放大转发中继网络中绿色的物理层安全通信技术

王 东[①②③] 李永成[①] 白 铂[*②] 王满喜[①]
[①](电子信息系统复杂电磁环境效应国家重点实验室 洛阳 471003)
[②](清华大学电子工程系 北京 100084)
[③](新星技术研究所 合肥 230031)

摘 要：该文基于物理层安全理论，针对能量受限的无线中继网络提出一种绿色的保密通信方案。该方案在节点功率约束和系统最小目标保密速率要求下，通过最优功率控制实现系统的安全能效最大化，并基于分式规划、对偶分解和 DC(Difference of Convex functions)规划理论提出了一种迭代的功率分配算法。通过仿真比较，能效优化可以显著提升系统的安全能效，然而相对于保密速率最大化会有一定保密速率损失，这是由于能效和保密之间存在固有的折中。但是，能效优化的保密速率仍然大于发送总功率最小化的保密速率。

关键词：信息安全；能量效率；物理层安全；功率分配；放大转发中继
中图分类号： TN918.91 **文献标识码**： A **文章编号**：1009-5896(2016)04-0841-07
DOI: 10.11999/JEIT150695

Green Communications Based on Physical-layer Security for Amplify-and-forward Relay Networks

WANG Dong[①②③] LI Yongcheng[①] BAI Bo[②] WANG Manxi[①]
[①](*State Key Laboratory of Complex Electromagnetic Environmental Effects on Electronics and Information System*, *Luoyang* 471003, *China*)
[②](*Department of Electronic Engineering*, *Tsinghua University*, *Beijing* 100084, *China*)
[③](*New Star Research Institute of Applied Technology*, *Hefei* 230031, *China*)

Abstract: In this paper, a green communication scheme based on physical layer security is addressed considering the energy and secrecy constraints. This scheme maximizes the secure Energy Efficiency (EE) of the network by power allocation subject to the maximum power constraint of each node and the target secrecy rate constraint of the network. Furthermore, an iterative algorithm for power allocation is developed based on fractional programming, dual decomposition, and Difference of Convex functions (DC) programming. It is verified by simulations that the proposed algorithm can lead to a significant gain of secure EE yet with some loss of secrecy rate compared with secrecy rate maximization. This is because that there is an inherent tradeoff between EE and secrecy. However, the achievable secrecy rate of the proposed scheme is still superior over that of total transmission power minimization.

Key words: Information security; Energy efficiency; Physical-layer security; Power allocation; Amplify-and-forward relaying

1 引言

为了满足各种不同的应用业务和通信需求，移动互联网必须支持平滑的 IP 接入和完整的互连互通，以适应各种异构网络相互融合的发展趋势。网络的高度融合发展，必然带来严峻的信息安全问题。目前的信息安全技术主要分为传统的加密技术和物理层安全技术。传统的加密技术以密码学为基础，对密钥的管理和分发要求极高。然而，在一些分布式无线网络中，譬如移动 Ad hoc 网络，中心节点的缺乏和网络拓扑的动态变化，使得密钥的管理和分发非常困难[1]。物理层安全利用无线信道固有的随机性和信道之间的衰落差异实现保密通信，故不存在密钥管理问题。作为上层加密技术的补充，物理层安全技术可以进一步提高网络的安全性。然而，和一般的没有安全要求的通信系统一样，物理层安全通信也会受到通信节点的最大功率和能量的限制[2,3]。因此，绿色的物理层安全通信技术非常值得关注[4]。

收稿日期：2015-06-08；改回日期：2015-12-25；网络出版：2016-02-26
*通信作者：白铂 eebobai@tsinghua.edu.cn
基金项目：CEMEE 国家重点实验室开放课题基金(CEMEE2015K0204B)
Foundation Item: The Open Project Foundation of CEMEE State Key Laboratory (CEMEE2015K0204B)

