中继网络中不准确信道状态信息下抗多窃听者的物理层安全方案

雷维嘉 左莉杰* 江 雪 谢显中
(重庆邮电大学移动通信技术重庆市重点实验室 重庆 400065)

摘 要：该文研究存在多个相互勾结的单天线窃听者的多中继传输系统中，采用零空间人工噪声和放大转发的中继波束赋形的物理层安全传输方案。在中继—窃听端的信道状态信息不准确的情况下，基于半定规划理论，对中继的波束赋形加权矩阵和人工噪声协方差矩阵进行联合优化，有效减少相互勾结的多个窃听者所获得的信息量，显著提高系统保密容量，是一种具有良好鲁棒性的物理层安全传输方案。仿真结果显示方案具有良好的性能。

关键词：物理层安全；保密速率；多窃听者；不准确信道状态信息；半定规划
中图分类号： TN925 **文献标识码**： A **文章编号**：1009-5896(2015)09-2191-07
DOI: 10.11999/JEIT141579

Physical Layer Security Scheme Resistant to Multi-eavesdroppers with Inaccurate Channel State Information in Relay Network

Lei Wei-jia Zuo Li-jie Jiang Xue Xie Xian-zhong
(*Chongqing Key Laboratory of Mobile Communications Technology*,
Chongqing University of Posts and Telecommunications, *Chongqing* 400065, *China*)

Abstract: This paper investigates the relay transmission system in the presence of multiple collusion single-antenna eavesdroppers. A physical layer security scheme employing nullspace Artificial Noise (AN) and Amplify-and-Forward (AF) relay beamforming is designed. In the case that channel state information can not be accurately obtained, the weighted matrice of relay beamforming and the nullspace AN covariance are jointed optimized based on the Semi-Definite Programs (SDP), which can effectively reduce the amount of the information likely to be obtained by the multiple collusion eavesdroppers and significantly improve the security capacity of the system. It is an effective physical security transmission scheme with good robustness. Simulation results verify that the scheme has good performance.

Key words: Physical layer security; Secrecy rate; Multi-eavesdroppers; Inaccurate channel state information; Semi-Definite Program (SDP)

1 引言

信息传输的安全性是通信中的重要问题，而无线通信由于传输的开放性使得安全性更为复杂和困难。研究表明，除通过高层的加密外，无线通信中实现信息的安全传输也可在物理层通过物理层安全技术[1]来解决，且系统的安全性可用保密容量[2]、保密中断概率等指标来量化。从信号处理角度，一般通过多发射天线技术，利用无线信道的随机衰落特性获得对合法用户有利的波束赋形来提高物理层安全性能。但前提条件是需要获得各节点间的完整信道状态信息(Channel State Information, CSI)。在许多文献的研究中都假设所有 CSI 都是已知的[3,4]，这时可以充分利用多天线技术和协作通信技术来改善安全性。文献[3,4]在放大转发(Amplify-and-Forward, AF)中继波束赋形的网络模型下，提出了在总功率或中继功率约束下的增强物理层安全性能的方案，并利用半定松弛方法来解决凸半定规划(Semi-Definite Programs, SDP)问题，获得最优的系统保密速率。然而，在实际中所有 CSI 都可获得是一种理想情况，因此一些文献也对只能获得部分 CSI 时的物理层安全问题进行研究。在文献[5]中，给出中继—窃听端的 CSI 在一定范围具有不确定性的情况下保密速率最大化的设计方案。文献[6]在中继—窃听端的 CSI 未知的情况下，从用户服务质量的角度提出了一种两阶段的模拟网络编码方案，通过中继加入人工噪声的方法改善了双向中继传输系统的安全性能。

2014-12-10 收到，2015-05-04 改回，2015-06-18 网络优先出版
国家自然科学基金(61471076, 61271259, 61301123)，长江学者和创新团队发展计划(IRT1299)以及重庆市科委重点实验室专项经费资助课题
*通信作者：左莉杰 zuolijie1111@163.com

在考虑存在多个窃听者的情况时，一种是认为窃听者之间没有关联，最大保密速率取决于接收信噪比最大的那一个窃听者。另一种是多个窃听者之间可能存在相互勾结的情况。窃听者间的勾结一般指窃听者之间能够交换或者合并它们窃听得到的信息，这样窃听者能获得更多的信息，再经过处理后可提高接收信息速率，相应保密速率会受到更大的影响。文献[7]基于三节点系统模型，讨论存在多个相互勾结的窃听者时的保密通信问题。文献[8,9]假设存在分散的勾结窃听者，其位置分布服从空间泊松过程，在已知全部 CSI 的情况下，将多个分散的勾结窃听者看作是一个多天线的窃听者。文献[10]在协作无线网络中假设已知全部 CSI 并且窃听者的位置分布服从齐次泊松过程，中继采用随机转发协议时，对多窃听者勾结的安全性问题进行研究。文献[11]在有多个天线、非勾结窃听者的 AF 中继网络中，基于窃听端 CSI 不准确的情况，提出了一个联合协作波束赋形和协作干扰的鲁棒性设计方案，以求得最大保密速率的下界。本文考虑多个单天线窃听者能相互勾结的情况，并将这些相互勾结的单天线窃听者等效为一个多天线的窃听者[7]。由于不易获得窃听者准确的 CSI，本文考虑在仅能获得不准确的窃听者 CSI 时，在 CSI 误差最大的情况下保密速率最大化的鲁棒性方案。该方案利用零空间人工噪声和 AF 中继波束赋形方法，对中继的波束赋形权值和人工噪声协方差进行联合优化，尽可能地提高信息传输的安全性。

与现有进行类似研究的文献相比，本文工作考虑多个窃听者相互勾结，同时窃听者的 CSI 不能准确地获得的情况。这两种情况下，物理层安全性的处理和分析都较为困难。现有的文献中，有些考虑了无中继节点的三节点系统模型中窃听者勾结的问题，但假设能获得完整、准确的 CSI，如文献[8,9]；有些考虑了中继网络中已知全部 CSI 情况下窃听者勾结的情况，但没有考虑窃听者的 CSI 不能准确获得的情况，如文献[10]；有些虽然考虑了 CSI 不完整或不准确的问题，但没有考虑中继网络中窃听者勾结的问题，如文献[5]。本文研究的模型更符合实际的情况，方法和结论具有更大的实际意义。

