第 48 卷第 5 期
2016 年 10 月

南 京 航 空 航 天 大 学 学 报
Journal of Nanjing University of Aeronautics & Astronautics

Vol. 48 No. 5
Oct. 2016

DOI:10.16356/j.1005-2615.2016.05.004

非理想条件下认知蜂窝网络物理层安全传输方案

张 涛[1] 杨炜伟[1] 杨 爽[1] 柴新代[2]

(1.解放军理工大学通信工程学院,南京,210007; 2.中国人民解放军 61932 部队,北京,100080)

摘要:认知无线电技术可以解决频谱实际利用率不高的问题,作为关键技术之一被引入下一代蜂窝移动网络中。同时,由于无线信道的广播特性和不确定性,非理想条件下的信息安全传输问题不可回避。由于认知无线网络中主、次网络间存在相互干扰,文中借鉴干扰对准思想,高效地管理和利用主、次网络之间的相互干扰,通过优化设计发送预编码矩阵,尽量避免干扰合法用户接收,同时尽可能地对窃听节点实施阻塞干扰。Monte Carlo 仿真验证了非理想条件下干扰对准设计预编码矩阵的优越性,同时也证实了信道估计精度在提高蜂窝移动系统传输性能和安全性能方面的重要性。

关键词:非理想条件;认知蜂窝网络;干扰对准;中断概率

中图分类号:TN828.6 **文献标志码**:A **文章编号**:1005-2615(2016)05-0637-05

Secure Transmission Protocol in Cognitive Cellular Networks Under Imperfect Conditions

Zhang Tao[1], *Yang Weiwei*[1], *Yang Shuang*[1], *Chai Xindai*[2]

(1. College of Communications Engineering, PLA University of Science and Technology, Nanjing, 210007, China; 2. Unit 61932 of PLA, Beijing, 100080, China)

Abstract: Cognitive radio possesses the ability of solving the low spectrum utilization problem, which is introduced to the next-generation cellular networks. And the security under imperfect conditions should not be neglected due to the broadcast and uncertain characteristics of the wireless channels. In cognitive radio systems, interference between primary users and secondary users greatly affects the system performance. Based on interference alignment technique, the mutual interference between the primary network and the second network is efficiently managed and utilized, and the optimal precoding/beamforming schemes are designed to enhance the physical layer security performance. Finally, Monte Carlo simulations validate and prove the feasibility of the application of interference alignment technique in the next-generation cellular networks under imperfect conditions.

Key words: imperfect conditions; cognitive cellular networks; interference alignment; outage probability

随着信息时代的飞速发展,无线通信已经融入 到人类社会的各个方面,一方面,由于电子商务、社

基金项目:国家自然科学基金(61471393)资助项目;2013 年中国博士后科学基金第六批特别项目(2013T60912)资助项目。

收稿日期:2016-01-29;**修订日期**:2016-04-24

通信作者:杨炜伟,男,副教授,E-mail:wwyang1981@163.com。

引用格式:张涛,杨炜伟,杨爽,等.非理想条件下认知蜂窝网络物理层安全传输方案[J].南京航空航天大学学报,2016,48(4):637-641. Zhang Tao, Yang Weiwei, Yang Shuang, et al. Secure transmission protocol in cognitive cellular networks under imperfect conditions[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2016, 48(4): 637-641.

交网络、公共安全等对无线服务的需求持续升高，导致可用的无线频谱资源十分紧张，因此认知无线电技术得到了广泛的关注。另一方面，由于无线传输媒介的开放性、信息传输的无界性、无线网络的互动性等特点，无线通信在给人们生活带来极大便利的同时，也使得用户的个人信息、个人隐私、财产安全受到了严重威胁。鉴于认知无线网络中主、次网络间存在的相互干扰，人们利用多天线技术引入了预编码、集中式或分布式波束赋形、协同人工干扰等信号处理方法，用于增强认知无线网络的物理层安全性能。文献[1]以认知网络安全速率为目标，设计了主网络干扰温度约束下多天线认知网络的最优和次优波束赋形方案。文献[2]将人工干扰应用于认知无线传感器网络，以改善网络的安全中断性能。进而，文献[3]考虑配置多中继的两跳协同认知网络，研究了主、次网络之间的相互干扰对安全速率的影响，并通过设计中继处不同的分布式波束赋形向量来增强物理层安全性能。

