DOI:10.11721/cqnuj20160120

基于协作干扰器的 OFDM-CR 保密通信系统功率控制*

李 林[1,2], 蒋卫恒[1], 冯文江[1]
(1. 重庆大学 通信工程学院, 重庆 400044; 2. 重庆电子工程职业学院, 重庆 401331)

摘要:针对 OFDM-CR 系统中认知收发信机在独立并行高斯窃听信道上的安全通信与功率控制展开研究。以无协作干扰器的 OFDM-CR 系统为对象,导出了最大化安全速率的认知发射机功率分配表达式;为了提高信道资源利用率,在 OFDM-CR 系统中引入协作干扰器,并讨论最大化安全速率的联合认知发射机与协作干扰器功率控制策略。首先不考虑主用户干扰约束,分析引入协作干扰器能获得安全速率增益的信道条件,并计算各子信道固定发射功率下的干扰功率,然后将安全速率最大化模型用混合整数非线性规划近似,基于启发式贪婪算法求解其次优解,最后就提出的功率控制策略与其他几种典型的功率控制策略进行了性能对比仿真,结果表明,提出的功率控制策略在不同条件下均有性能提升。

关键词:认知无线电;并行高斯窃听信道;协作干扰器;功率分配
中图分类号:TN92 **文献标志码**:A **文章编号**:1672-6693(2016)01-0154-09

由于无线媒介的广播特性,无线通信一直面临着传输安全威胁。认知无线电[1]作为一种智能无线电设计理念,其具备的环境感知和学习能力,能有效提高频谱利用率。尽管认知无线电具备高级信号处理和智能频谱使用能力,但仍然面临譬如窃听、攻击等传统无线网络中的各种安全威胁。

基于信息论的无线网络安全传输研究可追溯到 20 世纪 70 年代 Wyner 等人关于窃听信道的研究工作,文献[2]给出了基于信息论的安全容量定义,即授权发射机到授权接收机能可靠传输且泄露给窃听节点近似为零信息量的最大传输速率。研究表明,如果窃听节点探测到的信号是授权接收机观察信号的退化,即使不使用任何加密机制,授权用户之间的安全通信也是可能的。随后,Csiszar 等将退化信道模型扩展到一般广播信道[3],研究表明,即使窃听节点探测到的信号不是授权接收机观察信号的退化或授权收发节点之间的信道在平均意义下差于授权发射机与窃听节点之间的信道,利用无线信道的衰落特性,无密钥加密授权收发节点之间的安全通信也是可能的。

认知无线网络信息论安全研究起始于文献[4],假设认知收发信机之间有信息传输需求,且该信息对另一非认知接收机保密,针对离散无记忆认知干扰信道(Cognitive interference channel, CIC)模型和高斯 CIC 信道模型,分别导出了容量-疑义率区域闭合表达式。文献[5-7]研究衬底型(Underlay)频谱共享模式下的认知无线网络信息安全传输策略,文献[5]分析了窃听信道与衬底型频谱共享模式之间的对偶关系;文献[6]通过分析多输入单输出(Multiple-input single-output, MISO)认知无线信道的安全容量,提出了两种达到安全容量的传输协方差矩阵设计机制;文献[7]扩展了文献[6]的应用场景,假设认知发射机具有不完全信道状态信息(Channel state information,CSI),设计了两种稳健功率控制算法。针对认知无线网络与主用户(Primary user, PU)网络混合共存场景,文献[8]提出一种主次网络协作机制,认知用户通过协助主用户保密信息传输获得频谱使用机会,而主用户则通过可信认知用户协作获得安全速率提升,将认知无线网络与主用户网络间协作决策过程用 Stackelberg 非合作博弈模型描述,并设计了求解该博弈均衡的分段线性搜索算法;文献[9]在认知发射机配置了多天线情况下研究主次网络安全协作,协作认知节点自由度提升能更好地辅助主用户网络提高安全传输速率,分别导出了主用户安全传输速率约束下最优认知传输策略和认知用户传输速率约束下最大化主用户网络安全传输策略。针对并行独立高斯窃听信道的安全通信问题,文献[10]分析了多载波广播窃听信道下安全速率权重和最大化问题,提出了一种安全速率最大化功率控制策略;文献[11]研究下行 OFDMA(Orthogonal frequency

* **收稿日期**:2015-03-25 **网络出版时间**:2015-12-02 13:27
资助项目:国家自然科学基金(No. 60872038);重庆市教委科学技术研究项目(No. KJ102201)
作者简介:李林,副教授,研究方向为通信信号处理、软件无线电,E-mail: mzlsml@126.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.n.20151202.1327.024.html

division multiple access)窃听系统联合功率控制与子载波分配，将网内用户划分为具有安全约束的特殊用户和无安全约束的常规用户，目标是在满足特殊用户安全速率约束下最大化常规用户速率，提出基于内点法的最优资源分配算法和基于对偶分解的次优资源分配算法；文献[12]研究具有不可信中继节点协作的 OFDMA 联合子载波分配和功率控制，给出了基于降价拍卖机制的功率控制算法和基于对偶分解的子载波分配算法；文献[13]在 OFDM 系统中引入协作干扰器以提高安全速率，针对窃听信道退化和非退化两种情形，提出了基于交替优化的联合发射机与干扰器功率分配机制。

本文从信息论角度研究存在窃听节点的认知无线网络安全通信，由于存在主用户干扰约束，引入协作干扰器在获得安全速率增益的同时会对主用户产生干扰。针对无协作干扰器的 OFDM-CR(OFDM cognitive radio-based)系统，导出了最大化安全速率的认知发射机功率分配表达式；为了提高信道资源利用率，在 OFDM-CR 系统中引入协作干扰器，提出一种最大化安全速率的联合认知发射机与协作干扰器功率控制策略，首先不考虑主用户干扰约束，分析引入协作干扰器能获得安全速率增益的信道条件，并计算各子信道固定发射功率下的干扰功率，然后将安全速率最大化模型用混合整数非线性规划近似，基于启发式贪婪算法求解其次优解，最后就提出的功率控制策略与其他几种典型的功率控制策略进行了性能对比仿真。

1 系统模型与安全速率最大化问题

1.1 系统模型

考虑认知发射机 Alice 与认知接收机 Bob 在一组并行独立高斯窃听信道上执行保密通信，且在该场景中还存在潜在窃听节点 Eve 和协作干扰器节点 Jammer，系统模型如图 1 所示。认知无线网络基于频谱感知获得主用户网络未使用的空闲频谱，并将其分割成一系列独立并行子信道，采用 OFDM 执行信息传输。假设窃听节点 Eve 是被动安全威胁源，即仅执行监听而不主动发射干扰信息，并基于监听信号解码 Alice 传输给 Bob 的信息。为了协助 Alice-Bob 之间安全通信，Jammer 在 Alice 工作子信道上注入服从高斯分布的加性噪声信号，以恶化 Alice-Eve 信道来增强 Alice-Bob 信道的安全容量。

