

## 基于 C-RAN 前向压缩的物联网安全通信方法

王勇, 周牧, 田增山, 吴金君

(重庆邮电大学通信与信息工程学院移动通信技术重庆市重点实验室, 重庆 400065)

**摘要:** 提出了一种云无线接入网络 (C-RAN, cloud radio access network) 安全通信系统下行资源分配算法, 该算法在满足物联网信息终端的信干噪比、物联网窃听终端信干噪比和前向链路容量等约束条件下, 通过联合优化基站模式、量化噪声和波束成形等参数实现系统功率最小化。此设计是一个非凸优化问题, 为了有效求解该问题, 采用分步优化方法将原问题进行分解。提出利用半定松弛技术和函数平滑方法, 并通过迭代差分凸函数法求得原问题的次优解。通过二分法确定基站模式, 再优化基站发射功率。仿真结果表明, 所提联合优化算法相比组稀疏优化算法和基准算法具有更好的性能, 且其性能接近穷举法。

**关键词:** C-RAN; 前向压缩; 物理层安全; 物联网通信

**中图分类号:** TP391

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-3750.2018.00064

## Secure communication approach for Internet of things based on C-RAN fronthaul compression

WANG Yong, ZHOU Mu, TIAN Zengshan, WU Jinjun

Chongqing Key Lab of Mobile Communications Technology, School of Communication and Information Engineering,  
Chongqing University of Posts and Telecommunications, Chongqing 400065, China

**Abstract:** A resource allocation algorithm was proposed for downlink C-RAN secure communication system. This algorithm jointly optimized the parameters of base station (BS) mode, quantized noise and beamforming under the constraints of SINR requirements of Internet of things information receiver, eavesdropped receiver and fronthaul link capacity. Such a design was a non-convex optimization problem, and a step-by step optimization algorithm was proposed to decompose the original optimization problem efficiently. Semi-definite technique and function smoothing approach were adopted, and the local optimization solution of the original problem was obtained by the iterative different of convex method. Bi-section approach was further proposed to determine BS mode, and the transmitting power of the BSs were finally optimized. Simulation results indicate that the proposed joint optimization algorithm achieves better performance than group sparse optimization algorithm and baseline algorithm, and it has approximate optimal performance as the exhaustive search algorithm.

**Key words:** C-RAN, fronthaul compression, physical layer security, Internet of things communication

**收稿日期:** 2018-05-25; **修回日期:** 2018-08-24

**基金项目:** 国家自然科学基金资助项目 (No.61771083, No.61704015); 长江学者和创新团队发展计划基金资助项目 (No.IRT1299); 重庆市科委重点实验室专项经费基金资助项目 (No.cstc2017jcyjAX0380); 重庆市基础与前沿研究计划基金资助项目 (No.cstc2015jcyjBX0065); 重庆市高校优秀成果转化基金资助项目 (No.KJZH17117); 重庆市教委科学技术研究项目 (No.KJ1704083)

**Foundation Items:** The National Natural Science Foundation of China (No.61771083, No.61704015), The Program for Changjiang Scholars and Innovative Research Team in University (No.IRT1299), The Special Fund of Chongqing Key Laboratory (No.cstc2017jcyjAX0380), The Fundamental and Frontier Research Project of Chongqing (No.cstc2015jcyjBX0065), The University Outstanding Achievement Transformation Project of Chongqing (No.KJZH17117), The Scientific and Technological Research Foundation of Chongqing Municipal Education Commission (No.KJ1704083)

## 1 引言

### 1.1 背景

随着无线通信在人们生产生活过程中起到越来越重要的作用,用户对于高速数据传输和无处不在的通信服务需求不断增长,物联网(IoT, Internet of things)技术<sup>[1-2]</sup>已经受到工业和学术界的广泛关注。云无线接入网络(C-RAN, cloud radio access network)<sup>[3-4]</sup>作为一种新的无线接入网架构,将云计算应用到无线接入网中,是5G无线网络实现软件定义和绿色通信的候选技术之一。IoT终端的基带信号通过前向链路传送到基带处理池(BBU pool, baseband unit pool),从而实现BBU pool能够对基带信号进行联合处理。然而,在提高频谱效率的同时,也给无线通信网络带来了一系列挑战,其中最直接的就是能耗问题。

由于潮汐现象,例如办公区域在夜间通常只有极少量甚至没有活动的IoT终端,如果C-RAN一直处于工作状态,则极易造成能耗的浪费。因此,根据系统资源和IoT终端需要进行基站模式选择<sup>[5-8]</sup>(关闭基站和前向链路),能够有效降低系统能耗。同时,由于用户数据需要在基站间共享,C-RAN前向链路上的基带数字信号传输速率开销非常大,如宽带LTE-A系统使用5个20 MHz载波时,其速率达到10 Gbit/s以上<sup>[9]</sup>。因此,前向链路容量受限时,如何降低前向链路的容量对提高C-RAN系统的性能有着十分重要的意义<sup>[10]</sup>。基于此,学者们提出了数据共享<sup>[11]</sup>和前向压缩<sup>[12-13]</sup>两种策略。Dai等人<sup>[13]</sup>证明了前向压缩策略比数据共享策略的节能效果更好,同时,考虑无线信道具有广播特性,C-RAN的通信网络容易被各种新型设备或IoT终端窃听攻击<sup>[14-16]</sup>。这些非授权的设备或IoT窃听终端不但会窃取用户的有用信息,还可能会发射信号来影响授权用户对信息的接收。因此,C-RAN系统在安全传输方面也面临严峻的挑战<sup>[15-16]</sup>。根据上述分析,本文研究在前向链路容量约束下基于前向压缩的安全通信方法,以实现系统能耗的最小化。

### 1.2 相关研究

关闭C-RAN的一部分基站及其前向链路使得在节省电路能耗的同时,激活基站的发射功率将会增加。因此,Cheng等人<sup>[5]</sup>提出了利用分枝剪切法来实现基站模式选择与发射功率的折中。为了降低分枝剪切法的计算复杂度,Shi等人<sup>[6]</sup>提出了迭代组

稀疏波束成形算法,通过寻找波束成形的稀疏解来确定激活基站。Li等人<sup>[8]</sup>研究了考虑时延的C-RAN系统基站模式选择问题,并提出了基于迭代组稀疏波束成形和整数规划的求解方法。然而,上述文献没有考虑前向链路容量受限情况下的前向压缩技术,也没有考虑物理层安全技术。

前向压缩是对信号进行量化,将量化后的数据信号通过前馈链路传输到基站,基站端再根据量化码本恢复(解压缩)出量化前的数据信号。前向链路的压缩和解压缩过程可以建模为一个测试信道<sup>[12-17]</sup>,即在需要传输的信号上加一个量化噪声,通过控制量化噪声的大小来控制对信号的压缩程度。Park等人<sup>[12]</sup>通过联合优化波束成形和量化噪声以实现加权和速率最大,并证明了提出的迭代方法能够收敛到一个定点。Park等人<sup>[18]</sup>还研究了考虑簇内簇间干扰时的和速率最大问题,并提出了迭代的求解方法。尽管通过前向压缩能降低前向链路容量开销、提高系统性能,但是上述文献并没有考虑物理层安全,使得网络存在安全威胁。