面向下一代移动应用的认知蜂窝网络中有复杂的网络结构、众多的网络节点，大大扩展了信号处理的可用维度，为通过信号处理增强物理层安全性能提供了可能。文献[4]中设计了一种联合协同人工干扰和波束赋形的混合预编码传输方案，可明显改善协同无线网络的物理层安全性能。类似地，在认知蜂窝网络中进行联合信号处理，充分发挥各种信号处理方法的优势亦是改善物理层安全性能的有效途径之一。值得一提的是，干扰对准技术可将多个发送信号在多个信号维度上进行编码传输，通过联合设计收发信机可以在任意接收端将干扰信号对准到某个低维度的信号子空间中，从而实现有用信号在其他信号子空间中无干扰传输[5]，这为增强物理层安全性能的联合信号处理提供参考。文献[6]将干扰对准思想应用于协同无线网络中，通过合法用户的发送预编码矩阵、接收滤波矩阵设计将协同人工干扰信号对准窃听节点，且在合法接收端实现无干扰传输，提高了系统的安全性能。上述的研究工作主要是在信道信息精确已知下进行的，在非理想条件下的认知蜂窝网络中如何借鉴干扰对准思想，高效地管理和利用主、次网络之间的相互干扰及协同人工干扰，设计优化的预编码或波束赋形方案来增强物理层安全性能值得深入研究。

本文在非理想的认知蜂窝系统中借鉴干扰对准思想，高效地管理和利用主、次网络之间的相互干扰，通过迭代求解优化设计发送预编码矩阵和接收滤波矩阵，在避免干扰合法用户接收的同时尽可能对窃听节点实施阻塞干扰。通过理论分析和 Monte Carlo 仿真发现：基于干扰对准设计预编码矩阵的系统性能明显优于随机预编码设计的系统性能，但随着信道非精确程度的增大，干扰对准方案相较于随机预编码设计的性能下降严重，揭示了信道估计精度对系统设计的重要意义。

1 系统模型

1.1 干扰对准模型

本文分析的认知网络无线下的系统模型如图 1 所示，其次用户系统有一个发送者 C_Tx，一个接收者C_Rx，主用户系统由一个发送者 P_Tx 和一个接收者 P_Rx 组成。主用户发送端和接收端分别配备 M_P 和 N_P 根天线，次用户发送端和接收端分别配备 M_C 和 N_C 根天线，同时考虑存在窃听节点(Eve)窃听次网络的传输信息。

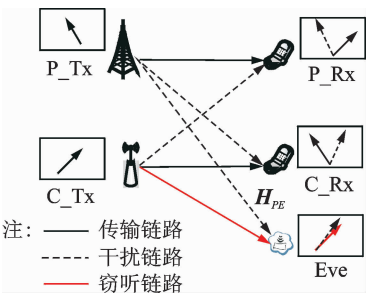

图 1 系统模型

Fig. 1 System model

假定主网络中发送预编码矩阵为 $\boldsymbol{U}_P$，接收滤波矩阵为 $\boldsymbol{V}_P$，次网络中发送预编码矩阵为 $\boldsymbol{U}_C$，接收滤波矩阵为 $\boldsymbol{V}_C$。如果直接借鉴干扰对准思想，可通过设计主、次网络中的发送预编码矩阵和接收滤波矩阵，使主、次网络发送信号在对应的接收信号空间上相互分离，以保障无干扰传输，同时使主网络发送的信号对于窃听节点实施最大化干扰，即使得次网络信号和主网络信号在窃听节点的接收信号空间混叠。这就要求主、次网络中发送预编码矩阵和接收滤波矩阵满足以下条件

$$\begin{cases}\boldsymbol{V}_C\boldsymbol{H}_{CP}\boldsymbol{U}_P=0\\ \boldsymbol{V}_P\boldsymbol{H}_{PC}\boldsymbol{U}_C=0\\ \boldsymbol{H}_{EP}\boldsymbol{U}_P=\boldsymbol{H}_{EC}\boldsymbol{U}_C\end{cases}\tag{1}$$