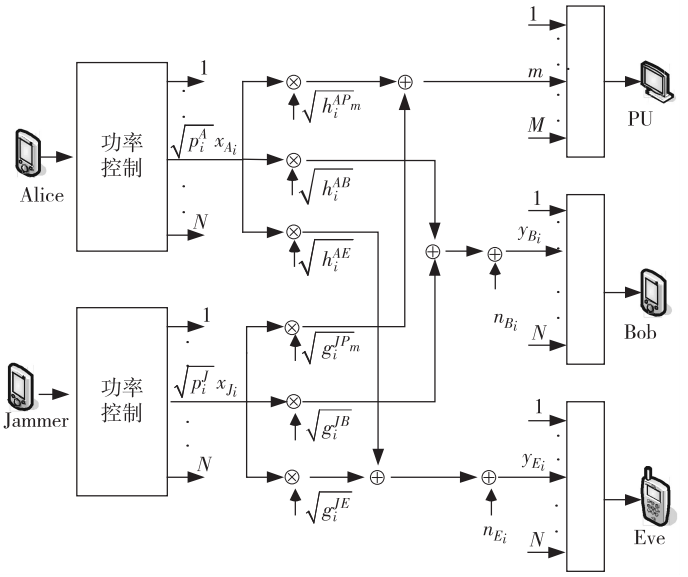


图 1　系统模型

假定认知无线网络获得的可用子信道集合为 N 且 $N=|N|$，各子信道具有单位带宽；$\sqrt{h_i^{AB}}$ 和 $\sqrt{g_i^{JB}}$ 分别表示在子信道 i($\forall i\in N$)上 Alice-Bob 和 Jammer-Bob 的信道系数；$\sqrt{h_i^{AE}}$ 和 $\sqrt{g_i^{JE}}$ 分别表示在子信道 i 上 Alice-Eve 和 Jammer-Eve 的信道系数。各子信道经历平坦衰落，且在多个功率分配周期内保持不变。Alice 和 Jammer 在子信道 i 上传输符号分别为 x_{Ai} 和 x_{Ji}，服从高斯分布且具有单位平均功率，则 Bob 和 Eve 在信道 i 上探测到的信号分别为：

$$y_{Bi}=\sqrt{p_i^A h_i^{AB}}x_{Ai}+\sqrt{p_i^J g_i^{JB}}x_{Ji}+n_{Bi}, \tag{1}$$

$$y_{Ei}=\sqrt{p_i^A h_i^{AE}}x_{Ai}+\sqrt{p_i^J g_i^{JE}}x_{Ji}+n_{Ei}, \tag{2}$$

其中 n_{Bi}，n_{Ei} 分别为 Bob 和 Eve 在子信道 i 的零均值高斯噪声，分别具有方差 σ_m^2，σ_{Ei}^2，p_i^A 和 p_i^J 分别为 Alice 和 Jammer 在子信道 i 的发射功率。进一步假设 Alice 和 Jammer 已知完美信道状态信息，对于认知-主用户共存场景(同区域不同频段)，当主用户未采用多载波传输或主用户与认知用户调制载波不完全正交时，Alice 和 Jammer 传输将对邻频段工作的主用户产生干扰[14]，为此应考虑主用户干扰保护。假设主用户占用信道集合为 M 且 $M=|M|$，主用户占用信道 m，$\forall m\in M$，其干扰约束为 I_m^{th}。令 h_i^{APm} 是工作在子信道 i 的 Alice 和工作在信道 m 的主用户接收机之间的互干扰信道增益，g_i^{JPm} 是工作在子信道 i 的 Jammer 和工作在信道 m 的主用户接收机之间的互干扰信道增益，互信道增益包括信道衰落系数和谱相关系数。

1.2 基于协作干扰器的安全速率最大化问题

令 Alice 和 Jammer 在子信道集合 N 上的功率分配矢量分别为 $p^A=\{p_1^A,\cdots,p_N^A\}$ 和 $p^J=\{p_1^J,\cdots,p_N^J\}$，安全

速率最大化问题如下：

$$\mathrm{OP1}:\max_{(p^A,p^J)} R^{\mathrm{safe}}(p^A,p^J)=\sum\nolimits_{i\in N}[\log(1+\gamma_i^{AB}(p_i^A,p_i^J))-\log(1+\gamma_i^{AE}(p_i^A,p_i^J))]^+, \tag{3}$$

$$\text{s.t.}\ \sum\nolimits_{i\in N}p_i^A<P^A,\sum\nolimits_{i\in N}p_i^J<P^J。 \tag{4}$$

其中 $R^{\mathrm{safe}}(p^A,p^J)$ 是高斯噪声干扰下系统的可达安全速率；$\gamma_i^{AB}(p_i^A,p_i^J)=p_i^A h_i^{AB}/(p_i^J g_i^{JB}+\sigma_{Bi}^2)$ 和 $\gamma_i^{AE}(p_i^A,p_i^J)=p_i^A h_i^{AE}/(p_i^J g_i^{JE}+\sigma_{Ei}^2)$ 是 Jammer 协作下 Alice 信号在 Bob 和 Eve 处的信噪比；$[z]^+=\max(0,z)$，即当 Alice 信号在 Bob 处的信噪比小于在 Eve 处的信噪比时停止使用该信道；p^A 和 p^J 分别为 Alice 和 Jammer 处的总功率约束。此外，主用户干扰约束使认知无线网络资源使用还应满足如下约束：

$$\sum\nolimits_{i\in N}(p_i^A h_i^{APm}+p_i^J g_i^{JPm})<I_{th}^m,\forall m\in M。 \tag{5}$$

由上可知，Alice 和 Bob 的功率约束以及主用户干扰约束都是线性的，但求解 OP1 仍面临如下挑战：一是(3)式定义的目标函数非光滑且关于决策变量非凸；二是联合 Alice 和 Jammer 多信道功率分配；三是 Alice 和 Jammer 同时传输将使两者信号在主用户接收机处互耦。为此，下面首先分析无协作干扰器系统认知发射机功率分配，然后研究协作干扰器系统联合认知发射机与协作干扰器功率分配。

2 无协作干扰器并行高斯窃听信道功率分配

考虑 OP1 的一种特殊情形，即无协作干扰器并行高斯窃听信道功率分配，此时，OP1 退化为 OP2，

$$\mathrm{OP2}:\max_{(p^A,p^J)} R^{\mathrm{safe}}(p^A)=\sum\nolimits_{i\in N}[\log(1+\gamma_i^{AB}(p_i^A))-\log(1+\gamma_i^{AE}(p_i^A))]^+, \tag{6}$$