保证安全通信的传统方法是由网络层通过密码学算法<sup>[19]</sup>实现加密,然而由于IoT窃听终端计算能力的提升,密码学方法的安全性越来越难以保障。因此,在Wyner<sup>[14]</sup>定义窃听信道模型后,物理层安全(PHY Security, physical layer security)技术<sup>[20]</sup>得到了广泛的关注和讨论。物理层安全作为上层加密方法的一种补充,充分利用物理层信道特性,以Shannon信息论为理论基础,从底层提高无线通信系统的安全性。因此,学者们对不同场景下的系统安全容量最大化问题开展了大量的研究工作<sup>[21-22]</sup>。若以安全速率为优化目标能够获得较高的安全速率,但是系统开销比较大。因此,Ng等人<sup>[23]</sup>研究了如何设计顽健性波束成形以实现系统功率的最小化。而Zhou等人<sup>[24]</sup>则将认知无线电与信息能量同传系统相结合,研究了不同信道误差约束条件下人工噪声辅助的顽健性波束成形和功率分流方法。尽管上述文献取得了很好的性能增益,但是并没有针对前向链路容量受限情况下C-RAN系统的基站模式进行讨论。

### 1.3 本文贡献

根据上述分析,本文的主要贡献包括:1) 将基站模式选择、波束成形和前向压缩的安全通信问题建模为一个非凸非线性规划问题。利用平滑函数对目标函数进行近似,将问题转化为差分规划题的一

般形式, 并利用 S 准则和半定松弛技术, 提出一种迭代差分半定规划 (IDC-SDP, iterative difference of convex semi-definite programming) 算法。2) 为了确定基站模式, 本文利用 IDC-SDP 算法求得解, 提出一种增强稀疏解的后激活基站选择方法, 再求解一个功率最小化问题。3) 本文通过大量仿真, 验证了提出算法的有效性。实验结果表明, 本文提出的算法能够快速收敛且其性能与穷举法性能相近, 证明了通过基站模式选择能够有效降低系统功耗。

## 2 系统模型与问题建模

### 2.1 信号传输模型

本文考虑一个下行 C-RAN 安全系统, 它有  $L$  个基站且每个基站配置  $N$  根天线。系统中有  $K$  个被调度的单天线 IoT 信息终端 (IR, IoT information receiver) 和  $M$  个单天线 IoT 窃听终端 (ER, IoT eavesdropped receiver), 并且  $L$  和  $K$  均为正整数。其中, 激活基站数为  $A$ , 且  $A \leq L$ , 用  $A$  表示激活基站的集合。所有的基站均通过前向链路连接一个 BBU pool, 且 BBU pool 接收所有 IR 的 CSI, 并且 BBU pool 拥有所有 IR 的数据信息。由于基站通过前馈链路与 BBU pool 相连, 各个基站的时钟完全同步 IR  $k$  的基带信号并用标量  $s_k$  表示, 它服从独立同分布, 且均值为 0, 方差为 1。IR 的基带信号过波束成形编码之后, 通过前向链路发送到各个基站, 基站再将信号经由天线发射, 最后 IR 接收信道衰落后的基站发射信号。该下行 C-RAN 安全系统的信号模型如图 1 所示。

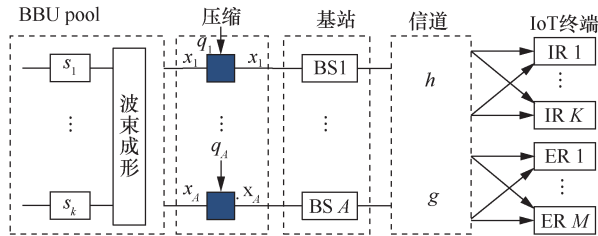


图 1 C-RAN 安全前向压缩下的信号传输模型

由图 1 可知, 每个 IR 的基带信号在发送前, 在 BBU pool 中采用波束成形对其进行编码。那么, 第  $l$  个基站的发射信号为

$$\mathbf{x}_l = \sum_{k \in U_l} \mathbf{w}_{kl} s_k, \forall l \in A \quad (1)$$

其中,  $U_l$  表示基站  $l$  的服务 IR 集合,  $\mathbf{w}_{kl} \in \mathcal{C}^{N \times 1}$  为基站  $l$  到 IR  $k$  的波束成形向量。

### 2.2 前向压缩

根据文献[11]可知, 该前向压缩过程可以建模为一个测试信道, 其中, 输入为已编码的信号, 输出为经压缩后的信号。则第  $l$  条前馈链路上的压缩过程, 可表示为 IR  $k$  的接收信号为

$$\tilde{\mathbf{x}}_l = \mathbf{x}_l + \mathbf{q}_l, \forall l \in A \quad (2)$$

其中,  $\mathbf{q}_l \in \mathcal{C}^{N \times 1}$  为量化噪声, 其均值为 0、方差为  $\mathbf{Q}_l = \mathbf{q}_l \mathbf{q}_l^H$ , 而  $\mathbf{x}_l$  和  $\tilde{\mathbf{x}}_l$  分别为测试信道的输入和输出。令  $\mathbf{x} = [\tilde{\mathbf{x}}_1, \dots, \tilde{\mathbf{x}}_A]$ , 那么 IR  $k$  和 ER  $m$  接收的信号可以分别表示为

$$\mathbf{y}_k^{\text{IR}} = \mathbf{h}_k^H \tilde{\mathbf{x}} + \mathbf{n}_k^{\text{IR}}, \forall k = 1, \dots, K \quad (3)$$

$$\mathbf{y}_m^{\text{ER}} = \mathbf{g}_m^H \tilde{\mathbf{x}} + \mathbf{n}_m^{\text{ER}}, \forall m = 1, \dots, M \quad (4)$$

其中,  $\mathbf{h}_k = [\mathbf{h}_{k1}^T, \dots, \mathbf{h}_{kA}^T]^T \in \mathcal{C}^{N \times A}$  为  $A$  个激活基站到 IR  $k$  的信道, 同理  $\mathbf{g}_m = [\mathbf{g}_{m1}^T, \dots, \mathbf{g}_{mA}^T]^T \in \mathcal{C}^{N \times A}$ ,  $\mathbf{n}_k^{\text{IR}}$  和  $\mathbf{n}_m^{\text{ER}}$  满足均值为 0、方差分别为  $\sigma_{\text{IR}_k}^2$  和  $\sigma_{\text{ER}_m}^2$  的加性高斯噪声。

### 2.3 信道模型

C-RAN 基站到 IR 的下行信道是利用信道对偶性, 通过上行导频烟火信号获得的。因此, 在调度时隙开始时, IR 信道就可以在 IR 处被估计出来。在传输过程中, IR 发送确认包 (ACK, acknowledgement) 通知基站端已成功接收信息。从而, 基站端能够根据 ACK 包中的导频序列来估计基站到 IR 的下行信道。所以, 本文假设在一个传输周期内, IR 信道是可以完全已知的。

根据文献[23], 由于基站与 ER 之间没有信息交互, ER 信道状态信息通常会有延迟, 可以将 ER 信道建模为

$$\mathbf{g}_m = \tilde{\mathbf{g}}_m + \Delta \mathbf{g}_m, \forall m \quad (5)$$

