储能-发送模式的单天线两跳中继系统保密速率的优化

雷维嘉* 杨小燕 江 雪 谢显中
(重庆邮电大学移动通信技术重庆市重点实验室 重庆 400065)

摘 要：该文研究节点具有能量收集能力的两跳中继系统的物理层安全传输方案。考虑窃听节点与源和中继节点间都有直接链路的情况。每个数据传输时隙分为能量收集和数据传输两个阶段，各节点用收集的能量发送信号。中继采用放大转发方式，目的节点发送人工噪声进行协作干扰，保护在两跳传输中传输的保密信息。以最大化保密速率为目标，采用迭代算法优化能量吸收和数据传输两阶段的时间分配比例系数和协作干扰功率分配因子。仿真结果表明优化算法准确，优化后的协作干扰方案能显著提高系统的保密传输速率。由于考虑了窃听节点在两跳传输中都能接收到信号的可能性，文中方案更贴近实际，并解决了一个复杂的优化问题。

关键词：保密速率；能量收集；储能-发送；协作干扰；中继
中图分类号： TN925 **文献标识码**： A **文章编号**：1009-5896(2016)09-2233-08
DOI: 10.11999/JEIJ151371

Secrecy Rate Optimization for Single Antenna Two-hop Relay System in Energy-saving-then-transmitting Mode

LEI Weijia YANG Xiaoyan JIANG Xue XIE Xianzhong
(*Chongqing Key Laboratory of Mobile Communications Technology*, *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: A physical layer security transmission protocol in a two-hop relay system is studied. All nodes are equipped with an antenna and have the ability of energy harvesting. There are direct links between the source node and the eavesdropper as well as the relay node and the eavesdropper. Each transmission time slot is divided into two stages, which are respectively used for energy harvesting and data transmitting. The energy harvested is used to send data. The amplify-and-forward protocol is adopted, and the destination node sends artificial noise to protect the information transmitted in the first and second hop. To maximize the secrecy rate, iterative algorithm is used to optimize two variables of the time for energy harvesting and the power of artificial noise. Simulation results show that the optimization algorithm is accurate and the cooperative jamming can effectively improve the secrecy rate. Considering that eavesdropper can intercept the information transmitted in the two hops, the proposed scheme is more practical and can solve a complicate optimization problem.

Key words: Secrecy rate; Energy harvesting; Save-then-transmit; Cooperative jamming; Relay

1 引言

随着多天线技术、协作通信技术、编码技术的发展，利用无线信道的随机性实现信息安全传输的物理层安全技术[1]近年来成为学术界研究的热点问题。物理层安全的研究主要有两个方面，一是防窃听，另一是抗干扰。目前物理层安全技术多指的是防窃听技术，即信息的保密传输技术。物理层上的防窃听是利用无线信道的多径、互易性、空间唯一性等特征，在香农信息论的安全模型之上通过利用调制、编码、信号处理等方法来实现的。协作通信技术[2]是在无线通信网络中，多个通信节点以一定方式进行协作和共享资源，提高系统性能的技术。中继节点的信号转发技术是协作通信中的基本技术，根据中继节点在协作传输过程中对接收信号处理方式的不同，有放大转发(Amplify-and-Forward, AF)、解码转发方式等。在物理层安全的应用中，协作节点除采用信号转发的工作方式外，还有一种工作方式是不接收和转发来自源节点发送的消息，而是发送干扰信号干扰窃听者。由中继或目的端引入人工

收稿日期：2015-12-08；改回日期：2016-05-10；网络出版：2016-07-04
*通信作者：雷维嘉 Leiwj@cqupt.edu.cn
基金项目：国家自然科学基金(61471076, 61301123)，长江学者和创新团队发展计划(IRT1299)，重庆市重点实验室专项经费
Foundation Items: The National Natural Science Foundation of China (61471076, 61301123), The Program for Changjiang Scholars and Innovative Research Team in University (IRT1299), The Special Fund of Chongqing Key Laboratory

噪声[3]对窃听者进行干扰，提高保密速率的协作方式称为协作干扰。中继协作转发和协作干扰技术是提高物理层安全性能的有效方法[4,5]。文献[4]研究无线自组织网络中安全传输问题。系统模型中有多对源节点和目的节点，多个中继节点，并存在多个窃听节点。中继分为两组，一组完成多个源-目的节点对间的信号传输，另一组作为干扰者干扰窃听节点的窃听。文献提出了一种中继分组的优化算法，同时给出了信号转发和人工噪声的波束赋形优化算法，最大化保密速率。文献[5]研究由源节点，目的节点，中继(AF)节点，窃听节点各一个组成的系统模型的安全传输问题。目的节点作为干扰者发送干扰噪声，根据目的端信道状态信息(Channel State Information, CSI)的可用情况，给出了 3 种安全中断概率最小化的干扰功率分配方案，并分析了每种方案下的安全中断概率。理论分析和仿真的结果表明目的端的协作干扰可提高保密速率，降低安全中断概率。

一些无线通信网络，如传感器网络，其节点一般采用电池供电，电量耗尽后就需要充电或更换。在地理条件限制下，电池的充电或更换很不方便。近年来受到广泛关注的无线能量收集技术[6,7]是解决无线节点电能供应的有效手段。作为一类特殊的无线通信系统，具有能量收集的无线通信系统仍然存在信息的安全传输问题。由于受到能量收集的约束，在这种通信系统中应用常规无线通信系统中物理层安全技术时会面临一些新的问题，如在数据传输和能量收集不能同时进行时，需对数据传输和能量收集的时间进行优化分配；能量和信息同时传输时，需要考虑能量传输中不泄露保密信息。文献[8]中，多天线发射机发送保密消息给一个单天线信息接收机，同时转移能量给一个多天线能量接收机。为防止能量接收机获得保密信息，发射机发射人工噪声保护携带保密信息的信号，而该人工噪声也同时用于传输能量。文献在 CSI 不完整的情况下，通过联合设计人工噪声和携带保密信息的信号的协方差矩阵使保密速率最大。

本文研究节点采用“储能—发送”模式的两跳中继系统的安全传输问题，系统模型与文献[5]类似，都包含单天线的源节点、目的节点、中继节点、窃听节点各一个，源节点与目的节点间无直接链路，需要通过中继进行转发，由目的端发送人工噪声对窃听者进行干扰，以实现保密信息的传输。但与文献[5]不同，本文考虑源与窃听节点有直接链路和节点具能量收集能力的情况，所有发送信号的能量均来自收集的能量。同时，本文的优化目标是保密速率，而文献[5]是安全中断概率。本文方案在信息传输的第 1 跳中，目的节点在源节点发送信息的同时发送人工噪声，该噪声同时干扰中继和窃听节点的接收；在第 2 跳中中继转发叠加了干扰的信号，目的端由于知道中继转发信号中的干扰，可采用干扰对消技术将其消除，而窃听端则不能。通过目的端在第 1 跳传输中的协作干扰，可同时抑制窃听节点在两跳信息传输中的信号接收，提高保密传输能力。论文对系统可获得的保密速率进行分析，以最大化保密传输速率为目标，对能量吸收时间比例和干扰功率分配因子进行优化。

