doi:10.3772/j.issn.1002-0470.2020.02.006

窃听场景下的无线传感网络中继功率分配算法①

刘海江②* 金 勇③* 胡振涛* 武国栋* 李继方**

(*河南大学计算机与信息工程学院 开封 475004)

(**华北水利水电大学电力学院 郑州 450045)

摘 要 多窃听与多中继下的信息安全率研究为无线传感器网络的研究热点。针对信道状态已知条件下传统中继功率固定分配算法的信息安全率较低的问题,提出一种中继功率优化分配算法,以最大信息安全率为目标函数,以中继功率为约束条件,采用变量松弛技术和 Charnes-Cooper 变换将非凸目标函数转化为凸形式,进而利用一维搜索方法找到最优功率分配权值。仿真结果表明了本文算法的有效性。

关键词 信道状态信息;能量最优;信息安全率;权值矢量

0 引 言

无线传感器网络由于具有网络设备灵活、位置可以随时更改的特点,在军事、救灾和勘探领域获得了广泛应用[1]。常规条件下,该网络性能受限于节点能量,极大地限制了它的应用领域。近年来,出现了一种新机制无线传感器网络架构[2-4],该架构能够把无线通信过程中的射频段信号能量转化为网络节点能量,从而延长网络节点的工作时间[5]。

节点是具有能量获取能力的无线传感器,该节点网络的通信安全问题是当前研究热点[6-11]。多窃听场景下,中继合作干扰是提高信息传输安全率的有效手段[12]。该方法将收集到的能量依据分配参数分成两部分,一部分用于中继转发信息,另一部分用于产生人工干扰信号,从而来保证用户最大的信息安全率[13]。可以发现,信道状态信息已知条件下,该方法的性能依赖于分配参数,但文献[12]未对分配参数的设置展开讨论。针对上述问题本文提出了一种最优功率分配(BEST-CJ-SPS)的算法。该算法结合变量松弛[12]和半正定规划方法[14,15],通过一维搜索法确定最优的中继功率分配参数以及相应的最大信息安全率。

本文中,$(.)^{\mathrm{T}}$、$(.)^{\dagger}$、$(.)^{\mathrm{H}}$、$(.)^{*}$ 分别表示转置、共轭、共轭转置以及最优解。再者 $[.]_{i,j}$ 定义为一个矩阵的第 i 行第 j 列的值,$\|.\|$ 与 $\|.\|^2$ 分别表示欧几里得范数与欧几里得范数的平方,$[.]_{i=1}^{N}$ 表示一个 $N\cdot 1$ 维的向量,$CN(0,\boldsymbol{X})$ 表示以 0 向量为均值、$\boldsymbol{X}$ 为协方差矩阵的复高斯分布。

1 问题描述

本文的系统模型如图 1 所示,发送者(Tx)与接收者(Rx)在 N 个静态能量分割(static power splitting, SPS)中继(如图 2 所示)的帮助下建立通信,在 Rx 的周围存在 K 个分布在半径为 $R(R=2.5\ \mathrm{m})$ 的安全范围[16]之内的窃听者(eavesdropper, EVE),且均配备单天线。

SPS 中继将通信过程中的射频段信号(radio frequency segment signal, RFSG)转换为自身所需能量并把收集到的能量(假设收集到的总能量为 1)按

① 国家自然科学基金(61771006,61976080,U1804149),河南省科技发展计划科技攻关项目(192102210254),河南省高等学校重点研究计划(19A413006)和河南省高等学校重点科研项目指导计划(20B510001)资助项目。

② 男,1992 年生,硕士生;研究方向:无线窃听网络信息安全;E-mail: lhj_dahai@163.com

③ 通信作者,E-mail: jy@henu.edu.cn

(收稿日期:2019-01-15)

如下原则进行分配。(1)将收集到的能量分为 $1-\bar{a}_i$ 和 $\bar{a}_i$ 两部分,$\bar{a}_i \in [0,1]$。(2)将 $1-\bar{a}_i$ 部分能量用于接收传递信息,而 $\bar{a}_i$ 部分能量分为 ρ_i 与 $1-\rho_i$ 两部分。(3) ρ_i 部分能量用于产生干扰信号,$1-\rho_i$ 部分能量用于放大接收信号,其中 η 为能量传输效率。