其中,  $\tilde{\mathbf{g}}_m$  为  $A$  个激活基站到第  $m$  个 ER 信道的估计值,  $\Delta \mathbf{g}_m = [\Delta \mathbf{g}_{m1}^T, \dots, \Delta \mathbf{g}_{mA}^T]^T \in \mathcal{C}^{N \times A}$  为对应的信道不确定性部分。当信道不确定性  $\Delta \mathbf{g}_m$  为椭球模型时, 满足  $\Delta \mathbf{g}_m^H \mathbf{\Omega}_m \Delta \mathbf{g}_m \leq 1$ , 其中  $\mathbf{\Omega}_m \in H^{N \times N}$  且  $\mathbf{\Omega}_m$  半正定矩阵。当  $\mathbf{\Omega}_m = (1/\varepsilon^2) \mathbf{I}$  时, 椭球误差模型退化为球面误差模型。此时,  $\Delta \mathbf{g}_m$  的约束可以写成  $\|\Delta \mathbf{g}_m\|_2 \leq \varepsilon$ 。当  $\varepsilon = 0$  时, ER 信道是完美的。

IR  $k$  的接收信干噪比 (SINR, signal to interference plus noise ratio) 为

$$\text{SINR}_k = \frac{|h_k^H \mathbf{w}_k|^2}{\sum_{i \neq k} |h_k^H \mathbf{w}_i|^2 + |h_k^H \mathbf{Q} h_k| + \sigma_{\text{IR}_k}^2} \quad (6)$$

ER  $m$  接收来自 IR  $k$  的 SINR 为

$$\text{SINR}_m^k = \frac{|g_m^H \mathbf{w}_k|^2}{\sum_{i \neq k} |g_m^H \mathbf{w}_i|^2 + |g_m^H \mathbf{Q} g_m| + \sigma_{\text{ER}_m}^2} \quad (7)$$

根据文献[23],  $\text{SINR}_m^k$  的上界可以表示为

$$\text{SINR}_m^k \leq \frac{|g_m^H \mathbf{w}_k|^2}{|g_k^H \mathbf{Q} g_k| + \sigma_{\text{ER}_k}^2} \triangleq \overline{\text{SINR}}_m^k \quad (8)$$

### 2.4 功率模型

C-RAN 系统的功耗主要包括基站功耗和前向链路功耗, 其中, 基站功耗由基站模式(激活/休眠)和发射功率决定, 基站激活或休眠时的功耗是固定的, 但激活时的基站功耗大于休眠时的基站功耗。因此, 可以通过休眠来降低 C-RAN 基站功耗。而前向链路由一个光线路终端(OLT, optical line terminal)和多个光网络单元(ONU, optical network unit)组成。其中 ONU 有休眠和激活两种模式, 可以通过休眠 ONU 降低其功耗, 而 OLT 的功耗  $P_{\text{olt}}$  是固定的。根据文献[6], C-RAN 的总功耗可以表示为

$$P_{\text{tot}} = \frac{1}{\eta} \sum_{l \in A} \left( \sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \right) + \sum_{l \in A} P_l^c + \sum_{l \in A} P_l^s + P_{\text{olt}} \quad (9)$$

其中, 第一项为基站发射总功率,  $P_l^s$  为基站  $l$  与其对应的 ONU 均处于休眠时的功耗,  $P_l^c$  为静态功率, 它是将激活基站  $l$  与对应的 ONU 进行休眠能够获得的功率增益。由于  $P_{\text{olt}}$  和  $\sum_{l \in A} P_l^s$  均为常数, 在优化功率时可以将其省掉。在后续分析中, 定义

$$P_{\text{总}} = \frac{1}{\eta} \sum_{l \in A} \left( \sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \right) + \sum_{l \in A} P_l^c \quad \text{为系统总功率。}$$

### 2.5 问题建模

本文通过同时优化基站模式、发射功率和量化噪声, 在满足用户服务质量需求、前向链路容量约束及保障物理层安全条件下, 实现下行 C-RAN 安全系统总功率最小化。该优化问题可以建模为

$$\min_{\mathbf{w}, \mathbf{q}, A} \frac{1}{\eta} \sum_{l \in A} \left( \sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \right) + \sum_{l \in A} P_l^c \quad (10a)$$

$$\text{s.t. } \text{SINR}_k \geq \gamma_k, \forall k \quad (10b)$$

$$\max_{\Delta g_m} \overline{\text{SINR}}_m^k \leq \Gamma_m^k, \forall m, k \quad (10c)$$

$$\sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \leq P_l^{\text{max}}, \forall l \in A \quad (10d)$$

$$\log_2 \left( 1 + \frac{\sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2}{\|\mathbf{q}_l\|_2^2} \right) \leq C_l, \forall l \in A \quad (10e)$$

其中,  $\mathbf{w} = [\mathbf{w}_1, \dots, \mathbf{w}_K]$ ,  $\gamma_k$  为 IR  $k$  的 SINR 门限,  $\Gamma_m^k$  为 ER  $m$  成功解调 IR  $k$  的 SINR 门限,  $P_l^{\text{max}}$  为基站  $l$  的最大发射功率, (10e) 为前向链路容量约束,  $C_l$  为前向链路  $l$  的最大容量。

式(10)的求解难度在于: 1) 目标函数含有组合变量  $A$ ; 2) 非凸二次约束(10b); 3) 无穷多个非凸物理层安全约束条件(10c); 4) 非凸对数约束。本文将提出一种分步优化算法求解式(10)。

## 3 所提分步优化算法

### 3.1 问题近似

由于式(10)求解困难, 需要将其进行近似转化, 本文将其转化为组稀疏波束成形问题, 再进行近似。考虑基站休眠时, 基站的发射功率为零, 即

$$\sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 = 0 \text{ 且 } \|\mathbf{q}_l\|_2^2 = 0 \text{。引入非负辅助变量}$$

$$s_l = \sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \text{ 表示基站的软发射功率, 得到}$$

$$f(s_l) = \begin{cases} 0, & s_l = 0, \forall l \\ 1, & \text{其他} \end{cases} \quad (11)$$

根据零范数的定义,  $f(s_l)$  与零范数等价。因此, 原始式(10)可以等效为

$$\min_{\mathbf{w}, \mathbf{q}, s} \frac{1}{\eta} \sum_{l \in A} s_l + \|s_l P_l^c, \mathbf{L}, s_l P_l^c\|_0 \quad (11a)$$

$$\text{s.t. } \sum_{k=1}^K \|\mathbf{w}_{kl}\|_2^2 + \|\mathbf{q}_l\|_2^2 \leq s_l, \forall k \quad (11b)$$

$$s_l \leq P_l^{\text{max}}, \forall l \in L \quad (11c)$$

$$(10b), (10c), (10e)$$

其中,  $\mathbf{s} = \{s_l\}_{l \in L}$ , 基站模式的稀疏性可以通过控制  $\mathbf{s}$  的稀疏性来实现。需要注意的是, 当参数  $\gamma_k$ 、 $\Gamma_m^k$  和  $P_l^{\text{max}}$  选择不当时, 式(11)可能没有可行解, 此时可以通过对 IR 接入控制或降低信息用户的 SINR 需求等来实现, 本文不做讨论。