本文使用的特殊符号说明如下：$\mathrm{dd}(\boldsymbol{A})$ 表示以矩阵 $\boldsymbol{A}$ 的对角线元素为对角线元素的对角矩阵；$\boldsymbol{A}\succeq\boldsymbol{0}$ 表示 $\boldsymbol{A}$ 是一个 Hermite 正半定矩阵；$\|\boldsymbol{A}\|_{\mathrm{F}}$ 是矩阵 $\boldsymbol{A}$ 的 F-范数；$\nu(\boldsymbol{A})$ 表示矩阵 $\boldsymbol{A}$ 的非零特征值个数。

2 系统模型

考虑包括一个源节点(Source), N 个中继节点(Relays)、一个目的节点(Destination)和 J 个窃听节点(Eavesdroppers)的无线网络模型，如图 1 所示。在此网络中，源节点距目的节点较远，因此认为不存在直接链路 S-D。假设源节点不知道窃听节点的确切位置，但知道其距离源节点较远，因此可以认为不存在直接链路 S-E。每个节点均安装单天线。假设所有节点处的噪声均是均值为 0、方差为 σ^2 的复高斯白噪声。将多个单天线的勾结窃听者看作一个多天线的窃听者来处理。S-R, R-D, R-E 的信道增益分别用 $\boldsymbol{f}$,$\boldsymbol{c}$,$\boldsymbol{G}$ 表示。

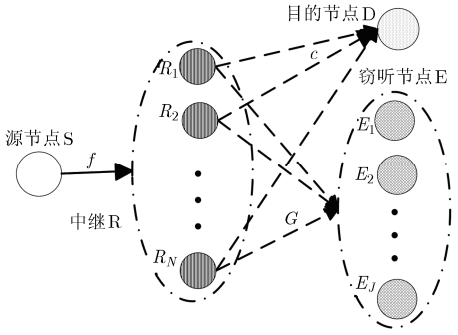

图 1 系统模型

本文采用放大转发中继辅助的两阶段线性波束赋形方案。在第 1 阶段，源节点向中继节点发送信息；在第 2 阶段，中继对信号进行处理，并转发给目的节点，同时窃听节点也会接收到信号。在一个传输时隙内，源节点发送 m 个编码符号到中继节点。不失一般性地，我们用标量 x 表示在一个传输时隙内传输的符号。符号 x 具有单位功率，即 $E\{|x|^2\}=1$。另外，为了符号的书写方便，省略时间下标。

在第 1 阶段，中继接收到的信号矢量为

$$\boldsymbol{y}_{\mathrm{R}}=\sqrt{P_{\mathrm{S}}}\boldsymbol{f}x+\boldsymbol{n}_{\mathrm{R}} \tag{1}$$

式中，$\boldsymbol{y}_{\mathrm{R}}\triangleq[y_{\mathrm{R},1}\ y_{\mathrm{R},2}\ \cdots\ y_{\mathrm{R},N}]^{\mathrm{T}}$，$y_{\mathrm{R},N}$ 表示在第 N 个中继节点处接收到的信号，P_{S} 是源节点的发送功率。

在第 2 阶段，N 个中继节点对接收到的信号进行放大转发，并加入人工噪声，发送的信号为

$$\boldsymbol{x}_{\mathrm{R}}=\widetilde{\boldsymbol{W}}\boldsymbol{y}_{\mathrm{R}}+\boldsymbol{n}_{\mathrm{a}} \tag{2}$$

式中，$\widetilde{\boldsymbol{W}}=\mathrm{diag}(\boldsymbol{w})$, $\boldsymbol{w}=[w_1\ w_2\ \cdots\ w_N]^{\mathrm{T}}$, $\boldsymbol{n}_{\mathrm{a}}=\boldsymbol{U}_{\perp}\boldsymbol{z}$ 是在中继节点中加入的 N 维人工噪声矢量，其中 $\boldsymbol{U}_{\perp}$ 是映射在主信道 $\boldsymbol{U}\triangleq\boldsymbol{c}$ 的零空间的投影矩阵，即 $\boldsymbol{c}^{\mathrm{T}}\boldsymbol{n}_{\mathrm{a}}=0$。其中的向量 $\boldsymbol{z}$ 是服从均值为 0、方差为 σ_z^2 的高斯分布的 $(N-1)$ 维列向量。人工噪声的协方差矩阵为 $\boldsymbol{n}_{\mathrm{a}}\boldsymbol{n}_{\mathrm{a}}^{\mathrm{H}}=\boldsymbol{U}_{\perp}\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}\boldsymbol{U}_{\perp}^{\mathrm{H}}=\widetilde{\boldsymbol{\Sigma}}$。令 $\boldsymbol{\Sigma}=\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}$，则 $\widetilde{\boldsymbol{\Sigma}}=\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}$。

在此阶段，中继转发消息信号和人工噪声所消

耗的总功率为

$$P_{\mathrm{R}}=P_{\mathrm{S}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{f}^{\mathrm{H}})\mathrm{diag}(\boldsymbol{f})\boldsymbol{w}+\sigma^2\left\|\widetilde{\boldsymbol{W}}\right\|^2+\mathrm{tr}\left(\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\right) \tag{3}$$