2 系统模型

本文研究一个两跳的中继通信系统，由源节点 s, AF 中继节点 r，目的节点 d 和窃听节点 e 各一个组成，每个节点都为单天线，采用半双工模式。系统中所有节点均具有能量收集能力，采用“储能—发送”模式工作。源节点到目的节点无直接链路，由中继进行转发。源节点到窃听节点有直连链路，为提高传输的安全性，在数据传输时由目的节点发送人工噪声对窃听端进行干扰。假设接收端已知 CSI，而发送端未知。

在每个传输时隙的时间 T 内，节点的工作分为能量收集和数据传输两个阶段。

(1)能量收集阶段：在$(0,\rho T)$内，节点从周围环境中收集能量，将其转换为电能后储存在电池中，$\rho(0<\rho<1)$ 是能量吸收时间比例，表示一个时隙 T 内用于能量收集的时间比例。

(2)数据传输阶段：在$(\rho T, T)$内进行数据的两跳传输，$(\rho T,(1+\rho)T/2)$为第 1 跳，源节点发送信号到中继节点，为防止窃听节点获取保密信息，目的节点同时发送人工噪声，同时干扰窃听节点和中继节点的接收。$((1+\rho)T/2, T)$为第 2 跳，中继节点转发叠加了人工噪声的信号。由于目的节点已知人工噪声，可将第 2 跳收到信号中的人工噪声消除。而窃听节点则无法消除人工噪声，抑制了其信号接收质量。

每个传输时隙中，若分配给能量收集阶段的时间越长，即 ρ 越大，收集的能量越多，用于数据传输的发送功率越大，有利于提高传输速率，但用于数据传输的时间越短，信道利用率就越低。同时，ρ 值的大小也影响目的节点可用于发送人工干扰噪声的最大功率。另一方面，目的节点以可用的最大功率发送干扰时不一定就能获得最大的保密速率。人工噪声的功率过小，不能有效防止窃听节点的窃听；但人工噪声的功率过大，则中继节点接收到信号中

噪声的比重就越大，虽然能有效防窃听，但由于中继节点转发信号的功率有限，其中传输保密信息的信号功率就会过低，也会导致保密速率较低。因此，为了获得最大的保密速率，需要对能量吸收时间比例 ρ 和目的节点发送人工噪声的功率进行优化。定义目的节点干扰分配功率因子 $\alpha(0 \le \alpha \le 1)$ 为目的节点发送干扰的功率与最大可用功率的比值，对干扰功率的优化也就是对 α 进行优化。

各节点在第 1 个阶段 ρT 的时间内储存的能量为

$$E_i = v_i \rho T, \quad i \in \{\mathrm{s,r,d}\} \tag{1}$$

式中，s, r, d 分别对应源节点、中继节点、目的节点。v_i 为节点 i 在单位时间内收集的能量，也就是能量吸收速率，单位为 J/s。

在第 2 阶段 $(1-\rho)T$ 的时间内各节点可持续发送信号的最大功率为

$$P_i = 2v_i\rho/(1-\rho), \quad i \in \{\mathrm{s,r,d}\} \tag{2}$$

在数据传输阶段，记 x 为源节点发送的消息，z 为目的节点发送的干扰，满足功率约束 $E[|x|^2]=E[|z|^2]=1$，其中 E 表示期望运算；源节点和中继节点发送信号的功率分别为 $P_\mathrm{s}, P_\mathrm{r}$，目的节点发送干扰信号的功率为 P_d; n_r, n_e1 分别是第 1 跳中继节点和窃听节点的噪声，n_d, n_e2 分别是第 2 跳目的节点和窃听节点的噪声，均为均值为零、方差为 σ^2 的复高斯白噪声；g 是中继为满足功率约束条件 $E[|gy_\mathrm{r}|^2]=P_\mathrm{r}$ 而设置的转发增益。所有信道为具有互易性的准静态平坦瑞利衰落信道，信道系数 h_sr, h_se, h_re, h_rd, h_de 为独立同分布的随机变量，服从零均值、单位方差的复高斯分布。

数据传输的第 1 跳，中继节点和窃听节点接收到的信号分别为

$$y_\mathrm{r} = \sqrt{P_\mathrm{s}}h_\mathrm{sr}x + \sqrt{\alpha P_\mathrm{d}}h_\mathrm{rd}z + n_\mathrm{r} \tag{3}$$

$$y_\mathrm{e1} = \sqrt{P_\mathrm{s}}h_\mathrm{se}x + \sqrt{\alpha P_\mathrm{d}}h_\mathrm{de}z + n_\mathrm{e1} \tag{4}$$

数据传输的第 2 跳，中继节点采用 AF 方式转发信号，目的节点和窃听节点接收到的信号分别为

$$y_\mathrm{d} = gh_\mathrm{rd}y_\mathrm{r} + n_\mathrm{d} = gh_\mathrm{rd}h_\mathrm{sr}\sqrt{P_\mathrm{s}}x + gh_\mathrm{rd}h_\mathrm{rd}\sqrt{\alpha P_\mathrm{d}}z + gh_\mathrm{rd}n_\mathrm{r} + n_\mathrm{d} \tag{5}$$

$$y_\mathrm{e2} = gh_\mathrm{re}y_\mathrm{r} + n_\mathrm{e2} = gh_\mathrm{re}h_\mathrm{sr}\sqrt{P_\mathrm{s}}x + gh_\mathrm{re}h_\mathrm{rd}\sqrt{\alpha P_\mathrm{d}}z + gh_\mathrm{re}n_\mathrm{r} + n_\mathrm{e2} \tag{6}$$

对于目的节点，由于人工噪声 z 是自己产生的，在已知 CSI 的条件下，可用干扰对消技术消除。于是目的节点的接收信号又可写为

$$y_\mathrm{d} = gh_\mathrm{rd}h_\mathrm{sr}\sqrt{P_\mathrm{s}}x + gh_\mathrm{rd}n_\mathrm{r} + n_\mathrm{d} \tag{7}$$

