

## 基于非信任中继协作的保密通信联合功率控制

冯文江, 蒋卫恒, 邓艺娜, 袁杨

(重庆大学 通信工程学院, 重庆 400044)

**摘 要:** 针对多个与基站(BS, base station)无直达链路蜂窝边缘移动站(MS, mobile station)在上行链路具有保密信息传输需求且存在不信任中继(UR, untrusted relay)协作通信场景, 引入目的节点(即 BS)干扰机制, 并研究 MS 固定传输功率下 UR 与 BS 功率分配以最大化系统安全速率问题。分析表明, 该联合功率控制问题等价于联合接入控制与功率分配问题因而是 NP-难。通过问题松弛, 提出一种次优 MS 接入控制与基于交替优化的功率分配算法, 并证明该次优算法具有多项式复杂度且至少收敛到原始问题一个次优解。仿真结果表明, 所提次优算法相对于同场景各种参考算法在系统可达安全速率性能上有显著提高。

**关键词:** OFDMA; 非信任中继; 功率控制; 信息论安全

中图分类号: TN919.1

文献标识码: A

文章编号: 1000-436X(2014)11-0059-10

## Joint power control for untrusted relay cooperation-based confidential communication

FENG Wen-jiang, JIANG Wei-heng, DENG Yi-na, YUAN Yang

(College of Communication Engineering, Chongqing University, Chongqing 400044, China)

**Abstract:** The scenario that multiple cell-edge mobile stations (MS) all without direct-links to the base station (BS) but have confidential messages in the uplink in the presence of untrusted relay (UR) cooperation was considered. In order to implement the secure communication between BS and multiple MS, destination-based jamming (DBJ) scheme was adopted. With the assumption that all MS had fixed transmit power, the joint UR and BS power control which aims at maximizing system sum secrecy rate was discussed. For this problem, analysis indicated that it was equivalent to joint access control and power allocation problem thus its NP-hard. Through problem relaxation, a suboptimal MS access control and alternatively power allocation algorithm was provided. This algorithm is proved to have polynomial complexity and can converge to at least a suboptimal solution for original problem. Simulation results show that compared with the benchmark algorithms, the proposed suboptimal algorithm is better in the achievable secrecy rate performance.

**Key words:** OFDMA; untrusted relay; power control; information-theoretic security

### 1 引言

由于无线媒质的广播特性, 存在窃听节点下无线网络的通信安全一直面临着严峻挑战。当前, 一种新的无线通信安全技术, 即利用无线信道自身的随机性来增强信息传输安全的信息论安全机制得到了广泛关注。

从信息论角度研究存在窃听节点下无线传输

安全最先由 Wyner<sup>[1]</sup>提出, 通过构建有噪窃听信道模型, 并定义该信道模型的安全容量为授权发射机到授权接收机之间能可靠传输且不被窃听节点获取任何消息的最大可达速率。研究表明, 当窃听节点截获信号是授权接收机接收信号的退化时, 即使不使用任何加密机制, 授权收发信机之间的安全通信也是可能的, 且保证窃听节点不能截获任何来自授权用户的信息。基于 Wyner 的工作, Csiszar 和

收稿日期: 2014-09-21; 修回日期: 2014-11-01

基金项目: 中央高校基本科研业务费基金资助项目 (CDJXS11162236)

**Foundation Item:** The Fundamental Research Funds for the Central Universities (CDJXS11162236)

Korner<sup>[2]</sup>针对广播信道开展研究, 结果表明, 利用无线信道固有随机性, 即使窃听节点截获信号不是授权接收机的退化, 授权收发信机之间的安全通信仍是可能的。

本文针对协作安全通信系统开展相关研究, 多个位于蜂窝边缘的移动站(MS, mobile station)在上行链路具有到基站(BS, base station)的保密通信需求, 由于这些 MS 到 BS 的距离较远, 无直达链路或直达链路衰落过大, 此时存在安全等级较低的协作节点愿作为中继完成 MS 到 BS 的保密信息传输。可知, 本文涉及的是非信任中继协作安全通信问题。针对该问题已有初步研究<sup>[3-11]</sup>, 基于三节点中继信道, 文献[3]研究了中继节点具有较低安全等级时的协作安全通信问题, 结果表明, 当中继信道是退化信道时, 系统安全容量为零; 而如果中继信道是逆退化的, 则系统安全容量等于传统窃听信道的安全容量。是否存在某些情形或某种机制使基于非信任中继的协作能增强安全速率, He 等<sup>[4]</sup>的研究表明, 基于压缩前传的非信任中继(UR, untrust relay)协作能获得更高安全速率。文献[5]指出, 即使源节点与目的节点之间无直达链路, 通过引入基于目的节点干扰(DBJ, destination-based jamming)机制同样能保证源节点与目的节点之间安全通信。基于信息论, 文献[6]研究非信任多入多出(MIMO, multiple-input multiple-output)中继信道下联合源节点与中继节点的波束成形问题; 文献[7]导出了非信任放大前传(AF, amplify-and-forward)协作中继保密通信的中断概率; 文献[8]研究基于友好干扰器的非信任中继双向通信安全速率最大化问题, 利用非合作博弈构建友好干扰器选择与功率控制模型, 并给出了分布式干扰器选择与功率分配算法。

综上所述, 已有的研究都是针对单对源一目的节点场景开展。本文研究多用户蜂窝系统基于非信任中继协作安全通信, 更具现实意义。

## 2 系统模型与协作协议

### 2.1 系统模型

如图 1 所示, 针对一个 BS 和多个蜂窝边缘 MS 构成的单蜂窝系统, 且这些 MS 在上行链路具有到 BS 的保密业务传输需求。定义 MS 集合为  $\mathcal{N}$ , 且  $N=|\mathcal{N}|$ , MS 索引为  $i=1, \dots, N$ 。此外, 假设为所有 MS 分配独立正交传输信道, 正交信道在频域定义。该模型适用于正交频分多址接入(OFDMA, or-

thogonal frequency duplex multiple access)的宽带接入系统, 且所有 MS 与 BS 之间无直达链路。进一步假设在当前状态下, 存在另一个 MS (不属于集合  $\mathcal{N}$ ) 或一个异构网络节点恰巧处于恰当位置且愿作为中继与属于集合  $\mathcal{N}$  的 MS 合作完成保密信息传输, 该中继与集合  $\mathcal{N}$  中的 MS 或 BS 属于不同运营商或具有较低安全等级。此时, 需在系统中引入有效机制来实现保密信息传输, 同时保护信息不被非信任中继节点窃听。本文不配置外在干扰器, 而是基于 DBJ 机制, 即 BS 充当干扰器。假设中继基于 AF 协作协议, 所有节点具有完全信道状态信息 (类似假设可见文献[6, 8, 11]。事实上, 针对非信任中继假设完全信道状态信息并不符合实际应用, 但在激励机制下协作 UR 窃听而不执行恶意攻击并获得准确信道状态信息是可行的 (通过信道估计与反馈实现), 关于 UR 协作激励机制的讨论是后续研究内容), 工作于半双工模式且所有 MS 具有固定发射功率, 即  $p_i^s (> 0), \forall i \in \mathcal{N}$ , 考虑联合优化 UR 和 BS 功率分配以最大化系统安全速率。

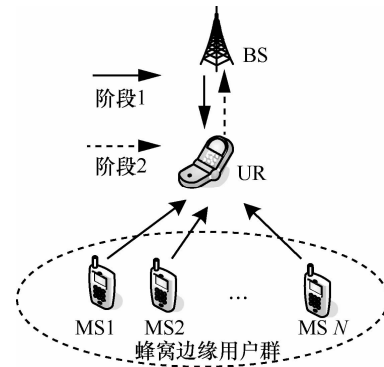


图 1 系统模型

### 2.2 协作协议

基于 DBJ 机制, 即 MS 为源节点, BS 既是干扰器也是目的节点, 则保密消息经由 UR 协作传输过程分为 2 个阶段。

**阶段 1** 各 MS 在自身工作信道上发送保密消息到 UR, 与此同时, BS 在各 MS 工作信道上注入基于高斯噪声的干扰信号。在信道  $i$  上 UR 的接收信号为

$$y_i^R = \sqrt{p_i^S} h_i^{SR} x_i^S + \sqrt{p_i^B} g_i^{BR} x_i^B + n_i^R \quad (1)$$