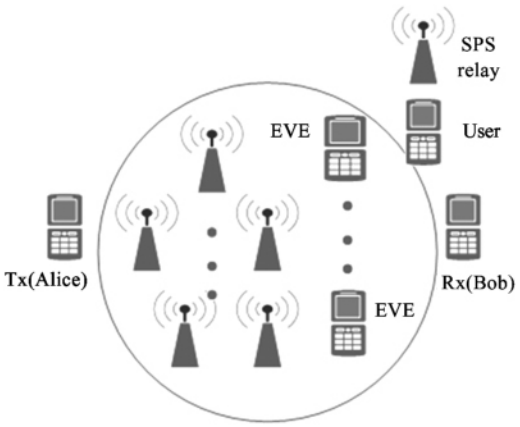

图 1　系统模型

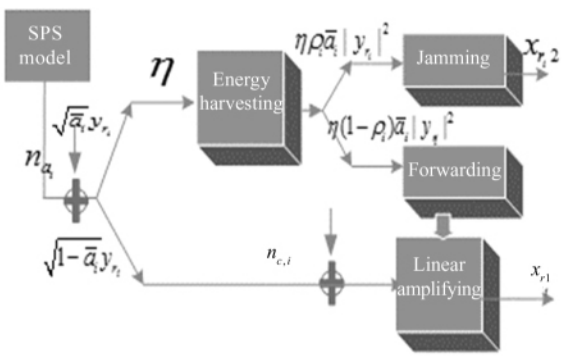

图 2　SPS 中继

系统模型可描述为:首先,发送者将待发送信息发送给中继 i,则其接收信息如下:

$$y_{ri} = h_{sri}\sqrt{P_s}s + n_{a,i},\ i \in [1,2,\cdots,N] \tag{1}$$

其中,s 为待发送的信号,且 $s \sim CN(0,1)$,h_{sri} 为 Tx 到中继 i 的高斯信道,$\sqrt{P_s}$ 表示信号发射能量,$n_{a,i}$ 为单位加性高斯白噪声。

其次,中继对接收信息进行放大处理,如式(2)和式(3)所示:

$$x_{ri1} = \beta_i(\sqrt{1-\bar{\alpha}_i}y_{ri} + n_{c,i}) \tag{2}$$

$$\beta_i = \sqrt{\frac{\eta(1-\rho_i)\bar{\alpha}_i |h_{sri}|^2 P_s}{(1-\bar{\alpha}_i)|h_{sri}|^2 P_s + (1-\bar{\alpha}_i)\sigma_{na}^2 + \sigma_{nc}^2}}e^{\angle\beta_i} \tag{3}$$

其中,β_i 为中继 i 的系数,$n_{c,i} \sim CN(0,\sigma_{nc}^2)$,$\angle\beta_i$ 为中继 i 相位。

为抑制窃听,首先介绍中继 CJ[5-8] 方案,对于 N 个 SPS 中继产生干扰信号定义为 $\boldsymbol{x}_{r2} = [x_{r12}, x_{r22}, \cdots, x_{rN2}]^{\mathrm{T}}$,其协方差矩阵可表示为 $\boldsymbol{S} = \boldsymbol{E}(\boldsymbol{x}_{r2}\boldsymbol{x}_{r2}^{\mathrm{H}})$。对 $\boldsymbol{S}$ 做特征分解即 $\boldsymbol{S} = \widetilde{\boldsymbol{V}}\widetilde{\boldsymbol{\Sigma}}\widetilde{\boldsymbol{V}}^{\mathrm{H}}$,其中 $\widetilde{\boldsymbol{V}}\widetilde{\boldsymbol{V}}^{\mathrm{H}} = \boldsymbol{I}$,$\boldsymbol{I}$ 为单位阵,$\widetilde{\boldsymbol{\Sigma}} = diag([\sigma_1,\sigma_2,\cdots,\sigma_d])$。则中继产生的干扰信号可表示为

$$\boldsymbol{x}_{r2} = \sum_{j=1}^{d}\sqrt{\sigma_j}\,\boldsymbol{v}_j s'_j \tag{4}$$

其中,$\boldsymbol{v}_j$ 表示 $\widetilde{\boldsymbol{V}}$ 的第 j 列,$\widetilde{\boldsymbol{V}} = [\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_j, \cdots, \boldsymbol{v}_d]$,$s'_j \sim CN(0,1)$,由 SPS 中继的能量分配可知,此时转发干扰信号所需的能量约束为

$$trace(\boldsymbol{S}\boldsymbol{E}_i) \leqslant \eta\rho_i\alpha_i P_s |h_{sri}|^2 \tag{5}$$

式(5)中 $\boldsymbol{E}_i$ 表示一个对角矩阵,其对角线上元素为向量 $\boldsymbol{e}_i$(第 i 个元素为 1 的单位向量),此时中继 i 接收的信息为

$$x_{ri} = x_{ri1} + x_{ri2},\quad \forall i \tag{6}$$

由式(1)、式(2)、式(4)和式(6)可知,N 个中继接收到信息可表示为

$$\boldsymbol{x}_r = \boldsymbol{D}_{\beta\alpha}\boldsymbol{h}_{sr}\sqrt{P_s}\boldsymbol{s} + \boldsymbol{D}_{\beta\alpha}\boldsymbol{n}_a + \boldsymbol{D}_{\beta}\boldsymbol{n}_c + \sum_{j=1}^{d}\sqrt{\sigma_j}\boldsymbol{v}_j s'_j \tag{7}$$