式(5)~式(7)中，满足功率约束的中继增益 g 为

$$g = \sqrt{P_\mathrm{r}\Big/\left(|h_\mathrm{sr}|^2 P_\mathrm{s} + |h_\mathrm{rd}|^2 \alpha P_\mathrm{d} + \sigma^2\right)} \tag{8}$$

目的节点的接收信噪比为

$$\gamma_\mathrm{d} = \frac{\gamma_\mathrm{sr}\gamma_\mathrm{rd}}{\alpha\gamma_\mathrm{dr} + \gamma_\mathrm{rd} + \gamma_\mathrm{sr} + 1} \tag{9}$$

窃听节点两跳中的接收信噪比分别为

$$\left.\begin{aligned} \gamma_\mathrm{e1} &= \frac{\gamma_\mathrm{se}}{\alpha\gamma_\mathrm{de} + 1} \\ \gamma_\mathrm{e2} &= \frac{\gamma_\mathrm{sr}\gamma_\mathrm{re}}{\alpha\gamma_\mathrm{re}\gamma_\mathrm{dr} + \alpha\gamma_\mathrm{dr} + \gamma_\mathrm{sr} + \gamma_\mathrm{re} + 1} \end{aligned}\right\} \tag{10}$$

其中，$\gamma_\mathrm{sr} = \dfrac{2v_\mathrm{s}\rho|h_\mathrm{sr}|^2}{(1-\rho)\sigma^2}$，$\gamma_\mathrm{se} = \dfrac{2v_\mathrm{s}\rho|h_\mathrm{se}|^2}{(1-\rho)\sigma^2}$，$\gamma_\mathrm{rd} = \dfrac{2v_\mathrm{r}\rho|h_\mathrm{rd}|^2}{(1-\rho)\sigma^2}$，$\gamma_\mathrm{dr} = \dfrac{2v_\mathrm{d}\rho|h_\mathrm{rd}|^2}{(1-\rho)\sigma^2}$, $\gamma_\mathrm{de} = \dfrac{2v_\mathrm{d}\rho|h_\mathrm{de}|^2}{(1-\rho)\sigma^2}$，$\gamma_\mathrm{re} = \dfrac{2v_\mathrm{r}\rho|h_\mathrm{re}|^2}{(1-\rho)\sigma^2}$。

目的端的信道容量为

$$C_\mathrm{d} = \frac{(1-\rho)}{2}\log_2(1+\gamma_\mathrm{d}) \tag{11}$$

窃听节点采用最大比合并方式合并两跳接收到的信号，因此窃听端的信道容量为

$$C_\mathrm{e} = \frac{(1-\rho)}{2}\log_2(1+\gamma_\mathrm{e1}+\gamma_\mathrm{e2}) \tag{12}$$

式(11)、式(12)中因子 1/2 是由于两跳传输，传输阶段分成两半，分别由源节点和中继节点发送信息；$(1-\rho)$ 表示在一个单位时隙内用于数据传输的时间比例。可实现保密速率为

$$R_\mathrm{s} = [C_\mathrm{d} - C_\mathrm{e}]^+ = \frac{(1-\rho)}{2}\left[\log_2(1+\gamma_\mathrm{d}) - \log_2(1+\gamma_\mathrm{e1}+\gamma_\mathrm{e2})\right]^+ \tag{13}$$

其中，$[x]^+=\max(0,x)$。将式(8)、式(9)、式(10)代入式(13)，整理后得到

$$R_\mathrm{s}(\rho,\alpha) = \left[\frac{(1-\rho)}{2}\log_2\frac{(\alpha\gamma_\mathrm{dr}+\gamma_\mathrm{sr}+\gamma_\mathrm{rd}+\gamma_\mathrm{sr}\gamma_\mathrm{rd}+1)(\alpha\gamma_\mathrm{dr}\gamma_\mathrm{re}+\alpha\gamma_\mathrm{dr}+\gamma_\mathrm{re}+\gamma_\mathrm{sr}+1)}{(\alpha\gamma_\mathrm{dr}+\gamma_\mathrm{sr}+\gamma_\mathrm{rd}+1)[(\gamma_\mathrm{se}/(\alpha\gamma_\mathrm{de}+1)+1)(\alpha\gamma_\mathrm{dr}\gamma_\mathrm{re}+\alpha\gamma_\mathrm{dr}+\gamma_\mathrm{re}+\gamma_\mathrm{sr}+1)+\gamma_\mathrm{sr}\gamma_\mathrm{re}]}\right]^+ \tag{14}$$

3　干扰功率分配因子和能量吸收比例的优化

3.1 优化问题

如前节所述，保密速率的取值与 ρ, α 有关。ρ 在 $(0,1)$ 之间取值，R_s 一定是 ρ 的凸函数。α 在 $[0,1]$ 之间取值，与信道条件有关。尽管可能 R_s 不是 α 的凸函数，但由于 α 取值有限，使 R_s 最大的 α 值一定存在，该值可能是边界点 0, 1，或者是使 R_s 对 α 的偏导为 0 的极值点。在 $\rho \in (0,1), \alpha \in [0,1]$ 内，一定存在使 R_s 最大的 ρ - α 组合。优化问题为

$$\left.\begin{aligned}&\arg\max_{\rho,\alpha} R_{\mathrm{s}}(\rho,\alpha)\\ &\text{s.t.}\quad \begin{cases}0\le\alpha\le 1\\ 0<\rho<1\end{cases}\end{aligned}\right\} \tag{15}$$

式(14)是保密速率 R_{s} 关于 ρ,α 的方程，理论上要求得 R_{s} 的最大值，应先找到该二元函数的极值点，再联合边界点找到使 R_{s} 最大的最大值点。而要找到极值点，需要求解 R_{s} 关于 ρ,α 的联合偏导数为 0 的解，但该解析解很难获得。注意到式(14)中所有的γ中都包含 ρ，因此 R_{s} 是关于 ρ 的高次方程且含有对数函数，不能得到 $\partial R_{\mathrm{s}}(\rho,\alpha)/\partial\rho=0$ 时 ρ 的解析解。而在 ρ 给定的情况下，则可求取满足 $\partial R_{\mathrm{s}}(\rho,\alpha)/\partial\alpha=0$ 的解析解。本文采用迭代方法来求解式(15)的优化问题：第 1 次迭代时给定一个 α 的初值，通过 1 维搜索的方式得到使 R_{s} 最大的 ρ 值；在第 2 次迭代中将该 ρ 值代入式(15)，通过求解方程 $\partial R_{\mathrm{s}}(\rho,\alpha)/\partial\alpha=0$ 得到 R_{s} 极值点处的 α 值，将该极值点与边界点处的保密速率比较，更新 α 为最大保密速率值对应的 α 值，再在该 α 值下搜索使 R_{s} 最大的 ρ 值，完成一次迭代；在此 α 和 ρ 值基础上再进行下一次迭代，获得新的 ρ 和 α 值。经过这样有限次的迭代后，ρ,α 值将逐渐逼近最优值 ρ^*,α^*，并获得最大化的保密速率。下面对α值的优化问题进行讨论。