目的节点和窃听节点接收到的信号分别为

$$y_{\mathrm{D}}=\boldsymbol{c}^{\mathrm{H}}\boldsymbol{x}_{\mathrm{R}}+n_{\mathrm{D}}=\boldsymbol{c}^{\mathrm{H}}\left(\widetilde{\boldsymbol{W}}\boldsymbol{y}_{\mathrm{R}}+\boldsymbol{n}_{\mathrm{a}}\right)+n_{\mathrm{D}}$$
$$=\sqrt{P_{\mathrm{S}}}\boldsymbol{c}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\boldsymbol{f}x+\boldsymbol{c}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\boldsymbol{n}_{\mathrm{R}}+n_{\mathrm{D}} \tag{4}$$

$$\boldsymbol{y}_{\mathrm{E}}=\boldsymbol{G}^{\mathrm{H}}\boldsymbol{x}_{\mathrm{R}}+\boldsymbol{n}_{\mathrm{E}}=\boldsymbol{G}^{\mathrm{H}}\left(\widetilde{\boldsymbol{W}}\boldsymbol{y}_{\mathrm{R}}+\boldsymbol{n}_{\mathrm{a}}\right)+\boldsymbol{n}_{\mathrm{E}}$$
$$=\sqrt{P_{\mathrm{S}}}\boldsymbol{G}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\boldsymbol{f}x+\boldsymbol{G}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\boldsymbol{n}_{\mathrm{R}}+\boldsymbol{G}^{\mathrm{H}}\boldsymbol{n}_{\mathrm{a}}+\boldsymbol{n}_{\mathrm{E}} \tag{5}$$

记 $\boldsymbol{R}_{\mathrm{ff}}\triangleq\mathrm{diag}\left(|f_{\mathrm{R},1}|^2\ |f_{\mathrm{R},2}|^2\ \cdots\ |f_{\mathrm{R},N}|^2\right)$，$\boldsymbol{G}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{f})\triangleq\boldsymbol{G}_f^{\mathrm{H}}$，$\boldsymbol{c}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{f})\triangleq\boldsymbol{c}_f^{\mathrm{H}}$，$\boldsymbol{W}\triangleq\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$，则式(3)，式(4)和式(5)可写为

$$P_{\mathrm{R}}=P_{\mathrm{S}}\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{ff}})+\sigma^2\mathrm{tr}(\boldsymbol{W})+\mathrm{tr}\left(\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\right) \tag{6}$$

$$y_{\mathrm{D}}=\sqrt{P_{\mathrm{S}}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{w}x+\boldsymbol{w}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{c}^{\mathrm{H}})\boldsymbol{n}_{\mathrm{R}}+n_{\mathrm{D}} \tag{7}$$

$$\boldsymbol{y}_{\mathrm{E}}=\sqrt{P_{\mathrm{S}}}\boldsymbol{G}_f^{\mathrm{H}}\boldsymbol{w}x+\boldsymbol{G}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\boldsymbol{n}_{\mathrm{R}}+\boldsymbol{G}^{\mathrm{H}}\boldsymbol{n}_{\mathrm{a}}+\boldsymbol{n}_{\mathrm{E}} \tag{8}$$

根据式(7)，式(8)可以得出在目的接收端和窃听端所能达到的信息传输速率分别为

$$R_{\mathrm{D}}(\boldsymbol{W},\boldsymbol{\Sigma})=\frac{1}{2}\lg\left(1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{c}^{\mathrm{H}})\mathrm{diag}(\boldsymbol{c})\boldsymbol{w}}\right) \tag{9}$$

$$R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{\Sigma})=\frac{1}{2}\lg\det\left(\boldsymbol{I}+\frac{P_{\mathrm{S}}\boldsymbol{G}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_f}{\sigma^2\boldsymbol{I}+\sigma^2\boldsymbol{G}^{\mathrm{H}}\widetilde{\boldsymbol{W}}\widetilde{\boldsymbol{W}}^{\mathrm{H}}\boldsymbol{G}+\boldsymbol{G}^{\mathrm{H}}\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\boldsymbol{G}}\right) \tag{10}$$

这里，产生标量系数1/2的原因是采用中继方式传输时，源和中继各使用一半的信道资源进行传输。记 $\boldsymbol{R}_{\mathrm{cc}}\triangleq\mathrm{diag}\left(|c_{\mathrm{R},1}|^2\ |c_{\mathrm{R},2}|^2\ \cdots\ |c_{\mathrm{R},N}|^2\right)$，$\boldsymbol{N}_{\mathrm{EP}}\triangleq\sigma^2\boldsymbol{I}+\sigma^2\boldsymbol{G}^{\mathrm{H}}\mathrm{dd}(\boldsymbol{W})\boldsymbol{G}+\boldsymbol{G}^{\mathrm{H}}\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\boldsymbol{G}$，代入式(9)，式(10)得

$$R_{\mathrm{D}}(\boldsymbol{W},\boldsymbol{\Sigma})=\frac{1}{2}\lg\left(1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}})}\right) \tag{11}$$

$$R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{\Sigma})=(1/2)\lg\det(\boldsymbol{I}+P_{\mathrm{S}}\boldsymbol{N}_{\mathrm{EP}}^{-1}\boldsymbol{G}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_f) \tag{12}$$

因此，系统可获得的最大保密速率[12]可以表示为

$$R_{\mathrm{S}}=\max\{0,R_{\mathrm{D}}(\boldsymbol{W},\boldsymbol{\Sigma})-R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{\Sigma})\} \tag{13}$$

这里，保密速率是关于中继波束赋形加权矩阵 $\boldsymbol{W}$ 和人工噪声协方差矩阵 $\boldsymbol{\Sigma}$ 的函数。在源端发送功率和中继总功率固定的情况下，通过中继优化波束加权矩阵和人工噪声方差矩阵，可以使保密速率最大。

3　联合波束赋形和人工噪声的鲁棒性设计方案

3.1 设计方案的数学表述

假设已知 R-E 信道的 CSI 的不准确范围，利用零空间人工噪声和放大转发的中继波束赋形方法，基于半定规划理论，对中继的波束赋形加权矩阵和人工噪声协方差矩阵进行联合优化，以使在 CSI 误差最大的情况(称之为“最差情况”)下，减少可能勾结的多个窃听者获得的信息速率，使系统保密速率达到最大。这种最差情况下的优化方案称为零空间人工噪声辅助的保密速率最大化的鲁棒性设计(null-AN-aided Worst-Case Robust Secrecy Rate Maximization, null-AN-aided WCR-SRM)。假设

$$\boldsymbol{G}=\overline{\boldsymbol{G}}+\Delta\boldsymbol{G} \tag{14}$$

其中，$\boldsymbol{G}$ 表示 R-E 链路的实际 CSI，$\overline{\boldsymbol{G}}$ 表示获得的 R-E 链路的 CSI 估计值，$\Delta\boldsymbol{G}$ 表示信道的 CSI 误差，且该误差在一个范围内，可表示为[13]

$$\Delta\boldsymbol{G}^{\mathrm{H}}\boldsymbol{K}\Delta\boldsymbol{G}\le 1 \tag{15}$$