式(7)中 $\boldsymbol{D}_{\beta\alpha}$、$\boldsymbol{D}_{\beta}$ 均表示对角矩阵,其对角线上的元素分别为 $[\beta_1\sqrt{1-\bar{\alpha}_1}, \beta_2\sqrt{1-\bar{\alpha}_2}, \cdots, \beta_N\sqrt{1-\bar{\alpha}_N}]$ 和 $[\beta_1,\beta_2,\cdots,\beta_N]$,另外,$\boldsymbol{h}_{sr} = [h_{sri}]_{i=1}^{N}$,$\boldsymbol{n}_a = [n_{a,i}]_{i=1}^{N}$,$\boldsymbol{n}_c = [n_{c,i}]_{i=1}^{N}$。

最后,中继将处理后的信息转发至接收者(Rx 与 EVE),其形式如下:

$$y = \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{x}_r + n_d \tag{8}$$

定义 Rx 收到信息为 y_d,EVE 接收到的信息为 $y_{e,k}$,由式(7)与式(8)得:

$$\begin{cases} y_d = \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{h}_{sr}\sqrt{P_s}\boldsymbol{s} + \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{n}_a \\ \qquad + \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta}\boldsymbol{n}_c + \boldsymbol{h}_{rd}^{\mathrm{T}}\sum_{j=1}^{d}\sqrt{\sigma_j}\boldsymbol{v}_j s'_j + n_d \\ y_{e,k} = \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{h}_{sr}\sqrt{P_s}\boldsymbol{s} + \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{n}_a \\ \qquad + \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta}\boldsymbol{n}_c + \boldsymbol{h}_{re,k}^{\mathrm{T}}\sum_{j=1}^{d}\sqrt{\sigma_j}\boldsymbol{v}_j s'_j + n_{e,k} \end{cases} \tag{9}$$

其中，$\boldsymbol{h}_{rd}=[h_{r1,d},h_{r2,d},\cdots,h_{rN,d}]$，$n_d\sim CN(0,\sigma_{nd}^2)$，$n_{e,k}\sim CN(0,\sigma_{ne,k}^2)$，$\boldsymbol{h}_{re,k}=[h_{r1e,k},h_{r2e,k},\cdots,h_{rNe,k}]$。同时，定义 Rx 和 EVE 的信噪比分别为 $SINR_{S,D}$，$SINR_{S,E,k}$，则由式(9)可知：

$$\begin{cases}SINR_{S,D}=P_s\mid \boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{h}_{sr}\mid^2/(trace(\boldsymbol{S}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}})\\ \quad+\sigma_{na}^2\parallel\boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\parallel^2+\sigma_{nc}^2\parallel\boldsymbol{h}_{rd}^{\mathrm{T}}\boldsymbol{D}_{\beta}\parallel^2+\sigma_{nd}^2)\\ SINR_{S,E,k}=P_s\mid \boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\boldsymbol{h}_{sr}\mid^2/(trace(\boldsymbol{S}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}})\\ \quad+\sigma_{na}^2\parallel\boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta\alpha}\parallel^2+\sigma_{nc}^2\parallel\boldsymbol{h}_{re,k}^{\mathrm{T}}\boldsymbol{D}_{\beta}\parallel^2+\sigma_{ne,k}^2)\end{cases}\tag{10}$$

定义该模型的信息安全率 r_{sec} 为：

$$r_{\mathrm{sec}}=0.5\times\log2(1+SINR_{S,D})-\max_{k\in K}0.5\times\log2(1+SINR_{S,E,k})\tag{11}$$

定义 $r_{S,D}$ 与 $r_{S,E,k}$ 为 Rx 和 EVE 的最大信息传输速率，则由式(10)与式(11)可知：

$$\begin{cases}r_{S,D}=\dfrac{1}{2}\log2\left(1+\dfrac{P_s\mid\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}\boldsymbol{w}_1\mid^2}{trace(\boldsymbol{S}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}})+\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{D}_{sd}^{\wedge}\boldsymbol{w}_1+\sigma_{nd}^2}\right)\\ r_{S,E,k}=\\ \dfrac{1}{2}\log2\left(1+\dfrac{P_s\mid\tilde{\boldsymbol{h}}_{se,k}^{\mathrm{T}}\boldsymbol{w}_1\mid^2}{trace(\boldsymbol{S}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}})+\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{D}_{se,k}^{\wedge}\boldsymbol{w}_1+\sigma_{ne,k}^2}\right)\end{cases}\tag{12}$$