3.2 $\partial R_{\mathrm{s}}(\rho,\alpha)/\partial\alpha=0$ 的解析解

推导过程中假定 $R_{\mathrm{s}}(\rho,\alpha)>0$，将保密速率表达式中的上标+省略。将式(14)简记为

$$R_{\mathrm{s}}(\rho,\alpha)=\frac{(1-\rho)}{2}\log_2\left[\frac{\gamma_1\alpha^3+\gamma_2\alpha^2+\gamma_3\alpha+\gamma_4}{\gamma_1\alpha^3+\gamma_5\alpha^2+\gamma_6\alpha+\gamma_7}\right] \tag{16}$$

式中，

$$\begin{aligned}
\gamma_1&=\gamma_{\mathrm{dr}}^2\gamma_{\mathrm{de}}(\gamma_{\mathrm{re}}+1)\\
\gamma_2&=\gamma_{\mathrm{dr}}\gamma_{\mathrm{de}}\gamma_{\mathrm{sr}}+\gamma_{\mathrm{dr}}(\gamma_{\mathrm{re}}+1)\\
&\quad\cdot(\gamma_{\mathrm{de}}\gamma_{\mathrm{sr}}+\gamma_{\mathrm{de}}\gamma_{\mathrm{rd}}+\gamma_{\mathrm{rd}}\gamma_{\mathrm{de}}\gamma_{\mathrm{sr}}+2\gamma_{\mathrm{de}}+\gamma_{\mathrm{dr}})\\
\gamma_3&=\gamma_{\mathrm{dr}}(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{re}}+1)+[(\gamma_{\mathrm{de}}+\gamma_{\mathrm{dr}})(\gamma_{\mathrm{re}}+1)\\
&\quad+\gamma_{\mathrm{de}}\gamma_{\mathrm{sr}}](\gamma_{\mathrm{sr}}+\gamma_{\mathrm{rd}}+1+\gamma_{\mathrm{sr}}\gamma_{\mathrm{rd}})\\
\gamma_4&=(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{re}}+1)(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{rd}}+1+\gamma_{\mathrm{sr}}\gamma_{\mathrm{rd}})\\
\gamma_5&=\gamma_{\mathrm{dr}}(\gamma_{\mathrm{re}}+1)[2\gamma_{\mathrm{de}}(\gamma_{\mathrm{sr}}+1)+\gamma_{\mathrm{rd}}\gamma_{\mathrm{de}}+\gamma_{\mathrm{dr}}(\gamma_{\mathrm{se}}+1)]\\
\gamma_6&=(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{rd}}+1)[\gamma_{\mathrm{de}}(\gamma_{\mathrm{sr}}+1)+\gamma_{\mathrm{dr}}(\gamma_{\mathrm{se}}+1)](\gamma_{\mathrm{re}}+1)\\
&\quad+\gamma_{\mathrm{dr}}(\gamma_{\mathrm{se}}+1)(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{re}}+1)+\gamma_{\mathrm{dr}}\gamma_{\mathrm{re}}\gamma_{\mathrm{sr}}\\
\gamma_7&=(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{rd}}+1)[(\gamma_{\mathrm{se}}+1)(\gamma_{\mathrm{sr}}+\gamma_{\mathrm{re}}+1)+\gamma_{\mathrm{re}}\gamma_{\mathrm{sr}}]
\end{aligned}$$

对式(16)求关于 α 的偏导，得到

$$\frac{\partial R_{\mathrm{s}}(\rho,\alpha)}{\partial\alpha}=\frac{(1-\rho)}{2\ln 2}\left[\frac{3\gamma_1\alpha^2+2\gamma_2\alpha+\gamma_3}{\gamma_1\alpha^3+\gamma_2\alpha^2+\gamma_3\alpha+\gamma_4}-\frac{3\gamma_1\alpha^2+2\gamma_5\alpha+\gamma_6}{\gamma_1\alpha^3+\gamma_5\alpha^2+\gamma_6\alpha+\gamma_7}\right] \tag{17}$$

令式(17)等于零，整理后得

$$\begin{aligned}
&\gamma_1(\gamma_5-\gamma_2)\alpha^4+2\gamma_1(\gamma_6-\gamma_3)\alpha^3+[\gamma_2\gamma_6-\gamma_3\gamma_5\\
&\quad+3\gamma_1(\gamma_7-\gamma_4)]\alpha^2+2(\gamma_2\gamma_7-\gamma_4\gamma_5)\alpha\\
&\quad+(\gamma_3\gamma_7-\gamma_6\gamma_4)=0
\end{aligned} \tag{18}$$

式(18)是一个一元四次方程，分 4 种情况对具体求解过程进行讨论。

情况 1 $\gamma_5\ne\gamma_2$ 时，式(18)为一元四次实系数方程，可采用文献[9]的方法对方程进行求解。令 $a=\gamma_1(\gamma_5-\gamma_2),b=\gamma_1(\gamma_6-\gamma_3)/2,c=[\gamma_2\gamma_6-\gamma_3\gamma_5+3\gamma_1(\gamma_7-\gamma_4)]/6,d=(\gamma_2\gamma_7-\gamma_4\gamma_5)/2,e=(\gamma_3\gamma_7-\gamma_6\gamma_4)$，$H=b^2-ac,I=ae-4bd+3c^2$，$\Delta=I^3-27J^2$，$G=a^2d-3abc+2b^3,J=(4H^3-a^2HI-G^2)/a^3$。

(1) 当 $\Delta<0$，$G\ne0$，$I^2+J^2\ne0$ 时，方程的 4 个根为

$$\left.\begin{aligned}\alpha_{1,2}&=\left(-b-\mathrm{sgn}(G)\sqrt{t}\pm\sqrt{|G|/\sqrt{t}-t+3H}\right)\Big/a\\ \alpha_{3,4}&=\left(-b+\mathrm{sgn}(G)\sqrt{t}\pm i\sqrt{|G|/\sqrt{t}-t+3H}\right)\Big/a\end{aligned}\right\} \tag{19}$$

