsymbol{0},t\ge0\end{aligned}\right\}\tag{14}$$

由于存在椭球范围内的信道状态信息不确定性，优化问题式(14)含有无限多个约束条件。为了解决这个问题，借助于 S-Procedure [12]，可以把无限多个约束转化为有限个约束条件。根据 S-Procedure 定理以及式(12)中的信道模型，式(14)中的优化问题等价于：

$$
\left.\begin{aligned}
&\max_{\widehat{\boldsymbol{X}},\widehat{\boldsymbol{\Sigma}},t,\tau,s_1,s_2,p,\{e_k\}} \quad \tau \\
&\text{s.t.} \begin{bmatrix} s_1\boldsymbol{W}_s-\widehat{\boldsymbol{\Sigma}} & -\widehat{\boldsymbol{\Sigma}}\boldsymbol{h}_s \\ -\boldsymbol{h}_s^{\mathrm{H}}\widehat{\boldsymbol{\Sigma}} & 1-t\sigma_s^2-\hat{\boldsymbol{h}}_s^{\mathrm{H}}\widehat{\boldsymbol{\Sigma}}\hat{\boldsymbol{h}}_s-s_1 \end{bmatrix} \succeq \boldsymbol{0}, \exists\, s_1\geq 0 \\
&\quad \begin{bmatrix} \widehat{\boldsymbol{X}}+s_2\boldsymbol{W}_s & \widehat{\boldsymbol{X}}\boldsymbol{h}_s \\ \boldsymbol{h}_s^{\mathrm{H}}\widehat{\boldsymbol{X}} & \hat{\boldsymbol{h}}_s^{\mathrm{H}}\widehat{\boldsymbol{X}}\hat{\boldsymbol{h}}_s-\tau-s_2 \end{bmatrix} \succeq \boldsymbol{0}, \exists\, s_2\geq 0 \\
&\quad \begin{bmatrix} \gamma_{e_k}\widehat{\boldsymbol{\Sigma}}-\widehat{\boldsymbol{X}}+e_k\boldsymbol{W}_{e_k} & (\gamma_{e_k}\widehat{\boldsymbol{\Sigma}}-\widehat{\boldsymbol{X}})\hat{\boldsymbol{h}}_{e_k} \\ \hat{\boldsymbol{h}}_{e_k}^{\mathrm{H}}(\gamma_{e_k}\widehat{\boldsymbol{\Sigma}}-\widehat{\boldsymbol{X}}) & \gamma_{e_k}t\sigma_{e_k}^2+\hat{\boldsymbol{h}}_{e_k}^{\mathrm{H}}(\gamma_{e_k}\widehat{\boldsymbol{\Sigma}}-\widehat{\boldsymbol{X}})\hat{\boldsymbol{h}}_{e_k}-e_k \end{bmatrix} \succeq \boldsymbol{0}, \exists\, e_k\geq 0, k=1,\cdots,K \\
&\quad \begin{bmatrix} p\boldsymbol{W}_p-\widehat{\boldsymbol{X}}-\widehat{\boldsymbol{\Sigma}} & -(\widehat{\boldsymbol{X}}+\widehat{\boldsymbol{\Sigma}})\hat{\boldsymbol{h}}_p \\ -\hat{\boldsymbol{h}}_p^{\mathrm{H}}(\widehat{\boldsymbol{X}}+\widehat{\boldsymbol{\Sigma}}) & t\Gamma-\hat{\boldsymbol{h}}_p^{\mathrm{H}}(\widehat{\boldsymbol{X}}+\widehat{\boldsymbol{\Sigma}})\hat{\boldsymbol{h}}_p-p \end{bmatrix} \succeq \boldsymbol{0}, \exists\, p\geq 0 \\
&\quad \mathrm{tr}(\widehat{\boldsymbol{X}})+\mathrm{tr}(\widehat{\boldsymbol{\Sigma}})\leq tP_T,\ \ \widehat{\boldsymbol{\Sigma}}\succeq\boldsymbol{0},\ \widehat{\boldsymbol{X}}\succeq\boldsymbol{0}, t\geq 0
\end{aligned}\right\} \tag{15}
$$

关于 S-Procedure 定理及其具体的使用，可以参考文献[10]和文献[17]。容易看出，式(15)中的所有约束条件均为线性矩阵不等式(linear matrix inequality)[15]，因此该优化也是一个半定规划问题，同样可以利用已有的内点算法工具箱 CVX[16]有效求解。