在目前的物理层安全文献中，从能量的角度来看，主要是以有限的功率传输尽可能多的保密数据，即保密速率最大化；或是在保证基本的保密速率要求下尽可能地节省功率，即发送总功率最小化[5,6]。然而，从能量效率的角度来看，这两种系统优化都不能达到最优能效。为了衡量系统资源的有效利用，文献[7]提出了单位成本的保密容量的概念，研究了高成本效率的保密通信问题。根据文献[7]，绿色通信中的能量效率概念可以扩展到物理层安全，即安全能效，其定义为消耗单位能量所能传输的保密信息量。文献[8]在考虑信息安全的基础上，着重研究了正交频分多址系统的高能效资源分配问题。文献[9]基于物理层安全理论，研究了物理层能量和保密的折中问题。然而，这些文献只研究了特定场景中的能效问题，并且只考虑了点对点的直接传输系统，没有考虑分布式协作中继网络。

所以，本文主要研究存在窃听者的放大转发(Amplify-and-Forward, AF)中继网络中的绿色物理层安全通信技术：即在节点最大功率限制和系统最小保密速率要求下，通过自适应功率控制最大化系统的安全能效，达到以有限的能量传输更多的保密数据。该问题的数学形式可划归为分数形式的非凸优化问题。本文运用分式规划、对偶分解，以及 DC (Difference of Convex functions)规划理论，将原始优化问题逐层转化和分解，转变成一系列相对较容易的凸的子问题进行迭代求解，并提出了一种迭代的求解算法。数值仿真表明，相比于最大化保密速率和最小化发送总功率，本文提出的安全能效最大化算法能大大提高系统能效。

2 系统模型与问题建模

2.1 AF 中继模型

如图 1 所示，源节点要传输保密数据给目的节点，由于受到障碍物遮挡，需寻求 M 个中继节点进行信息转发。中继节点采用 AF 中继方式，这种中继方式只是将接收到的信号放大后转发给目的节点，因此实现复杂度比较低。另外，即使源节点到中继节点的信道条件较差，由于中继节点不需要解码，故而 AF 中继方式依然能够起到协作传输的作用。在实际通信过程中，为了降低协作传输的复杂度，放大转发是比较合适的选择。在该系统中存在一个非法用户，试图窃听保密数据。假设窃听者不便于靠近源节点，比如不知道源节点具体位置或者源节点处于移动中。为了达到更好的窃听效果，窃听者努力使自己和目的节点处于同一区域。为了降低被窃听到的概率，在传输的第 1 时隙源节点以很低的固定功率广播保密信息，只使中继节点能够接收到。这样，源节点和目的节点以及窃听者之间没有直达链路。

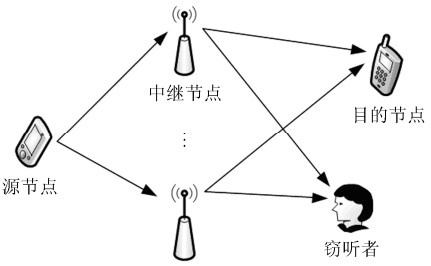

图 1 存在窃听者的 AF 中继网络模型

假设所有节点都是单天线的，以半双工模式工作。所有信道是相互独立的准静态平坦瑞利衰落信道[10]。另外，假设发送端知道精确的信道状态信息。在有些实际场景中，精确的信道状态信息是可以获得的，比如窃听者在网络中是活动的，其信息传输可被监听到，如在联合的多播和单播传输网络中[11]，用户可能具有双重角色，对一些信号是合法用户而对另一些信号可能就是窃听者[12]。还比如窃听者也是网络的合法用户，只是它和目的节点的通信业务不同[5]。对于私密业务来说目的节点以外的用户应该当做窃听者。对于这种情况，窃听者可以说是一种半信任的用户，即就是在服务级是可以相信的，而在数据级是不可以相信的[13]。服务级可信意味着这种所谓的半信任用户愿意反馈精确的信道状态信息给发送端，而数据级不可信意味着源节点的私密消息必须对目的节点以外的其他用户保密。