其中,  $x_i^S$  和  $x_i^B$  分别为 MS  $i$  的单位能量调制符号和 BS 在信道  $i$  上的干扰信号,  $p_i^B$  为 BS 在信道  $i$  上的干扰信号功率。假设所有信道互易,  $h_i^{SR}$  和  $g_i^{RB}$  分别

表示 MS  $i$  到 UR 和 UR 到 BS 在信道  $i$  上的信道系数,  $n_i^R$  为中继在信道  $i$  上的复值加性高斯白噪声 (AWGN, additive white Gaussian noise), 且满足  $n_i^R \sim CN(0, \sigma_i^2)$ 。

**阶段 2** UR 对所有信道上的接收信号分别执行归一化并放大前传, 信道  $i$  上 UR 的再生信号为

$$x_i^R = \zeta_i \sqrt{p_i^R} y_i^R \quad (2)$$

其中,  $\zeta_i = \left( p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2 \right)^{-1/2}$  为 UR 对 MS  $i$  信号的归一化因子,  $p_i^R$  为 UR 分配给 MS  $i$  信号的中继功率。BS 处接收来自 MS  $i$  的信号为

$$y_i^B = \zeta_i \sqrt{p_i^R} g_i^{RB} y_i^R + n_i^B, \forall i \in \mathcal{N} \quad (3)$$

其中,  $n_i^B$  为 BS 处信道  $i$  上的高斯白噪声, 且满足  $n_i^B \sim CN(0, \sigma_i^2)$ 。在执行自干扰消除, 即消除  $\zeta_i \sqrt{p_i^R} p_i^B g_i^{BR} g_i^{RB} x_i^B$  后, BS 通过信道  $i$  接收来自 MS 的信号为

$$y_i^B = \frac{\sqrt{p_i^S p_i^R} h_i^{SR} g_i^{RB}}{\sqrt{p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2}} x_i^S + \frac{\sqrt{p_i^R} g_i^{RB}}{\sqrt{p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2}} n_i^R + n_i^B \quad (4)$$

为简化计算, 令  $|h_i^{SR}|^2 / \sigma_i^2 = \gamma_i^{SR}$ ,  $|g_i^{BR}|^2 / \sigma_i^2 = \gamma_i^{BR}$ ,  $|g_i^{RB}|^2 / \sigma_i^2 = \gamma_i^{RB}$ 。UR 和 BS 处接收来自 MS  $i$  信号的瞬时信噪比(SNR, signal noise ratio)分别为

$$\chi_i^R = \frac{p_i^S \gamma_i^{SR}}{1 + p_i^B \gamma_i^{BR}}, \chi_i^B = \frac{p_i^S p_i^R \gamma_i^{SR} \gamma_i^{RB}}{1 + p_i^S \gamma_i^{SR} + p_i^R \gamma_i^{RB} + p_i^B \gamma_i^{BR}} \quad (5)$$

### 3 联合中继与干扰器功率控制

#### 3.1 安全速率最大化问题

如前所述, 总体目标是通过优化 UR 和 BS 功率分配以最大化系统安全速率, 其中 BS 充当干扰器, 而中继是非信任的。由文献[11,18]可知, MS  $i$  的可达安全速率为

$$R_i(p_i^B, p_i^R) = \frac{1}{2} \left[ R_i^B(p_i^B, p_i^R) - R_i^R(p_i^B) \right]^+ \quad (6)$$

其中, 系数 1/2 源于消息传输分为 2 阶段, 略去该系数不影响本文结论。用  $[\cdot]^+ \triangleq \max\{0, \cdot\}$ ,  $R_i^B(p_i^B, p_i^R) = \log(1 + \chi_i^B)$  和  $R_i^R(p_i^B) = \log(1 + \chi_i^R)$

分别表示 MS  $i$  和 UR 之间以及 MS  $i$  和 BS 之间的无安全约束信道容量。基于  $\chi_i^R$  和  $\chi_i^B$  的定义可知, 任意 MS 的可达安全速率依赖于中继功率  $p_i^R$  和干扰功率  $p_i^B$ 。因此, 需要执行联合功率优化以最大化安全速率。由于 UR 和 BS 具有独立功率约束, 则该问题的数学模型为

$$\text{OP1: } \max_{(p_i^R, p_i^B)} R(p_i^B, p_i^R) = \sum_{i \in \mathcal{N}} R_i(p_i^B, p_i^R) \quad (7a)$$

$$\text{s.t. } 0 \leq \sum_{i \in \mathcal{N}} p_i^R \leq P^R \text{ 和 } 0 \leq \sum_{i \in \mathcal{N}} p_i^B \leq P^B \quad (7b)$$

$$\mathbb{I}\{p_i^R > 0\} = \mathbb{I}\{p_i^B > 0\}, \forall i \in \mathcal{N} \quad (7c)$$

其中,  $\mathbf{p}^R = (p_1^R, \dots, p_N^R)$  和  $\mathbf{p}^B = (p_1^B, \dots, p_N^B)$  分别为在 UR 和 BS 分配给集合  $\mathcal{N}$  中 MS 的功率矢量,  $P^R$  和  $P^B$  分别为 UR 和 BS 的功率约束。  $\mathbb{I}\{X\}$  是示性函数, 当事件  $X$  为真时  $\mathbb{I}\{X\} = 1$ , 否则  $\mathbb{I}\{X\} = 0$ 。约束式(7c)源于本文讨论的系统中, BS 和 MS 之间无直达链路, 因而零干扰功率或零中继功率会导致零安全速率。分析 OP1 可知, 几个因素使 OP1 难以直接处理: 1)  $R_i(p_i^B, p_i^R)$  中的非负约束使目标函数非光滑; 2) 约束式(7c)使  $p_i^B$  和  $p_i^R$  之间存在二进制耦合关系; 3) 对安全速率  $R_i(p_i^B, p_i^R)$ , 即使去掉  $[\cdot]^+$ , 也不是关于决策变量  $p_i^B$  和  $p_i^R$  的联合凸/凹函数<sup>[14]</sup>, 因而不能直接用 KKT 条件<sup>[14]</sup>求解。下面基于 OP1 中安全速率定义非负约束  $[\cdot]^+$  给出引理 1, 其揭示在数学结构上 OP1 等价于一个联合接入控制与功率分配问题。

**引理 1** 对 MS  $i$ ,  $\forall i \in \mathcal{N}$  及给定传输功率  $p_i^S$  和安全速率式(6), MS  $i$  获得正安全速率的条件是中继功率  $p_i^R$  和干扰功率  $p_i^B$  满足

$$p_i^R > p_{i,th}^R = \left( 1 + (1 + p_i^S \gamma_i^{SR}) / p_i^B \gamma_i^{RB} \right) / \gamma_i^{RB} \text{ 和 } p_i^B > 0 \quad (8)$$

此外,  $\mathcal{N}$  中所有 MS 获得正安全速率的条件是 UR 总中继功率  $P^R$  满足

$$P^R > \sum_{i \in \mathcal{N}} 1 / \gamma_i^{RB} \quad (9)$$

**证明** 由 MS  $i$  安全速率定义式(6)可知, 在给定  $p_i^S > 0$  下 MS  $i$  获得正安全速率等价于  $\chi_i^B > \chi_i^R$ , 将(5)代入该 SNR 关系式有

$$p_i^B \gamma_i^{BR} p_i^R \gamma_i^{RB} > 1 + p_i^S \gamma_i^{SR} + p_i^B \gamma_i^{BR}$$

如前所述, 零干扰功率与零中继功率都将导致

零安全速率, 因而必有  $p_i^B > 0$ , 结合上述不等式关系可得式(8)。基于式(8), 可知  $\mathcal{N}$  中所有 MS 获得正安全速率的条件是  $P^R \geq \sum_{i \in \mathcal{N}} p_i^R > \sum_{i \in \mathcal{N}} p_{i,th}^R > \sum_{i \in \mathcal{N}} 1/\gamma_i^{RB}$ 。其中, 最后一个严格不等式基于  $p_i^B > 0, \forall i \in \mathcal{N}$ 。