4　仿真及性能分析

本节对前面提出的算法进行仿真验证并分析结果，仿真结果取 1000 次独立蒙特卡洛试验的平均值。除非特殊说明，我们假设信道增益服从零均值单位方差的独立瑞利分布；主用户的干扰温度门限值为 $\Gamma=0$ dB；窃听用户的接收信噪比门限值为 $\gamma_e=0$ dB；所有接收端的噪声方差也为 0 dB；次用户发射端 SU-Tx 的天线数为 $N_t=3$；窃听用户数为 $K=2$；发射功率为 $P_T=10$ dB。

4.1 完美信道状态信息的情况

首先分析完美信道状态信息条件下的 MISO 认知无线电网络的物理层安全性能。图 2 给出了不同发射功率条件下的次用户接收端SU-Rx的接收信噪比。从图 2(a)可以看出，通过在发送信号中加入适当的人为噪声，可以有效地提高网络的物理层安全性能，而且随着发射功率的增加，其性能提升更为明显。另外，增加发射天线数也可以在很大程度上提高网络的物理层安全性能。值得注意的是，当天线数较大时，系统拥有较大的空间维度，这本身就可以有效提高系统的安全性能，需要分配给人为噪声的功率较小，因而采用人为噪声的方法和不采用人为噪声的方法所获得的性能较为接近。在非噪声辅助的情况下，当发射天线数较少时，随着发射功率的增加，次用户接收端 SU-Rx 的接收信噪比趋于饱和。也就是说，继续增加发射功率并不能有效提高次用户接收端 SU-Rx 的接收信噪比，这主要是由于受窃听用户条件约束的原因。在这种情况下，我们可以通过把更多的功率分配给人为噪声，从而提高系统的物理层安全性能。在图 2(b)中，假设窃听信道的方差分别为 $\sigma_{h_e}^2=20$ dB，这表示窃听用户的

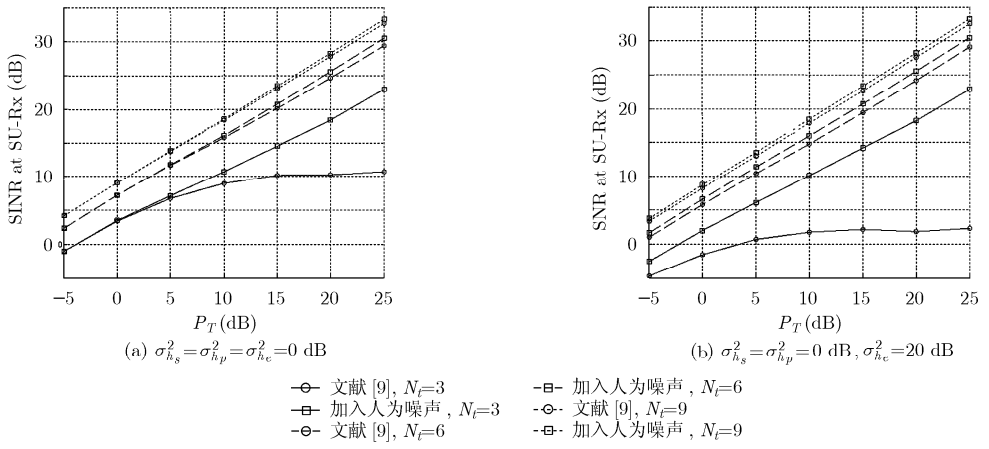

图 2 不同发射功率时的次用户接收端 SU-Rx 的接收信噪比

信道状况好于次用户的通信信道状况。相比于图 2(a)中的结果，我们可以看出，在窃听用户拥有更好的信道状况的情况下，在发射信号中加入人为噪声的方法能更有效的提高系统性能。

图 3 说明了存在不同窃听用户数时的次用户接收端 SU-Rx 的接收信噪比。可以看出当窃听用户数增加时，次用户接收端 SU-Rx 可获得的信噪比随之下降。但基于人为噪声辅助的方法在窃听用户数很大的情况下仍然可以有较好的性能。另一方面，随着窃听用户数的变化，基于人为噪声辅助的方法在不同信道状况下的性能差别不大。图 4 反映了不同干扰温度 Γ 限制的次用户接收端SU-Rx的接收信噪比。随着对限制条件的放宽，次用户接收端 SU-Rx 的接收信噪比也随之增加，其中在发射天线数较小的情况下变化更为明显。