$\boldsymbol{w}_1=[w_{1,1},w_{1,2},\cdots,w_{1,N}]$，其中，$w_{1,i}=\sqrt{1-\rho_i}e^{j\angle\beta_i}$ 表示 $\boldsymbol{w}_1$ 中 i 个中继权值。另外，

$$[\tilde{\boldsymbol{h}}_{sd}]_i\triangleq h_{sri}h_{rid}\sqrt{\frac{\eta\bar{a}_i(1-\bar{a}_i)\mid h_{sri}\mid^2P_s}{(1-\bar{a}_i)(\mid h_{sri}\mid^2P_s+\sigma_{na}^2)+\sigma_{nc}^2}},$$

$$[\tilde{\boldsymbol{h}}_{se,k}]_i\triangleq h_{sri}h_{rie,k}\sqrt{\frac{\eta\bar{a}_i(1-\bar{a}_i)\mid h_{sri}\mid^2P_s}{(1-\bar{a}_i)(\mid h_{sri}\mid^2P_s+\sigma_{na}^2)+\sigma_{nc}^2}},$$

$$[\tilde{\boldsymbol{h}}_{se,k}]_i\triangleq h_{sri}h_{rie,k}\sqrt{\frac{\eta\bar{a}_i(1-\bar{a}_i)\mid h_{sri}\mid^2P_s}{(1-\bar{a}_i)(\mid h_{sri}\mid^2P_s+\sigma_{na}^2)+\sigma_{nc}^2}},$$

$$[\boldsymbol{D}_{se,k}^{\wedge}]_{i,i}=\frac{\eta\bar{a}_iP_s\mid h_{sri}\mid^2\mid h_{rie,k}\mid^2((1-\bar{a}_i)\sigma_{na}^2+\sigma_{nc}^2)}{(1-\bar{a}_i)(\mid h_{sri}\mid^2P_s+\sigma_{na}^2)+\sigma_{nc}^2}。$$

由式(5)、式(11)和式(12)可知，该模型满足中继能量约束条件的最大信息安全率问题，可描述为 P1。

P1：

$$\begin{cases}\max\limits_{\boldsymbol{w}_1,\boldsymbol{S}}(r_{S,D}-\max\limits_{k\in K}r_{S,E,k})\\ \text{s.t}\quad trace(\boldsymbol{S}\boldsymbol{E}_i)\\ \leqslant\eta\bar{a}_iP_s\mid h_{sri}\mid^2(1-\mid w_{1,i}\mid^2),\ \forall i\end{cases}$$

2 SPS 中继下的优化算法

可以发现，上述 P1 问题的目标函数和约束条件均具有非凸属性，直接处理比较困难。本节利用松弛变量技术、半正定规划[9]和 Charnes-Cooper 转换来解决上述问题。

首先引入松弛变量 τ，且 $\tau\in[0,1]$，则 P1 可写为如下 P1.1 形式：

P1.1：

$$\begin{cases}\max\limits_{\boldsymbol{w}_1,\boldsymbol{S}\geqslant0}\dfrac{P_s\mid\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}\boldsymbol{w}_1\mid^2}{trace(\boldsymbol{S}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}})+\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{D}_{sd}^{\wedge}\boldsymbol{w}_1+\sigma_{nd}^2}\\ \text{s.t}\quad trace(\boldsymbol{S}\boldsymbol{E}_i)\leqslant\eta\bar{a}_iP_s\mid h_{sri}\mid^2(1-\mid w_{1,i}\mid^2),\forall i,\\ 1+\dfrac{P_s\mid\tilde{\boldsymbol{h}}_{se,k}^{\mathrm{T}}\boldsymbol{w}_1\mid^2}{trace(\boldsymbol{S}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}})+\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{D}_{se,k}^{\wedge}\boldsymbol{w}_1+\sigma_{ne,k}^2}\\ \leqslant\dfrac{1}{\tau}\end{cases}$$

定义 P1.1 中目标函数的最优值为 $f_1(\tau)$，且定义 $H_1(\tau)=\tau f_1(\tau)$，则 P1 中的目标方程可表示为

$$\frac{1}{2}\log2(1+f_1(\tau))-\frac{1}{2}\log2\left(\frac{1}{\tau}\right)=\frac{1}{2}\log2(\tau+H_1(\tau))\tag{13}$$

由 P1.1 与式(13)可知，P1 问题可写为如下 P1.2 形式：

P1.2：

$$\begin{cases}\max\limits_{\tau_{\min,1}\leqslant\tau\leqslant1,\ S\geqslant0}\log2(\tau+H_1(\tau))\\ \text{s.t}\quad trace(\boldsymbol{S}\boldsymbol{E}_i)\leqslant\eta\bar{a}_iP_s\mid h_{sri}\mid^2(1-\mid w_{1,i}\mid^2),\forall i\end{cases}$$

其中，$\tau_{\min,1}=\dfrac{1}{1+NP_s\parallel\tilde{\boldsymbol{h}}_{sd}\parallel^2/\sigma_{nd}^2}$。

其次，针对 P1.2 问题，引入变量 $\boldsymbol{X}_1$，令 $\boldsymbol{X}_1=\boldsymbol{w}_1\boldsymbol{w}_1^{\mathrm{H}}$，且松弛 $rank(\boldsymbol{X}_1)=1$ 的约束，则 P1.1 可描述为 P1.1-SDR 问题，如下所示：