引理 1 中式(8)刻画了  $p_i^B$  和  $p_i^R$  之间非线性耦合的精确关系。式(9)仅是必要而非充分条件, 即如果式(9)不成立, 则由于系统过载必然导致集合  $\mathcal{N}$  中部分 MS 被拒绝, 而如果式(9)成立, 仍然可能存在集合  $\mathcal{N}$  中的 MS 被系统拒绝。基于此, 本质上 OP1 等价于如下联合接入控制和功率分配问题

$$\text{OP2: } \max_{\mathcal{N}^\circ \subseteq \mathcal{N}, (\mathbf{p}^R, \mathbf{p}^B)} R^\circ(\mathbf{p}^B, \mathbf{p}^R) = \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^R) \quad (10a)$$

$$\text{s.t. } \sum_{i \in \mathcal{N}^\circ} p_i^R \leq P^R \text{ 和 } \sum_{i \in \mathcal{N}^\circ} p_i^B \leq P^B \quad (10b)$$

$$\mathbb{I}\{p_i^R > p_{i,th}^R\} = \mathbb{I}\{p_i^B > 0\}, \forall i \in \mathcal{N}^\circ \quad (10c)$$

其中,  $\mathcal{N}^\circ$  表示成功接入系统的 MS 集合, 即集合  $\mathcal{N}^\circ$  中的 MS 将获得正安全速率。定义  $\mathcal{N}^\circ = |\mathcal{N}^\circ|$ ,  $\mathbf{p}^R = (p_1^R, \dots, p_{\mathcal{N}^\circ}^R)$  和  $\mathbf{p}^B = (p_1^B, \dots, p_{\mathcal{N}^\circ}^B)$  分别表示 UR 和 BS 分配给集合  $\mathcal{N}^\circ$  中 MS 的功率矢量。在式(10a)中, 定义  $R_i^\circ(p_i^B, p_i^R) = R_i^B(p_i^B, p_i^R) - R_i^R(p_i^B)$ , 当且仅当  $R_i^B(p_i^B, p_i^R) > 0$  时表示安全速率, 本文定义  $R_i^\circ(p_i^B, p_i^R)$  为可以取负值的广义安全速率。式(10c)源于式(8)和式(7c), 由式(8)可知,  $p_{i,th}^R$  是  $p_i^B$  的函数。对于 OP2 可能存在的争论是: 尽管基于引理 1 能够移除运算  $[\cdot]^+$  并获得平滑的目标函数以及  $p_i^B$  和  $p_i^R$  之间精确的耦合关系, 但约束式(10c)和接入控制使 OP2 是一个混合整数非线性规划问题(MINLP, mixed integer non-linear programming), 因而难以求解。为此, 基于 OP2, 本文引出 OP2 松弛问题 OP3,

$$\text{OP3: } \max_{\mathcal{N}^\circ \subseteq \mathcal{N}} \left\{ \begin{array}{l} \max_{(\mathbf{p}^R, \mathbf{p}^B)} R^\circ(\mathbf{p}^B, \mathbf{p}^R) = \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^R) \\ \text{s.t. } \sum_{i \in \mathcal{N}^\circ} p_i^R \leq P^R, \sum_{i \in \mathcal{N}^\circ} p_i^B \leq P^B \end{array} \right\} \quad (11)$$

可以看出, 通过移除 OP2 的约束式(10c)以获得 OP3。对比 OP2 和 OP3 可发现, 在可处理性上 OP3 有 2 个显著特点: 1) OP3 可分解为 2 个子问题, 内部联合功率分配子问题和外部 MS 接入选择子问题; 2) 在给定接入控制集合  $\mathcal{N}^\circ$  下, 联合功率控制问题的约束集合为凸。但求解 OP3 仍面临挑战: 1) 从数学结构上看, OP3 仍是混合整数非线性规划,

该问题已证明是 NP-难; 2) 给定  $\mathcal{N}^\circ$  下, 尽管 OP3 的内部子问题具有凸约束, 但其目标函数关于决策变量是非凸/非凹的, 因而整个问题仍是非凸; 3) 直接求解 OP3 的外部子问题, 即 MS 接入选择问题, 具有指数复杂度, 且当前不能构造出确定最优集合  $\mathcal{N}^\circ$  的准则; 4) 交替求解 OP3 内部子问题和外部子问题获得的解可能仅是 OP3 的次优解, 且对比 OP2 和 OP3 的定义可知, OP3 的可行解可能位于 OP2 可行域外部。尽管如此, 基于 OP3 仍能获得系统性方法以求解 OP2 的可行次优解。

求解 OP3 的方法: 1) 基于交替机制求解 OP3 的内部子问题和外部子问题; 2) 内部子问题利用交替优化分别执行中继功率与干扰功率分配, 尽管 OP3 定义的目标函数是非凹, 但在给定中继功率分配下, OP3 内部子问题最优干扰功率分配具有唯一解, 而在给定干扰功率分配下, OP3 内部子问题最优中继功率分配是凸规划; 3) 对于 OP3 外部子问题, 基于证明命题 1 的思想设计一种启发式机制求解, 即在初始阶段, 假设所有 MS 都接入, 随后在每轮 OP3 外部子问题与内部交替结束后, 排除获得最小安全速率的 MS, 该流程重复直到所获得的安全速率非增为止。

令  $\mathcal{F}_{OP2}$  和  $\mathcal{F}_{OP3}$  分别表示 OP2 和 OP3 的可行域, 用  $\mathcal{S}_{OP3} = \{\mathcal{N}_{OP3}^*, p_{i,OP3}^{*R}, p_{i,OP3}^{*B} : \forall i \in \mathcal{N}_{OP3}^*\}$  表示 OP3 的任一次优/最优解, 则有如下命题。

**命题 1** 对于 OP2 和 OP3, 有  $\mathcal{F}_{OP2} \subseteq \mathcal{F}_{OP3}$  和  $\mathcal{S}_{OP3} \in \mathcal{F}_{OP2}$ 。

**证明** OP2 的可行域为  $\mathcal{F}_{OP2} = \{(\mathcal{N}^\circ, \mathbf{p}^R, \mathbf{p}^B) \mid \mathcal{N}^\circ \subseteq \mathcal{N}, (\mathbf{p}^R, \mathbf{p}^B) \text{ 满足式(10b)和式(10c)}\}$ , 而 OP3 的可行域为  $\mathcal{F}_{OP3} = \{(\mathcal{N}^\circ, \mathbf{p}^R, \mathbf{p}^B) \mid \mathcal{N}^\circ \subseteq \mathcal{N}, (\mathbf{p}^R, \mathbf{p}^B) \text{ 满足式(10b)}\}$ , 即有  $\mathcal{F}_{OP2} \subseteq \mathcal{F}_{OP3}$ 。基于此, 证明  $\mathcal{S}_{OP3} \in \mathcal{F}_{OP2}$  等价于证明对  $\forall i \in \mathcal{N}_{OP3}^*$ , 有  $0 < p_{i,th}^{*R}(p_{i,OP3}^{*B}) < p_{i,OP3}^{*R}$  和  $p_{i,OP3}^{*B} > 0$ 。下面利用反证法给出该结论的证明。

如果  $\exists i \in \mathcal{N}_{OP3}^*$  使下面 4 种情况之一成立。

**情况 1** 如果  $p_{i,OP3}^{*B} = 0$  和  $p_{i,OP3}^{*R} = 0$ , 则有

$$\begin{aligned} & \left[ R_i^B(p_{i,OP3}^{*B}, p_{i,OP3}^{*R}) - R_i^R(p_{i,OP3}^{*B}) \right] \\ & = \log 1 - \log(1 + p_i^S \gamma_i^{SR}) < 0 \end{aligned}$$

**情况 2** 如果  $p_{i,OP3}^{*B} = 0$  和  $p_{i,OP3}^{*R} > 0$ , 则有

$$\left[ R_i^B(p_{i,OP3}^{*B}, p_{i,OP3}^{*R}) - R_i^R(p_{i,OP3}^{*B}) \right]$$

$$= \log \left( 1 + \frac{p_i^S p_{i,OP3}^{*R} \gamma_i^{SR} \gamma_i^{RB}}{1 + p_i^S \gamma_i^{SR} + p_{i,OP3}^{*R} \gamma_i^{RB}} \right) - \log(1 + p_i^S \gamma_i^{SR}) < 0$$