其中，$\boldsymbol{K}=(1/\varepsilon)\boldsymbol{I}$ 是正定的 $J\times J$ 阶矩阵，$\varepsilon>0$ 决定了窃听信道不准确范围的大小。式(15)可以等效为

$$\left\|\Delta\boldsymbol{G}\right\|_{\mathrm{F}}\le\varepsilon \tag{16}$$

因此，WCR-SRM 设计问题可以表述为

$$\left.\begin{aligned}R_{\mathrm{S}}=&\max_{\boldsymbol{W}\succeq\boldsymbol{0},\boldsymbol{\Sigma}\succeq\boldsymbol{0}}\ \left\{R_{\mathrm{D}}(\boldsymbol{W},\boldsymbol{\Sigma})-R_{\mathrm{E}}^{\mathrm{ws}}(\boldsymbol{W},\boldsymbol{\Sigma})\right\}\\ \text{s.t.}\ \ &P_{\mathrm{S}}\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{ff}})+\sigma^2\mathrm{tr}(\boldsymbol{W})+\mathrm{tr}\left(\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\right)\le P\end{aligned}\right\} \tag{17}$$

其中，$R_{\mathrm{E}}^{\mathrm{ws}}(\boldsymbol{W},\boldsymbol{\Sigma})=\max\limits_{\boldsymbol{G}\in\boldsymbol{\Omega}}\ (1/2)\lg\det(\boldsymbol{I}+P_{\mathrm{S}}\boldsymbol{N}_{\mathrm{EP}}^{-1}\boldsymbol{G}_f^{\mathrm{H}}\cdot\boldsymbol{W}\boldsymbol{G}_f)$ 是窃听者在 CSI 误差最大情况下所获得的信息速率，$\boldsymbol{\Omega}\triangleq\{\boldsymbol{G}\mid\boldsymbol{G}=\overline{\boldsymbol{G}}+\Delta\boldsymbol{G},\left\|\Delta\boldsymbol{G}\right\|_{\mathrm{F}}\le\varepsilon\}$ 是所有可能的窃听信道增益的集合。问题式(17)是关于最优化 $(\boldsymbol{W},\boldsymbol{\Sigma})$ 的一个安全设计，系统所得出的实际保密速率一定不小于本方案所得出的保密速率。

3.2 优化问题的求解

由于 $R_{\mathrm{E}}^{\mathrm{ws}}(\boldsymbol{W},\boldsymbol{\Sigma})$ 的复杂度比较高，本文引入一个松弛变量 β，以简化优化问题的目标函数。假设窃听端所获得的信息速率有一个上限 $(1/2)\lg\beta$，则式(17)的 null-AN-aided WCR-SRM 优化问题可以写为

$$R_{\mathrm{S}}=\max_{\boldsymbol{W}\succeq\boldsymbol{0},\boldsymbol{\Sigma}\succeq\boldsymbol{0},\beta\ge1}\ \frac{1}{2}\lg\left(1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}})}\right)-\frac{1}{2}\lg\beta \tag{18}$$

$$\text{s.t.}\quad(1/2)\lg\det(\boldsymbol{I}+P_{\mathrm{S}}\boldsymbol{N}_{\mathrm{EP}}^{-1}\boldsymbol{G}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_f)\le(1/2)\lg\beta,\ \ \forall\boldsymbol{G}\in\boldsymbol{\Omega} \tag{18a}$$

$$P_{\mathrm{S}}\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{ff}})+\sigma^2\mathrm{tr}(\boldsymbol{W})+\mathrm{tr}(\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}})\le P \tag{18b}$$

可以看出，由于变量 $\boldsymbol{G}$ 包含于一个集合 $\boldsymbol{\Omega}$ 中，因此约束条件式(18a)对应于多个不等式。为了对优化问题进行简化，可以利用强化松弛的方法对式(18a)进行等效变换。

命题 1 当 $\boldsymbol{W}\succeq\boldsymbol{0}$, $\boldsymbol{\Sigma}\succeq\boldsymbol{0}$ 时，由式(18a)可以推导出式(19)

$$(\beta-1)\boldsymbol{N}_{\mathrm{EP}}/P_{\mathrm{S}}\succeq\boldsymbol{G}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{G}_f,\ \forall\boldsymbol{G}\in\boldsymbol{\Omega}\tag{19}$$

特殊地，当 $\nu(\boldsymbol{W})=1$ 时，式(18a)与式(19)是等价的(证明可参考文献[5])。

令 $\boldsymbol{X}=\Delta\boldsymbol{G}$，则 $\boldsymbol{G}=\overline{\boldsymbol{G}}+\boldsymbol{X}$，$\boldsymbol{G}_f^{\mathrm{H}}=\boldsymbol{G}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{f})=(\overline{\boldsymbol{G}}+\boldsymbol{X})^{\mathrm{H}}\mathrm{diag}(\boldsymbol{f})$，式(19)又可写为

$$\begin{aligned}&(\beta-1)(\sigma^2\boldsymbol{I}+(\overline{\boldsymbol{G}}+\boldsymbol{X})^{\mathrm{H}}\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}(\overline{\boldsymbol{G}}+\boldsymbol{X}))\\&\quad\succeq(\overline{\boldsymbol{G}}+\boldsymbol{X})^{\mathrm{H}}\boldsymbol{M}(\overline{\boldsymbol{G}}+\boldsymbol{X}),\quad\forall\boldsymbol{G}\in\boldsymbol{\Omega}\\&\quad\Leftrightarrow\boldsymbol{X}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{X}+\boldsymbol{X}^{\mathrm{H}}\boldsymbol{B}+\boldsymbol{B}^{\mathrm{H}}\boldsymbol{X}+\boldsymbol{C}\succeq\boldsymbol{0},\ \forall\boldsymbol{G}\in\boldsymbol{\Omega}\end{aligned}\tag{20}$$