$$\text{s.t.}\ \sum\nolimits_{i\in N}p_i^A<P^A, \tag{7}$$

$$\sum\nolimits_{i\in N}p_i^A h_i^{APm}<I_{th}^m,\forall m\in M。 \tag{8}$$

其中 $\gamma_i^{AB}(p_i^A)=p_i^A h_i^{AB}/\sigma_{Bi}^2$ 和 $\gamma_i^{AE}(p_i^A)=p_i^A h_i^{AE}/\sigma_{Ei}^2$。可以看出，如果无主用户干扰约束式(8)，OP2 退化为文献[15]研究的并行高斯窃听信道功率控制问题。由于在 OP2 中有无主用户干扰约束不会改变 OP2 的数学结构，且总功率约束式(7)和主用户干扰约束式(8)都是线性的，因此目标函数式(6)是非凸的。尽管如此，对于信道 i，$\forall i\in N$，若 $p_i^A h_i^{AB}/\sigma_{Bi}^2\leqslant p_i^A h_i^{AE}/\sigma_{Ei}^2$，无论 Alice 为其分配多大的发射功率，其可达安全速率都为零，即对 Alice 而言，最优传输策略是关闭该子信道的[15]。为此，本文引入有效子信道集合(Valid subchannel set, VSS)概念，定义为 $v=\{i,\forall i\in N,p_i^A h_i^{AB}/\sigma_{Bi}^2>p_i^A h_i^{AE}/\delta_{Ei}^2\}$，直接基于集合 v 研究 OP2。显然，对于 $\forall i\in v$，目标函数关于决策变量 p_i^A 凹，因而基于集合 v 的 OP2 是凸规划，则有如下退化 OP2 的拉格朗日函数，

$$L(\lambda,\mu,p^A)=\sum_{i\in V}\left(\log\left(\frac{1+\gamma_i^{AB}(p_i^A)}{1+\gamma_i^{AE}(p_i^A)}\right)-\lambda p_i^A-p_i^A\sum_{m\in M}\mu_m h_i^{APm}\right)+\lambda P^A+\sum\nolimits_{m\in M}\mu_m I_m^{th}, \tag{9}$$

其中 $\lambda\geqslant 0,\mu=\{\mu_1,\cdots,\mu_M\}\geqslant 0$ 分别为 Alice 总功率约束和主用户干扰约束对应的拉格朗日乘子。定义退化 OP2 的最优解为 $\{p_i^{*A},i\in v,\lambda^*,\mu^*\}$，则由 KKT 条件得该最优解为 $\partial L(\lambda,\mu,p^A)/\partial p_i^A=0$ 的根[15]，即子信道 i($\forall i\in v$)上 Alice 的最优发射功率为

$$p_i^{*A}=\frac{1}{2}\left[\sqrt{\left(\frac{\sigma_{Bi}^2}{h_i^{AB}}-\frac{\sigma_{Ei}^2}{h_i^{AE}}\right)^2-\frac{4}{\lambda^*+\sum\limits_{m\in M}\mu_m^* h_i^{APm}}\left(\frac{\sigma_{Bi}^2}{h_i^{AB}}-\frac{\sigma_{Ei}^2}{h_i^{AE}}\right)}-\left(\frac{\sigma_{Bi}^2}{h_i^{AB}}+\frac{\sigma_{Ei}^2}{h_i^{AE}}\right)\right],\forall i\in V。 \tag{10}$$

由于 $p_i^{*A}\geqslant 0$，上述最优发射功率还需满足

$$h_i^{AB}/\sigma_{Bi}^2-h_i^{AE}/\sigma_{Ei}^2\geqslant\lambda^*+\sum\nolimits_{m\in M}\mu_m^* h_i^{APm}。 \tag{11}$$

由此可知，最大化并行高斯窃听信道安全速率发射功率分配类似于非认知系统结论[17]，唯一区别是主用户干扰约束使非认知系统最优功率分配表达式中的 $4/\lambda^*$ 替换为 $4/\left(\sum_{m\in M}\mu_m^* h_i^{APm}\right)$。此外，对比(11)式与文献[15]定理 2 可知，对应子信道非负传输功率条件也发生了变化。上述结论表明，对于工作在并行高斯窃听信道上的认知无线网络，空闲信道并未充分利用，原因有 2 个：一是仅考虑了有效信道子集 v 上的保密信息传输；二是非负功率约束条件进一步减少了认知无线网络使用信道数。为此，需引入辅助机制在保证信息安全传输的同时尽可能提高信道资源利用率。

3 干扰器协作并行高斯窃听信道功率控制

基于信息论的无线网络安全传输研究表明[18]，在特定网络场景中引入协作干扰（Cooperative jamming，CJ）或噪声前传（Noise forwarding，NF）协作节点，能提升安全速率非零子信道的可达安全速率。

在认知-主用户共存场景中，由于 Alice 的发射功率和 Jammer 的干扰功率在主用户接收机处会形成耦合干扰，尽管引入 CJ 能获得安全速率增益，但其干扰功率将对主用户造成附加干扰，从而减少认知无线网络的可用信道资源，又会导致认知无线网络安全速率损失。显然，如果 Jammer 对 Eve 的干扰远大于对 Bob 的干扰，且对主用户接收机影响小，则引入 CJ 是合理的。采用启发式机制求解 OP1：首先，不考虑主用户干扰约束分析引入 CJ 能获得安全速率增益的信道条件，并计算各子信道固定发射功率下的干扰功率，然后将 OP1 用混合整数非线性规划（Mixed integer non-linear programming，MINIP）近似，并基于启发式贪婪算法求解 OP1 的次优解。

3.1 子信道 CJ 条件与最优干扰策略

1）子信道 CJ 条件：分析无主用户干扰约束时引入 CJ 能获得安全速率增益的充要条件。

引理　给定子信道 i 和发射功率 $p_i^A>0$，在子信道 i 引入 CJ 的充要条件为

$$\exists\, p_i^J\in(0,P^J] \text{使得 } R_i^{\text{safe}}(p_i^A,p_i^J)>R_i^{\text{safe}}(p_i^A), \tag{12}$$

令 $\alpha_i^{AB}=h_i^{AB}/\sigma_{Bi}^2$，$\alpha_i^{AE}=h_i^{AE}/\sigma_{Ei}^2$，$\beta_i^{JB}=g_i^{JB}/\sigma_{Bi}^2$，$\beta_i^{JE}=g_i^{JE}=g_i^{JE}/\sigma_{Ei}^2$，则对任意子信道 i，$\forall i\in N$ 以及引理中的充要条件，有且仅有如下 4 种情形：

情形 1：对于 $\forall\, p_i^A\in(0,P^A]$ 有 $R_i^{\text{safe}}(p_i^A)=0$，且对 $\forall\, p_i^A\in(0,P^A]$ 和 $p_i^J\in(0,P^J]$，有 $R_i^{\text{safe}}(p_i^A,p_i^J)=0$。基于 $R_i^{\text{safe}}(p_i^A)$ 和 $R_i^{\text{safe}}(p_i^A,p_i^J)$ 的定义，有如下条件

$$1\leqslant\alpha_i^{AE}/\alpha_i^{AB} \text{ 和 } \beta_i^{JE}/\beta_i^{JB}\leqslant\alpha_i^{AE}/\alpha_i^{AB}, \tag{13}$$

$$\text{或 } 1\leqslant\alpha_i^{AE}/\alpha_i^{AB}<\beta_i^{JE}/\beta_i^{JB} \text{ 和 } p_i^J\leqslant(\alpha_i^{AE}-\alpha_i^{AB})/(\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB})。 \tag{14}$$