情况 3 如果  $p_{i,OP3}^{*B} > 0$  和  $p_{i,OP3}^{*R} = 0$ , 则有

$$\begin{aligned} & \left[ R_i^B(p_{i,OP3}^{*B}, p_{i,OP3}^{*R}) - R_i^R(p_{i,OP3}^{*B}) \right] \\ & = \log 1 - \log \left( 1 + \frac{p_i^S \gamma_i^{SR}}{1 + p_{i,OP3}^{*B} \gamma_i^{BR}} \right) < 0 \end{aligned}$$

情况 4 如果  $0 < p_{i,OP3}^{*R} < p_{i,th}^{*R}(p_{i,OP3}^{*B})$  和  $p_{i,OP3}^{*B} > 0$ ,

则基于引理 1 有

$$\begin{aligned} & \left[ R_i^B(p_{i,OP3}^{*B}, p_{i,OP3}^{*R}) - R_i^R(p_{i,OP3}^{*B}) \right] \\ & = \log \left( 1 + \frac{p_i^S p_{i,OP3}^{*R} \gamma_i^{SR} \gamma_i^{RB}}{1 + p_i^S \gamma_i^{SR} + p_{i,OP3}^{*R} \gamma_i^{RB} + p_{i,OP3}^{*B} \gamma_i^{BR}} \right) \end{aligned}$$

由此可知, 对  $\forall i \in \mathcal{N}_{OP3}^*$ , 如果  $(p_{i,OP3}^{*B}, p_{i,OP3}^{*R})$  不满足条件  $0 < p_{i,th}^{*R}(p_{i,OP3}^{*B}) < p_{i,OP3}^{*R}$  和  $p_{i,OP3}^{*B} > 0$ , 则该 MS 获得负目标函数值, 此时在 OP3 外部子问题优化下移除该 MS 即使不重新分配功率也将增加系统广义安全速率。这种 MS 移除不违反已有功率约束。因此,  $\mathcal{S}_{OP3}$  对 OP3 并非最优也不是严格意义上次优, 即必有  $\mathcal{S}_{OP3} \in \mathcal{F}_{OP2}$ 。综上, 有命题 1 成立。

基于命题 1, 接下来将着重分析 OP3, 即通过求解 OP3 获得 OP2 的次优解。其中 OP3 求解思路如下: 执行 OP3 内部子问题与外部子问题交替优化, 针对内部子问题执行干扰功率与中继功率分配交替优化。

### 3.2 交替优化与次优化算法

#### 3.2.1 固定干扰功率下的最优中继功率分配

假设干扰功率  $\mathbf{p}^B$  和接入 MS 集合  $\mathcal{N}^\circ$  已确定, 考虑中继功率分配问题。由 OP3 可知, 中继功率分配问题具有如下形式。

$$\text{OP4: } \max_{\mathbf{p}^R} \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^{*B}, p_i^R) \quad (12a)$$

$$\text{s.t. } \sum_{i \in \mathcal{N}^\circ} p_i^R \leq P^R, \text{ 固定 } \mathbf{p}^{*B} \quad (12b)$$

由于  $R_i^\circ(p_i^{*B}, p_i^R) = R_i^B(p_i^{*B}, p_i^R) - R_i^R(p_i^{*B})$ , 以及固定干扰功率分配  $\mathbf{p}^{*B}$ , 因此中继功率最优化仅涉及到  $\sum_{i \in \mathcal{N}^\circ} R_i^B(p_i^{*B}, p_i^R)$ 。从形式上看, 该问题类似于并行正交高斯信道下基于 AF 协作协议的中继功率分配问题<sup>[12]</sup>, 则 OP4 的最优解由如下定理刻画。

定理 1 对于给定  $\mathbf{p}^{*B}$  和  $\mathcal{N}^\circ$  下优化问题 OP4, 集合  $\mathcal{N}^\circ$  中 MS  $i$  分配的中继功率为

$$p_i^{*R} = \left[ \frac{\sqrt{B_i^2 - 4A_i C_i} - B_i}{2A_i} \right], \quad \forall i \in \mathcal{N}^\circ \quad (13)$$

其中,  $A_i = (\gamma_i^{RB})^2 (1 + p_i^S \gamma_i^{SR})$ ,  $B_i = \gamma_i^{RB} (2 + p_i^S \gamma_i^{SR}) \cdot (1 + p_i^S \gamma_i^{SR} + p_i^{*B} \gamma_i^{BR})$ ,  $C_i = C_{i0}^2 - p_i^S \gamma_i^{SR} \gamma_i^{RB} C_{i0} / \lambda^*$ ,  $C_{i0} = (1 + p_i^S \gamma_i^{SR} + p_i^{*B} \gamma_i^{BR})$ ,  $\lambda^*$  取值满足  $\sum_{i \in \mathcal{N}^\circ} p_i^{*R} \cdot (\lambda^*, p_i^{*B}) = P^R$ 。

证明 给定  $\mathcal{N}^\circ$  和  $\mathbf{p}^{*B}$ , 可知约束式(12b)是凸集, 仅需分析目标函数凹凸性。求  $\sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^{*B}, p_i^R)$  和  $R_i^\circ(p_i^B, p_i^R) = R_i^B(p_i^B, p_i^R) - R_i^R(p_i^B)$  关于  $p_i^R$  和  $p_j^R (j \neq i)$  的偏导, 有

$$\begin{aligned} & \partial \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^{*B}, p_i^R) / \partial p_i^R = \partial R_i^\circ(p_i^{*B}, p_i^R) / \partial p_i^R > 0; \\ & \partial^2 R_i^\circ(p_i^{*B}, p_i^R) / \partial (p_i^R)^2 < 0; \quad \partial^2 R_i^\circ(p_i^{*B}, p_i^R) / \partial p_i^R \partial p_j^R = 0. \end{aligned}$$

可知, 目标函数是  $p_i^R, \forall i \in \mathcal{N}^\circ$  的单调增函数, 且关于  $\mathbf{p}^R$  凹, 即 OP4 是关于  $\mathbf{p}^R$  的凸优化问题, 可用 KKT 条件获得 OP4 的最优解, 即式(13)。

#### 3.2.2 固定中继功率下的最优干扰功率分配

给定中继功率分配  $\mathbf{p}^{*R}$  和 MS 接入集合  $\mathcal{N}^\circ$  时, 由 OP3 可知, 此时干扰功率分配问题形式如下

$$\text{OP5: } \max_{\mathbf{p}^B} \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^{*R}) \quad (14a)$$

$$\text{s.t. } \sum_{i \in \mathcal{N}^\circ} p_i^B \leq P^B, \text{ 固定 } \mathbf{p}^{*R} \quad (14b)$$

由于干扰功率约束式(14b)是凸集, 仅需分析目标函数的凹凸性。对  $\sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^{*R})$  求关于  $p_i^B, \forall i \in \mathcal{N}^\circ$  的偏导, 有

$$\frac{\partial \sum_{i \in \mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^{*R})}{\partial p_i^B} = p_i^S \gamma_i^{SR} \gamma_i^{BR} \frac{D_i (p_i^B)^2 + E_i p_i^B + F_i}{O_i} \quad (15)$$

其中,  $D_i = (1 - p_i^{*R} \gamma_i^{RB}) (\gamma_i^{BR})^2$ ,  $E_i > 0$ ,  $F_i > 0$ ,  $O_i > 0$ 。如果  $p_i^{*R} \gamma_i^{RB} > 1$ , 则  $R_i^\circ(p_i^B, p_i^{*R})$  为  $p_i^B$  的拟凹函数, 且在如下干扰功率取值下达到最大

$$p_{i,1}^{*B} = \frac{-E_i - \sqrt{E_i^2 - 4D_i F_i}}{2D_i} \quad (16)$$

即  $R_i^\circ(p_i^B, p_i^{*R})$  是关于  $p_i^B$  在区间  $p_i^B \in [0, p_{i,1}^{*B}]$  上的