P1.1-SDR：

$$\begin{cases}\max_{\tau,\ \boldsymbol{X}_1,\ \boldsymbol{S}\geqslant0}\ \tau P_s trace(\boldsymbol{X}_1\tilde{\boldsymbol{h}}_{sd}^{\dagger}\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}})/\\ trace(\boldsymbol{S}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}})+trace(\boldsymbol{X}_1\boldsymbol{D}_{sd}^{\wedge})+\sigma_{nd}^2)\\ \text{s.t}\quad P_s trace(\boldsymbol{X}_1\tilde{\boldsymbol{h}}_{se,k}^{\dagger}\tilde{\boldsymbol{h}}_{se,k}^{\mathrm{T}})/\\ trace(\boldsymbol{S}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}})+trace(\boldsymbol{X}_1\boldsymbol{D}_{se,k}^{\wedge})+\sigma_{ne,k}^2\leqslant\frac{1}{\tau}-1\\ trace((\boldsymbol{S}+\eta\bar{a}_iP_s\mid\boldsymbol{h}_{sri}\mid^2\boldsymbol{X}_1)\boldsymbol{E}_i)\leqslant\eta\bar{a}_iP_s\mid h_{sri}\mid^2,\forall i\end{cases}$$

可以发现,P1.1-SDR 为凸问题非标准形式,可以利用线性 CCT[10] 等价变换将其转化为标准凸函数。此时,令 $\boldsymbol{X}_1 = \hat{\boldsymbol{X}}_1/\xi, \boldsymbol{S} = \hat{\boldsymbol{S}}/\xi$,将 $\hat{\boldsymbol{X}}_1$ 与 $\hat{\boldsymbol{S}}$ 代入 P1.1-SDR 中,其形式如下:

P1.1-SDP:

$$\begin{cases} \max_{\tau,\hat{\boldsymbol{X}}_1,\hat{\boldsymbol{S}}\succeq 0,\xi\geqslant 0} P_s trace(\hat{\boldsymbol{X}}_1\tilde{\boldsymbol{h}}_{sd}^{\dagger}\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}}) \\ \text{s.t} \quad trace(\hat{\boldsymbol{S}}\boldsymbol{h}_{rd}^{\dagger}\boldsymbol{h}_{rd}^{\mathrm{T}}) + trace(\hat{\boldsymbol{X}}_1\boldsymbol{D}_{sd}^{\wedge}) + \xi\sigma_{nd}^2 = \tau, \\ (\dfrac{1}{\tau}-1)(trace(\hat{\boldsymbol{S}}\boldsymbol{h}_{re,k}^{\dagger}\boldsymbol{h}_{re,k}^{\mathrm{T}}) + trace(\hat{\boldsymbol{X}}_1\boldsymbol{D}_{se,k}^{\wedge}) + \xi\sigma_{ne,k}^2) \\ \geqslant P_s trace(\hat{\boldsymbol{X}}_1\tilde{\boldsymbol{h}}_{se,k}^{\dagger}\tilde{\boldsymbol{h}}_{se,k}^{\mathrm{T}}), \forall k \\ trace((\hat{\boldsymbol{S}} + \eta\bar{a}_i P_s \mid \boldsymbol{h}_{sri}\mid^2 \hat{\boldsymbol{X}}_1)\boldsymbol{E}_i) \leqslant \xi\eta\bar{a}_i P_s \mid \boldsymbol{h}_{sri}\mid^2, \forall i \end{cases}$$

通过上述分析可知,P1.1-SDP 为标准的凸函数,采用二分法来找该凸函数的最优解[11] $\boldsymbol{X}_1^*$ 以及用户的最大信息安全率 r_{sec}。

在 P1.1-SDP 中存在一个问题,即 r_{sec} 是否为该场景下的用户最大信息安全率。通过对 P1.1-SDP 分析可知,r_{sec} 仅为中继功率分配参数 $\bar{a}_i = 0.5$ 下的最大信息安全率,而非该场景下用户的最大信息安全率,若中继的分配参数发生改变,利用 P1.1-SDP,可相应地找到一个与之对应的最大信息安全率。那么,对于如何合理分配中继功率参数,从而找到该场景下的用户最大信息安全率 r_{sec}^*,值得深入讨论。

为解决该问题,本文在 P1.1-SDP 基础上,通过一维搜索法来确定最优的中继功率分配策略(如下 BEST-CJ-SPS 算法),进而确定该场景下的全局最优中继分配参数以及该场景下用户的最大信息安全率。需要注意的是,一维搜索法是以损耗大量时间为代价来提高用户的信息安全率。

最优分配算法(BEST-CJ-SPS)

算法流程:

(1) for $\bar{a}_i = a0:step:1$

(2) 求解 P1.1-SDP,且令

$r_{\mathrm{sec}} = \max_{\tau,\hat{\boldsymbol{X}}_1,\hat{\boldsymbol{S}}\succeq 0,\xi\geqslant 0} P_s * trace(\hat{\boldsymbol{X}}_1\tilde{\boldsymbol{h}}_{sd}^{\dagger}\tilde{\boldsymbol{h}}_{sd}^{\mathrm{T}})$

(3) end for

(4) 最后,令 $r_{\mathrm{sec}}^* = \max(r_{\mathrm{sec}})$,输出相应的最优的 $\bar{a}^*$。

3 仿真结果与分析

本文仿真参数如表 1 所示,其中 L 表示道路损失模型,A_0 为道路损失因子,d 定义为中继到用户(Tx,Rx,EVE)的相对距离,d_0 是参考距离,a_0 表示 SPS 中继功率分配的初始值。

表 1 仿真参数设置

参数	数值	参数	数值
G	1 000	R	2.5
$\sigma_{n_a}^2$	−80 dB	A_0	0.001
$\sigma_{n_c}^2$	−50 dB	k	2.5
$\sigma_{n_d}^2$	$\sigma_{n_d}^2 = \sigma_{n_a}^2 + \sigma_{n_c}^2$	d	不定
$\sigma_{n_{e,k}}^2$	$\sigma_{n_{e,k}}^2 = \sigma_{n_d}^2$	d_0	1 m
$\bar{a}_i$	0.5	L	$L = A_0(\frac{d}{d_0})^{-k}$
a_0	0	步长	0.01
η	50%	信道	$CN(0,L)$

3.1 多中继单窃听下的仿真分析

图 3 显示发射功率的改变对信息安全率的影响情况。从图 3 中可以看出,在相同的发射功率下,BEST-CJ-SPS 算法的性能优于 CJ-SPS 算法,其原因在于 CJ-SPS 算法下的能量分配 $\bar{a}_i$ 并非最优值,相反地,BEST-CJ-SPS 为最优的能量分配,此时的 $\bar{a}^* = 0.61$ 为最优分配方式。最后,NO-CJSPS[14] 算法与

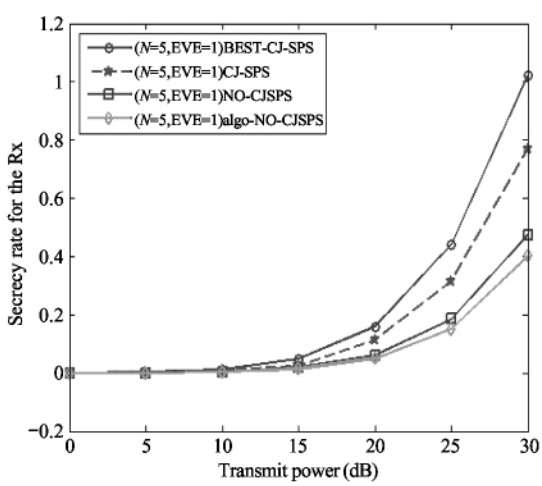

图 3 单用户对、1 个窃听者、5 个中继下的最大信息安全率($\bar{a}^* = 0.61$)

algo-NO-CJSPS 算法的安全率相较于其他算法的安全率较低，其原因在于后 2 种算法中 SPS 中继均没有产生干扰信号，即 $\boldsymbol{S}$ 为 0 矩阵，从而使得后面 2 种算法的信息安全率均较低。

图 4 显示发射功率的改变对安全率的影响情况。将图 3 与图 4 进行对比可以发现，在窃听者个数相同的情况下，中继越多，信息传输越为完整，相应的信息安全率越大。实际上，由于中继发射的干扰信号仅对窃听者有效，因此，中继个数的增加会提高接收者信噪比，同时降低窃听者的信噪比，进而提高了用户的信息安全率。

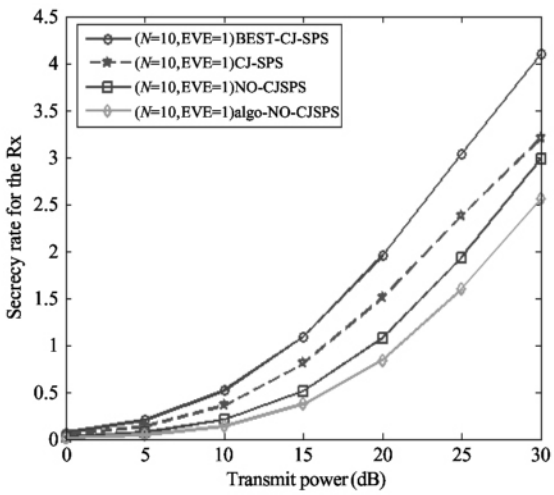

图 4　单用户对、1 个窃听者、10 个中继下的最大信息安全率（$\bar{a}^*=0.59$）

3.2　多中继多窃听下的仿真分析

图 5 为图 6 中的 SPS 中继与窃听者在半径为 R 的圆内随机分布情况，图 7 为图 8 中的 SPS 中继与窃听者在半径为 R 的圆内的随机分布情况，图 6 与图 8 均显示了发射功率的改变对安全率的影响情况，各算法的分析结果如图 3 所示。