信息传输分为两个时隙[14]：在第 1 时隙，源节点广播信号；在第 2 时隙，各个中继节点在相互正交的子信道上转发信号[15]。第 1 时隙源节点的广播带宽和第 2 时隙每个中继节点的子信道带宽相同并归一化。源节点到中继节点的信道增益用 a_j 表示，$j=1,2,\cdots,M$。另外，用 h_j 和 g_j 分别表示从第 j 个中继节点到目的节点和窃听者的信道增益。在第 1 时隙，源节点以固定功率 p_{s} 广播编码符号 s ($\mathbb{E}\{|s|^2\}=1$)，则中继节点的接收信号为[16]

$$x_j=\sqrt{p_{\mathrm{s}}}a_j s+z_{\mathrm{r}_j} \tag{1}$$

其中，z_{r_j} 表示中继节点的加性白高斯噪声，其均值为零，方差为 σ^2。在第 2 时隙，中继节点以功率 p_{r_j} 转发收到的信号。中继节点的增益可表示为

$$\rho_j=\sqrt{\frac{p_{\mathrm{r}_j}}{|x_j|^2}}=\sqrt{\frac{p_{\mathrm{r}_j}}{p_{\mathrm{s}}|a_j|^2+\sigma^2}} \tag{2}$$

这样，目的节点和窃听者接收到的第 j 个中继节点转发的信号分别表示为

$$y_{\mathrm{d}_j}=h_j\rho_j x_j+z_{\mathrm{d}_j}=\sqrt{p_{\mathrm{s}}}\rho_j h_j a_j s+\rho_j h_j z_{\mathrm{r}_j}+z_{\mathrm{d}_j} \tag{3}$$

$$y_{\mathrm{e}_j}=g_j\rho_j x_j+z_{\mathrm{e}_j}=\sqrt{p_{\mathrm{s}}}\rho_j g_j a_j s+\rho_j g_j z_{\mathrm{r}_j}+z_{\mathrm{e}_j} \tag{4}$$

其中，z_{d_j} 和 z_{e_j} 分别表示信道 h_j 和 g_j 上的均值为零、方差为 σ^2 的加性白高斯噪声。由式(2)和式(3)可得信道 h_j 上的信噪比为

$$\gamma_{\mathrm{d}_j}=\frac{\alpha_{\mathrm{r}_j}\beta_{\mathrm{d}_j}p_{\mathrm{s}}p_{\mathrm{r}_j}}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{d}_j}p_{\mathrm{r}_j}} \tag{5}$$

其中，$\alpha_{\mathrm{r}_j}=|a_j|^2/\sigma^2$，$\beta_{\mathrm{d}_j}=|h_j|^2/\sigma^2$。同样地，信道 g_j 上的信噪比为

$$\gamma_{\mathrm{e}_j}=\frac{\alpha_{\mathrm{r}_j}\beta_{\mathrm{e}_j}p_{\mathrm{s}}p_{\mathrm{r}_j}}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{e}_j}p_{\mathrm{r}_j}} \tag{6}$$

其中，$\beta_{\mathrm{e}_j}=|g_j|^2/\sigma^2$。假设目的节点和窃听者采用最大比合并，可得到它们的接收速率分别为

$$R_{\mathrm{d}}=\frac{1}{2}\log_2\left(1+\sum_{j=1}^{M}\gamma_{\mathrm{d}_j}\right) \tag{7}$$

$$R_{\mathrm{e}}=\frac{1}{2}\log_2\left(1+\sum_{j=1}^{M}\gamma_{\mathrm{e}_j}\right) \tag{8}$$

这里假定一次完整的信息传输耗费单位时间。系数 1/2 是因为每一阶段的传输时间是总时间的一半。因此，系统的保密速率定义为[5]

$$R_{\mathrm{s}}=\left[R_{\mathrm{d}}-R_{\mathrm{e}}\right]^{+} \tag{9}$$

其中，$[x]^{+}$ 表示 $\max\{0,x\}$。

2.2 功率消耗模型

每一节点消耗的功率包括功放的功率和其他电路单元的基础功耗，比如混频器、滤波器、A/D 或 D/A 转换器等。源节点在第 1 时隙广播信号而在第 2 时隙静默，故源节点的能量消耗可表示为

$$E_{\mathrm{s}}=\frac{1}{2}\left(\frac{p_{\mathrm{s}}}{\eta}+p_{\mathrm{c_s}}\right) \tag{10}$$

其中，$p_{\mathrm{c_s}}$ 是源节点的电路基础功耗，η 表示功率放大器的效率系数。注意，p_{s} 是源节点的发送功率，即功放输出功率，而功放消耗的功率应该是 p_{s}/η，中继节点类似。对于中继节点，在第 1 时隙处于接收状态，仅在第 2 时隙放大转发信号，故其能量消耗可以表示为

$$E_{\mathrm{r}}=\frac{1}{2}\sum_{j=1}^{M}\frac{p_{\mathrm{r}_j}}{\eta}+Mp_{\mathrm{c_r}} \tag{11}$$