增函数, 是关于  $p_i^B$  在区间  $p_i^B \in (p_i^{*B}, \infty)$  上的减函数。如果  $p_i^{*R} \gamma_i^{RB} \leq 1$ , 则有  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B > 0$  和  $\partial^2 R_i^\circ(p_i^B, p_i^{*R}) / \partial (p_i^B)^2 < 0$ , 即目标函数是关于  $p_i^B$  的单调增且凹函数。由 BS 处的功率约束  $P^B$  可知,  $R_i^\circ(p_i^B, p_i^{*R})$  在  $p_i^B = P^B$  处取最大值。基于此, 虽然  $R_i^\circ(p_i^B, p_i^{*R})$  不是关于  $p_i^B, \forall i \in \mathcal{N}^\circ$  的凹函数, 即 KKT 条件不是 OP5 最优解的充分条件, 但由于目标函数光滑, KKT 条件仍可作为最优解的必要条件。基于上述分析, 有

$$\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B - \xi = 0, \forall i \in \mathcal{N}^\circ \quad (17)$$

其中,  $\xi$  是功率约束式(14b)的拉格朗日乘子。基于式(17), 定理 2 刻画了问题 OP5 最优解性质。

**定理 2** 对于 OP5 及给定  $\mathbf{p}^{*R}$  和  $\mathcal{N}^\circ$ , 若对  $i \in \mathcal{N}^\circ$  有  $p_i^{*R} \gamma_i^{RB} > 1$ , 则  $p_i^{*B}$  为式(16); 若对  $i \in \mathcal{N}^\circ$  有  $p_j^{*R} \gamma_j^{RB} \leq 1$ , 则  $p_i^{*B} = P^B$ 。定义  $p_{i,2}^{*B}(\xi)$  为给定  $\xi$  式(17)的第  $i$  个等式的实正根, 且  $\mathcal{X}_i = \{p_{i,2}^{*B}(\xi) | p_{i,2}^{*B}(\xi) > 0, \partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B |_{p_{i,2}^{*B}(\xi)} - \xi = 0\}$ , OP5 的唯一解表示为  $\xi^*, \{p_i^{*B} : \forall i \in \mathcal{N}^\circ\}$ , 则有:

**性质①** 如果  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B} \leq P^B$ , 有  $p_i^{*B} = p_{i,1}^{*B}$  和  $\xi^* = 0$ ; 否则  $p_i^{*B} = \tilde{p}_i^{*B} \cdot \mathbb{I}\{\mathcal{X}_i \neq \Phi\} + 0 \cdot \mathbb{I}\{\mathcal{X}_i = \Phi\}$ , 其中  $\tilde{p}_i^{*B} = \arg \max_{p_{i,2}^{*B} \in \mathcal{X}_i} p_{i,2}^{*B}$ ,  $\Phi$  为空集,  $\xi^*$  取值满足  $\sum_{i \in \mathcal{N}^\circ} p_i^{*B}(p_i^{*R}, \xi) = P^B$ ;

**性质②** 如果  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B} > P^B$ ,  $\sum_{i \in \mathcal{N}^\circ} p_i^{*B}(p_i^{*R}, \xi)$  是关于  $\xi$  的减函数。

**证明** 限于篇幅, 这里仅给出性质①第二部分结论的证明, 性质①第一部分结论和性质②可依据本文分析得出。

证明性质①第二部分, 即条件  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B}(p_i^{*R}) > P^B$  为真。分析可知, 该条件为真只可能是 3 种情形: 1) 对  $\forall i \in \mathcal{N}^\circ$ , 有  $p_i^{*R} \gamma_i^{RB} > 1$  和  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B}(p_i^{*R}) > P^B$ ; 2)  $\exists i \in \mathcal{N}^\circ$  使  $p_i^{*R} \gamma_i^{RB} \leq 1$ , 也  $\exists j \in \mathcal{N}^\circ$  使  $p_j^{*R} \gamma_j^{RB} > 1, j \neq i$ ; 3) 对  $\forall i \in \mathcal{N}^\circ$ , 有  $p_i^{*R} \gamma_i^{RB} \leq 1$  和  $|\mathcal{N}^\circ| > 1$ 。尽管如此, 此时不论系统处于上述 3 种情形的哪一种, OP5 的最优解仍满足 KKT 条件。依据  $p_i^{*R} \gamma_i^{RB}$  的

取值, 下面分别讨论式(17)的解。

S1: 如果对  $i \in \mathcal{N}^\circ$  有  $p_i^{*R} \gamma_i^{RB} \leq 1$ , 则由式(15)可知,  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B |_{p_i^B=0} = \xi_{th} > 0$  和  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B |_{p_i^B=\infty} = 0$ 。另外, 容易证明  $\partial^2 R_i^\circ(p_i^B, p_i^{*R}) / \partial (p_i^B)^2 < 0$ , 这意味着  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B$  是关于  $p_i^B$  的单调减函数, 在  $p_i^B = 0$  时取最大值  $\xi_{th}$ 。基于对  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B$  的分析, 式(17)在  $p_i^{*R} \gamma_i^{RB} \leq 1$  时的解有 2 种情况: 1) 如果  $\xi < \xi_{th}$ , 则式(17)有唯一正实根, 定义该正实根为  $p_{i,2}^{*B}$ , 即  $|\mathcal{X}_i| = 1$  和  $p_i^{*B} = p_{i,2}^{*B}$ ; 2) 如果  $\xi \geq \xi_{th}$ , 则式(17)无正实根, 有  $\mathcal{X}_i = \Phi$  和  $p_i^{*B} = 0$ 。

S2: 如果  $i \in \mathcal{N}^\circ$  和  $p_i^{*R} \gamma_i^{RB} > 1$ , 则由式(15)可知, 在  $p_i^B \in [0, p_{i,1}^{*B})$  有  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B > 0$ , 在  $p_i^B \in (p_i^{*B}, \infty)$  有  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B < 0$ 。如果  $p_{i,2}^{*B}$  在  $\xi > 0$  下式(17)有正实根, 则  $0 < p_{i,2}^{*B} < p_{i,1}^{*B}$ 。为了分析式(17)的正实根数, 将式(15)代入式(17)并化简, 有如下 4 次函数

$$H_{i,4}(p_i^B)^4 + H_{i,3}(p_i^B)^3 + (H_{i,2}\xi - D_i)(p_i^B)^2 + (H_{i,1}\xi - E_i)p_i^B + H_{i,0}\xi - F_i = 0 \quad (18)$$

可知,  $H_{i,j} > 0, \forall j = 0, \dots, 4, E_i > 0$  和  $F_i > 0$ 。由于  $p_i^{*R} \gamma_i^{RB} > 1$ , 即有  $D_i < 0$  和  $H_{i,2}\xi - D_i > 0$ 。基于笛卡尔符号规则, 式(18)的正实根数最多为 2。如果  $H_{i,1}\xi - E_i < 0$  和  $H_{i,0}\xi - F_i > 0$ , 则式(18)的正实根数最大为 2; 如果  $H_{i,1}\xi - E_i \geq 0$  和  $H_{i,0}\xi - F_i < 0$  或  $H_{i,1}\xi - E_i < 0$  和  $H_{i,0}\xi - F_i = 0$ , 则式(18)的正实根数最多为 1; 如果  $H_{i,1}\xi - E_i \geq 0$  和  $H_{i,0}\xi - F_i \geq 0$ , 则式(18)的正实根数为 0。定义式(18)的正实根集合为  $\mathcal{X}_i (\forall i \in \mathcal{N}^\circ)$ , 则可能存在以下情况,  $|\mathcal{X}_i| = 2$  或  $|\mathcal{X}_i| = 1$  或  $|\mathcal{X}_i| = 0$ 。若  $|\mathcal{X}_i| = 2$ , 令  $\mathcal{X}_i = \{p_{i,2,1}^{*B}, p_{i,2,2}^{*B}\}$ , 不失一般性, 假设  $0 < p_{i,2,1}^{*B} < p_{i,2,2}^{*B} < p_{i,1}^{*B}$ 。由于已知在  $p_i^B \in [0, p_{i,1}^{*B})$ , 有  $\partial R_i^\circ(p_i^B, p_i^{*R}) / \partial p_i^B > 0$ , 即广义安全速率函数  $R_i^\circ(p_i^B, p_i^{*R})$  在  $p_i^B \in [0, p_{i,1}^{*B})$  是增函数, 因此有  $R_i^\circ(p_{i,2,2}^{*B}, p_i^{*R}) > R_i^\circ(p_{i,2,1}^{*B}, p_i^{*R})$  和  $\tilde{p}_i^{*B} = p_{i,2,2}^{*B}$ , 即  $\tilde{p}_i^{*B} = \arg \max_{p_{i,2}^{*B} \in \mathcal{X}_i} p_{i,2}^{*B}$  为最优解; 若  $|\mathcal{X}_i| = 1$ , 有  $\mathcal{X}_i = \{p_{i,2}^{*B}\}$ , 即  $p_{i,2}^{*B}$  是最优解; 若  $|\mathcal{X}_i| = 0$ , 有  $\mathcal{X}_i = \Phi$ ,