其中，

$$\mathrm{sgn}(G)=\begin{cases}1, & (G>0)\\ -1, & (G<0)\end{cases}$$

$$t=\frac{a}{2}\left(\sqrt[3]{-J+\sqrt{-\Delta/27}}+\sqrt[3]{-J-\sqrt{-\Delta/27}}\right)+H$$

(2)当 $\Delta\ge0$，$G\ne0$，$I^2+J^2\ne0$ 时，方程的 4 个根为

$$\left.\begin{aligned}\alpha_1&=\left(-b-\mathrm{sgn}(G)\sqrt{y_1}+\sqrt{y_2}+\sqrt{y_3}\right)\Big/a\\ \alpha_2&=\left(-b-\mathrm{sgn}(G)\sqrt{y_1}-\sqrt{y_2}-\sqrt{y_3}\right)\Big/a\\ \alpha_3&=\left(-b+\mathrm{sgn}(G)\sqrt{y_1}+\sqrt{y_2}-\sqrt{y_3}\right)\Big/a\\ \alpha_4&=\left(-b+\mathrm{sgn}(G)\sqrt{y_1}-\sqrt{y_2}+\sqrt{y_3}\right)\Big/a\end{aligned}\right\} \tag{20}$$

式中，$y_1=a\sqrt{|I|/3}\cos(\theta/3)+H$，$y_{2,3}=a\sqrt{|I|/3}\cdot\cos(\theta/3\pm2\pi/3)+H$，$\theta=\arccos\left(J/\sqrt{|I|^3/27}\right)$。

(3)当 $G\ne0$，$I=J=0$ 时，方程的 4 个根为

$$\left.\begin{aligned}\alpha_{1,2,3}&=\left(-b+\mathrm{sgn}(G)\sqrt{H}\right)\Big/a\\ \alpha_4&=\left(-b-3\,\mathrm{sgn}(G)\sqrt{H}\right)\Big/a\end{aligned}\right\} \tag{21}$$

(4) 当 $G=0$ 时，方程的 4 个根为

$$\alpha_{1,2,3,4}=\left(-b\pm\sqrt{3H\pm\sqrt{12H^2-a^2I}}\right)\Big/a \tag{22}$$

情况 2 当 $\gamma_5=\gamma_2$ 且 $\gamma_6\ne\gamma_3$ 时，式(18)为一元三次实系数方程，采用文献[10,11]的方法进行求解。令式(18)中 $a=2\gamma_1(\gamma_6-\gamma_3)$，$b=\gamma_2\gamma_6-\gamma_3\gamma_5+3\gamma_1(\gamma_7-\gamma_4)$，$c=2(\gamma_2\gamma_7-\gamma_4\gamma_5)$，$d=\gamma_3\gamma_7-\gamma_6\gamma_4$，$A=b^2-3ac$，$B=bc-9ad$，$C=c^2-3bd$，$\Delta=B^2-4AC$，$y_{1,2}=Ab+1.5a\left(-B\pm\sqrt{B^2-4AC}\right)$。

(1) 当 $\Delta=0$ 时，$A=0$ 和 $A\ne0$ 时的 3 个根分别为

$$\left.\begin{aligned}&\alpha_1=\alpha_2=\alpha_3=-b/3a\,(A=0)\\ &\alpha_1=-b/a+B/A,\ \alpha_{2,3}=-B/2A\,(A\ne0)\end{aligned}\right\} \tag{23}$$

(2)当 $\Delta>0$ 时，方程有一个实根、两个虚根，由于α应为实数，只需要实根：

$$\alpha_1=\left(-b-\sqrt[3]{y_1}-\sqrt[3]{y_2}\right)\Big/3a \tag{24}$$

(3)当 $\Delta<0$ 时，由文献[10]给出的定理可知 A 一定大于 0，令 $N=(2Ab-3aB)/2\sqrt{A^3}$ 时，一定在 $(-1,1)$ 之间，$\theta=\arccos N$，所求的 3 个根为

$$\begin{aligned}\alpha_1&=\left(-b-2\sqrt{A}\cos(\theta/3)\right)\Big/3a\\ \alpha_{2,3}&=\left(-b+\sqrt{A}\left[\cos(\theta/3)\pm\sqrt{3}\sin(\theta/3)\right]\right)\Big/3a\end{aligned} \tag{25}$$

情况 3　当式(18)的四次项与三次项都为零时，令 $a=\gamma_2\gamma_6-\gamma_3\gamma_5+3\gamma_1(\gamma_7-\gamma_4)$,$b=2(\gamma_2\gamma_7-\gamma_4\gamma_5)$, $c=\gamma_3\gamma_7-\gamma_6\gamma_4$，两个根为

$$\alpha_{1,2}=\left(-b\pm\sqrt{b^2-4ac}\right)\Big/2a \tag{26}$$

情况 4　当式(18)二，三，四次项都为零时，令 $a=2(\gamma_2\gamma_7-\gamma_4\gamma_5)$，$b=\gamma_3\gamma_7-\gamma_6\gamma_4$。方程的解为

$$\alpha_1=b/a \tag{27}$$

在方程求解中得到的根如果不在[0,1]之间，则不是可能的最优值，可直接丢弃。

3.3 迭代算法优化过程

要得到最大保密速率，需对 ρ,α 进行反复迭代优化，最终逼近最优值。具体迭代算法过程为：

步骤 1　第 1 次迭代中，先设定 α 的初值 α_1，代入式(14)中，运用 1 维搜索方法找到使 R_s 最大的 ρ_1 值。

步骤 2　在第 n 次迭代中($n\geq2$)过程中包含 3 个步骤：

(1)将上次迭代中得到的 ρ_{n-1} 的值代入式(18)中，解出在 0,1 之间满足 $\partial R_s(\rho,\alpha)/\partial\alpha=0$ 的 α 值，将其对应的保密速率值与 0, 1 边界点处的保密速率值比较，将其中最大值对应的 α 值赋值给 α_n；

(2)将 α_n 的值代入式(14)中，运用 1 维搜索方法找到使 R_s 最大的ρ_n值；

(3)计算 $|\rho_n-\rho_{n-1}|$，如果 $|\rho_n-\rho_{n-1}|<\delta$，其中$\delta$是控制迭代计算精度的小的正数，表示迭代过程已经收敛，迭代过程结束，否则转步骤 2(1)步进行下一次迭代。