由于式(11)的目标函数中含有零范数, 使得对该式的求解变得困难。本文利用平滑函数法对零范数进行近似, 该平滑函数  $f(x)$  需要满足 3 个性质: 1)  $f(x)$  是凹函数, 且在  $x \geq 0$  上非减; 2)  $\lim_{x \rightarrow 0^+} f(x) = 0$ ; 3)  $f(x)$  连续且可微。根据文献[25], 满足 3 个性质的函数有指数函数、对数函数和反正切函数, 如下

$$f_\tau(x) = \begin{cases} 1 - \exp(-x\tau^{-1}) \\ \log_2(1 + x\tau^{-1}) \\ \log_2(1 + \tau^{-1}) \\ \arctan(x\tau^{-1}) \end{cases} \quad (12)$$

其中,  $\tau > 0$  表示  $f_\tau(x)$  对零范数的近似程度,  $\tau$  越大,  $f_\tau(x)$  越平滑, 但对零范数近似程度越差, 反之近似程度越好。

利用式(12)近似处理后, 可以得到

$$\min_{w, q, s} \frac{1}{\eta} \sum_{l \in L} s_l + \sum_{l \in L} f_\tau(s_l) P_l^c \quad (13)$$

s.t. (10b), (10c), (10e), (11b), (11c)

由于式(13)目标函数的第一个求和项是凸函数, 而第二个求和项是凹函数, 构成了凸函数加凹函数的 DC (difference of convex) 形式。所以, 式(13)是一个 DC 规划问题。

### 3.2 IDC-SDP 算法

尽管 3.1 节已经将问题转化为一个 DC 规划问题, 由于约束条件的非凸性且涉及无穷多个约束, 使得对式(13)的求解十分困难。因此, 解决式(13)的关键在于如何将约束条件转化为凸约束。

令  $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ ,  $\mathbf{H}_k = \mathbf{h}_k \mathbf{h}_k^H$ , 约束条件(10b)可以转化为

$$\sum_{i \neq k} \text{Tr}(\mathbf{H}_k^H \mathbf{W}_i) + \text{Tr}(\mathbf{H}_k^H \mathbf{Q}) + \sigma_{\text{IR}_k}^2 \leq \frac{1}{\gamma_k} \text{Tr}(\mathbf{H}_k^H \mathbf{W}_k) \quad (14)$$

约束条件(10c)等效为

$$\max_{\text{Ag}_m} \text{Tr}(\mathbf{G}_m^H \mathbf{W}_k) / \Gamma_m^k - \text{Tr}(\mathbf{G}_m^H \mathbf{Q}) \leq \sigma_{\text{ER}_k}^2 \quad (15)$$

根据 S 准则<sup>[26]</sup>, 约束条件(15)可以转化为线性矩阵不等式

$$\mathbf{S}(\mathbf{W}_k, \mathbf{Q}, \alpha_m^k) = -\mathbf{U}_{g_m}^H \mathbf{W}_k \mathbf{U}_{g_m} / \Gamma_m^k + \mathbf{U}_{g_m}^H \mathbf{Q} \mathbf{U}_{g_m} + \alpha_m^k \mathbf{T}_m^k + \tilde{\mathbf{T}}_m \quad (16)$$

其中,  $\alpha_m^k \geq 0$  是引入的辅助变量,  $\mathbf{U}_{g_m} = [\mathbf{I}_{\text{NL}}, \tilde{\mathbf{g}}_m]$ ,

$$\mathbf{T}_m^k = \begin{bmatrix} \Omega_m & \mathbf{0} \\ \mathbf{0} & -1 \end{bmatrix}, \quad \mathbf{T}_m = \begin{bmatrix} \mathbf{0}_{\text{NL}} & \mathbf{0}_{\text{NL} \times 1} \\ \mathbf{0} & \sigma_{\text{ER}_k}^2 \end{bmatrix}.$$

约束条件(10e)可以转化为

$$\frac{1}{2^{C_i} - 1} \sum_{k=1}^K \text{Tr}(\Phi_l \mathbf{W}_k) \leq \text{Tr}(\Phi_l \mathbf{Q}) \quad (17)$$

式(13)的目标函数满足 DC 函数, 可以利用一阶泰勒展开将目标函数的凹函数转化为凸函数。从而, 通过迭代方式求解凸优化问题来获得式(13)的解。根据一阶泰勒展开,  $f_\tau(s_l)$  函数可以表示为

$$f_\tau(s_l^{(t)}) = f_\tau(s_l^{(t-1)}) + \nabla f_\tau(s_l^{(t-1)})(s_l^{(t)} - s_l^{(t-1)}) \quad (18)$$

其中,  $t \geq 1$  为迭代步数,  $f_\tau(s_l^{(t)})$  表示函数  $f_\tau(s_l)$  的点  $s_l$  在第  $t$  次迭代的值,  $\nabla f_\tau(s_l^{(t-1)})$  表示  $f_\tau(s_l)$  在点  $s_l$  在第  $t-1$  次迭代时的导数。因此, 将式(18)代入式(13)的目标函数后, 目标函数等价于

$$\sum_{l \in L} \mathcal{G}_l s_l \quad (19)$$

其中,  $\mathcal{G}_l = 1/\eta + \nabla f_\tau(s_l^{(t-1)}) P_l^c$ , 目标函数中的常数项已省略。

给定初始点  $\mathbf{s}^{(0)} = \{s_l^{(0)}\}_{l \in L}$  时, 式(13)可以通过迭代求解下面的问题来解决

$$\min_{W, Q, s, \alpha} \sum_{l \in L} \mathcal{G}_l s_l \quad (20a)$$

$$\text{s.t.} \sum_{k=1}^K \text{Tr}(\Phi_l \mathbf{W}_k) + \text{Tr}(\Phi_l \mathbf{Q}) \leq s_l \quad (20b)$$

$$s_l \leq P_l^{\max} \quad (20c)$$

$$\sum_{k=1}^K \text{Tr}(\Phi_l \mathbf{W}_k) + \text{Tr}(\Phi_l \mathbf{Q}) \leq P_l^{\max} \quad (20c)$$

(15), (16), (17)

其中,  $\Phi_l \triangleq \text{diag}(\underbrace{0, \dots, 0}_{(l-1)N}, \underbrace{1, \dots, 1}_N, \underbrace{0, \dots, 0}_{(L-l)N})$ ,  $\forall l \in L$ ,

$\mathbf{W} = \{\mathbf{W}_k\}$ ,  $\alpha = \{\alpha_m^k\}$ 。由于  $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ , 约束条件中引入  $\text{rank}(\mathbf{W}_k) = 1$  约束, 式(20)已利用半定松弛技术, 将  $\text{rank}(\mathbf{W}_k) = 1$  约束去掉。式(20)是一个半定规划问题, 可以利用工具箱 CVX<sup>[29]</sup> 求解。

在文献[27]中,  $f_\tau(s_l)$  是一个单调递减函数, 迭代算法收敛, 且收敛到式(13)的一个局部最优点。

由于平滑因子  $\tau$  直接影响  $f_\tau(x)$  函数对零范数的近似程度, 在算法迭代过程中需要对其进行更新。根据文献[27], 当选择  $\tau$  来最大化  $f_\tau(x)$  函数的梯度时, 式(12)中的 3 种近似函数的性能基本一样。