情形 2：对于 $\forall\, p_i^A\in(0,P^A]$ 有 $R_i^{\text{safe}}(p_i^A)=0$，但对 $p_i^A\in(0,P^A]$，$\exists\, p_i^J\in(0,P^J]$ 使得 $R_i^{\text{safe}}(p_i^A,p_i^J)>0$。经简化，有如下条件

$$1\leqslant\alpha_i^{AE}/\alpha_i^{AB}<\beta_i^{JE}/\beta_i^{JB} \text{ 和 } p^J\geqslant p_i^J>(\alpha_i^{AE}-\alpha_i^{AB})/(\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB})。 \tag{15}$$

情形 3：对于 $\forall\, p_i^A\in(0,P^A]$ 有 $R_i^{\text{safe}}(p_i^A)>0$，但对 $\forall\, p_i^A\in(0,P^A]$ 和 $\forall\, p_i^J\in(0,P^J]$，$R_i^{\text{safe}}(p_i^A,p_i^J)\leqslant R_i^{\text{safe}}(p_i^A)$。经简化，有如下条件

$$\alpha_i^{AE}/\alpha_i^{AB}<1 \text{ 和 } \beta_i^{JE}/\beta_i^{JB}<1。 \tag{16}$$

情形 4：对于 $\forall\, p_i^A\in(0,P^A]$ 有 $R_i^{\text{safe}}(p_i^A)>0$，且对 $p_i^A\in(0,P^A]$，$\exists\, p_i^J\in(0,P^J]$ 使得 $R_i^{\text{safe}}(p_i^A,p_i^J)>R_i^{\text{safe}}(p_i^A)$。经简化，有如下条件

$$\alpha_i^{AE}/\alpha_i^{AB}<1<\beta_i^{JE}/\beta_i^{JB} \text{ 和 } p_i^J<[(\alpha_i^{AE}\beta_i^{JE}-\alpha_i^{AB}\beta_i^{JB})+p_i^A\alpha_i^{AB}\alpha_i^{AE}(\beta_i^{JE}-\beta_i^{JB})]/\beta_i^{JB}\beta_i^{JE}(\alpha_i^{AB}-\alpha_i^{AE})。 \tag{17}$$

由（13）～（17）式可知，联合发射机与干扰器功率分配的基本原则是：1）分配零干扰功率到满足（13），（14）和（16）式的子信道；2）分配零发射功率到满足（13）和（14）式的子信道。干扰器协作下安全速率增益源于两方面：一是无干扰器协作时具有零安全速率，引入干扰器协作后能获得正安全速率，即满足（15）式的子信道；二是无干扰器协作时具有正安全速率，引入干扰器协作后能获得正安全速率增益，即满足（17）式的子信道。

2）固定发射功率的最优干扰机制：分析固定子信道发射功率下最优干扰功率分配，即如下优化问题：

$$\begin{aligned}\text{OP3}:&\max_{p_i^J} R_i^{\text{safe}}(p_i^A,p_i^J)\\ &\text{s.t. } p_i^J\in[0,p^J],\forall i\in J_1\cup J_2,\end{aligned} \tag{18}$$

其中 $J_1=\{i\mid\forall i\in N$ 且子信道 i 满足（15）式$\}$，$J_2=\{i\mid\forall i\in N$ 且子信道 i 满足（17）式$\}$，即上述优化问题是基于集合 $J_1\cup J_2$，因为认知无线网络仅能在该子信道集上获得安全速率增益。由于认知发射机在子信道上的发射功率固定，则 OP3 仅涉及优化变量 p_i^J，其最优解可由如下定理概括。

定理 1　OP3 的最优解为 p_i^{*J}，$\forall i\in J_1\cup J_2$，

$$p_i^{*J}=\begin{cases}\min(P^J,p_i^{J0}),\text{如果 } P^J>(\alpha_i^{AE}-\alpha_i^{AB})/(\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}),\\ 0,\text{否则}。\end{cases} \tag{19}$$

其中 $p_i^{J0}=(-b_i-\sqrt{b_i^2-4a_ic_i})/2a_i$，$a_i=g_i^{AB}g_i^{JE}(h_i^{AE}g_i^{JB}-h_i^{AB}g_i^{JE})$，$b_i=2g_i^{JB}g_i^{JE}(h_i^{AE}\sigma_{Bi}^2-h_i^{AB}\sigma_{Ei}^2)$，$c_i=p_i^Ah_i^{AB}h_i^{AE}(g_i^{JE}\sigma_{Bi}^2-g_i^{JB}\sigma_{Ei}^2)+(h_i^{AE}g_i^{JE}\sigma_{Bi}^4-h_i^{AB}g_i^{JB}\sigma_{Ei}^4)$。

证明 由于OP3仅涉及单决策变量 p_i^J,且约束集合为凸,则其最优解可直接由KKT条件获得。子信道 i 的可达安全速率为:$R^{\text{safe}}(p_i^A,p_i^J)=\log(1+\gamma_i^{AB}(p_i^A,p_i^J))-\log(1+\gamma_i^{AE}(p_i^A,p_i^J))$,则 $R^{\text{safe}}(p_i^A,p_i^J)$ 关于 p_i^J 的偏导为

$$\frac{\partial R^{\text{safe}}(p_i^A,p_i^J)}{\partial p_i^J}=\frac{p_i^A}{f(p_i^A,p_i^J)}[a_i(p_i^J)^2+b_ip_i^J+c_i], \tag{20}$$

其中 $f(p_i^A,p_i^J)=[(p_i^Jg_i^{JE}+\sigma_{Ei}^2)^2+p_i^Ah_i^{AE}(p_i^Jg_i^{JE}+\sigma_{Ei}^2)][(p_i^Jg_i^{JB}+\sigma_{Bi}^2)^2+p_i^Ah_i^{AB}(p_i^Jg_i^{JB}+\sigma_{Bi}^2)]>0$,则OP3的最优解可能为 $p_i^J=0$ 或 $p_i^J=P^J$,或是 $\partial R^{\text{safe}}(p_i^A,p_i^J)/\partial p_i^J=0$ 的根,

$$p_i^{J0}=(-b_i-\sqrt{b_i^2-4a_ic_i})/2a_i \text{ 和 } p_i^{J1}=(-b_i+\sqrt{b_i^2-4a_ic_i})/2a_i。$$

协调干扰器仅需在子信道集合 $J_1\cup J_2$ 上分配干扰功率,子信道满足的条件分别为:

1)若 $\forall i\in J_1$,子信道满足(15)式,$1\leqslant\alpha_i^{AE}/\alpha_i^{AB}<\beta_i^{JE}/\beta_i^{JB}$,因而 $\beta_i^{JE}>\beta_i^{JB}\frac{\alpha_i^{AE}}{\alpha_i^{AB}}$,$\alpha_i^{AE}-\alpha_i^{AB}\leqslant0$,$\beta_i^{JE}-\beta_i^{JB}>0$ 和 $\alpha_i^{AE}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}>\alpha_i^{AE}\beta_i^{JB}=\frac{\alpha_i^{AE}}{\alpha_i^{AB}}-\alpha_i^{AB}\beta_i^{JB}=\frac{\beta_i^{JB}}{\alpha_i^{AB}}[(\alpha_i^{AE})^2-(\alpha_i^{AB})^2]\geqslant0$。基于此,有:

$$a_i=g_i^{JB}g_i^{JE}\sigma_{Bi}^2\sigma_{Ei}^2(\alpha_i^{AE}\beta_i^{JB}-\alpha_i^{AB}\beta_i^{JE})<0,$$

$$b_i=2g_i^{JB}g_i^{JE}\sigma_{Bi}^2\sigma_{Ei}^2(\alpha_i^{AE}-\alpha_i^{AB})\geqslant0,$$

$$c_i=p_i^Ah_i^{AB}h_i^{AE}\sigma_{Bi}^2\sigma_{Ei}^2(\beta_i^{JE}-\beta_i^{JB})+\sigma_{Bi}^4\sigma_{Ei}^4(\alpha_i^{AE}\beta_i^{JE}-\alpha_i^{AB}\beta_i^{JB})>0,$$

即 $p_0^{J0}>0$,$p_i^{J1}<0$,且 $a_i(p_i^J)^2+b_ip_i^J+c_i$ 是$(0,p_i^{J0})$上的增函数,在(p_i^{J0},∞)上单调递减。基于此,安全速率 $R_i^{\text{safe}}(p_i^A,p_i^J)$ 在 $p_i^J=p_i^{J0}$ 达到最大。此外,由于Jammer具有总功率约束 P^J,且由(15)式可知,为了获得正安全速率增益,要求 $P^J\geqslant p_i^J>\frac{\alpha_i^{AE}-\alpha_i^{AB}}{\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}}$。因此,若 $P^J\leqslant\frac{\alpha_i^{AE}-\alpha_i^{AB}}{\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}}$ 或 $p_i^{J0}\leqslant\frac{\alpha_i^{AE}-\alpha_i^{AB}}{\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}}$,OP3的最优解为 $p_i^{*J}=0$。由于

$$p_i^{J0}=-\frac{b_i}{2a_i}-\frac{\sqrt{b_i^2-4a_ic_i}}{2a_i}>-\frac{b_i}{2a_i}=\frac{\alpha_i^{AE}-\alpha_i^{AB}}{\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}},$$

则只需考虑 $P^J\leqslant\frac{\alpha_i^{AE}-\alpha_i^{AB}}{\alpha_i^{AB}\beta_i^{JE}-\alpha_i^{AE}\beta_i^{JB}}$情形,该情形的最优干扰策略为(19)式。

2)若 $\forall i\in J_2$,即子信道满足(17)式,$\alpha_i^{AE}/\alpha_i^{AB}<1<\beta_i^{JE}/\beta_i^{JB}$。同样可以证明 $a_i<0$,$b_i<0$,$c_i>0$,即有 $p_i^{J0}>0$,$p_i^{J1}<0$。该情形的最优干扰策略也为(19)式。

基于定理1,有如下推论。

推论 对于,$\forall i\in N$,$p_i^A\in(0,P^A]$和 $p_i^J\in[0,P^J]$,如果 $R_i^{\text{safe}}(p_i^A,p_i^J)>0$,则 $R_i^{\text{safe}}(p_i^A,p_i^J)$在区间$[0,P^A]$上关于 p_i^A 单调增;对于 $\forall i\in J_1\cup J_2$,如果 $R_i^{\text{safe}}(p_i^A,p_i^J)>0$ 且 $p_i^J\neq0$,则最优干扰功率 p_i^{*J} 是 p_i^A 的非减函数。在上述两种情形下,$p^A<\infty$,$P^J<\infty$。

3.2 次优联合发射机和干扰器功率控制

结合上述分析,给出求解OP1的次优算法。首先离散化Alice的发射功率,然后将OP1用MINLP近似,最后利用(13)~(17)式和定理1并结合贪婪机制联合分配发射机与干扰器功率,即在单位发射机功率分配时计算每个子信道的单位发射机功率增量与最优干扰功率分配下计算收益-成本比,并将单位发射机功率和对应的最优干扰功率分配给具有最大收益-成本比的子信道,重复上述过程直到至少一个约束不满足为止。

1)OP1的MINLP近似。将Alice发射功率 P^A 执行 K 等分,$\Delta p^A=p^A/K$,每等份功率由 $K=\{1,\cdots,K\}$ 索引。用 x_i^k 表示等分功率分配变量,若 $x_i^k=1$,则 $x_j^k=0$,$\forall j\in N$,表示将第 k 个等分功率分配给子信道 i。OP1写成如下MINLP,

$$\text{OP4}:\max_{(\boldsymbol{X},p^J)}R^{\text{safe}}(\boldsymbol{X},p^J)=\sum_{i\in N}\left[\log\left(1+\gamma_i^{AB}\left(\Delta p^A\sum_{k\in K}x_i^k,p_i^J\right)\right)-\log\left(1+\gamma_i^{AE}\left(\Delta p^A\sum_{k\in K}x_i^k,p_i^J\right)\right)\right]^+, \tag{21}$$

$$\text{s.t. } \Delta p^A\sum_{i\in N}\sum_{k\in K}x_i^k\leqslant P^A, \tag{22}$$

$$\sum_{i\in N}p_i^J\leqslant P^J, \tag{23}$$

$$\sum_{i\in N}\left(\Delta p^A\left(\sum_{k\in K}x_i^k\right)h_i^{APm}+p_i^Jg_i^{JPm}\right)\leqslant I_m^{th},\forall m\in M, \tag{24}$$

其中 X 是 $N\times K$ 的 0-1 功率分配矩阵，x_i^k 为第 i 行第 k 列元素，$p^J=\{p_1^J,\cdots,p_N^J\}$ 为子信道集合 N 的干扰功率分配，且 $\forall i\in N, p_i^J\in[0,P^j]$。显然，OP4 属 NP-hard，难以给出闭式解。接下来基于启发式贪婪机制求解 OP4，并给出次优解。

2）基于启发式贪婪机制的次优算法。贪婪算法定义收益函数来量化单位资源分配回报（如设置 $x_i^k=1$），定义成本函数来表征单位资源分配代价，将单位资源分配给具有最高收益-成本比的个体。下面定义求解 OP4 次优算法的收益函数、成本函数和资源分配规则。

收益函数：用安全速率增量表征资源分配收益。依据两种干扰功率分配策略分别定义如下收益函数，

$$\Delta R_{i1}^{\text{safe}}(p_i^A,\Delta p^A)=R_i^{\text{safe}}(p_i^A+\Delta p^A,p_i^{*J}(p_i^A))-R_i^{\text{safe}}(p_i^A,p_i^{*J}(p_i^A)),\tag{25}$$

$$\Delta R_{i2}^{\text{safe}}(p_i^A,\Delta p^A)=R_i^{\text{safe}}(p_i^A+\Delta p^A,p_i^{*J}(p_i^A+\Delta p^A))-R_i^{\text{safe}}(p_i^A,p_i^{*J}(p_i^A)),\tag{26}$$