步骤 3　获得优化的保密速率。将最后一次迭代得到的优化值 ρ^* 和 α^* 代入式(14)求出最大保密速率 R_s。

本文算法采用 1 维搜索和解析求解相结合的方案，通过迭代来获得最优解。在后面的仿真中可以看到，只需 2~3 次迭代，迭代过程即收敛。与 2 维搜索算法相比，本文算法的搜索计算量要低得多。假设 2 维搜索中 ρ 和 α 的搜索步长为Δ_1和Δ_2，则搜索计算量为 $1/(\Delta_1\Delta_2)$。本文算法中若同样假设 ρ 的搜索步长为Δ_1，则每次迭代的搜索计算量为 $1/\Delta_1$。如进行 3 次迭代，则总的搜索计算量为 $3/\Delta_1$。而 α 优化值通过求解方程得到，一次迭代仅需要求解一次，即计算式(19)~式(27)中的一个。另一方面，2 维搜索中 ρ 和 α 的精度都与搜索步长有关，而本文算法只有 ρ 的精度与搜索步长有关，α 为解析解，优化准确性也更高。

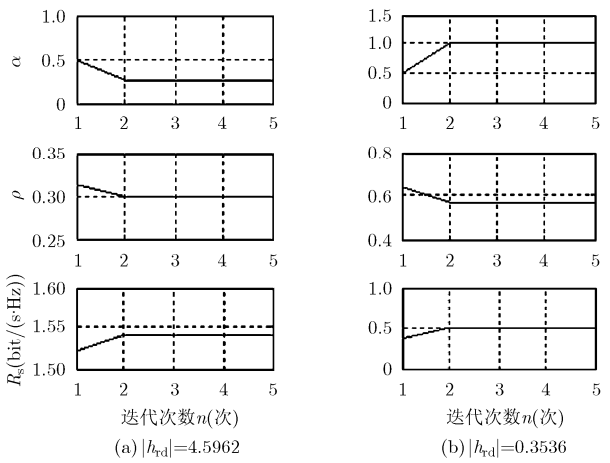
4　性能仿真

在本节仿真中，各节点处的噪声方差为 $\sigma^2=-50$ dBw，ρ值 1 维搜索的步长为 0.001，迭代停止门限 $\delta=10^{-3}$。

4.1 迭代优化算法的收敛性和准确性

图 1 为迭代优化算法迭代过程的仿真结果。信道系数的模为 $|h_{sr}|$=0.6364, $|h_{re}|$=0.9899, $|h_{se}|$=0.2121, $|h_{de}|$=1.0607, $|h_{rd}|$分别为 4.5962, 0.3536；各节点能量吸收速率均为 1 mJ/s；迭代优化过程中干扰功率分配因子的初值假设为 $\alpha_1=0.5$。图 1 中可以看出，保密速率 R_s 也随着迭代次数增加而提高，能量吸收时间比例 ρ，干扰功率分配因子 α 在迭代 2~3 次后逼近最优值而收敛。在其他随机产生信道的 500 次蒙特卡洛仿真中，算法的收敛情况相似。

为了验证本文算法所得结果的准确性，我们同时也用 2 维搜索的方式找到使保密速率 R_s 获得最大的 α 和 ρ 值。图 2 给出了信当道条件为$|h_{sr}|$=0.6364, $|h_{re}|$=0.9899, $|h_{se}|$=0.2121, $|h_{de}|$=1.0607, $|h_{rd}|$=4.5962，各节点能量吸收速率为 1 mJ/s 时的搜索过程。可以看到保密速率 R_s 是关于 α 和 ρ 的凸函数，2 维搜索得到 α=0.250, ρ=0.310 时，保密速率 R_s 取得最大值 1.58453 bit/(s·Hz)。相同条件下，用本文迭代优化算法得到的最优值为 α=0.2426, ρ=0.300，获得的保密速率 R_s 为 1.58454 bit/(s·Hz)，与全局搜索的结果基本一致。



(a) $|h_{rd}|$=4.5962　(b) $|h_{rd}|$=0.3536

图1 迭代优化算法的收敛过程

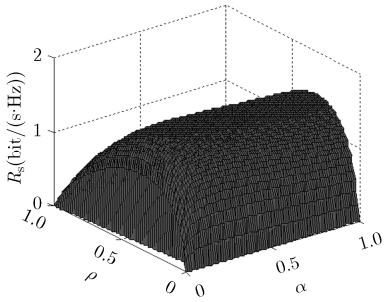


图 2 R_s 和 α,ρ 的关系

4.2 算法的性能

4.2.1 优化方案与其他方案的性能比较 为验证 ρ 值和 α 值优化后性能改善的效果，将 α 和 ρ 同时优化的方案(记为“α^*, ρ^*”)与另外 4 种 α 和 ρ 不同取值方案进行对比：(1) $\alpha=1$，优化 ρ，记为“$\alpha=1, \rho^*$”；(2) $\rho=0.5$，优化 α，记为“$\alpha^*, \rho=0.5$”；(3) $\alpha=1$, $\rho=0.5$；(4) $\alpha=0, \rho=0.5$。3 节点的能量吸收速率相同，从 1 mJ/s 变化到 20 mJ/s。图 3 是随机产生的 50000 组信道系数下保密速率 R_s 的平均值随能量吸收速率 v 变化的情况。对 5 种不同 α 和 ρ 取值方案进行对比。由图可知，本文方案性能最好。由于窃听端在数据传输的两跳中都能接收到传输保密信息的信号，而合法接收者仅能在第 2 跳中接收到保密信号，如果没有人工噪声的干扰，前者对两跳中接收的信号进行合并后的信号信噪比在绝大多数情况下都将高于后者，相应平均保密速率将趋近于零。目的节点不发送人工噪声的方案($\alpha=0$)保密速率的仿真结果趋于 0 表明了这一点，也进一步说明了人工噪声提高保密速率的有效性。$\alpha=1$，优化 ρ 的方案与本文方案性能接近。这是因为干扰功率分配因子 α 与各信道质量有关，在各信道系数为独立同分布的随机变量的仿真条件下，由于窃听者在数据传输的两跳中都能接收到信号，大部分情况下目的节点都需要以最大或接近最大的功率发送干扰，因此 $\alpha=1$，优化 ρ 的方案与本文方案有非常接近的性能。

4.2.2 α^*, ρ^*, R_s 随信道条件的变化情况 本节给出最优干扰功率分配因子 α^*，最优能量吸收时间比例 ρ^* 和保密速率 R_s 随信道系数变化的仿真结果。仿真中，各节点的能量吸收速率为 1 mJ/s。