初始化  $\tau$  时, 选择一个较大值, 并通过引入一个因子  $\zeta$  来降低  $\tau$ , 即  $\tau \leftarrow \zeta\tau$ 。迭代更新  $\tau$ , 直至  $\tau$  值足够小结束。IDC-SDP 算法流程如算法 1 所示。

**算法 1** IDC-SDP 算法

**初始化:** 设置  $\mathbf{W}_k^{(0)}$  和  $\mathbf{Q}^{(0)}$ , 并计算  $\mathbf{s}^{(0)} = \{s_l^{(0)}\}_{l \in L}$

**Repeat:**

**Step 1:** 固定  $\{g_l\}_{l \in \mathcal{L}}$ , 求解式 (20), 得到  $\{\mathbf{W}_k^*, \mathbf{Q}^*, \mathbf{s}^*\}$

**Step 2:** 更新  $\{\mathbf{W}_k \leftarrow \mathbf{W}_k^*\}$ ,  $\mathbf{Q} \leftarrow \mathbf{Q}^*$ ,  $\mathbf{s} \leftarrow \mathbf{s}^*$ ,  $\tau \leftarrow \zeta\tau$ , 并利用  $\mathbf{s}^*$ , 更新  $\{g_l\}_{l \in \mathcal{L}}$

**Until** 收敛或达最大迭代次数

算法 1 收敛时, 可以通过检查收敛时  $\mathbf{s}^*$  中的非零元素, 能够获得激活基站的粗略集。然而, 由于算法 1 以休眠基站数最多为目标, 且只能收敛到一个局部最优点, 无法得到最低的系统功率。同时, 根据文献[6]可知, 将系统参数与波束成形相结合, 能够提升系统性能。因此, 在算法 1 的基础上, 下一节提出进一步降低系统功耗的后续处理方法。

**3.3 后处理过程**

根据算法 1 得到  $\mathbf{s}^*$ , 休眠  $\mathbf{s}^*$  中零元素对应的基站, 即当  $s_l^* = 0$  时, 基站  $l$  与其对应的前向链路均休眠。 $s_l^*$  值的大小在一定程度上反映了基站休眠或激活的优先级。更重要的是, 文献[6]指出采用系统参数辅助选择激活基站, 能够增加选择激活基站的准确性。因此, 结合  $s_l^*$  和系统中的重要参数, 定义激励因子作为选择基站激活的依据, 其值越大, 则表明它处于激活状态的优先级越高。那么, 第  $l$  个基站的激励因子的表达式为

$$A_l = \frac{s_l^* \sum_{k=1}^K \|\tilde{\mathbf{h}}_{kl}\|_2^2}{P_l^c \sum_{m=1}^M \|\tilde{\mathbf{g}}_m \mathbf{q}_l\|_2^2} \quad (21)$$

其中,  $\sum_{k=1}^K \|\tilde{\mathbf{h}}_{kl}\|_2^2$  为基站  $l$  的信道增益。 $\sum_{m=1}^M \|\tilde{\mathbf{g}}_m \mathbf{q}_l\|_2^2$  表示基站  $l$  对窃听用户信号的贡献值, 其值越大, 该基站处于激活状态的优先级越低。

对所有基站的激励因子按升序排列  $\{A_{\pi_1}, \dots, A_{\pi_L}\}$ 。基于此排列结果, 利用二分法来确定激活基站的集合。该二分法是为了寻找到升序排列中激励因子所对应的应该休眠的最大基站数。具

体过程如下: 1) 初始化基站序列号  $S_{\min} = 0$  和  $S_{\max} = A$ , 分别表示最小激活基站数目和最大激活基站数目; 2) 用  $A$  表示已经将基站序列号低于  $S_{\min}$  的基站处于休眠模式所对应的激活基站集合, 根据  $A$  求解下面的可行性问题

$$\begin{aligned} & \text{find } \{\mathbf{W}, \mathbf{Q}\} \\ & \text{s.t. (15)~(17), (20c)} \end{aligned} \quad (22)$$

如果式 (22) 有可行解, 则更新  $S_{\max} = \lfloor (S_{\max} + S_{\min})/2 \rfloor$  和激活基站集  $A$ 。否则, 更新  $S_{\min} = \lfloor (S_{\max} + S_{\min})/2 \rfloor$  和激活基站集  $A$ ; 3) 重复第二步直至  $S_{\max} - S_{\min} = 1$ ; 4) 返回  $S_{\min}$ 。需要注意的是, 第二步中设置基站序列号大于  $S_{\max}$  则处于激活状态, 从而得到了激活基站集  $A^* = \{A_{\pi_{S_{\max}}}, \dots, A_{\pi_L}\}$ 。

**3.4 发射功率优化**

根据 3.2 节和 3.3 节得到的激活基站集  $A^*$ , 为了得到最终的系统功耗, 需要求解一个联合波束成形和量化噪声优化的功率最小化问题

$$\begin{aligned} & \min_{\mathbf{W}, \mathbf{Q}, \alpha} \frac{1}{\eta} \sum_{l \in A^*} \left( \sum_{k=1}^K \text{Tr}(\Phi_l \mathbf{W}_k) + \text{Tr}(\Phi_l \mathbf{Q}) \right) + \sum_{l \in A^*} P_l^c \\ & \text{s.t. (15)~(17), (20c)} \end{aligned}$$

其中, 式(15)~式(17)和式(20c)中  $l \in A^*$ , 该问题是一个 SDP 问题, 可以利用内点法进行求解。

**3.5 计算复杂度分析**

利用内点法求解 SDP 问题时, IDC-SDP 算法的计算复杂度为  $O(I_{\max} \sqrt{MKNL} (MK^3(NL)^2 + MK^2(NL)^3))$  [29], 其中  $I_{\max}$  表示算法 1 的最大迭代次数。采用二分法确定基站模式最多需要求解  $\log_2 A$  次可行性式(22), 而发射功率优化问题只需要求解一次。所以, 本文提出的分步优化算法的总计算复杂度为  $O(\sqrt{MKNL} (MK^3(NL)^2 + MK^2(NL)^3) \log_2 L)$ 。

**4 实验结果与分析**

假设下行 C-RAN 安全通信系统由 7 个双天线基站、4 个单天线 IR 和 1 个单天线 ER 构成。基站和 IoT 终端的分布如图 2 所示, 其中, 基站 1 位于圆心, 其余 6 个基站均匀分布在半径为 0.2 km 的圆上, 而 IR 和 ER 均随机分布在长为 0.4 km 的正方形内。令每个基站的静态功率和最大发送功率相等, 即  $P^c = P_l^c, \forall l$  和  $P^{\max} = P_l^{\max}, \forall l$ , 且每条前向链路容量均为  $C = C_l, \forall l$ 。假设 IR 的 SINR 门限为  $\gamma = \gamma_k, \forall k$ , ER 的 SINR 门限为  $\Gamma = \Gamma_m^k, \forall m, k$ , 背