其中，$p_{\mathrm{c_r}}$ 表示中继节点的电路基础功耗。另外，目的节点接收信号也要消耗功率，记为 $p_{\mathrm{c_d}}$。所以，系统的整体功耗为

$$\begin{aligned}P_{\mathrm{sum}}&=E_{\mathrm{s}}+E_{\mathrm{r}}\\&=\frac{1}{2\eta}\left(p_{\mathrm{s}}+\sum_{j=1}^{M}p_{\mathrm{r}_j}\right)+\frac{1}{2}p_{\mathrm{c_s}}+\frac{1}{2}p_{\mathrm{c_d}}+Mp_{\mathrm{c_r}}\end{aligned} \tag{12}$$

2.3 问题建模

为了衡量物理层安全通信的能量利用情况，定义系统的安全能效指标为单位能量传输的保密比特量，即就是系统的保密速率与总功率的比值。系统的安全能效函数为

$$\begin{aligned}\mu(\boldsymbol{p})=\frac{R_{\mathrm{s}}(\boldsymbol{p})}{P_{\mathrm{sum}}(\boldsymbol{p})}=&\left[\log_2\left(1+\sum_{j=1}^{M}\frac{\alpha_{\mathrm{r}_j}\beta_{\mathrm{d}_j}p_{\mathrm{s}}p_{\mathrm{r}_j}}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{d}_j}p_{\mathrm{r}_j}}\right)\right.\\&\left.-\log_2\left(1+\sum_{j=1}^{M}\frac{\alpha_{\mathrm{r}_j}\beta_{\mathrm{e}_j}p_{\mathrm{s}}p_{\mathrm{r}_j}}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{e}_j}p_{\mathrm{r}_j}}\right)\right]^{+}\\&\Bigg/\left[\frac{1}{\eta}\left(p_{\mathrm{s}}+\sum_{j=1}^{M}p_{\mathrm{r}_j}\right)+p_{\mathrm{c_s}}+p_{\mathrm{c_d}}+2Mp_{\mathrm{c_r}}\right]\end{aligned} \tag{13}$$

其中，$\boldsymbol{p}\triangleq\left[p_{\mathrm{r}_1},p_{\mathrm{r}_2},\cdots,p_{\mathrm{r}_M}\right]$。

我们的目的是以有限的能量尽可能地传输更多的数据量，所以单位能量传输的数据量应该最大，即安全能效最大化，同时应该考虑系统的最低保密速率要求。该问题可以建模成如式(14)形式。

$$\begin{aligned}&\max\ \mu(\boldsymbol{p})\\&\text{s.t.}\quad\begin{cases}0\le p_{\mathrm{r}_j}\le P_{\mathrm{r}_j}^{0},\quad j=1,2,\cdots,M\\R_{\mathrm{s}}(\boldsymbol{p})\ge r_0\end{cases}\end{aligned} \tag{14}$$

其中，$P_{\mathrm{r}_j}^{0}$ 表示第 j 个中继节点的最大功率约束，r_0 表示系统的最小目标保密速率要求。约束 $R_{\mathrm{s}}(\boldsymbol{p})\ge r_0$ 可以保证系统在能效最大化时不至于保密速率太低。另外，如果最小保密速率要求不能满足，表明系统当前不能进行保密通信，所以发送功率、保密速率和安全能效都应置为零。

3　迭代的安全能效优化算法

在问题式(14)中，由于目标函数是分数形式，保密速率是两个对数函数相减，这些特征导致该优化问题是非凸的，直接求解比较困难。为了有效求解该问题，我们基于分式规划、对偶分解、DC 规划等优化方法，将原始问题逐层转化为一系列较简单的子问题进行求解，并提出了一种迭代的优化算法。

3.1 基于分式规划的目标函数转化

能效函数具有分数形式，故问题式(14)可以划归为分式规划。用 μ^{*} 和 $\boldsymbol{p}^{*}$ 分别表示该问题的最大能效和最优的功率分配。为了方便描述，问题式(14)的可行域记为

$$\mathcal{D}=\left\{R_{\mathrm{s}}(\boldsymbol{p})\ge r_0,0\le p_{\mathrm{r}_j}\le P_{\mathrm{r}_j}^{0},j=1,2,\cdots,M\right\} \tag{15}$$