式中：$\boldsymbol{H}_{CP}$ 为主网络发送端到次网络接收端的信道矩阵；$\boldsymbol{H}_{PC}$ 为次网络发送端到主网络接收端的信道矩阵；$\boldsymbol{H}_{EP}$ 为主网络发送端到窃听节点的信道矩阵；$\boldsymbol{H}_{EC}$ 为次网络发送端到窃听节点的信道矩阵。

1.2 信道误差模型

类似于文献[7,8]的假设，在分布式的过程中

假定发送预编码矩阵和接收滤波矩阵都受限于非精确的信道状态信息，本文所分析时考虑的信道非理想条件主要是由于“反馈时延”的影响，研究分析中发送端通常需要获知信道估计的链路信息以便进行有用数据的信号处理，然而由于无线信道的时变性和信道估计、反馈等处理过程，该信道状态信息与实际发送数据符号时所经历的信道不可避免的存在时延，假设为 T_d。普通的方法是通过高斯马尔科夫过程表征 $\widetilde{\boldsymbol{H}}_{ab}$ 与 $\boldsymbol{H}_{ab}$ 间的数学关系

$$\widetilde{\boldsymbol{H}}_{ab}=\rho\boldsymbol{H}_{ab}+\boldsymbol{E}_{ab} \tag{2}$$

式中：$\rho=E[\widetilde{\boldsymbol{H}}_{ab}^{\dagger}\boldsymbol{H}_{ab}]/E[\boldsymbol{H}_{ab}^{\dagger}\boldsymbol{H}_{ab}]$ 表示时延相关函数，由文献[9]可知，Clarke 信道模型下有 $\rho=J_0(2\pi f_d T_d)$，其中 $J_0(\cdot)$ 表示文献[10]中的第一类零阶贝塞尔函数，f_d 为最大多普勒频移，T_d 为信道时延。同时假定时延误差复高斯矩阵 $\boldsymbol{E}_{ab}$ 与信道矩阵 $\boldsymbol{H}_{ab}$ 相互独立，其由均值为零，方差为 $1-\rho^2$ 的元素组成，即

$$\mathrm{vec}(\boldsymbol{E}_{ab})\sim N_C(\boldsymbol{0},(1-\rho^2)\boldsymbol{I}) \tag{3}$$

式中：$\mathrm{vec}(\cdot)$ 表示对矩阵的向量化。

2　干扰对准方案

基于文献[11]干扰对准的思想，认知蜂窝网络中主次用户干扰对准后次网络的安全传输速率可以表示为

$$R_S=\log\left|\boldsymbol{I}_{d_C}+\boldsymbol{V}_C\boldsymbol{H}_{CC}\boldsymbol{U}_C\boldsymbol{U}_C^{\dagger}\boldsymbol{H}_{CC}^{\dagger}\boldsymbol{V}_C^{\dagger}\frac{P_C}{d_C}\right|-\log\left|\boldsymbol{I}_{d_E}+\frac{\boldsymbol{V}_E\boldsymbol{H}_{EC}\boldsymbol{U}_C\boldsymbol{U}_C^{\dagger}\boldsymbol{H}_{EC}^{\dagger}\boldsymbol{V}_E^{\dagger}}{\boldsymbol{V}_E\boldsymbol{H}_{EP}\boldsymbol{U}_P\boldsymbol{U}_P^{\dagger}\boldsymbol{H}_{EP}^{\dagger}\boldsymbol{V}_E^{\dagger}(P_P/d_P)+\boldsymbol{I}_{EN_O}}\frac{P_C}{d_C}\right| \tag{4}$$