4.2 信道状态信息存在误差的情况

假设所有信道状态信息存在范数有界的不确定性，并且有 $\boldsymbol{W}_s=(1/\varepsilon_s)I$ ， $\boldsymbol{W}_p=(1/\varepsilon_p)I$ 和 $\boldsymbol{W}_e=(1/\varepsilon_e)I$ ，其中 $(\varepsilon_s,\varepsilon_p,\varepsilon_e)$ 决定了不确定域的大小，ε 值越大，表示信道存在的误差越大。图 5 给出了存在 CSI 误差情况下非鲁棒优化的约束违反概率，图中假设信道状态信息误差的不确定域为 $(10^{-3},10^{-3},10^{-2})$ 。从图中可以看出，当信道状态信息存在误差时，非鲁棒优化的结果无法确保系统对主用户的干扰及窃听用户的接收信噪比低于预设值，且随着发射功率的增大，违反约束的概率也增大。另一方面，由于窃听信道状态信息存在更大的误差，其违反约束的概率也相对更大。

图 6 给出了鲁棒性优化方法下的次用户接收端 SU-Rx 的接收信噪比。由于采用了最差性能最优的鲁棒性设计，系统不存在类似于图 5 所示的违反约束条件的情况。也就是说，即使在信道状态信息误差最大的情况下，系统依然可以满足已知的约束条件。因为当信道状态信息存在误差时，非鲁棒性优化的结果可能已经不满足已知的约束条件，此时次用户接收端信噪比的大小并不能反映系统的性能，所以图 6 中我们只给出了鲁棒性优化方法下的系统性能。从图中可以看出，随着信道状态信息不确定度的增加，系统的性能也随之下降。