$|h_{se}|$在 0.2~4 范围内变化，$|h_{sr}|=|h_{de}|=|h_{re}|=1$, $|h_{rd}|=1.5$。仿真结果如图 4 所示。$|h_{se}|$增大时，源节点到窃听节点的传输性能改善。为了抑制窃听节点的接收质量，需要提高人工噪声功率，直至达到上限。ρ^* 递增表明目的节点需要吸收更多的能量用于提高人工噪声的发射功率。从保密速率上看，随着 $|h_{se}|$提高，一方面 α^* 增加以抑制窃听节点的信号接收质量，导致中继转发的信号中信息比重下降，目的节点接收信噪比下降；另一方面，ρ^* 增加导致信息传输时间减少；再一方面，尽管有目的节点的协作干扰，但窃听信道质量改善仍能带来窃听节点接收信噪比改善。综合 3 方面的因素，导致保密速率 R_s 随$|h_{se}|$的增加而减小。

$|h_{re}|$在 0.2~4 范围内变化，$|h_{sr}|=|h_{de}|=1$, $|h_{se}|=0.5$, $|h_{rd}|=1.5$。仿真结果如图 5 所示。$|h_{re}|$增大时，中继节点到窃听节点的传输性能提高。为了抑制窃听节点接收质量的改善，需要提高人工噪声的功率，直至达到上限。而 ρ^* 开始时递增，最后稳定在 0.32 附近，说明人工噪声的功率并不需要随着$|h_{re}|$的增加而持续增加。这是因为中继转发的信号中包含人工噪声，当其功率达到一定程度后，已经能很好地保护转发信号中的保密信息，窃听者的接收信噪比不会随着$|h_{re}|$的提高而有明显的改善，就不需要再增加人工噪声功率，也就不需要分配更多的时间用于能量的吸收。因此，随着$|h_{re}|$提高，开始时保密速率 R_s 下降，随后 R_s 趋近于一个定值，不再明显减小。

$|h_{rd}|$在 0.2~4 范围内变化，$|h_{sr}|=|h_{re}|=|h_{de}|=1$, $|h_{se}|=0.5$。仿真结果如图 6 所示。$|h_{rd}|$增大时带来两方面的好处，一是目的节点发送的人工噪声到达中继节点的损耗减少，能更好地保护中继转发信号中的保密信息；二是目的节点的接收信噪比改善。因此，$|h_{rd}|$增大到一定程度后就不再需要最大功率的人工噪声，且随$|h_{rd}|$的增大而下降，即 α^* 将随$|h_{rd}|$增

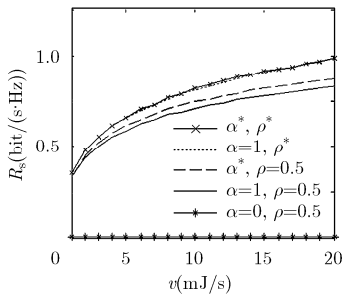


图 3 R_s 平均值随能量吸收速率的变化

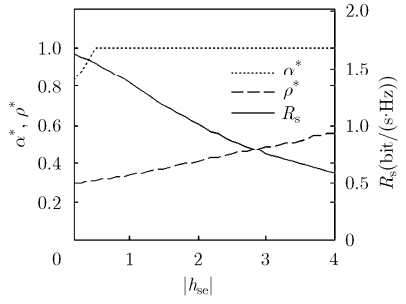


图 4 信道系数$|h_{se}|$的影响

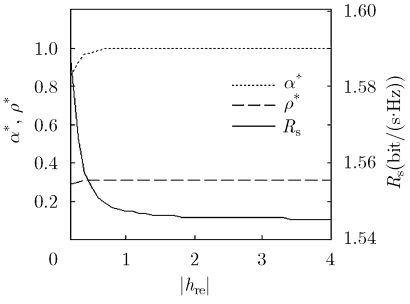


图 5 信道系数$|h_{re}|$的影响

加而下降。相应地，ρ^* 也在递减，可以分配更多的时间用于信息的传输。最终体现在保密速率 R_s 随 $|h_{rd}|$的增加而持续提高。

$|h_{de}|$在 0.2~4 范围内变化，$|h_{sr}|=|h_{re}|=1$, $|h_{se}|=0.5$, $|h_{rd}|=1.5$。仿真结果如图 7 所示。$|h_{de}|$增大时，人工噪声对窃听节点在第 1 跳中接收信号的抑制作用越好。目的节点在$|h_{de}|$增大到一定程度后就不再需要以最大功率发送人工噪声，且随$|h_{de}|$的增大而下降，即 α^* 将随$|h_{de}|$增加而下降。这样中继节点转发信号中的保密信息与人工噪声的功率比也相应提高，目的节点的接收信噪比将得到改善。相应人工噪声功率下降，ρ^* 也在递减，并趋于一个定值，可以分配更多的时间用于信息的传输。最终体现在 R_s 随$|h_{de}|$的增加而持续提高。

4.3 与其他方案性能的比较

为验证本文方案的性能，给出另外两种与本文方案应用场景相同的方案进行比较。对比方案 1：干扰方式与本文方案类似，但人工噪声不是由目的节点发送，而是增加一个由收集的能量供电的单天线协作干扰节点，在数据传输第 1 跳发送人工噪声对窃听节点进行干扰。目的节点已知人工噪声序列，可将其从接收信号中消除。仿真时优化人工噪声功率使保密速率最大。对比方案 2：目的节点不发干扰，增加一个由收集的能量供电的多天线协作干扰节点，在数据传输的两跳中都发干扰。协作干扰节点采用波束赋形技术，在第 1 跳时不对中继造成干扰，在第 2 跳时不对目的节点造成干扰，在此约束条件下优化波束赋形矢量使窃听端接收到的噪声功率最大。根据文献[12]，最优波束赋形矢量为

$$\boldsymbol{w}_i = \sqrt{P_j}\boldsymbol{V}_i\boldsymbol{h}_{je}/\left\|\boldsymbol{V}_i\boldsymbol{h}_{je}\right\|,\quad i\in\{r,d\} \tag{28}$$

其中 $P_j = v_j\rho/(1-\rho)$ 是干扰节点发送功率，$\boldsymbol{w}_r$, $\boldsymbol{w}_d$ 分别第 1 跳和第 2 跳时的波束赋形矢量，$\boldsymbol{V}_i = \boldsymbol{I}_N - \boldsymbol{h}_{ji}\left(\boldsymbol{h}_{ji}^H\boldsymbol{h}_{ji}\right)^{-1}\boldsymbol{h}_{ji}^H$, $i\in\{r,d\}$, $\boldsymbol{V}_r$, $\boldsymbol{V}_d$ 分别为 $\boldsymbol{h}_{jr}$, $\boldsymbol{h}_{jd}$ 的零空间上的投影矩阵，$\boldsymbol{I}_N$ 为 $N\times N$ 的单位矩阵。