式中：$\boldsymbol{H}_{CC}$ 为次网络发送端到次网络接收端的信道矩阵；P_P 为主网络发送功率；P_C 为次网络发送功率；d_C 和 d_E 分别为次网络和窃听链路的传输自由度，其分别满足 $d_C=\mathrm{rank}\{\boldsymbol{V}_C\boldsymbol{H}_{CC}\boldsymbol{U}_C\}\geqslant 1$ 和 $d_E=\mathrm{rank}\{\boldsymbol{V}_E\boldsymbol{H}_{EC}\boldsymbol{U}_C\}\geqslant 1$；$\boldsymbol{I}_{EN_O}$ 为窃听节点处噪声功率的 $d_E\times d_E$ 维单位对角阵。

本文发送预编码矩阵和接收滤波矩阵的迭代求解是基于过时的非精确的信道状态信息。求得的发送接收预编码矩阵是非精确的，分别用 $\widetilde{\boldsymbol{U}}_C$，$\widetilde{\boldsymbol{U}}_P$，$\widetilde{\boldsymbol{V}}_P$ 和 $\widetilde{\boldsymbol{V}}_C$ 表示。另外，本文对式(4)中的策略进行了改进，即主、次用户间的相互干扰没有必要完全对准到各自的零空间。事实上，针对频谱共享的认知蜂窝网络，对主网络来说只要满足给定的干扰温度约束 Γ 即可。此时，基于非理想信道信息的最大化次网络安全传输速率的发送预编码矩阵和接收滤波矩阵对应于如下优化问题的解

$$\begin{aligned}R_S=\underset{\boldsymbol{U}_P,\boldsymbol{U}_C,\boldsymbol{V}_P,\boldsymbol{V}_C,\boldsymbol{V}_E}{\mathrm{argmax}}\ &\log\left|\boldsymbol{I}_{d_C}+\mathrm{SINR}_C\right|-\\ &\log\left|\boldsymbol{I}_{d_E}+\mathrm{SINR}_E\right|\\ \text{s.t.}\quad &\mathrm{SINR}_P\leqslant\Gamma\end{aligned} \tag{5}$$

式中：$\mathrm{SINR}_P=\dfrac{\widetilde{\boldsymbol{V}}_P\boldsymbol{H}_{PP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\boldsymbol{H}_{PP}^{\dagger}\widetilde{\boldsymbol{V}}_P^{\dagger}}{\widetilde{\boldsymbol{V}}_P\boldsymbol{H}_{PC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\boldsymbol{H}_{PC}^{\dagger}\widetilde{\boldsymbol{V}}_P^{\dagger}(P_C/d_C)+\boldsymbol{I}_{PN_O}}\cdot\dfrac{P_P}{d_P}$，$\mathrm{SINR}_C=\dfrac{\widetilde{\boldsymbol{V}}_C\boldsymbol{H}_{CC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\boldsymbol{H}_{CC}^{\dagger}\widetilde{\boldsymbol{V}}_C^{\dagger}}{\widetilde{\boldsymbol{V}}_C\boldsymbol{H}_{CP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\boldsymbol{H}_{CP}^{\dagger}\widetilde{\boldsymbol{V}}_C^{\dagger}(P_P/d_P)+\boldsymbol{I}_{CN_O}}\cdot\dfrac{P_C}{d_C}$ 和 $\mathrm{SINR}_E=\dfrac{\widetilde{\boldsymbol{V}}_E\boldsymbol{H}_{EC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\boldsymbol{H}_{EC}^{\dagger}\widetilde{\boldsymbol{V}}_E^{\dagger}}{\widetilde{\boldsymbol{V}}_E\boldsymbol{H}_{EP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\boldsymbol{H}_{EP}^{\dagger}\widetilde{\boldsymbol{V}}_E^{\dagger}(P_P/d_P)+\boldsymbol{I}_{EN_O}}\cdot\dfrac{P_C}{d_C}$ 分别表示经过干扰对准后主、次网络接收端和窃听节点接收端的信干噪比，$\boldsymbol{H}_{PP}$ 为主网络发送端到主网络接收端的信道矩阵，d_P 为主网络的传输自由度，其满足 $d_P=\mathrm{rank}\{\boldsymbol{V}_P\boldsymbol{H}_{PP}\boldsymbol{U}_P\}\geqslant 1$，$\boldsymbol{I}_{PN_O}$ 和 $\boldsymbol{I}_{CN_O}$ 分别为主用户接收端和次用户接收端噪声功率的 $d_P\times d_P$ 维和 $d_C\times d_C$ 维单位对角阵。