景噪声均为  $\sigma = \sigma_{\text{IR}_k}^2 = \sigma_{\text{IR}_m}^2$ 。不失一般性，令窃听用户信道的不确定性满足  $\Omega_m = (1/\varepsilon^2)\mathbf{I}$ 。无特殊说明，仿真中给出的所有结果均是 40 次独立的物联网终端位置，且每个位置取一次随机信道取平均值得到，其他仿真参数如表 1 所示。

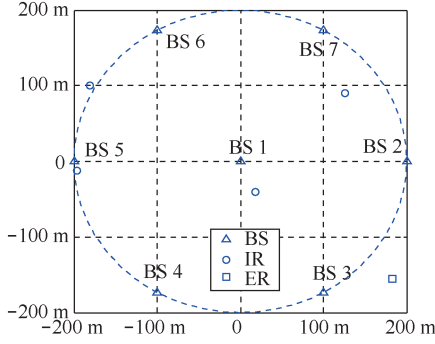


图 2 基站和 IoT 终端的分布

表 1 仿真参数设置

参数	取值	参数	取值
路径损耗	$148.1+37.6\log_2 d_{kl}$	$\eta$	1/4
信道带宽	10 MHz	$P^{\max}$	1 W
天线增益	9 dBi	$P^c$	5 W
阴影衰落	8 dB	$\varepsilon^2$	0.02
收敛误差	$10^{-5}$	$I_{\max}$	50
$C$	3 bit/(s·Hz)	$\sigma$	-104 dBm
$\gamma$	10 dB	$\Gamma$	-10 dB

### 4.1 基站发射功率分布

当不考虑基站模式选择时，令 7 个基站均处于激活状态，即  $A=L$ ，此时只需要求解一个发射功率最小化的优化问题。前向链路功率不变，本节分析了任意 4 个不同信道下的基站发射功率分布，如表 2 所示。为方便表示，表 2 中信道用“Ch”表示。

表 2 不同信道下基站功率/mW

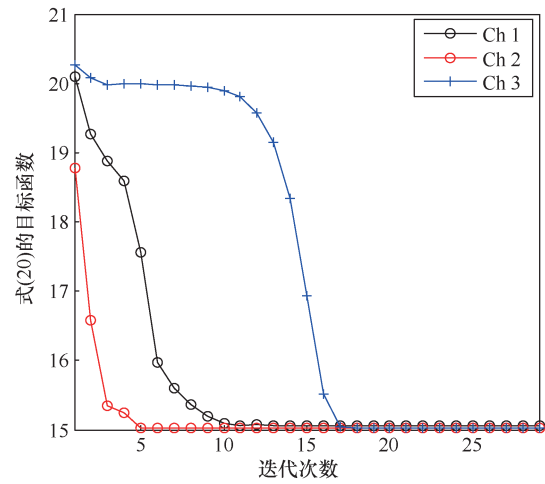
	Ch 1	Ch 2	Ch 3	Ch 4
BS 1	28.00	5.35	3.95	18.00
BS 2	2.89	9.89	1.46	20.00
BS 3	12.00	2.88	3.22	2.36
BS 4	6.39	23.00	2.01	19.00
BS 5	7.79	2.64	5.59	27.00
BS 6	13.00	5.88	1.56	7.24
BS 7	15.00	1.48	7.34	3.54

由表 2 可以看出，7 个基站的发射功率在不同

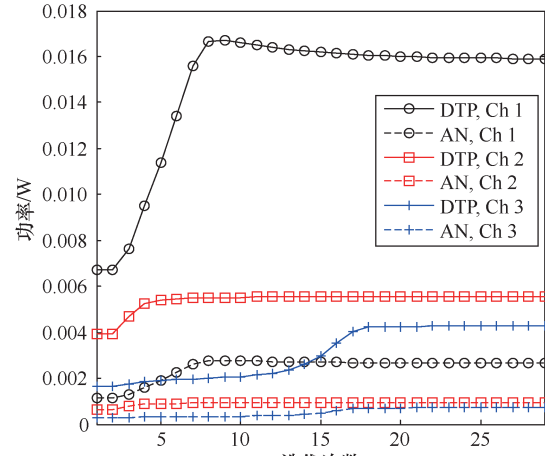
的信道条件下均不为零。也就是说，不进行基站模式选择，基站会一直存在发射功率，不利于节省系统功耗。由表 2 还可以看出，部分基站的发射功率比较低，如信道条件 1 下的基站 2、4 和 5 的发射功率比其余 4 个基站的发射功率低很多，而信道条件 4 下的基站 3、6 和 7 的发射功率比较低。

### 4.2 算法收敛性分析

为了说明所提算法迭代求解过程的收敛速度，选取 3 个随机信道分析 IDC-SDP 算法的收敛性。图 3 给出了式(20)目标函数和发射功率与迭代次数的变化关系。



(a) 系统总功率



(b) 发射功率

图 3 IDC-SDP 算法不同信道下收敛性分析

由图 3(a)可以看出，随着迭代次数的增加，式(20)的目标函数均随着迭代的进行而降低。这是因为随着迭代的进行，算法强迫部分基站发射功率降低。为了满足服务质量保障和安全通信需求，余下的基站发射功率将增加。由图 3(b)可以看出，量化

噪声 (QN, quantized noise) 功率与数据传输功率 (DTP, data transmission power) 相比, 3 个不同信道下的 QN 功率所占比例都非常小。由于采用波束成形能够使信息尽量对准信息终端, 只需要使用少量量化噪声干扰窃听终端即可保证安全通信。

### 4.3 算法性能对比分析

为了说明所提算法的有效性, 本节分析对比了提出的算法与其他 3 种算法的性能。

组稀疏优化算法<sup>[6]</sup>: 该算法也称加权 1 范数算法, 利用加权 1 范数近似目标函数中的零范数, 迭代更新权重直至收敛, 再休眠发射功率为零的基站。

穷举法: 该算法通过枚举方式, 寻找到使得系统功率最低的最优激活基站, 是全局最优算法。

基准算法: 该算法不考虑基站模式选择, 即所有基站均处于激活状态。

#### 4.3.1 激活基站数

为了分析基站的模式选择情况, 本文进一步对比了不同算法的激活基站情况。图 4 给出了表 2 中

的信道条件 4 (Ch 4) 下 4 种算法激活基站情况。由图 4 可以看出, 为了满足服务质量和安全通信需求, 本文所提算法与穷举法所需激活基站数均为 3 个, 而组稀疏优化算法需要 4 个激活基站。因为组稀疏算法以优化基站数为目的, 且只收敛到一个局部最优点。由于休眠基站 6 能够节省的系统功率比发射功率带来的功率开销低, 因此本文所提方法能够进一步降低系统功率。

#### 4.3.2 前向链路容量对系统性能的影响

图 5 对比了前向链路容量对系统性能的影响, 由图 5 可以看出, 随着前向链路容量的增加, 系统功耗逐渐降低。值得注意的是, 当前向链路容量较小时, 如 1 bit/(s·Hz), 前向链路容量约束要求 QN 不小于 DTP, 而 QN 较大时增加了干扰, 从而降低了 IR 的 SINR。实验表明, 当前向链路容量为 1 bit/(s·Hz) 时, 式(20)无可行解。当前向链路容量大于 4 bit/(s·Hz) 时, 系统功耗不再保持恒定。这是因为当前向链路容量足够大时, QN 可以取值的范围更广, 使得前向链路容量约束条件不再起作用。