即式(18)的正实根集合为空,  $\tilde{p}_i^{*B} = 0$ 。由 KKT 条件可知, 在最优解  $\xi^*$ ,  $\{p_i^{*B} : \forall i \in \mathcal{N}^\circ\}$  处需满足 BS 的功率约束, 因此  $\xi^*$  的取值必满足  $\sum_{i \in \mathcal{N}^\circ} p_i^{*B}(p_i^{*R}, \xi) = P^B$ 。综上, 有性质①。

基于定理 2 及给定  $p^{*R}$  和  $\mathcal{N}^\circ$ , 首先由式(16)计算各 MS 干扰功率  $p_{i,1}^{*B}$ ,  $\forall i \in \mathcal{N}^\circ$ 。若  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B}(p_i^{*R}) \leq P^B$ , 即接入 MS 干扰功率和需求小于或等于 BS 总可用功率, 则所有接入 MS 获得干扰功率  $p_i^{*B} = p_{i,1}^{*B}, \forall i \in \mathcal{N}^\circ$ ; 若  $\sum_{i \in \mathcal{N}^\circ} p_{i,1}^{*B}(p_i^{*R}) > P^B$ , 则需依据定理 2 执行二分搜索以获得最优拉格朗日乘子  $\xi^*$ , 并根据式(17)计算相应干扰功率。

### 3.2.3 接入控制机制和交替优化算法

本文设计的联合接入控制的交替最优中继功率与最优干扰功率分配算法 (OptROptJam, alternatively optimization relay power and optimization jamming power allocation algorithm)的核心思想是: 当交替中继功率与干扰功率迭代收敛后, 通过动态排除接入 MS 集合中具有最小安全速率的 MS, 直到系统安全速率非递增。

#### 算法 1 OptROptJam

**step1** 初始化  $t = 0$ ,  $\mathcal{N}^\circ(t) = \mathcal{N}$ ,  $p^B(t) = p_0^B$ ;

**step2** 基于定理 1 和定理 2, 交替优化中继功率与干扰功率分配并获得  $p_i^B(t)$  和  $p_i^R(t)$ , 跳转到 step 3;

**step3** 计算系统广义安全速率  $\sum_{i \in \mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t))$ , 如果  $\sum_{i \in \mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t)) > \sum_{i \in \mathcal{N}^\circ(t-1)} R_i^\circ(p_i^B(t-1), p_i^R(t-1))$ , 则  $\mathcal{N}^\circ(t) = \mathcal{N}^\circ(t) \setminus \{i^*\}$  和  $t = t + 1$ , 跳转到 step 2, 其中  $i^* = \arg \min_{i \in \mathcal{N}^\circ(t)} R_i^\circ(t)$ ; 否则, 算法结束。

其中,  $t$  表示算法迭代时间,  $\mathcal{N}^\circ(t)$  表示在时刻  $t$  接入的 MS 子集, 初始阶段设置  $\mathcal{N}^\circ(0) = \mathcal{N}$ , 即所有 MS 都被系统接入。 $p_0^B$  是算法初始点, 即设置一个干扰功率矢量作为算法的初始点并执行中继功率迭代, 初始点设置应满足功率约束条件。step 2 的收敛条件是: 连续 2 轮中继功率迭代和干扰功率迭代的差值和小于门限值  $\varepsilon$ 。step 3 中如果运算

$\arg \min_{i \in \mathcal{N}^\circ(t)} R_i^\circ(t)$  反馈多个 MS, 则随机选择一个 MS 执行移除操作。

次优性和收敛性: 对于算法 1, 其最优性受 2 个因素影响: 1) 成功接入 MS 集合  $\mathcal{N}^\circ$  的最优性; 2) 交替迭代算法的最优性。对于前者, 因为构造最优接入 MS 子集的规则当前还不清楚, 因而其最优性无法评估, 本文将利用仿真结果进行评估。对于交替最优化, 其可能不收敛, 因而也可能无法收敛到全局最优解。但针对算法 1 有如下收敛性和次优性结论。

**命题 2** 算法 1 必收敛到稳定点, 且由算法 1 生成的稳定点对 OP2 而言至少是次优的。

**证明** 给定  $\mathcal{N}^\circ$ , 由文献[12,13]可知, 交替中继和干扰功率优化属于非线性高斯-赛德尔方法且决策矢量被分割为 2 组矢量。另外, 对于给定中继功率下干扰功率分配具有唯一解, 而给定干扰功率分配下中继功率分配同样有唯一解。因此, 由文献[13]和命题 1 可知, 该交替优化算法必收敛且至少获得一个 OP2 的次优可行解。

复杂性: 算法 1 复杂性取决于交替迭代和接入控制, 前者涉及 2 个最优拉格朗日乘子搜索, 分别具有近似复杂度  $O(N \text{lb}(\lambda^*/\varepsilon))$  和  $O(N \text{lb}(\xi^*/\varepsilon))$ , 其中,  $\lambda^*$  和  $\xi^*$  在定理 1 和定理 2 中给出,  $\varepsilon$  是算法 1 中 step 2 收敛时系统允许的误差因子。接入控制机制复杂度近似为  $O(N^2)$ ,  $N$  为系统中 MS 数。

### 3.2.4 其他次优算法

基于如下原因, 提出另一种次优算法: 1) 探索低复杂度算法; 2) 作为本文算法 1 性能分析的参考。具体地, 在算法迭代时刻  $t$ , 中继和干扰功率分配规则分别为

$$p_i^R(t) = P^R / |\mathcal{N}^\circ(t)| \quad (19)$$

$$p_i^B(t) = P^B \frac{p_{i,1}^{*B}(p_i^R(t))}{\sum_{i \in \mathcal{N}^\circ(t)} p_{i,1}^{*B}(p_i^R(t))} \mathbb{I} \left\{ \sum_{i \in \mathcal{N}^\circ(t)} p_{i,1}^{*B}(p_i^R(t)) > P^B \right\} + p_{i,1}^{*B}(p_i^R(t)) \mathbb{I} \left\{ \sum_{i \in \mathcal{N}^\circ(t)} p_{i,1}^{*B}(p_i^R(t)) \leq P^B \right\} \quad (20)$$

即 UR 均分功率给当前 MS 接入集合  $\mathcal{N}^\circ(t)$  中的所有 MS,  $p_{i,1}^{*B}(p_i^R(t))$  在定理 2 中定义。由此可知, BS 功率分配基于比例机制, 即当

$\sum_{i \in \mathcal{N}^o} p_{i,1}^{*B}(p_i^R) \leq P^B$  时, MS  $i$  获得定理 2 中定义的干扰功率  $p_{i,1}^{*B}(p_i^R(t))$ ; 否则, 干扰功率是自身干扰功率需求与系统总干扰功率之比, 即  $P^B p_{i,1}^{*B}(p_i^R(t)) / \sum_{i \in \mathcal{N}^o(t)} p_{i,1}^{*B}(p_i^R(t))$ 。接入控制机制与算法 1 相同, 即在完成中继与干扰功率分配后, 排除获得最小安全速率的 MS 并重复功率交替优化过程与 MS 移除程序直到系统安全速率非增。在以下对比分析中, 定义基于式(19)和式(20)的次优算法为算法 2, 即等中继功率分配和最优比例干扰功率分配(EROptPJam, equal relay power and optimal proportional jamming power allocation)。算法 2 相对于算法 1 具有更低的复杂度, 因为无需最优功率迭代, 但存在一定性能损失。