为了求解式(5)中的问题，先通过优化预编码矩阵 $\widetilde{\boldsymbol{U}}_C$，$\widetilde{\boldsymbol{U}}_P$ 和 $\widetilde{\boldsymbol{V}}_C$ 使式(5)中第一项达到最大，依据文献[11]中的分布式迭代方案，设计本文的迭代方案如下：

步骤 1　初始化主用户和次用户发送端预编码矩阵 $\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_C$，所取预编码矩阵要满足

$$\widetilde{\boldsymbol{U}}_P^{\dagger}\widetilde{\boldsymbol{U}}_P=\boldsymbol{I}_{d_P},\widetilde{\boldsymbol{U}}_C^{\dagger}\widetilde{\boldsymbol{U}}_C=\boldsymbol{I}_{d_C}$$

步骤 2　分别计算主用户接收端和次用户接收端的干扰和噪声协方差矩阵为

$$\widetilde{\boldsymbol{B}}_P=\widetilde{\boldsymbol{H}}_{PC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\widetilde{\boldsymbol{H}}_{PC}^{\dagger}(P_P/d_P)+\boldsymbol{I}_{PN_O}$$

$$\widetilde{\boldsymbol{B}}_C=\widetilde{\boldsymbol{H}}_{CP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\widetilde{\boldsymbol{H}}_{CP}^{\dagger}(P_C/d_C)+\boldsymbol{I}_{CN_O}$$

步骤 3　主用户和次用户接收端的接收滤波矩阵分别表示为

$$\widetilde{\boldsymbol{V}}_P=\frac{(\widetilde{\boldsymbol{B}}_C)^{-1}\widetilde{\boldsymbol{H}}_{PP}\widetilde{\boldsymbol{U}}_P}{\|(\widetilde{\boldsymbol{B}}_C)^{-1}\widetilde{\boldsymbol{H}}_{PP}\widetilde{\boldsymbol{U}}_P\|}\quad\widetilde{\boldsymbol{V}}_C=\frac{(\widetilde{\boldsymbol{B}}_P)^{-1}\widetilde{\boldsymbol{H}}_{CC}\widetilde{\boldsymbol{U}}_C}{\|(\widetilde{\boldsymbol{B}}_P)^{-1}\widetilde{\boldsymbol{H}}_{CC}\widetilde{\boldsymbol{U}}_C\|}$$

步骤 4　信道的互易性，互换上下行方向，且令

$$\hat{\widetilde{\boldsymbol{U}}}_C=\widetilde{\boldsymbol{V}}_C\quad\hat{\widetilde{\boldsymbol{U}}}_P=\widetilde{\boldsymbol{V}}_P$$