与问题式(14)相对应的参数规划定义为

$$\max_{\boldsymbol{p}\in\mathcal{D}}\left\{R_{\mathrm{s}}(\boldsymbol{p})-\mu P_{\mathrm{sum}}(\boldsymbol{p})\right\} \tag{16}$$

根据分式规划理论[8,17]，当式(17)条件成立时，问题

式(14)达到最优的 μ^* 和 $\boldsymbol{p}^*$：

$$\max_{\boldsymbol{p}\in\mathcal{D}}\left\{R_{\mathrm{s}}(\boldsymbol{p})-\mu^* P_{\mathrm{sum}}(\boldsymbol{p})\right\} = R_{\mathrm{s}}\left(\boldsymbol{p}^*\right)-\mu^* P_{\mathrm{sum}}\left(\boldsymbol{p}^*\right)=0 \tag{17}$$

式(17)中的参数规划可根据 Dinkelbach 方法求解：给定参数 μ 的一个合适的初始值 μ_0，问题式(16)的最优解可以通过迭代地求解式(18)的子问题而得到：

$$\max_{\boldsymbol{p}\in\mathcal{D}}\left\{R_{\mathrm{s}}(\boldsymbol{p})-\mu_i P_{\mathrm{sum}}(\boldsymbol{p})\right\} \tag{18}$$

其中，μ_i 表示第 $i-1$ 次迭代得到的安全能效，并被用于第 i 次迭代。问题式(18)的最优解用 $\boldsymbol{p}^*(\mu_i)$ 表示。迭代终止条件为

$$\left|R_{\mathrm{s}}\left(\boldsymbol{p}^*(\mu_i)\right)-\mu_i P_{\mathrm{sum}}\left(\boldsymbol{p}^*(\mu_i)\right)\right|\le\tau \tag{19}$$

其中，τ 是分式规划的收敛精度。在第 i 次迭代，如果式(19)成立则迭代停止，否则 μ_i 应被更新为

$$\mu_{i+1}=\frac{R_{\mathrm{s}}\left(\boldsymbol{p}^*(\mu_i)\right)}{P_{\mathrm{sum}}\left(\boldsymbol{p}^*(\mu_i)\right)} \tag{20}$$

这时算法进入下一次迭代。由上可见，分式规划并不要求原始问题是严格凸的，并且可以得到问题的最优解。另外，分式规划算法是单调收敛的，严格的收敛性证明可参考文献[8]和文献[17]。

3.2 基于对偶理论的非凸约束消除

在 3.1 节中，原始问题转化为参数规划，并通过迭代求解子问题式(18)而得到最优解。然而，由于非凸约束 $R_{\mathrm{s}}(\boldsymbol{p})\ge r_0$ 的存在，问题式(18)依然求解困难。为了把可行域转化成凸集，我们基于对偶理论把非凸约束合并到目标函数里。

根据对偶理论，构造 Lagrange 函数如式(21)：

$$L(\lambda,\boldsymbol{p})=R_{\mathrm{s}}(\boldsymbol{p})-\mu_i P_{\mathrm{sum}}(\boldsymbol{p})+\lambda\left(R_{\mathrm{s}}(\boldsymbol{p})-r_0\right) \tag{21}$$

其中，λ 表示 Lagrange 乘子。这样，问题式(18)的对偶问题表示为

$$\min_{\lambda\ge0}\max_{\boldsymbol{p}\in\mathcal{D}}L(\lambda,\boldsymbol{p}) \tag{22}$$

其中，可行域 $\overline{\mathcal{D}}=\left\{0\le p_{\mathrm{r}_j}\le P_{\mathrm{r}_j}^0, j=1,2,\cdots,M\right\}$ 是一个凸集。

根据文献[18]，对偶问题式(22)可以分成两层子问题求解。内层子问题是给定 λ 时的关于功率的最大化问题，即

$$\max_{\boldsymbol{p}\in\overline{\mathcal{D}}}L(\lambda_n,\boldsymbol{p}) \tag{23}$$