对比图 4、图 6、图 8 可以发现，在中继个数一定的情况下，窃听者的个数越多，各个算法对应的安全率越小。其原因在于窃听者的信噪比为 $\max\limits_{k\in K} SINR_{S,E,k}$，当中继个数确定时，窃听者越多，窃听者的信噪比只增不减。此时，由于中继个数不变，则 Rx 的信噪比基本不变。通过对信息安全率的定义可知，该情况下的信息安全率只减不增。

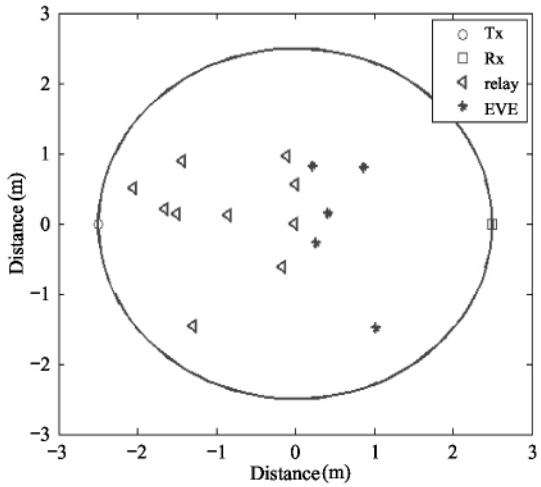

图 5　10 个中继、5 个窃听者下的随机位置分布

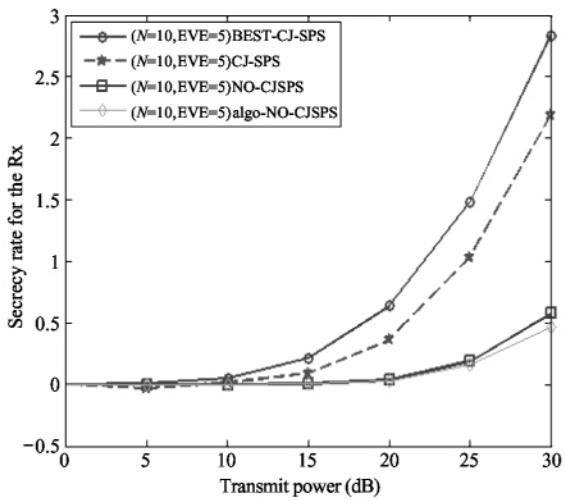

图 6　单用户对、10 个中继、5 个窃听者下的最大信息安全率（$\bar{a}^*=0.59$）

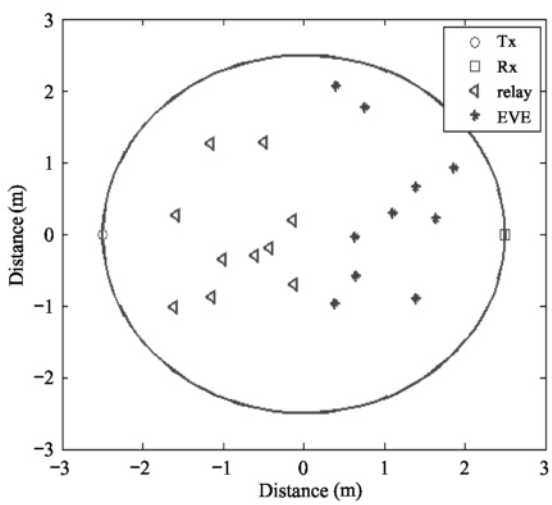

图 7　10 个中继、10 个窃听者下的随机位置分布

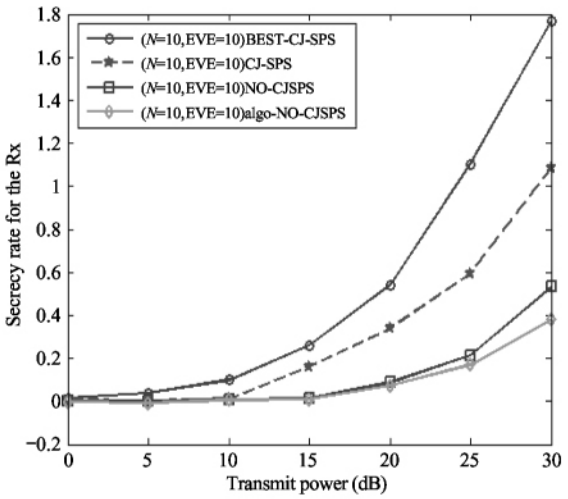

图 8　单用户对、10 个中继、10 个窃听者下的最大信息安全率($\bar{a}^*=0.60$)