步骤 5　计算互易网络中的干扰和噪声协方差矩阵

$$\hat{\widetilde{\boldsymbol{B}}}_C=\hat{\widetilde{\boldsymbol{H}}}_{CP}\hat{\widetilde{\boldsymbol{U}}}_C\hat{\widetilde{\boldsymbol{U}}}_C^{\dagger}\hat{\widetilde{\boldsymbol{H}}}_{CP}^{\dagger}(P_C/d_C)+\hat{\boldsymbol{I}}_{CN_O}$$

$$\hat{\widetilde{\boldsymbol{B}}}_P=\hat{\widetilde{\boldsymbol{H}}}_{PC}\hat{\widetilde{\boldsymbol{U}}}_P\hat{\widetilde{\boldsymbol{U}}}_P^{\dagger}\hat{\widetilde{\boldsymbol{H}}}_{PC}^{\dagger}(P_P/d_P)+\hat{\boldsymbol{I}}_{PN_O}$$

步骤 6　计算其接收滤波矩阵

$$\hat{\widetilde{\boldsymbol{V}}}_P=\frac{(\hat{\widetilde{\boldsymbol{B}}}_C)^{-1}\hat{\widetilde{\boldsymbol{H}}}_{PP}\hat{\widetilde{\boldsymbol{U}}}_P}{\|(\hat{\widetilde{\boldsymbol{B}}}_C)^{-1}\hat{\widetilde{\boldsymbol{H}}}_{PP}\hat{\widetilde{\boldsymbol{U}}}_P\|}\quad\hat{\widetilde{\boldsymbol{V}}}_C=\frac{(\hat{\widetilde{\boldsymbol{B}}}_P)^{-1}\hat{\widetilde{\boldsymbol{H}}}_{CC}\hat{\widetilde{\boldsymbol{U}}}_C}{\|(\hat{\widetilde{\boldsymbol{B}}}_P)^{-1}\hat{\widetilde{\boldsymbol{H}}}_{CC}\hat{\widetilde{\boldsymbol{U}}}_C\|}$$

步骤 7　互换上下行方向，且设

$$\widetilde{\boldsymbol{U}}_C=\hat{\widetilde{\boldsymbol{V}}}_C\quad\widetilde{\boldsymbol{U}}_P=\hat{\widetilde{\boldsymbol{V}}}_P$$

步骤 8 重复步骤 2～7，直至收敛或达到预先设定的最大迭代步数为止。

基于上述算法计算出了最优的发送和接收预编码矩阵 $\widetilde{\boldsymbol{U}}_C$，$\widetilde{\boldsymbol{V}}_C$ 和 $\widetilde{\boldsymbol{U}}_P$，$\widetilde{\boldsymbol{V}}_P$，现在需要求窃听端的窃听矩阵 $\widetilde{\boldsymbol{V}}_E$，根据窃听端的目的，窃听端的接收矩阵就要使窃听到的信息最大化

$$\widetilde{\boldsymbol{V}}_E = \max \operatorname{eig}_{\text{unit}}(\boldsymbol{B}^{-1}\boldsymbol{A}) \tag{6}$$

式中：$\boldsymbol{B} = \widetilde{\boldsymbol{H}}_{EP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\widetilde{\boldsymbol{H}}_{EP}^{\dagger}(P_P/d_P) + \boldsymbol{I}_{EN_O}$，$\boldsymbol{A} = \widetilde{\boldsymbol{H}}_{EC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\widetilde{\boldsymbol{H}}_{EC}^{\dagger}$，其中 $\widetilde{\boldsymbol{V}}_E$ 取 $\boldsymbol{B}^{-1}\boldsymbol{A}$ 最大的 d_E 个特征值对应的特征向量。