其中 $\Delta R_{i1}^{\text{safe}}(p_i^A,\Delta p^A)$ 为在子信道 i 上干扰功率保持不变，仅增加单位发射机功率时的安全速率增量；$\Delta R_{i2}^{\text{safe}}(p_i^A,\Delta p^A)$ 为子信道 i 上具有单位发射机功率增量且最优化干扰功率时的安全速率增量。$p_{i2}^{*J}(p_i^A)$ 和 $p_i^{*J}(p_i^A+\Delta p^A)$ 依据定理 1 获得。由推论可知，$p^{*J}(p_i^A+\Delta p^A)>p_i^{*J}(p_i^A)$。需要指出的是，对于不需执行干扰的子信道 i（即 $\forall i\notin J_1\cup J_2$），其最优干扰功率始终为零。此时，仍可认为该子信道最优干扰功率是发射功率的非递减函数，这种考虑不影响本文的分析和结论。(25)和(26)式代表了两种不同干扰功率分配策略：如果 $\Delta p^A\neq 0$，安全速率增量非负且 $\Delta R_{i2}^{\text{safe}}(p_i^A,\Delta p^A)$，即通过干扰功率优化可获得更大安全速率增益。尽管如此，最优干扰功率分配将带来干扰功率增量，即 $\Delta p_i^{*J}=p_i^{*J}(p_i^A+\Delta p^A)-p_i^{*J}(p_i^A)>0$。此时，会增加对主用户的干扰，从而导致认知无线网络可用资源减少或可达安全速率降低。因此从系统可达安全速率角度分析，上述两种策略孰优孰劣尚无定论。

成本函数：资源分配成本来自两方面：一是功率开销，包括 Alice 和 Jammer 的功率开销；二是主用户干扰。对于功率开销成本，虽然 Alice 每次功率分配具有相同功率开销（即 Δp^A），但由于不同子信道具有不同最优干扰功率，因此针对每个子信道的功率开销仍不同。本文不单独考虑干扰功率开销成本，而将其纳入主用户干扰成本中。显然，协作干扰器分配功率越大，对主用户造成的干扰也越大。因此，针对两种收益函数分别定义如下成本函数，

$$c_{i1}(m)=\Delta p^A h_i^{APm},m=1,\cdots,M,\tag{27}$$

$$c_{i2}(m)=\Delta p^A h_i^{APm}+\Delta p_i^{*J}h_i^{JPm},m=1,\cdots,M。\tag{28}$$

由此可知，对于子信道 i，有两个矢量成本 $c_{ij}=[c_{ij}(1),\cdots,c_{ij}(M)]$，$j=1,2$，其中 $c_{ij}(m)$ 是针对收益函数 j 与主用户干扰约束 m 的成本。基于 (27)和(28)式，需要确定表征最终资源使用成本的标量成本。本文定义矢量成本最大值为最终资源使用成本，即

$$c_{i1}=\max c_{i1}(m),c_{i2}=\max c_{i2}(m),m\in M。$$

资源分配规则：将 Alice 单位功率和对应的干扰功率（可能为 0 或非零干扰功率增量）分配给具有最高收益-成本比的子信道。本文定义了两个收益函数和成本函数，应首先确定哪种策略对特定子信道最优，随后比较多个子信道上的收益-成本比，并将 Alice 发射功率增量和相应的干扰功率分配给具有最高收益-成本比的子信道。联合发射机与干扰器贪婪次优功率分配（Joint transmitter and jammer power greedy-like allocation，JTJP-GLA）算法流程如下，其中 $\overline{P}^J$ 表示当前时刻 Jammer 的剩余功率。

算法：联合发射机与干扰器贪婪次优功率分配（JTJP-GLA）算法

1）初始化 $k=0,u_m=0,\forall m\in M$；

2）当 $k\leqslant K$ 和 $I_{th}^m-u_m>0,\forall m\in M$ 时，循环

①对于 $\forall i\in N$，基于 (13)～(17) 式，利用(25)和(26)式分别计算 $\Delta R_{i1}^{\text{safe}}(p_i^A,\Delta p^A)$ 和 $\Delta R_{i2}^{\text{safe}}(p_i^A,\Delta p^A)$，利用(27)和(28) 式分别计算 c_{i1},c_{i2}；

②分配发射功率增量 Δp^A 和干扰功率增量 $p_{i^*}^{*J}$ 到子信道 i^*，$i^*=\arg\max(\max \Delta R_{i1}^{\text{safe}}/c_{ij}),i\in v,j=1,2$；

③更新 $\overline{P}^J=\overline{P}^J-p_{i^*}^{*J}$ 和 $u_m=\Delta p^A\sum_{i\in N}k_i h_i^{APm}+\sum_{i\in N}p_i^{*J}g_i^{JPm},\forall m\in M$；

④k ++；

结束循环。

由上述算法描述可知，算法终止条件为如下两种情形之一：一是发射机功率分配完毕，即 $k=K$；二是违反主用户干扰约束。干扰器功率约束不构成算法结束条件，因为即使干扰器无剩余功率，推论表明，在不违反主用

户干扰约束下分配剩余发射功率仍可带来安全速率增益。

4 仿真结果和性能分析

分析评估JTJP-GLA算法的性能,仿真参数设置参考文献[15,17]。假设主-次网络共存区域总的信道集合为Ω,且$|\Omega|=24$,信道索引为$i=1,2,\cdots,24$。认知无线网络可用信道集合$N=\{1,2,3,9,10,11,12,13,16,17,18,19,20\}$,其余信道被主用户占用,即$\forall m\in M=\Omega\backslash N$。进一步假设主用户在所有信道上具有相同干扰约束$I_0^{th}=I_m^{th}=5\times10^{-5}$ W,$\forall m\in M$,且在各子信道传输功率均为1 W,各子信道经历瑞利衰落,其噪声功率均为10^{-5} W。为了评估算法性能,与下列算法进行比较。

Opt-w/o PU-IC(Optimal algorithm without considering the PU interference constraint[17])算法:该算法不考虑主用户干扰约束而以最大化安全速率为目标。因此,对认知无线网络而言,如果仅有唯一空闲子信道满足Alice-Bob信道增益大于Alice-Eve信道增益,则算法将分配所有可用功率给该子信道。

Opt-w PU-IC(Optimal algorithm with considering the PU interference constraint)算法:该算法依据(10)式执行功率分配。

Uniform算法:该算法均匀分配功率到集合中的子信道,且保证不违反主用户干扰约束。

TPD-GLA (Transmitter power discretization-based greedy-like power allocation)算法:该算法由JTJP-GLA在条件$p^J=0$ W退化而成,即基于发射机功率离散化的贪婪算法。