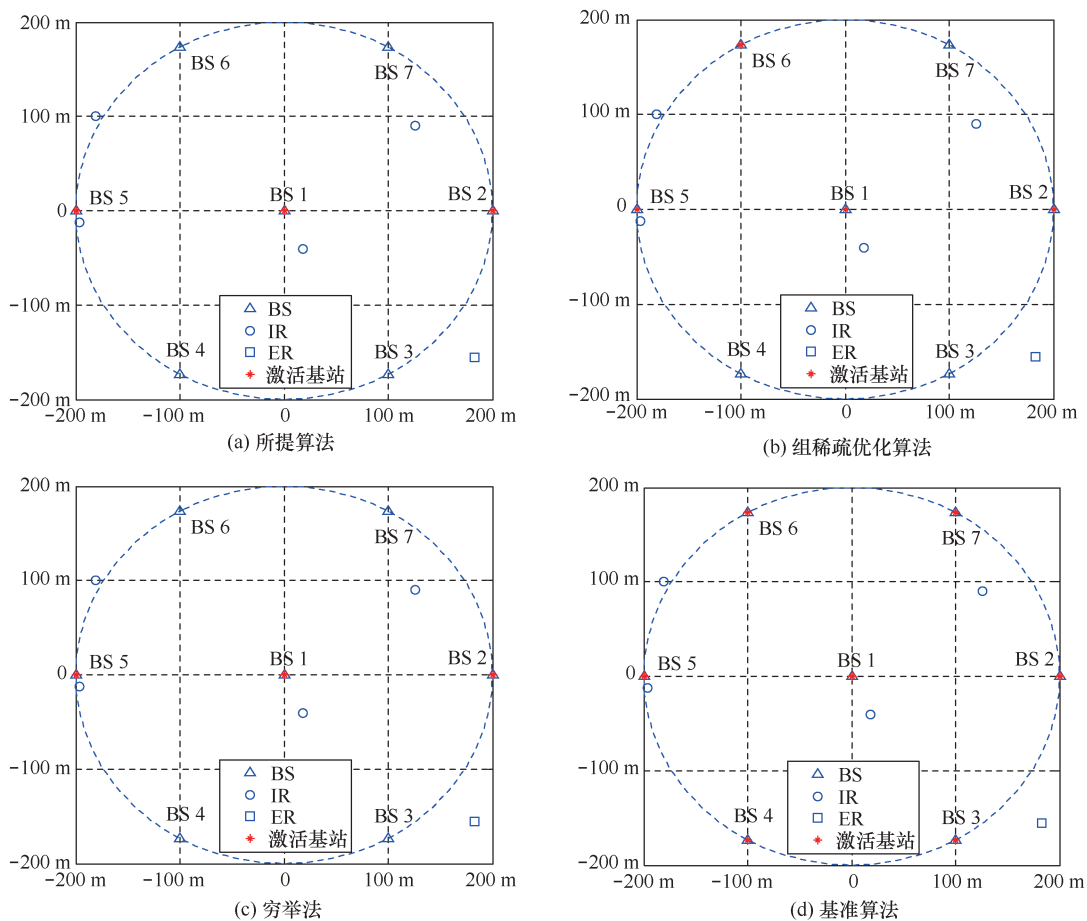


图 4 不同方法下激活基站对比

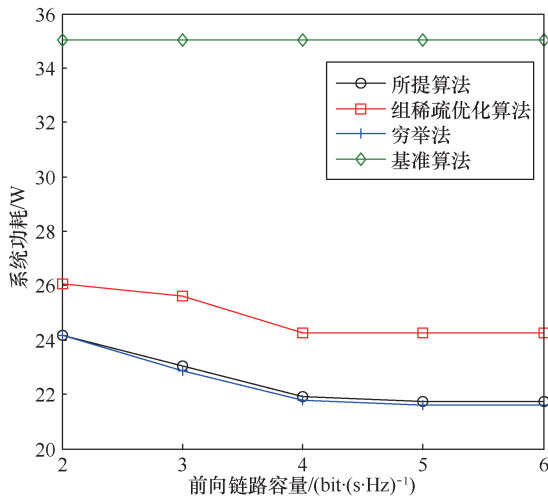


图5 前向链路容量对系统性能的影响

### 4.3.3 IR 终端 SINR 门限对系统性能的影响

为了分析 IR 终端 SINR 门限对系统性能的影响, 需要保证问题有可行解。值得注意的是, 当 IR 终端 SINR 门限过高时, 会导致问题没有可行解。此时需要考虑降低 IR 终端 SINR 门限或对 IR 终端进行接入控制。因此, 本文选取使得问题具有可行解的 40 次信道取平均值得到, 仿真结果如图 6 所示。

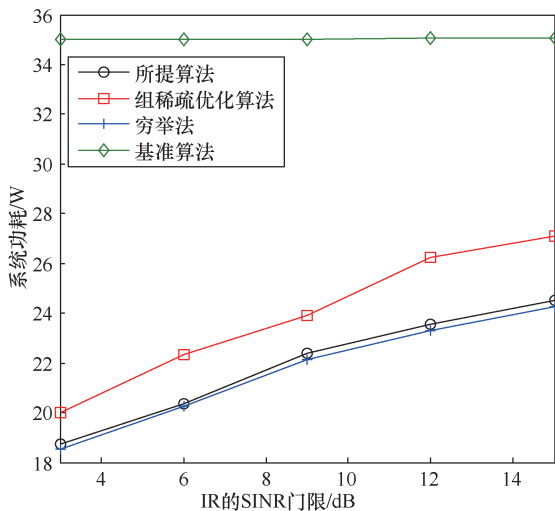


图6 IR 终端 SINR 门限对系统性能的影响

由图 6 可以看出, 随着 IR 终端 SINR 门限的增加, 系统总功耗也增加。这是因为只有增加基站的信息传输功率才能增大 IR 终端的 SINR, 而发射功率增加到一定程度往往会带来巨大的功耗开销。此时通过休眠基站获得的功率增益大于发射功率带来的功耗开销。因此, 本文提出的方法能够有效降低系统总功耗开销。

### 4.3.4 ER 终端 SINR 门限对系统性能的影响

本文还探讨了 ER 终端 SINR 门限对系统性能的影响, 如图 7 所示。由图 7 可知, 当 ER 终端 SINR 门限值调小时, 需要用来干扰 ER 的量化噪声小, 对 IR 造成的干扰也小, 从而 IR 终端能够获得更大的 SINR。显然, IR 终端 SINR 门限不变时, 所需的发射功率较小。而当 ER 终端 SINR 门限大于或等于 0 dB 时, 系统功率保持不变。这是因为在其他条件不变的情况下, ER 终端的 SINR 小于或等于 0 dB, 即约束条件(10c)恒成立。也就是说, 此时 ER 终端的 SINR 门限值不影响优化问题的解。所提算法的系统功耗接近于穷举法, 且比其他组稀疏优化算法和基准算法的系统功耗分别低约 6%和 50%。