基于用户可达速率的定义[7,12]，干扰对准后次用户的安全速率表示为

$$R_S = \log\left|\boldsymbol{I}_{d_C} + \frac{\widetilde{\boldsymbol{V}}_C\boldsymbol{H}_{CC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\boldsymbol{H}_{CC}^{\dagger}\widetilde{\boldsymbol{V}}_C^{\dagger}(P_C/d_C)}{\widetilde{\boldsymbol{V}}_C\boldsymbol{H}_{CP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\boldsymbol{H}_{CP}^{\dagger}\widetilde{\boldsymbol{V}}_C^{\dagger}(P_P/d_P) + \boldsymbol{I}_{CN_O}}\right| - \log\left|\boldsymbol{I}_{d_E} + \frac{\widetilde{\boldsymbol{V}}_E\boldsymbol{H}_{EC}\widetilde{\boldsymbol{U}}_C\widetilde{\boldsymbol{U}}_C^{\dagger}\boldsymbol{H}_{EC}^{\dagger}\widetilde{\boldsymbol{V}}_E^{\dagger}(P_C/d_C)}{\widetilde{\boldsymbol{V}}_E\boldsymbol{H}_{EP}\widetilde{\boldsymbol{U}}_P\widetilde{\boldsymbol{U}}_P^{\dagger}\boldsymbol{H}_{EP}^{\dagger}\widetilde{\boldsymbol{V}}_E^{\dagger}(P_P/d_P) + \boldsymbol{I}_{EN_O}}\right| \tag{7}$$

基于式(7)，次用户的安全中断概率表示为

$$P_{\text{out}} = \Pr\{R_S < R_{\text{th}}\} \tag{8}$$

式中 R_{th} 表示次用户安全传输的速率门限值。

3 仿真分析

本节中，针对认知网络下的多用户对系统，利用 Monte Carlo 仿真验证本文给出的分布式计算干扰对准的发送和接收预编码矩阵方案的有效性，分析时假设主次用户具有相同的功率配置 $P_P = P_C$，系统的安全传输速率门限为 $R_{\text{th}} = 2$。

图 2 给出了次用户的安全传输速率随 SNR 的变化情况。仿真时假定每个节点配备两根天线，也就是说每个节点的最大可达自由度为 1。可以看出，非理想条件下经干扰对准后次用户系统的最大安全传输速率优于预编码矩阵随机给定时的传输速率，验证了干扰对准技术在提高存在窃听节点认知网络下的多用户对系统安全传输的有效性。显而易见，信道时延较小时最大安全传输速率会向理想条件下的最大安全传输速率逼近（$\rho=1$）。信道时延较大时的安全传输速率趋近于预编码矩阵随机给定下的安全传输速率曲线，这是因为此时求得的预编码矩阵与实际传输信道间的随机不相关性加大，从而逼近于预编码矩阵随机给定时的场景。

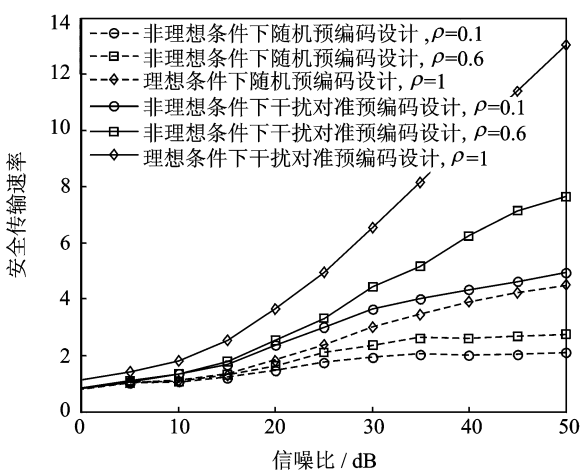

图 2 次用户的安全传输速率随信噪比的变化

Fig. 2 Secrecy transmission rate of the secondary user versus SNR

图 3 给出了次用户的安全中断概率随 SNR 的变化情况。和图 2 设定一样，假定每个节点配备两根天线。同样可以看出，在非理想条件下（$\rho \neq 1$）经干扰对准后次用户系统的中断概率性能优于预编码矩阵随机给定时的系统安全中断性能，验证了干扰对准技术在提高系统性能中的必要性。同时信道时时延误差较大时，经干扰对准下的安全中断概率也比较大，说明了信道估计的精度对系统设计有非常重要的影响。