这里，$\boldsymbol{A}=(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}$，$\boldsymbol{B}=[(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}]\overline{\boldsymbol{G}}$，$\boldsymbol{C}=(\beta-1)(\sigma^2\boldsymbol{I}+\overline{\boldsymbol{G}}^{\mathrm{H}}\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}\overline{\boldsymbol{G}})-\overline{\boldsymbol{G}}^{\mathrm{H}}\boldsymbol{M}\overline{\boldsymbol{G}}$，$\boldsymbol{M}=P_{\mathrm{S}}\mathrm{diag}(\boldsymbol{f})\boldsymbol{W}\mathrm{diag}(\boldsymbol{f}^{\mathrm{H}})-\sigma^2(\beta-1)\mathrm{dd}(\boldsymbol{W})$。

引理 1[14] 令 $f(\boldsymbol{X})=\boldsymbol{X}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{X}+\boldsymbol{X}^{\mathrm{H}}\boldsymbol{B}+\boldsymbol{B}^{\mathrm{H}}\boldsymbol{X}+\boldsymbol{C}$，$\boldsymbol{D}\succeq\boldsymbol{0}$，则有式(21)成立。

$$\begin{aligned}&f(\boldsymbol{X})\succeq\boldsymbol{0},\ \forall\boldsymbol{X}\in\{\boldsymbol{X}\mid\mathrm{tr}(\boldsymbol{D}\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}})\le1\},\\&\quad\Leftrightarrow\begin{bmatrix}\boldsymbol{C}&\boldsymbol{B}^{\mathrm{H}}\\\boldsymbol{B}&\boldsymbol{A}\end{bmatrix}-t\begin{bmatrix}\boldsymbol{I}&\boldsymbol{0}\\\boldsymbol{0}&-\boldsymbol{D}\end{bmatrix}\succeq\boldsymbol{0},\ \exists\ t\ge0\end{aligned}\tag{21}$$

由于 $\|\Delta\boldsymbol{G}\|_{\mathrm{F}}=\|\boldsymbol{X}\|_{\mathrm{F}}\le\varepsilon$，即 $\mathrm{tr}(\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}})\le\varepsilon^2$。令 $\boldsymbol{D}=(1/\varepsilon^2)\boldsymbol{I}$，满足 $\mathrm{tr}(\boldsymbol{D}\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}})\le1$。将引理 1 应用到式(20)可得

$$\boldsymbol{T}(\beta,\boldsymbol{W},\boldsymbol{\Sigma},t)=\begin{bmatrix}[\sigma^2(\beta-1)-t]\boldsymbol{I}+\overline{\boldsymbol{G}}^{\mathrm{H}}[(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}]\overline{\boldsymbol{G}}&\overline{\boldsymbol{G}}^{\mathrm{H}}[(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}]\\[(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}]\overline{\boldsymbol{G}}&(\beta-1)\boldsymbol{U}_{\perp}\boldsymbol{\Sigma}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\boldsymbol{M}+(t/\varepsilon^2)\boldsymbol{I}\end{bmatrix}\succeq\boldsymbol{0},\ \exists\ t\ge0\tag{22}$$

用式(22)代替约束条件式(18a)得到优化问题式(18)的一个紧松弛问题，可以表示为

$$\begin{aligned}&\overline{R}_{\mathrm{S}}=\max_{\boldsymbol{W}\succeq\boldsymbol{0},\boldsymbol{\Sigma}\succeq\boldsymbol{0},t,\beta\ge1}\ \frac{1}{2}\lg\left[\left(1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}})}\right)\Big/\beta\right],\\&\text{s.t.}\quad\boldsymbol{T}(\beta,\boldsymbol{W},\boldsymbol{\Sigma},t)\succeq\boldsymbol{0},t\ge0,\ (18\text{b})\end{aligned}\tag{23}$$

其中，$\overline{R}_{\mathrm{S}}$ 是问题式(23)的最优目标函数值。式(23)是式(18)的一个紧松弛问题，即 $R_{\mathrm{S}}=\overline{R}_{\mathrm{S}}$(证明过程参考文献[5])。

另外，由于在实际的无线通信系统中保密速率 $\overline{R}_{\mathrm{S}}\ge0$，则 β 应满足

$$\begin{aligned}\beta&\le1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}})}\le1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2}\\&\le1+\frac{P_{\mathrm{S}}}{\sigma^2}\mathrm{tr}(\boldsymbol{W})\|\boldsymbol{c}_f\|^2\le1+\frac{P_{\mathrm{S}}}{\sigma^2}\frac{P}{\sigma^2}\|\boldsymbol{c}_f\|^2\\&=1+P_{\mathrm{S}}P\|\boldsymbol{c}_f\|^2/\sigma^4\end{aligned}\tag{24}$$

由于 β 在范围 $[1,\ \alpha_0^{-1}]$ 内变化，$\alpha_0=1/(1+P_{\mathrm{S}}P||\boldsymbol{c}_f||^2/\sigma^4)$，式(23)的优化问题可以转换为 1 维变量优化问题，通过 1 维线性搜索方法来求解。

$$\left.\begin{aligned}&\overline{\gamma}=\max_{\alpha}\ \varphi(\alpha)\\&\text{s.t.}\ \ \alpha_0\le\alpha\le1\end{aligned}\right\}\tag{25}$$

$$\left.\begin{aligned}&\varphi(\alpha)=\max_{\boldsymbol{W},\boldsymbol{\Sigma}}\alpha\left(1+\frac{P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{W}\boldsymbol{c}_f}{\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}})}\right)\\&\text{s.t.}\quad\boldsymbol{T}(\alpha^{-1},\boldsymbol{W},\boldsymbol{\Sigma},t)\succeq\boldsymbol{0},\ t\ge0\\&\qquad\boldsymbol{W}\succeq\boldsymbol{0},\ \boldsymbol{\Sigma}\succeq\boldsymbol{0},\ (18\text{b})\end{aligned}\right\}\tag{26}$$

这里，$\alpha=1/\beta$，$\lg\overline{\gamma}=2\overline{R}_{\mathrm{S}}$，$\varphi(\alpha)$ 是优化问题式(23)在 β 给定的情况下的另外一种形式。