#### 4 仿真分析

本节给出验证本文提出算法性能的仿真结果, 仿真网络场景如图 2 所示, 相关仿真参数设置参考文献 [15, 16], 具体地, BS 位置是平面坐标点(100, 0), 多个 MS 随机分布于虚线矩形框内, 且矩形框的 X 坐标范围为-100 到 0, Y 坐标范围为-50 到 50。UR 的 Y 坐标固定为 0, 其 X 坐标变化范围为 0~100。信道增益模型是  $\eta(0.097/d^\tau)^{\frac{1}{2}}$ , 其中,  $d$  为任意两点之间的平面距离,  $\tau=4$  是路径损耗因子,  $\eta$  表示信道衰落且满足  $\eta \sim CN(0,1)$ 。可以看出, UR 相对于所有 MS 而言到 BS 具有更好的信道条件。仿真中, 噪声功率  $\sigma^2 = 10^{-8}$  W, 交替中继与干扰功率迭代收敛门限值因子  $\varepsilon=10^{-5}$ 。为了对比本文提出的算法, 引入 2 个基于 UR 和 BS 联合功率约束的次优算法如下。

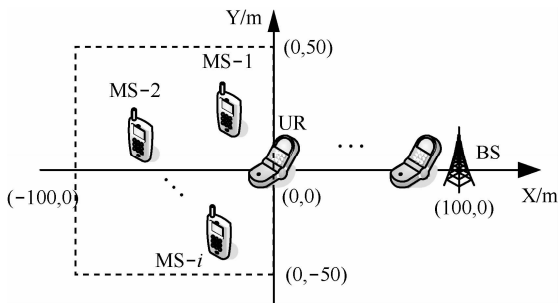


图 2 仿真网络拓扑

联合功率约束交替优化算法(JoPowerOpt, joint power constraint-base alternating optimization): 该算法基于 UR 和 BS 联合功率约束  $P^R + P^B = P$ , 显然, 此算法能平衡 UR 和 BS 功率使用从而获得更好的

性能<sup>[17]</sup>, 但联合功率约束在本文建立的非信任中继协作场景中适用性受限, 这里引入该算法的目的在于性能参考。

扩展联合功率约束交替优化算法 (ExJoPowerOpt, extension of joint power constraint-based alternating optimization): 为算法 JoPowerOpt 扩展到独立功率约束场景。具体地, 当算法 JoPowerOpt 收敛后判断其是否同时满足 UR 和 BS 独立功率约束, 如果是, 则结束算法; 否则执行  $P = P - \Delta$  操作并重复算法 JoPowerOpt 直到满足 UR 和 BS 独立功率约束。

首先, 在不同 UR 位置下分析本文提出算法性能, 结果如图 3 所示。在仿真中, UR 初始位置为(5,0), 沿  $Y=0$  直线运动到点(80,0), BS 和 UR 的功率约束分别为  $P^B = 2.0$  W,  $P^R = 1.5$  W, MS 数  $N=15$ , 假设所有 MS 具有相同发射功率  $p^S = p_i^S = 0.2$  W,  $\forall i \in \mathcal{N}$ 。图 3 是系统安全速率随 UR 的 X 坐标变化情况。可以看出, 随着 UR 从远离 BS 移动到 BS 附近, 系统安全速率在不同算法下逐渐增加, 主要原因有三: 1) 多 MS 接入分集增益; 2) BS 干扰效率提高; 3) UR 窃听能力减弱。对于多 MS 接入分集增益, 可由引理 1 解释, 即任意 MS  $i$  获得正安全速率的最小中继功率门限值是  $p_{i,th}^R$ , 由该门限值定义式(6)可看出, 其是  $\gamma_i^{BR}$  和  $(1 + p_i^S \gamma_i^{SR}) / p_i^B \gamma_i^{RB}$  的减函数。当 UR 向 BS 靠近方向移动时  $\gamma_i^{BR}$  减小, 基于干扰功率控制可认为  $(1 + p_i^S \gamma_i^{SR}) / p_i^B \gamma_i^{RB}$  保持不变, 则门限值  $p_{i,th}^R$  将减小, 使更多 MS 接入, 这点也可从图 4 印证, 即随着 UR 到 BS 距离越来越近, 成功接入 MS 数增多, 因而为系统提供了多 MS 接入分集增益。对于 BS 干扰效率提高, 可在分析图 5 时给出。而 UR 向 BS 靠近必然导致 MS 到 UR 信道增益减小, 导致安全速率定义式(4)第二项变小, 即 UR 窃听能力减弱。

从图 3 还可看出, 算法 JoPowerOpt 的安全速率性能优于其他 3 种算法, 且当 UR 远离 BS 时算法 JoPowerOpt 和算法 OptROptJam 性能差异较小, 而当 UR 向靠近 BS 方向移动时该性能差异先增大再减小。性能差异增大是由于算法 JoPowerOpt 在向 BS 靠近过程中, BS 干扰功率需求减小而使更多功率能够平衡给 UR 执行中继, 即获得联合功率约束下资源平衡使用带来的性能增益, 而性能差异减小主要是由于当 UR 移动到非常靠近 BS 时 UR 中继协作增益减小。另外, 算法 EROptPJam/

ExJoPowerOpt 和算法 OptROptJam 的性能差异起初较大,但随着 UR 移动到 BS 附近这种性能差异逐渐减小。需要指出的是,对于算法 EROptPJam 和算法 ExJoPowerOpt 而言,这种性能差异减小的原因是相似的:1) 对于算法 EROptPJam,当 UR 移动到 BS 附近时,最优比例干扰与最优干扰性能几乎一致,而 UR 中继带来的安全速率增益性能将趋近于算法 OptROptJam;2) 算法 ExJoPowerOpt 在 UR 靠近 BS 时也工作在最优干扰状态,但获得的中继协作增益趋于 OptROptJam。

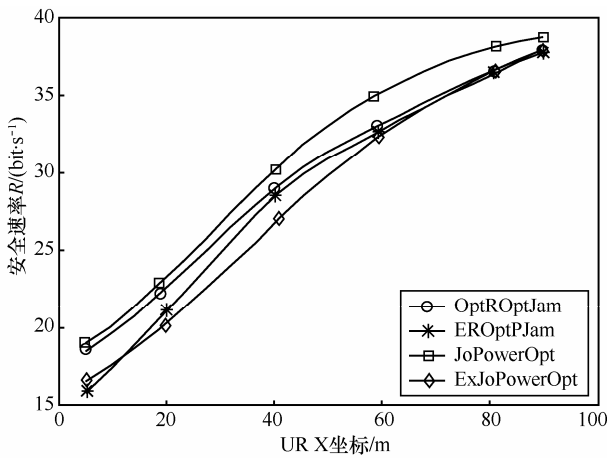


图 3 系统和安全速率随 UR X 坐标变化

图 4 是系统成功接入 MS 数随 UR X-坐标变化情况。可以看出,当 UR 向靠近 BS 方向移动时,系统成功接入 MS 数增加,其原因可用引理 1 解释。另外,当 UR 从(5, 0)移动到(30, 0)时,算法 JoPowerOpt 和 OptROptJam 在成功接入 MS 数性能上几乎一致,算法 EROptPJam 成功接入 MS 数较前两种算法少,而算法 ExJoPowerOpt 接入最少 MS 数。由图 3 和图 4 可知,尽管算法 EROptPJam 在平均接入 MS 数上与算法 OptROptJam/JoPowerOpt 差异不大,但获得的安全速率性能较低,特别是在 UR 远离 BS 时。由此可知,算法 OptROptJam/JoPowerOpt 能够获得更好的资源效率。

图 5 是 BS 处功率开销随 UR X 坐标变化情况,可以看出,当 UR 到 BS 距离越小,BS 的干扰功率开销越小。显然,BS 干扰功率开销减小符合理论和直觉分析:当 UR 从远离 BS 移动到 BS 附近时,MS 和 UR 之间信道增益减小而 UR 和 BS 之间信道增益增加,因而单位干扰功率效率增加。从图中还可以看出,当 UR 的 X 坐标小于 40 时,算法 OptROptJam 和算法 EROptPJam 的 BS 功率开销为