图 8 是 3 种方案的保密速率的仿真结果，为随机产生的 50000 组信道系数下得到的保密速率的平均值。仿真中，各节点能量吸收速率相同，从 1 mJ/s 变化到 20 mJ/s；对比方案 2 中干扰的天线节点数 N 为 3 和 4。从仿真结果中可以看到，本文方案与对比方案 1 的性能相近，本文方案稍好。但注意到对比方案 1 需要在协作干扰节点与目的节点间实现人工噪声序列的同步，同时还需要将干扰节点与中继节点间的信道系数传输给目的节点，目的节点才能将人工噪声从接收到的信号中消除。因此，对比方案 1 的实现复杂度要高于本文方案。对比方案 2 性能优于本文方案，这是由于对比方案 2 中采用了多天线的协作干扰节点，可对人工噪声进行波束赋形，获得阵列增益，提高了窃听节点处的干扰信号功率。天线数越多，阵列增益越大，性能越好。但波束赋形方案需要在节点配备多天线时才能使用。

5 总结

本文对由单天线节点组成的无线中继系统的物理层安全问题进行研究，其中节点具有能量收集能力。系统中，中继采用 AF 模式，而窃听端与源和中继节点间都存在直接链路。为保护两跳传输中的保密信息，目的端发送人工噪声进行协作干扰。各节点采用“储能—发送”工作模式，每个传输时隙分为能量收集与数据传输两个阶段，数据传输阶段中各节点利用收集的能量发送信号。与其他类似文献相比，本文模型考虑了窃听端与源和中继节点间都有直接链路的场景，模型更为合理。由于同时考虑了两跳传输中信息的保密，以及能量收集的约束，所以本文方案要解决的优化问题更为复杂。以最大化保密速率为目标，本文对两个阶段的时间分配比例 ρ 和目的端协作干扰功率分配因子 α 进行了优化，采用迭代方法得到 ρ 和 α 的联合优化结果。算法性能的仿真结果表明该迭代算法的收敛性好，优化结果准确，保密速率获得了明显的改善。

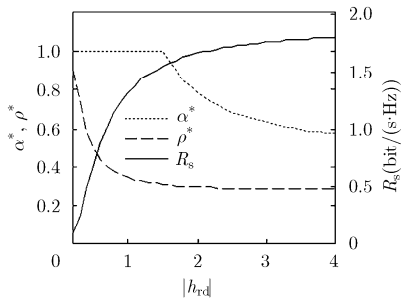


图 6 信道系数$|h_{rd}|$的影响

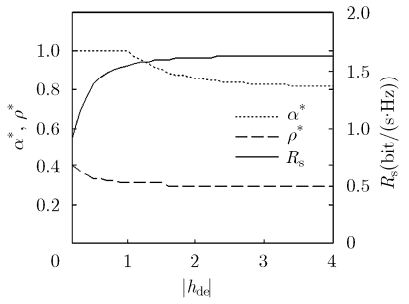


图 7 信道系数$|h_{de}|$的影响

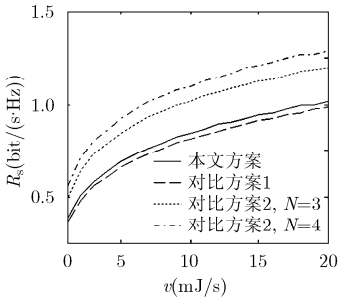


图 8　3 种方案性能比较

参 考 文 献

[1] MUKHERJEE A, FAKOORIAN S, HUANG J, *et al*. Principles of physical layer security in multiuser wireless networks: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2014, 16(3): 1550–1573. doi: 10.1109/SURV.2014.012314.00178.

[2] BASSILY R, EKREM E, HE X, *et al*. Cooperative security at the physical layer: A summary of recent advances[J]. *IEEE Signal Processing Magazine*, 2013, 30(5): 16–28. doi: 10.1109/MSP.2013.2260875.

[3] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189. doi: 10.1109/TWC.2008.060848.

[4] HAN B, LI J, SU J S, *et al*. Secrecy capacity optimization via cooperative relaying and jamming for WANETs[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(4): 1117–1128. doi: 10.1109/TPDS.2014.2316155.

[5] PARK K H, WANG T, and ALOUINI M S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1741–1750. doi: 10.1109/JSAC.2013.130908.

[6] HAGGSTROM F, GUSTAFSSON J, and DELSING J. Energy harvesting technologies for wireless sensors in rotating environments[C]. IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, 2014: 1–4. doi: 10.1109/ETFA.2014.7005364.

[7] VALENTA C R and DURGIN G D. Harvesting wireless power: survey of energy-harvester conversion efficiency in far-field, wireless power transfer Systems[J]. *IEEE Microwave Magezine*, 2014, 15(4): 108–120. doi: 10.1109/MMM.2014.2309499.

[8] LI Q, MA W K, and SO A M C. Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting[C]. IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP), Florence, 2014: 1596–1600. doi: 10.1109/ICASSP.2014.6853867.

[9] 谢国芳. 一般实系数四次方程的求根公式[OL]. http://wenku.baidu.com/link?url=D8kKnPDyfVfUbp7FlkM6PV484bd_ikEPvZnHkgwquiqapU4rlbgxUzsF1M9ck3puagGemFeQAn3A8Du_up4cvW0bRQQkRXj5jHhwrSrrdi_, 2013.

XIE G F. The general formula of real coefficient equations four[OL]. http://wenku.baidu.com/link?url=D8kKnPDyfVfUbp7FlkM6PV484bd_ikEPvZnHkgwquiqapU4rlbgxUzsF1M9ck3puagGEmFeQAn3A8Du_up4cvW0bRQQkRXj5jHhwrSrrdi_, 2013.

[10] LEONARD E D. Introduction to the Theory of Algebraic Equations[M]. New York: Rough Draft Printing, 1988: 67–72.

[11] 范盛金. 一元三次方程的新求根公式与新判别式[J]. 海南师范学院学报(自然科学版), 1989, 2(2): 91–98.

FAN S J. A new extracting formula and a new distinguishing means on the one variable cubic equation[J]. *Journal of Hainan Normal University* (*Natural Science*), 1989, 2(2): 91–98.

[12] ZHU F, GAO F, ZHANG T, *et al*. Physical-layer security for full-duplex communications with self-interference mitigation [J]. *IEEE Transactions on Wireless Communications*, 2016, 15(1): 329–340. doi: 10.1109/TWC.2015.2472527.

雷维嘉： 男，1969 年生，博士，教授，主要研究方向为无线通信和移动通信技术.

杨小燕： 女，1990 年生，硕士生，研究方向为无线通信和物理层安全.