式(26)的目标函数为拟凸函数，为了把式(26)转化为凸优化问题[15]，我们采用半定松弛方法[16]，并忽略隐含的约束条件 $\nu(\boldsymbol{W})=1$。同时根据 Charnes-Cooper 变换[17]，令 $\xi=\alpha(\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{W}\boldsymbol{R}_{\mathrm{cc}}))^{-1}$，$\boldsymbol{Q}=\xi\boldsymbol{W}$，$\boldsymbol{F}=\xi\boldsymbol{\Sigma}$，$\lambda=\xi t$，从而式(26)的优化问题等价于

$$\left.\begin{aligned}&\varphi(\alpha)=\max_{\boldsymbol{Q},\boldsymbol{F},\xi}\ \ \xi\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{Q}\boldsymbol{R}_{\mathrm{cc}})+P_{\mathrm{S}}\boldsymbol{c}_f^{\mathrm{H}}\boldsymbol{Q}\boldsymbol{c}_f\\&\text{s.t.}\quad\xi\sigma^2+\sigma^2\mathrm{tr}(\boldsymbol{Q}\boldsymbol{R}_{\mathrm{cc}})=\alpha\\&\qquad\widetilde{\boldsymbol{T}}(\boldsymbol{Q},\boldsymbol{F},\xi,\alpha,\lambda)\succeq\boldsymbol{0},\ \ \lambda\ge0\\&\qquad P_{\mathrm{S}}\mathrm{tr}(\boldsymbol{Q}\boldsymbol{R}_{\mathrm{ff}})+\sigma^2\mathrm{tr}(\boldsymbol{Q})+\mathrm{tr}(\boldsymbol{U}_{\perp}\boldsymbol{F}\boldsymbol{U}_{\perp}^{\mathrm{H}})\le\xi P\\&\qquad\boldsymbol{Q}\succeq\boldsymbol{0},\ \boldsymbol{F}\succeq\boldsymbol{0}\end{aligned}\right\}\tag{27}$$

其中，$\widetilde{\boldsymbol{M}}=\alpha\xi\boldsymbol{M}=\alpha P_{\mathrm{S}}\mathrm{diag}(\boldsymbol{f})\boldsymbol{Q}\mathrm{diag}(\boldsymbol{f}^{\mathrm{H}})-\sigma^2(1-\alpha)\cdot\mathrm{dd}(\boldsymbol{Q})$，

$$\widetilde{\boldsymbol{T}}(\boldsymbol{Q},\boldsymbol{F},\xi,\alpha,\lambda)=\begin{bmatrix}[\sigma^2\xi(1-\alpha)-\lambda\alpha]\boldsymbol{I}+\overline{\boldsymbol{G}}^{\mathrm{H}}[(1-\alpha)\boldsymbol{U}_{\perp}\boldsymbol{F}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\widetilde{\boldsymbol{M}}]\overline{\boldsymbol{G}}&\overline{\boldsymbol{G}}^{\mathrm{H}}[(1-\alpha)\boldsymbol{U}_{\perp}\boldsymbol{F}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\widetilde{\boldsymbol{M}}]\\[(1-\alpha)\boldsymbol{U}_{\perp}\boldsymbol{F}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\widetilde{\boldsymbol{M}}]\overline{\boldsymbol{G}}&(1-\alpha)\boldsymbol{U}_{\perp}\boldsymbol{F}\boldsymbol{U}_{\perp}^{\mathrm{H}}-\widetilde{\boldsymbol{M}}+(\lambda\alpha/\varepsilon^2)\boldsymbol{I}\end{bmatrix}$$

容易看出，式(27)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[18]，从而该问题是一个 SDP[15]问题，可利用已有的 CVX 工具箱[19]求解出全局最优解。由于变量 α 位于区间 $[\alpha_0,1]$ 内，问题式(25)是一个关于单变量 α 的优化问题，可通过 1 维线性搜索方法进行求解。这样，对于区间内任意一个固定的 α_i，都可以利用 CVX 工具箱解决式(27)的优化问题，从而计算出对应的 $\varphi(\alpha_i)$。然后可以得出最大的那个 $\varphi(\alpha)$，对应的 α 值即为问题式(25)的最优解。由于不需求导的 1 维线性搜索方法一般仅限于优化函数单谷(峰)函数的情况，而本文中的优化函数为多峰函数，无法应用常用的 1 维搜索算法

进行求解。因此在本文中外层采用全局搜索的方法求得其最优解。求解出问题式(25)的最优解后，对应地就可从式(27)的 SDP 问题中输出$(\boldsymbol{Q}^*,\boldsymbol{F}^*,\xi^*)$，从而得出$\boldsymbol{W}^*$和$\boldsymbol{\Sigma}^*$。另外，由于使用了半定松弛方法，在问题转化过程中忽略了约束条件$\nu(\boldsymbol{W})=1$。可通过拉格朗日法验证优化问题的 Karush-Kuhn-Tucker(KKT)条件[15]，证明最优解$\boldsymbol{W}^*$一定满足约束条件非零特征值个数等于 1，证明过程可参考文献[11]和文献[20]，限于篇幅，这里不再给出。

3.3 算法总结

由于本文方案的推导过程比较复杂，因此这里再对优化步骤总结如下：(1)根据信道系数$\boldsymbol{f}$，$\boldsymbol{c}$，$\boldsymbol{G}$，计算出 1 维变量α的线性搜索区间$[\alpha_0,1]$；(2)外层采用全局搜索的方法。首先初始化搜索变量α_0，并给出搜索步长δ。然后针对每一个$\alpha_i=\alpha_{i-1}+\delta,\alpha_i\le 1$，内层利用 CVX 工具箱解决 SDP 问题式(28)，可求解出对应的最大保密速率值$R(\alpha_i)=(1/2)\cdot\lg\varphi(\alpha_i)$。其中，$\delta$为一小正数，决定优化结果的精度；(3)根据步骤(2)可得到不同α下的多个保密速率值的最大值$R_{\max}(\alpha^{\mathrm{o}})=\max\{R(\alpha_1),R(\alpha_2),\cdots,R(\alpha_i),\cdots\}$，即是可获得的最大保密速率，相应的 1 维变量最优值α^{o}对应的$\boldsymbol{W}^*$和$\boldsymbol{\Sigma}^*$就是中继波束赋形加权矩阵和人工噪声协方差矩阵的最优解。