BS 处可用功率上限,即 BS 使用全部 2 W 功率执行干扰,当 UR 的 X 坐标大于 40 时,BS 干扰功率开销急剧减小。事实上,算法 ExJoPowerOpt 获得较差性能的原因是:当 UR 远离 BS 时,其 BS 干扰功率开销约为 1.5 W,此时,ExJoPowerOpt 和 JoPowerOpt 干扰功率开销一致。由于  $P = P^B + P^R = 3.5$ ,约 2 W 功率将分配给 UR 执行中继。但由于算法 ExJoPowerOpt 还需满足独立功率约束,因此获得的总功率将减小(通过执行操作  $P = P - \Delta$ ),直到分配给 UR 的功率为 1.5 W,这使算法 ExJoPowerOpt 的 BS 干扰功率限制在 1.2 W,即相对于其他 3 种算法,ExJoPowerOpt 遭受干扰功率限制安全速率损失。随着 UR 移动到 BS 附近,算法 ExJoPowerOpt 存在的干扰功率限制安全速率损失问题将消失,此时算法 ExJoPowerOpt/JoPowerOpt 总干扰功率需求超过另外 2 种算法,执行  $P = P - \Delta$  将使算法 ExJoPowerOpt 的干扰功率需求收敛到与算法 OptROptJam/EROptPJam 相同值。

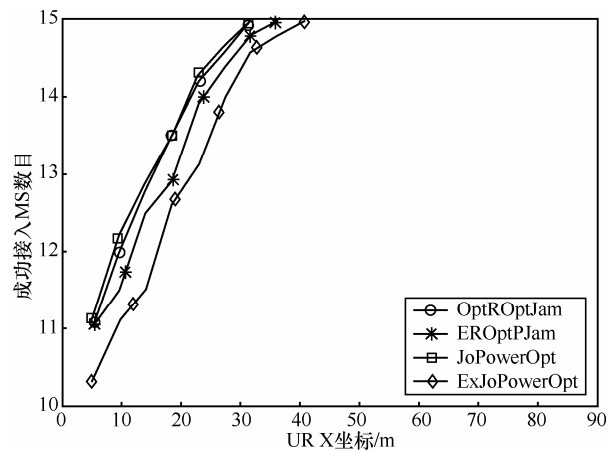


图 4 平均接入 MS 数目随 UR X 坐标变化

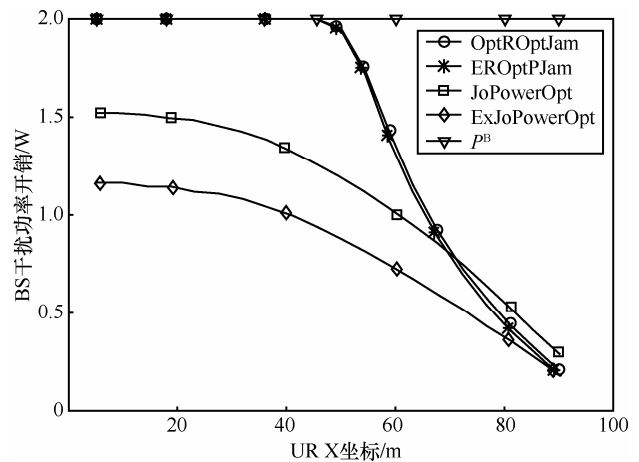


图 5 BS 功率开销随 UR X 坐标变化

最后, 比较 4 种算法在 BS 和 UR 可用功率变化下系统安全速率性能, 如图 6 所示。仿真参数: MS 数目  $N=15$ , UR 位置为(10, 0), BS 可用功率变化范围为 0.8~2.0 W, UR 可用功率变化范围为 [0.5, 1.5]。由图 6 可看出, 算法 OptROptJam、EROptPJam 和 JoPowerOpt 的安全速率都随 BS 和 UR 可用功率递增而增加。对于算法 ExJoPowerOpt, 尽管 UR 可用功率递增将显著增加系统安全速率, 但给定中继功率较小时, BS 可用功率的增加对系统可达安全速率的影响不明显。分析其原因是 ExJoPowerOpt 算法具有额外独立功率约束, 从而使算法性能出现“木桶短板现象”, 即受限的中继功率决定系统安全速率, 该现象随着中继功率的增加而逐渐消失。另外, 从图 6 可以观察到, 算法 JoPowerOpt 仍然具有最好性能, OptROptJam 次之。在某些可用功率组合区域, 算法 OptROptJam 的性能几乎与 JoPowerOpt 一致。对于算法 EROptPJam 和 ExJoPowerOpt, 给定可用功率平面(由 UR 和 BS 功率矢量组成)和由点(0.5, 0.8)到点(1.5, 2.0)的对角线, 在该对角线右侧, 算法 ExJoPowerOpt 算法获得更好的性能, 而在该对角线左侧, 算法 EROptPJam 获得更高的安全速率。

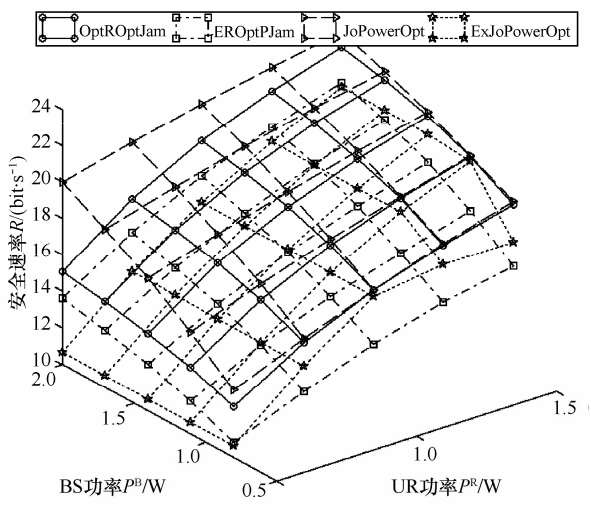


图 6 系统和安全速率随 BS 与 UR 功率变化

## 5 结束语

本文对基于 OFDMA 的多个蜂窝边缘 MS 无直达链路到 BS 但具有上行保密业务传输需求与非信任中继协作时的联合 UR 和 BS 功率分配问题进行了分析和研究, 构建了一种联合功率控制问题的数

学模型, 分析表明, 该联合功率控制问题等价于联合接入控制与功率分配问题, 通过问题松弛提出了一种次优的 MS 接入控制和交替迭代联合功率控制算法并分析了算法的次优性、收敛性和复杂度。最后, 仿真验证了本文提出算法的性能。基于本文的工作, 还可以进一步考虑不完全信道状态信息下的稳健功率控制、多个非信任中继场景以及非信任中继协作的激励机制等。

## 参考文献:

- [1] WYNER A. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8): 1355-1387.
- [2] CSISZAR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Trans Inf Theory, 1978, 24(5):339-348.
- [3] OOHAMA Y. Relay channels with confidential messages[EB/OL]. <http://arxiv.org/abs/cs/0611125>, 2007.
- [4] HE X, YENER A. Two-hop secure communication using an untrusted relay[J]. Eurasip Journal on Wireless Communication and Networking, 2009, 9:305146.
- [5] HE X, YENER A. Cooperation with an untrusted relay: a secrecy perspective[J]. IEEE Trans Inf Theory, 2010, 56(8):3807-3827.
- [6] JEONG C, KIM I, KIM D. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system[J]. IEEE Trans Signal Process, 2012, 60(1): 310-325.
- [7] HUANG J, MUKHERJEE A, SWINDLEHURST A L. Secure communication via an untrusted non-regenerative relay in fading channels[J]. IEEE Trans Signal Process, 2013, 61(10):2536-2550.
- [8] ZHANG R, SONG L, HAN Z, JIAO B. Physical layer security for two-way untrusted relaying with friendly jammers[J]. IEEE Trans Veh Technol, 2012, 61(8): 3693-3704.
- [9] HUANG J, SWINDLEHURST A L. Joint transmit design and node selection for one-way and two-way untrusted relay channels[A]. Proc of 47th Asilomar Conference on Signals, Systems, and Computers[C]. Pacific Grove, 2013.
- [10] SUN L, ZHANG T, LI Y. Performance study of two hop amplify-and-forward systems with untrustworthy relay nodes[J]. IEEE Trans Veh Technol, 2012, 61(8): 3801-3807.
- [11] MO J, TAO M, LIU Y. Secure beamforming for MIMO two-way communications with an untrusted relay[J]. IEEE Trans Signal Process, 2014, 62(9): 2185-2199.
- [12] MA Y, LIU A, HUA Y. A dual-phase power allocation scheme for multicarrier relay system with direct link[J]. IEEE Trans on Signal Processing, 2014, 62(1): 5-16.

(下转第 80 页)