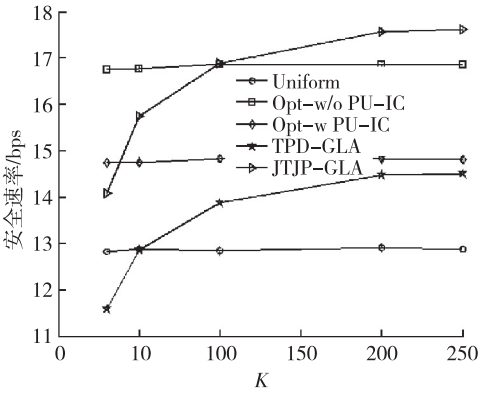
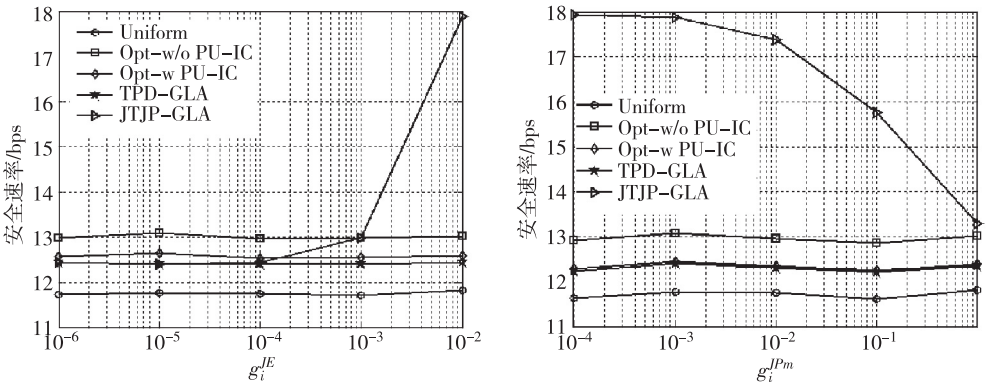


图2 安全速率随参数K变化, $P^A=1$ W,$P^J=0.2$ W,$E\{h_i^{APm}\}=10$,$E\{g_i^{JPm}\}=10$,$I_0^{th}=5\times10^{-5}$ W

首先分析JTJP-GLA算法可达安全速率随K的变化,如图2所示。由图可知,随着K值增大,TPD-GLA和JTJP-GLA算法获得的安全速率均增加,这是因为K值越大,发射功率划分粒度越小,从而使功率能更精细地分配给各子信道。针对给定仿真场景以及TDP-GLA和JTJP-GLA算法,当$K>200$时,由增加K值带来的安全速率增益逐渐趋缓;当$K<100$时,TPD-GLA算法的性能损失约为3 bps/Hz,当$K<40$时,JTJP-GLA算法不能带来安全速率增益(但并不意味引入CJ不会带来安全速率增益,因为JTJP-GLA仅是次优算法)。另外,由图还可以看出,Opt-w/o PU-IC,Opt-w PU-IC和Uniform算法的性能不受K值变化影响,且在这3种算法中,Opt-w/o PU-IC性能最好,而Uniform性能最差。

其次,分析各种算法可达安全速率随Jammer-Eve平均信道增益$E\{g_i^{JPm}\}$以及Jammer-PU接收机平均信道增益$E\{g_i^{JPm}\}$的变化,如图3所示。由图3a可知,当Jammer-Eve信道增益过小时(如$E\{g_i^{JE}\}<10^{-4}$,即Jammer干扰Eve能力弱),JTJP-GLA算法的性能接近TPD-GLA;当Jammer-Eve信道增益增大时(如$E\{g_i^{JE}\}<10^{-3}$),引入Jammer协作并利用JTJP-GLA算法执行联合发射机与干扰器功率分配将显著增加系统可达安全速率。上述分析可以直接扩展到$E\{g_i^{JPm}\}$变化对可达安全速率的影响分析,即随着Jammer-PU接收机信道增益的增加,引入CJ带来的安全速率增益将减小,这符合文中理论分析。此时,引入CJ虽然能带来安全速率增益,但同时对主用户干扰增加,特别是当Jammer-PU接收机信道增益较大时,将使认知无线网络可用信道资源减小,即可达安全速率降低。综上,除了针对非认知无线网络的因素外



a 安全速率随$E\{g_i^{JE}\}$变化,$E\{g_i^{JPm}\}=10^{-3}$ b 安全速率随$E\{g_i^{JPm}\}$变化

图3 $K=200$,$P^A=2$ W,$P^A=0.2$ W

(即 Bob 和 Jammer 到 Eve 的信道增益)，Jammer-PU 接收机信道增益 $E\{g_i^{JPm}\}$ 也影响认知无线网络对 CJ 的选择。基于上述结论，在认知无线网络中，需自适应引入 CJ 协作，并执行 JTJP-GLA 算法以增强可达安全速率，即 Jammer 估计 Eve 的信道增益，如果其值小，则认知无线网络应不引入 CJ，而是基于 TPD-GLA 或 Opt-w PU-IC 算法完成发射机功率分配。在两种仿真场景中，Opt-w/o PU-IC，Opt-w PU-IC 和 Uniform 算法的可达安全速率都不随信道增益参数变化，这与理论分析一致。

图 4 所示为可达安全速率随主用户干扰约束 I_0^{th} 的变化。可以看出，除 Opt-w/c PU-IC 算法外，其他算法的可达安全速率都是 I_0^{th} 的增函数，该结果类似于无安全约束认知无线网络的可达速率[17]。另外，JTJP-GLA 算法相对于其他算法具有较大的安全速率增益，而 Opt-w/oPU-IC，Opt-w PU-IC，Uniform 和 TPD-GLA 算法的性能差异随 I_0^{th} 增加而减小，直至忽略不计。这种性能差异减小的原因是随着 I_0^{th} 增加，不同算法可达安全速率性能都受限于可用发射机功率 P^A 而不是干扰约束 I_0^{th}。

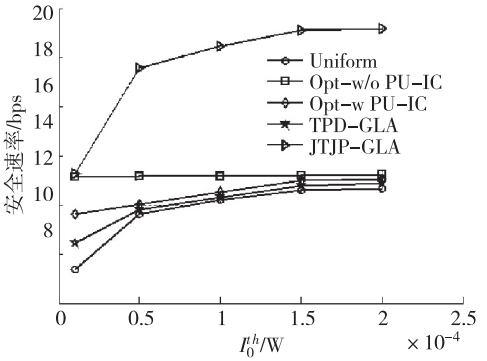


图 4　安全速率随参数 I_0^{th} 变化，$K=200$，$P^A=2$ W，$P^J=0.2$ W，$E\{g_i^{JPm}\}=10^{-3}$

图 5 是可达安全速率与功率开销随发射机可用功率 P^A 的变化。由图可知，所有算法的可达安全速率都是发射机可用功率的增加函数，但当发射机功率大于 1.5 W 时，可达安全速率增加趋缓，其原因是在高发射机功率区域，可达安全速率受主用户干扰和高斯信道安全容量约束。如果定义子信道 i 可达安全速率为 $R^{\text{safe}}=[\log(1+\gamma_i^{AB})-\log(1+\gamma_i^{AE})]^+$，则 $\lim\limits_{p_j^A\to\infty} R^{\text{safe}}=[\log(h_i^{AB}/h_i^{AE})]^+$[15]。另外，由图 5 还可知，JTJP-GLA 算法相对于其他算法具有显著安全速率增益，而 TPD-GLA 和 Opt-w PU-IC 算法的性能差异随 Alice 可用功率 P^A 增加而增加。这种性能差异递增源于：虽然发射机可用功率增加，但 TPD-GLA 算法中发射机功率离散化参数 K 保持不变，为了满足主用户干扰约束，从统计平均角度看，TPD-GLA 算法将使用相对于 Opt-w PU-IC 算法更少的传输功率。