4 仿真结果及性能分析

在仿真中，假设信道是瑞利信道，增益服从均值为 0、方差为 1 的独立复高斯分布，所有节点的噪声功率均为$\sigma^2=0$ dBW，并且只考虑小尺度衰落。仿真中使用 CVX[19]工具箱来解决 SDP 问题。

4.1 算法的搜索性能仿真

图 2 是算法的外层使用全局搜索的 1 维搜索方法，内层使用 SDP 方法时，不用搜索步长下可达到的最大保密速率的仿真曲线图。仿真中设置源端的发送功率为$P_{\mathrm{S}}=10$ dBW，中继发送总功率为 20 dBW 和 40 dBW，中继个数$N=6$，窃听者个数$J=2$。共进行了 500 次独立的蒙特卡洛仿真。从仿真结果曲线可以看出，当外层搜索次数越多，即搜索步长越小，得到的中继波束赋形加权矩阵和人工噪声协方差矩阵越准确，获得的保密速率越高。当外层搜索次数达到 10 次以上，即外层的全局搜索使用的搜索步长$\delta=0.1$以下时，系统可获得的保密速率值就已经很接近最大值，而搜索次数在 16 次以上，搜索次数再增加，保密速率的增加已不明显。本节的后续仿真中的搜索次数均设为 20，即搜索步长为$\delta=0.05$。

4.2 不同方案下的保密速率性能仿真及分析

以下所有仿真均是进行 2000 次独立的蒙特卡洛仿真，并对仿真结果取平均得到保密速率。

图 3 是不同窃听者个数、不同的窃听端 CSI 不准确性范围的情况下，中继消耗总功率与平均保密容量的关系曲线。仿真中固定设置源端的发送功率为$P_{\mathrm{S}}=10$ dBW，中继个数$N=6$。从仿真结果可以看到，对于固定的中继总功率P，窃听者数量 J 增加，使得窃听端所获得的保密速率增大，导致平均保密容量会减少。但是，随着中继总功率P的增加，不同窃听者个数下的平均保密容量的差距减少，这是因为P增加时，就有足够的功率用于发送人工噪声，从而减少信息的泄漏量。CSI 不准确性范围ε越小，得到的平均保密容量越大。这是因为ε越小，表示设计$\boldsymbol{W}$和$\boldsymbol{\Sigma}$时所使用的信道 CSI 估计值越接近真实值，最终得到的保密速率值越高。本文的方案具有很好的鲁棒性，CSI 的误差对最终性能影响并不严重。如图所示，当$\varepsilon=0.01$和$\varepsilon=0.2$时，后者的 CSI 不准确度是前者的 20 倍，而两种情况下应用本方案获得的保密速率值差距并不明显；同时，$\varepsilon=0.01$时本方案的性能与完美 CSI 时的方案的性能基本一致，体现了本方案较好的抵抗不准确 CSI 的能力。与没有人工噪声的 WCR(noAN-WCR)方案相比，随着中继消耗总功率P的增加，两种方案得出的保密速率曲线均是先增加，后趋于平行。这是因为当P较小时，较多的功率用于放大转发信号，没有多余的功率用来产生人工噪声，因此二者的性能基本一致。当P增大时，本文方案的保密速率继续上升，而 WCR 方案则增长缓慢。这是因为中继有更多的功率发送零空间人工噪声，能有效减少信息泄漏；当P增大到一定程度时，保密的速率增长趋于平缓，这是因为源端的发送功率固定，限制了信息的速率。

图 4 中设置中继总功率$P=40$ dBW , CSI 不准确性范围$\varepsilon=0.2$。在中继总功率足够大、CSI 不准确性范围固定的情况下，给出不同中继数量、不同源节点发送功率、不同窃听者个数时保密速率的仿真结果。从仿真结果可知，随着源节点发送功率的增加，保密速率也会增大，因为源端发送的信息速率增加了。从横轴方向看，随着中继个数的增加，保密速率不断增大，这是因为增加中继节点相当于增加发送天线，相应可增加阵列增益，目的端接收到的信息量多于信息的泄漏量，并且两者的差距逐渐增大，使得总的保密速率相应增大。但是当中继个数增加到 10 个时，保密速率基本不再增加。这是因为中继数量达到一定程度时，阵列增益已经相当