4　结　论

本文基于多窃听与多中继下用户最大信息安全率的研究,提出了一种中继功率最优的能量分配(BEST-CJ-SPS)算法。在该算法中,以新型的 SPS 中继为条件构建信息传输模型,在该模型中,固定中继处的能量分配方式为传统方式下的 CJ-SPS 算法,相较于传统算法,BEST-CJ-SPS 算法中的能量分配为动态分配,该算法通过一维搜索法找到最优情况下的 SPS 中继能量分配原则,从而完成对中继处的干扰信号以及中继所需的转发能量进行合理的分配,进而找到了最优的能量分配权值,从而来提高用户的信息安全率。另外,通过本文算法与其他几种算法的对比可以发现,本文算法的性能较优,同时,仿真结果也表明了本文提出的 BEST-CJ-SPS 算法的有效性。

本文算法通过合理分配中继功率,有效地提高了用户的信息安全率,是一种具有一定实际意义与实用价值的方法。需要注意的是,外界的干扰也会对信息传输造成影响,如天气、建筑物等外部环境,考虑到外部环境的不确定性以及不可预估性,因此,本文忽略了外部环境影响这一因素。随着科技的发展与进步,在不久的将来需要对此进行进一步的研究与完善。

参考文献

[1] Bi S, Ho C K, Zhang R. Wireless powered communication: opportunities and challenges[J]. *IEEE Communications Magazine*, 2015, 53(4): 117-125

[2] Lu X, Wang P, Niyato D, et al. Wireless networks with RF energy harvesting: a contemporary survey[J]. *IEEE Communications Surveys Tutorials*, 2015, 17(2): 757-789

[3] Ding Z G, Perlaza S M, Esnaola I, et al. Power allocation strategies in energy harvesting wireless cooperative networks[J]. *IEEE Transactions Wireless Communications*, 2014, 13(2): 846-860

[4] Xing H, Wong K K, Nallanathan A. Secure wireless energy harvesting-enabled AF-relaying SWIPT networks[C]//IEEE International Conference Communications(ICC), London, UK, 2015: 2307-2312

[5] Li Q, Yang Y, Ma W K, et al. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks[J]. *IEEE Transactions on Signal Processing*, 2015, 63(1): 206-220

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

[7] Ding Z, Leung K K, Goeckel D L, et al. Opportunistic relaying for secrecy communications: cooperative jammingvs relay chatting[J]. *IEEE Transactions on Wireless Communications*, 2011, 10(6): 1725-1729

[8] Luo S, Li J, Petropulu A P. Uncoordinated cooperative jamming for secret communications[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(7): 1081-1090

[9] 张鸿,张金波,周云. 大规模分布式系统的物理层安全技术研究[J]. 无线电工程,2019,49(1):1-5

[10] Lai L F, Gamal H E. The relay-eavesdropper channel: cooperation for secrecy[J]. *IEEE Transactions on Information Theory*, 2008, 54(9): 4005-4019

[11] 曹扬,张斌,邱雪松,等. 协作干扰下的无线安全传输联盟享乐博弈[J]. 北京邮电大学学报,2017,40(1):20-23

[12] Xing H, Wong K K, Nallanathan A, et al. Wireless powered cooperative jamming for secrecy multi-AF relaying networks[J]. *arXiv*:1511.03705, 2015

[13] Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays[J]. *IEEE*

Transactions on Signal Processing, 2010, 58(3): 1875-1888

[14] Luo Z Q, Ma W K, Ci A M, et al. Semidefinite relaxation of quadratic optimization problems[J]. *IEEE Signal Processing Magazine*, 2010, 27(3): 20-34

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

[16] Hasan A, Andrews J G. The guard zone in wireless adhocnetworks[J]. *IEEE Transactions on Wireless Communications*, 2007, 6(3): 897-906

Relay power allocation algorithm in wireless sensor network with multiple relays and multiple eavesdroppers

Liu Haijiang*, Jin Yong*, Hu Zhentao*, Wu Guodong*, Li Jifang**

(*School of Computer and Information Engineering, Henan University, Kaifeng 475004)

(**School of Electric Power, North China University of Water Resources and Electric Power, Zhengzhou 450045)

Abstract

The information security rate of wireless sensor network with multiple eavesdroppers and multiple relays has been a research hotspot in recent years. Given low information security rate of traditional fixed relay power allocation algorithm, the paper proposes an optimal distribution algorithm of relay power with the maximum information security rate as the objective function and in the condition of the relay power constraint. Firstly, variable relaxation techniques and the Charnes-Cooper transform are used to transform the non-convex optimization into a convex form, and then one dimensional search method is used to get the optimal weight of power distribution. Simulation results are presented to demonstrate the performance of the proposed scheme.

Key words: channel state information, energy optimal, information security rate, weight vector