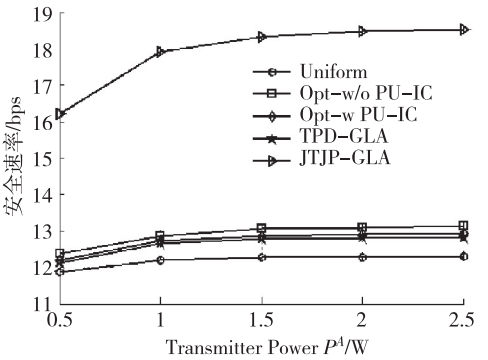


图 5　安全速率随参数 P^A 变化，$P^J=0.2$ W，$I_0^{th}=5\times10^{-5}$ W，$E\{g_i^{JPm}\}=10^{-3}$

5 结论

本文研究了 OFDM-CR 系统认知收发信机在独立并行高斯窃听信道上的安全通信与功率控制策略。以无协作干扰器的 OFDM-CR 系统为对象，导出了最大化安全速率的认知发射机功率分配表达式，其发射功率分配类似于非认知系统结论，但认知无线网络未充分利用空闲信道资源；为了提高信道资源利用率，进而在 OFDM-CR 系统中引入协作干扰器，构建了基于协作干扰器的 OFDM-CR 系统安全速率最大化优化模型，并提出了一种最大化安全速率的联合认知发射机与协作干扰器功率控制算法(JTJP-GLA)，该算法首先不考虑主用户干扰约束，分析引入协作干扰器能获得安全速率增益的信道条件，并计算各子信道固定发射功率下的干扰功率，然后将安全速率最大化模型用混合整数非线性规划近似，基于启发式贪婪算法求解其次优解。通过与 Opt-w/oPU-IC，Opt-wPU-IC，Uniform 和 TPD-GLA 算法对比仿真，结果表明，在大多数情况下，利用 JTJP-GLA 算法都能显著提升认知无线网络的可达安全速率，在最坏情况下，尽管引入协作干扰器不能带来安全速率提升，但 JTJP-GLA 算法也能获得近似无干扰器协作最优算法(Opt-wPU-IC)的性能。

参考文献：

[1] Mitola J, Maguire G Q. Cognitive radio: making software radios more personal[J]. IEEE Personal Communications, 1999, 6(4): 13-18.

[2] Wyner A. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(10): 1355-1387.

[3] Csiszar I, Korner J. Broadcast channels with confidential messages[J]. IEEE Trans Inform Theory, 1978, 24(7): 451-456.

[4] Liang Y, Somekh-Baruch A, Poor H V, et al. Capacity of cognitive interference channels with and without secrecy

[J]. IEEE Trans Inf Theory,2009,55(2):604-619.

[5] Zhang L,Zhang R. On the relationship between the multi-antenna secrecy communications and cognitive radio communications[J]. IEEE Trans Commun,2007,58(6):1877-1886.

[6] Pei Y, Liang Y, Teh K, et al. Secure communication over miso cognitive radio channels[J]. IEEE Trans Wireless Commun,2010,9(4):1494-1502.

[7] Pei Y, Liang Y, Teh K, et al. Secure communication in multi-antenna cognitive radio networks with imperfect channel state information[J]. IEEE Trans Signal Process, 2011,59(4):1683-1693.

[8] Wu Y,Liu K J R. An information secrecy game in cognitive radio networks[J]. IEEE Trans Inf Forens Security,2011,6(3):831-842.

[9] Lee K,Chae C B,Kang J. Spectrum leasing via cooperation for enhanced physical-layer secrecy[J]. IEEE Trans Veh Tech,2013,62(9):4672-4678.

[10] Jorswieck E A,Gerbracht S. Secrecy rate region of downlink OFDM systems: efficient resource allocation[C]// Proc of 14th International OFDM-Workshop, Hamburg: [s. n.],2009:7-12.

[11] Wang X,Tao M,Mo J,et al. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks[J]. IEEE Trans on Information Forensics and Security,2011,6(3):693-702.

[12] Wang A,Chen J,Cai Y,et al. Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks[J]. EURASIP Journal on Wireless Communications and Networking,2013(1):193-204.

[13] Ara M,Reboredo H. Power allocation strategies for OFDM Gaussian wiretap channels with a friendly jammer[C]// Proceedings of the IEEE International Conference on Communications. Hungary:[s. n.],2013:3413-3417.

[14] Weiss T, Hillenbrand J, Krohn A, et al. Mutual interference in OFDM based spectrum pooling systems[C]//Proc of IEEE 59th Vehicular Technology Conference. Kyoto: [s. n.],2004:1873-1877.

[15] Li Z, Yates R, Trappe W. Secrecy capacity of independent parallel channels[C]//44th Annual Allerton Conference on Communication, Control, and Computing Monticello. United States:[s. n.],2006:245-250.

[16] Boyd S, Vandenberghe L. Convex optimization[M]. Cambridge:Cambridge University Press,2004.

[17] Zhang Y H, Leung C. Resource allocation in an OFDM-based cognitive radio system[J]. IEEE Trans Commun, 2009,57(7):1928-1931.

[18] Tekin E, Yener A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming[J]. IEEE Trans Inf Theory,2008,54(6): 2735-2751.

Power Control for Cooperative Jammer-based OFDM-CR Secure Communication System

LI Lin[1,2], JIANG Weiheng[1], FENG Wenjiang[1]

(1. College of Communication Engineering, Chongqing University, Chongqing 400044;
2. Chongqing College of Electronic Engineering, Chongqing 401331, China)

Abstract: This paper investigates the OFDM-CR system secure communication and power allocation problem whether a cognitive-based transmitter and a cognitive-based receiver communicate over a bank of idle independent parallel Gaussian wiretap channels. We initially focus on the scenario without the assistance of a cooperative jammer (CJ) and characterize the secrecy rate maximization power allocation strategy. In order to improve the utilization of spectrum, we then extend our scenario by introducing a CJ and discuss the joint transmitter and CJ power control. For this extension problem, without considering the primary network interference constraints, we first analyze the channel conditions under which we can obtain positive secrecy rate gain by introducing CJ and calculate the optimal jamming power strategy under fixed transmit power, then a mixed integer non-linear programming is used to approximate the original secrecy rate maximization problem. Based on the greedy scheme, we proposed a heuristic algorithm to obtain a suboptimal solution. By comparing the proposed algorithm with some classical benchmark schemes, the simulation results indicates that our proposed algorithm outperforms them under different conditions.

Key words: cognitive radio; parallel Gaussian wiretap channel; cooperative jammer; power allocation

(责任编辑 游中胜)