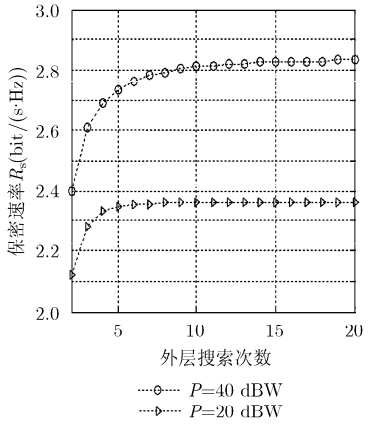

图 2 搜索次数对保密速率的影响

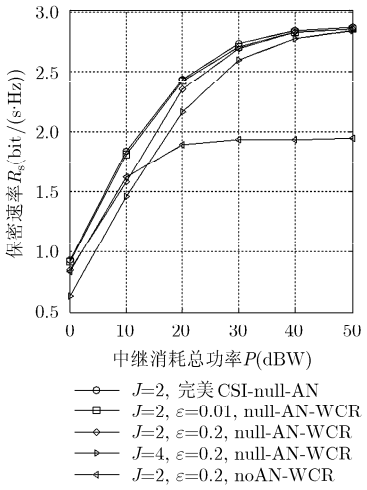

图 3 不同方案下中继消耗总功率对平均保密容量的影响

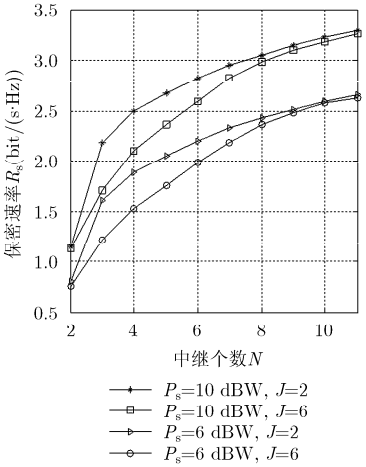

图 4 null-AN-aided WCR-SRM 方案下中继个数与保密速率的关系

可观，再增加中继数量时，阵列增益的增加已不明显。从纵轴方向看，当中继个数 $N=2$ 时，中继处的发送天线数过少，基本上没有阵列增益，不能将人工噪声波束准确指向窃听者，而传输信息的信号的波束也不够窄，因此无论是窃听者数目 $J=2$ 或 $J=6$，窃听端都能获得较大的信息量，这样能获得的保密速率都很低，$J=6$ 时保密速率更低一点。当中继个数增加时，中继天线数增多，阵列增益逐渐增大，人工噪声波束能更准确地指向窃听者。但是窃听者越多，需要的干扰波束越多。而波束数量增加，则每个波束的指向性能会相应下降，对窃听者的干扰效果会有所下降。因此窃听者数量越多，其可窃取到的信息量就越大，故 $J=6$ 时的保密速率要低于 $J=2$ 时的保密速率。但当中继个数增加时，多干扰波束的性能持续改善，因此 $J=2$ 和 $J=6$ 的性能差距在逐渐减小。到 $N=11$ 时，阵列增益已经相当可观，即使是在多个干扰波束的情况下，每个波束的效果也较好，因而在 $J=2$ 和 $J=6$ 时泄露的信息量差别已不大，相应能获得的保密速率值也趋近于相同。

5 结束语

本文对不存在直接链路的中继网络中的物理层安全传输技术进行研究。针对窃听端 CSI 不准确的情况，给出了一种中继波束赋形加人工噪声的传输方案，并采用全局搜索和半定规划方法对最差情况下的人工噪声的协方差和中继波束赋形矢量进行联合优化。同时也给出了相应的 WCR-SRM 保密速率的理论值。对于不同中继个数、不同窃听者个数、不同中继总功率、不同源节点发送功率以及不同的窃听信道 CSI 的不准确性范围等情况的保密速率进行了仿真和分析。仿真结果表明，采用本文的传输方案，即使在无法获得准确的窃听端 CSI 的情况下，系统的保密速率也能得到明显的改善。在实际运用中，可能会存在 S-E 间的直连链路，此情况下本文方案不再适用。在下一步的研究工作中，可针对 S-E 间存在直连链路的情况，对算法进行改进，对第 1 阶段传输中窃听者的接收性能进行抑制，提高保密传输速率。

参 考 文 献

[1] Shannon C E. Communication theory of secrecy system[J]. *Bell System Technical Journal*, 1949, 28(4): 656–715.

[2] Leung-Yan-Cheong S K and Hellman M E. The Gaussian wiretap channel[J]. *IEEE Transactions on Information Theory*, 1978, 24(4): 451–456.

[3] Yang Ye, Li Qiang, Ma W K, *et al*.. Cooperative secure beamforming for AF relay networks with multiple eavesdroppers[J]. *IEEE Signal Processing Letters*, 2013, 20(1): 35–38.

[4] Zhang Jun-wei and Gursoy M C. Collaborative relay beamforming for secrecy[C]. IEEE International Conference on Communications, Cape Town, 2010: 1–5.

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

[6] Wang Hui-ming, Yin Qin-ye, and Xia Xiang-gen. Distributed beamforming for physical-layer security of two-way relay networks[J]. *IEEE Transactions on Signal Processing*, 2012, 60(7): 3532–3545.

[7] Goel S and Negi R. Secret communication in presence of colluding eavesdroppers[C]. IEEE Military Communications Conference, Atlantic City, NJ, 2005, Vol.3: 1501–1506.

[8] Pinto P C, Barros J, and Win M Z. Secure communication in stochastic wireless networks—part II: maximum rate and collusion[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(1): 139–147.

[9] Pinto P C, Barros J, and Win M Z. Wireless physical-layer security: the case of colluding eavesdroppers[C]. IEEE International Symposium on Information Theory, Seoul, 2009: 2442–2446.

[10] Cai Chun-xiao, Cai Yue-ming, Yang Wei-wei, *et al*.. Secure connectivity using randomize-and-forward strategy in cooperative wireless networks[J]. *IEEE Communications Letters*, 2013, 17(7): 1340–1343.

[11] Wang Chao and Wang Hui-ming. Robust joing beamforming and jamming for secure AF networks: low complexity design[OL]. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6847741, 2015.

[12] Liang Ying-bin, Gerhard K, Vincent H, *et al*.. Compound wiretap channels[J]. *EURASIP Journal on Wireless Communications and Networking*, 2009, 3(1): 53–56.

[13] Li Quan-zhong, Zhang Qi, and Qin Jia-yin. Robust beamforming for cognitive multi-antenna relay networks with bounded channel uncertainties[J]. *IEEE Transactions on Communications*, 2014, 62(2): 478–487.

[14] Luo Z Q, Sturm J F, and Zhang S. Multivariate nonnegative quadratic mappings[J]. *Society for Industrial and Applied Mathematics Journal on Optimization*, 2004, 14(4): 1140–1162.

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

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

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

[18] Boyd S, Ghaoui L E, Feron E, *et al*.. Linear Matrix Inequalities in System and Control Theory[M]. Philadelphia: Society of Industrial and Applied Mathematics, 1994: 7–9.

[19] Grant M and Boyd S. CVX: Matlab software for disciplined convex programming[OL]. http://cvxr.com/cvx/, 2013.

[20] Liao Wei-cheng, 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.

雷维嘉： 男，1969 年生，博士，教授，研究方向为无线和移动通信技术.

左莉杰： 女，1989 年生，硕士生，研究方向为无线通信和物理层安全.

江　雪： 女，1988 年生，硕士生，研究方向为物理层安全.

谢显中： 男，1966 年生，博士生导师，教授，研究方向为无线和移动通信技术.