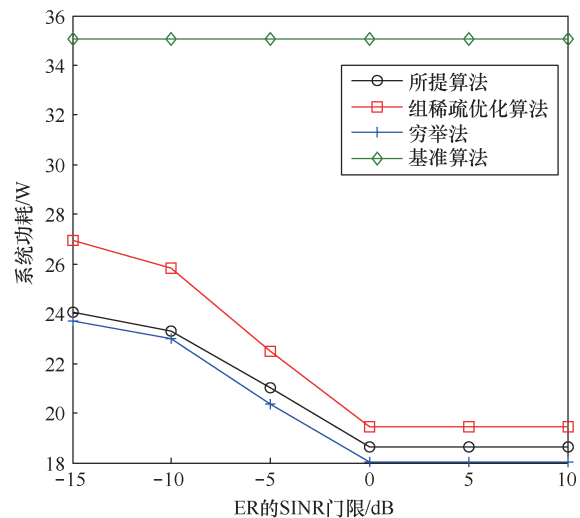


图7 ER 终端 SINR 门限对系统性能的影响

## 5 结束语

本文研究了基于 C-RAN 前向压缩的物联网安全通信问题, 通过对基站模式、波束成形和量化噪声进行联合优化设计, 实现系统功耗的最小化。本文利用分步优化思想, 首先通过 IDC-SDP 算法求得基站模式的粗略集, 然后利用二分法进行后处理, 得到最终的激活基站后, 再优化基站发射功率。仿真结果分析表明, 本文所提优化算法性能优于组稀疏优化算法和基准算法, 且其性能接近最优解。

### 参考文献:

- [1] ATZORI L, IERA A, MORABITO G. The Internet of things: a survey[J]. Computer Networks, 2010, 54(15): 2787-2805.
- [2] KOPETZ H. Internet of things[M]. Real-Time Systems. Boston: Springer, 2011.

- [3] 中国移动通信研究院. C-RAN: 无线接入网绿色演进[M]. 2010. China Mobile Research Institute. C-RAN: green revolution of wireless access networks[M]. 2010.
- [4] WU J, ZHANG Z, HONG Y, et al. Cloud radio access network (C-RAN): a primer[J]. IEEE Network, 2015, 29(1): 35-41.
- [5] CHENG Y, PESAVENTO M, PHILIPP A. Joint network optimization and downlink beamforming for comp transmissions using mixed integer conic programming[J]. IEEE Transactions on Signal Processing, 2013, 61(16): 3972-3987.
- [6] SHI Y, ZHANG J, LETAIEF K B. Group sparse beamforming for green cloud-ran[J]. IEEE Transactions on Wireless Communications, 2014, 13(5): 2809-2823.
- [7] WANG Y, MA L, XU Y, et al. Computationally efficient energy optimization for cloud radio access networks with csi uncertainty[J]. IEEE Transactions on Communications, 2017, 65(12): 5499-5513.
- [8] LI J, WU J, PENG M, et al. Queue-aware energy-efficient joint remote radio head activation and beamforming in cloud radio access networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(6): 3880-3894.
- [9] XIA P, LIU C H, ANDREWS J G. Downlink coordinated multi-point with overhead modeling in heterogeneous cellular networks[J]. IEEE Transactions on Wireless Communications, 2013, 12(8): 4025-4037.
- [10] CHIH-LIN I, HUANG J, DUAN R, et al. Recent progress on C-RAN centralization and cloudification[J]. IEEE Access, 2014, 2: 1030-1039.
- [11] ZHAO J, QUEK T Q S, LEI Z. Coordinated multipoint transmission with limited backhaul data transfer[J]. IEEE Transactions on Wireless Communications, 2013, 12(6): 2762-2775.
- [12] PARK S H, SIMEONE O, SAHIN O, et al. Joint precoding and multivariate backhaul compression for the downlink of cloud radio access networks[J]. IEEE Transactions on Signal Processing, 2013, 61(22): 5646-5658.
- [13] DAI B, YU W. Energy efficiency of downlink transmission strategies for cloud radio access networks[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(4): 1037-1050.
- [14] WYNER A D. The wire-tap channel[J]. Bell Labs Technical Journal, 1975, 54(8): 1355-1387.
- [15] KHISTI A, WORNELL G W. Secure transmission with multiple antennas I: the MISOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088-3104.
- [16] KHISTI A, WORNELL G W. Secure transmission with multiple antennas part II: the MISOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5515-5532.
- [17] PARK S H, SIMEONE O, SAHIN O, et al. Fronthaul compression for cloud radio access networks: signal processing advances inspired by network information theory[J]. IEEE Signal Processing Magazine, 2014, 31(6): 69-79.
- [18] PARK S H, SIMEONE O, SAHIN O, et al. Inter-cluster design of precoding and fronthaul compression for cloud radio access networks [J]. IEEE Wireless Communications Letters, 2014, 3(4): 369-372.
- [19] MASSEY J L. An introduction to contemporary cryptology[J]. Proceedings of the IEEE, 1988, 76(5): 533-549.
- [20] CHEN X, NG D W K, GERSTACKER W, et al. A survey on multiple-antenna techniques for physical layer security[J]. IEEE Communications Surveys & Tutorials, 2017, 19(2): 1027-1053.
- [21] LI Q, HONG M, WAI H T, et al. Transmit solutions for MIMO wiretap channels using alternating optimization[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1714-1727.
- [22] LI Q, 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.
- [23] NG D W K, LO E S, SCHOBER R. Robust beamforming for secure communication in systems with wireless information and power transfer[J]. IEEE Transactions on Wireless Communications, 2013, 13(8): 4599-4615.
- [24] ZHOU F, LI Z, CHENG J, et al. Robust an-aided beamforming and power splitting design for secure miso cognitive radio with swipt[J]. IEEE Transactions on Wireless Communications, 2017, 16(4): 2450-2464.
- [25] TAO M, CHEN E, ZHOU H, et al. Content-centric sparse multicast beamforming for cache-enabled cloud ran[J]. IEEE Transactions on Wireless Communications, 2016, 15(9): 6118-6131.
- [26] BOYD S, VANDENBERGHE L. Convex optimization[M]. UK: Cambridge University Press, 2004.
- [27] BOMZE I, LEMARECHAL C. Necessary conditions for local optimality in difference-of-convex programming[J]. Journal of Convex Analysis, 2010, 17(2): 673-680.
- [28] GRANT M. Cvx: matlab software for disciplined convex programming, version 1.21[J]. Global Optimization, 2008:155-210.
- [29] VANDENBERGHE L, BOYD S. Semidefinite programming[J]. SIAM Review, 1996, 38(1): 49-95.

## [作者简介]



王勇 (1987-), 男, 博士, 重庆邮电大学讲师, 主要研究方向为无线通信、能效优化、深度学习理论等。



周牧 (1984-), 男, 重庆邮电大学教授、博士生导师, 主要研究方向为无线定位与导航技术、信号侦察与检测技术、凸优化与深度学习理论等。



田增山 (1968-), 男, 重庆邮电大学教授、博士生导师, 主要研究方向为移动通信、个人通信、GPS 及蜂窝网定位技术等。



吴金君 (1994-), 男, 重庆邮电大学硕士生, 主要研究方向为模式识别与深度学习技术。