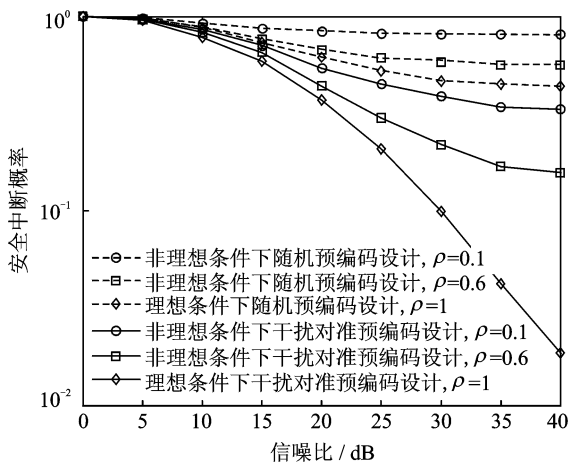

图 3 次用户的安全中断概率随信噪比的变化

Fig. 3 Secrecy outage probability of the secondary user versus SNR

4 结束语

为了估计干扰对准技术在下一代蜂窝移动通信系统中应用的可行性，本文基于存在窃听节点的信道非理想条件下的认知网络中的多用户对系统，以安全传输速率和安全中断概率为指标研究了系统的性能。仿真结果表明，非理想条件下经干扰对准后的系统性能明显优于预编码矩阵随机给定时的系统性能，验证文中理论分析的正确性。此外，随着信道时延误差的加大，系统的性能也会受到较

大的影响，证实了信道估计精确度是未来系统设计时不可缺少的重要因素。

参考文献：

[1] Pei Y，Liang Y，Zhang L，et al. Achieving cognitive and secure transmissions using multiple antennas [C]// IEEE 20th International Symposium on Personal，Indoor and Mobile Radio Communications (PIMRC). Tokyo：[s. n.]，2009：1-5.

[2] Araujo A，Blesa J，Romero E，et al. Artificial noise scheme to ensure secure communications in CWSN [C]// IEEE 8th International Conference on Wireless Communications and Mobile Computing (IWCMC). Limassol：[s. n.]，2012：1023-1027.

[3] Zahurul M，Sarkar I，Ratnarajah T. Aspect of security in the cognitive relay assisted interference channels [C] // IEEE Information Theory Workshop (ITW). Lausanne：[s. n.]，2012：652-656.

[4] Guan X，Cai Y，Yang W. Increasing secrecy capacity via joint design of cooperative beamforming and jamming [C]// IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications. Toronto：[s. n.]，2011：1274-1278.

[5] Cadambe V，Jafar S. Interference alignment and degrees of freedom of the K-user interference channel [J]. IEEE Transactions on Information Theory，2008，54(8)：3425-3441.

[6] Xie J，Ulukus S. Secure degrees of freedom of the Gaussian wiretap channel with helpers [C]// IEEE 50th Annual Allerton Conference on Communication，Control，and Computing. Monticello：[s. n.]，2012：193-200.

[7] Morteza Razavi S，Ratnarajah T. Performance analysis of interference alignment under CSI mismatch [J]. IEEE Transactions on Vehicular Technology，2014，63(9)：4740-4748.

[8] Ayach O E，Heath R W. Interference alignment with analog channel state feedback [J]. IEEE Transactions on Wireless Communications，2012，11(2)：626-636.

[9] Tan C C，Beaulieu N C. On first-order Markov modeling for the Raleigh fading channels [J]. IEEE Transactions on Communications，2000，48(12)：2032-2040.

[10] Gradshteyn I S，Ryzhik I M. Table of integrals，series，and products[M]. 7th ed. San Diego，CA：Academic，2007.

[11] Gomadam K，Cadambe V R，Jafar S A. A distributed numerical approach to interference alignment and applications to wireless interference networks [J]. IEEE Transactions on Information Theory，2011，57(6)：3309-3322.

[12] Xing J，Zhang X，Wang W. On the study of outage performance for Interference Alignment (IA) in cognitive relay networks [C]// IEEE 8th International Conference on Communications and Networking in China (CHINACOM). Guilin：[s. n.]，2013：75-79.