5 结束语

本文从用户服务质量(QoS)的角度分析了

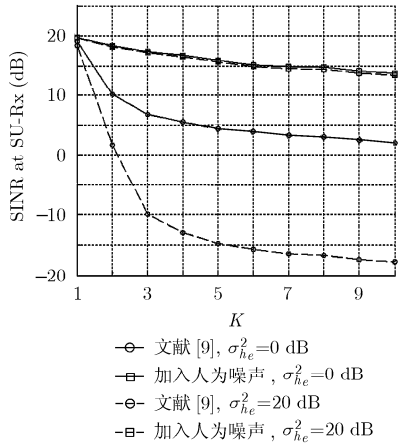

图 3 不同窃听用户数时的次用户接收端 SU-Rx 的接收信噪比

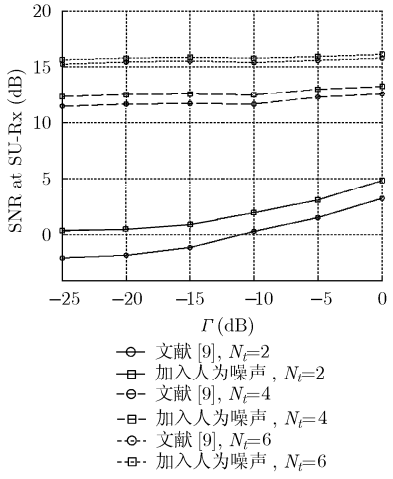

图 4 不同干扰温度限制时的次用户接收端 SU-Rx 的接收信噪比

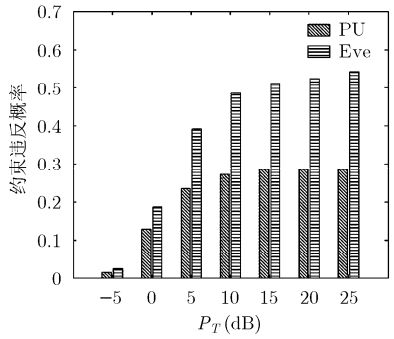

图 5 存在 CSI 误差情况下非鲁棒优化的约束违反概率

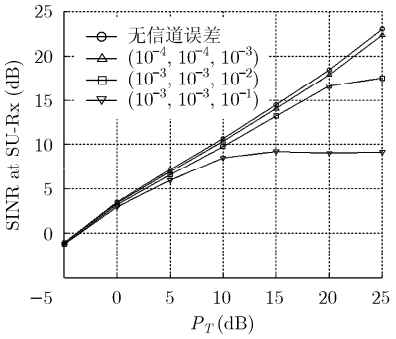

图 6 不同发射功率时的次用户接收端 SU-Rx 的鲁棒性接收信噪比

MISO 认知无线电网络的物理层安全性能。通过往发射信号中加入人为噪声，联合优化发射波束成形向量和噪声的协方差矩阵，可以有效地提高系统的安全特性。采用半定松弛技术，把复杂的优化问题转化为半定规划问题，从而可以有效得到系统最优发射方案。当次用户的发射端 SU-Tx 获得的信道状态信息存在误差时，我们使用最差性能最优的方法，对发射机进行了鲁棒性设计，确保在信道状态信息误差最大的情况下，系统依然可以满足已知的约束条件。仿真结果说明了算法的有效性。

参 考 文 献

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

[2] 魏飞, 杨震. MIMO 认知无线电分布式波形自适应算法[J]. 电子与信息学报, 2011, 33(6): 1356–1360.
Wei Fei and Yang Zhen. Decentralized waveform adaptation algorithm for MIMO cognitive radio[J]. *Journal of Electronics & Information Technology*, 2011, 33(6): 1356–1360.

[3] Baldini G, Sturman T, and Biswas A R. Security aspects in software defined radio and cognitive radio networks : a survey and a way ahead [J]. *IEEE Communications Surveys & Tutorials*, 2011: 1–25. http://ieeexplore.ieee.org/xpls/abs all.jsp?arnumber=5742780.

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

[5] 马春光, 张秉政, 孙原, 等. 基于按对平衡设计的异构无线传感器网络密钥预分配方案[J]. 通信学报, 2010, 31(1): 37–43.
Ma Chun-guang, Zhang Bing-zheng, Sun Yuan, *et al.*. Based on pair-wise balanced design key pre-distribution scheme for heterogeneous wireless sensor networks[J]. *Journal on Communications*, 2010, 31(1): 37–43.

[6] Khisti A and Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2009, 56(7): 3088–3104

[7] Negi R and Goel S. Secret communication using artificial noise[C]. IEEE Vehicular Technology Conference, Texas, USA, 2005: 1906–1910.

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

[9] Pei Y Y, Liang Y C, Teh K C, *et al.*. Secure communication over MISO cognitive radio channels [J]. *IEEE Transactions on Wireless Communications*, 2010, 9(4): 1494–1502.

[10] Pei Y Y, Liang Y C, Teh K C, *et al.*. Secure communication in multiantenna cognitive radio networks with imperfect channel state information[J]. *IEEE Transactions on Signal Processing*, 2011, 59(4): 1683–1693.

[11] Palomar D P, Lagunas M A, and Cioffi J M. Optimum linear joint transmit-receive processing for MIMO channels with QoS constraints [J]. *IEEE Transactions on Signal Processing*, 2004, 52(5): 1179–1197.

[12] Boyd S and Vandenberghe L. Convex Optimization Cambridge [M]. UK, Cambridge University. Press, 2004: 69–71, 168–169,655.

[13] Luo Z Q, Ma W K, So A M C, *et al.*. Semidefinite relaxation of quadratic optimization problems: from its practical deployments and scope of applicability to key theoretical results [J]. *IEEE Signal Processing Magazine, Special Issue on Convex Optimization for Signal Processing*, 2010, 27(3): 20–34.

[14] Charnes A and Cooper W W. Programming with linear fractional functionals [J]. *Naval Research Logistics Quarterly*, 1962, 9(3): 181–186.

[15] Boyd S, Ghaoui L E, Feron E, *et al.*. Linear Matrix Inequalities in System and Control Theory [M]. Philadelphia, PA, SIAM, 1994: 7–9.

[16] Grant M and Boyd S. CVX: matlab software for disciplined convex programming. http://stanford.edu/~ boyd/cvx, June. 2009.

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

陈　涛：男，1984 年生，博士生，研究方向为认知无线电、无线网络物理层安全.

余　华：男，1973 年生，副教授，硕士生导师，研究方向为无线通信、通信信号处理.

韦　岗：男，1963 年生，教授，博士生导师，研究方向为无线通信、通信信号处理.