其中，λ_n 表示 λ 的一个给定值。用 $\boldsymbol{p}^*(\lambda_n)$ 表示问题式(23)的最优解，则外层子问题是在已知 $\boldsymbol{p}^*(\lambda_n)$ 时的关于对偶变量 λ 的最小化问题：

$$\min_{\lambda\ge0}L\left(\lambda,\boldsymbol{p}^*(\lambda_n)\right) \tag{24}$$

对于外层子问题式(24)，可以用梯度下降法求解。对偶变量更新函数为

$$\lambda_{n+1}=\max\left\{0,\lambda_n-\nu_n\zeta\right\} \tag{25}$$

其中，$\zeta=R_{\mathrm{s}}(\boldsymbol{p}^*(\lambda_n))-r_0$ 是函数 $L(\lambda,\boldsymbol{p}^*(\lambda_n))$ 关于 λ 的梯度，ν_n 表示第 n 次迭代的步长。每一次迭代得到的对偶变量都会用于求解内层子问题式(23)。在外层子问题的求解过程中，当给定收敛精度 $\delta>0$，梯度下降法的终止条件可定义为 $|\lambda_n-\lambda_{n-1}|\le\delta$。

3.3 基于 DC 规划的内层子问题求解

在 3.2 节中，外层子问题式(24)可以采用梯度下降法求解，而内层子问题式(23)由于目标函数依然是非凸的，直接求解还是比较困难。在本小节，我们采用 DC 规划的思想来求解问题式(23)，其核心思想是通过迭代求解该问题的一系列凸的近似问题来逐步逼近该问题的最优解。

问题式(23)等价于 $\min_{\boldsymbol{p}\in\overline{\mathcal{D}}}\{-L(\lambda_n,\boldsymbol{p})\}$，其目标函数可以分解为

$$-L(\lambda_n,\boldsymbol{p})=L_1(\boldsymbol{p})-L_2(\boldsymbol{p}) \tag{26}$$

其中，$L_1(\boldsymbol{p})$ 和 $L_2(\boldsymbol{p})$ 分别为

$$L_1(\boldsymbol{p})=\mu_i P_{\mathrm{sum}}(\boldsymbol{p})+\lambda_n r_0-\left(\lambda_n+1\right)R_{\mathrm{d}}(\boldsymbol{p}) \tag{27}$$

$$L_2(\boldsymbol{p})=-\left(\lambda_n+1\right)R_{\mathrm{e}}(\boldsymbol{p}) \tag{28}$$

根据定理 1 可知 $L_1(\boldsymbol{p})$ 和 $L_2(\boldsymbol{p})$ 都是凸函数。

定理 1 函数 $L_1(\boldsymbol{p})$ 和 $L_2(\boldsymbol{p})$ 关于 $\boldsymbol{p}$ 都是凸函数。

证明 在函数 $L_1(\boldsymbol{p})$ 中，$R_{\mathrm{d}}(\boldsymbol{p})$ 可以展开写成式(29)的形式：

$$R_{\mathrm{d}}(\boldsymbol{p})=\log_2\left(1+\sum_{j=1}^{M}\left(\alpha_{\mathrm{r}_j}p_{\mathrm{s}}-\frac{\alpha_{\mathrm{r}_j}p_{\mathrm{s}}\left(1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}\right)}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{d}_j}p_{\mathrm{r}_j}}\right)\right) \tag{29}$$

由于 $\alpha_{\mathrm{r}_j}p_{\mathrm{s}}-\dfrac{\alpha_{\mathrm{r}_j}p_{\mathrm{s}}\left(1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}\right)}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{d}_j}p_{\mathrm{r}_j}}$ 关于 p_{r_j} 是凹函数，故其非负加权和也是凹函数。所以，$R_{\mathrm{d}}(\boldsymbol{p})$ 关于 $\boldsymbol{p}$ 也是凹函数，故 $-R_{\mathrm{d}}(\boldsymbol{p})$ 是凸函数。$P_{\mathrm{sum}}(\boldsymbol{p})$ 关于 $\boldsymbol{p}$ 是仿射函数。所以，$L_1(\boldsymbol{p})$ 是凸函数的非负加权和，故是凸函数。同样地，可以证明 $L_2(\boldsymbol{p})$ 关于 $\boldsymbol{p}$ 也是凸函数。

证毕

定理 1 表明式(26)是一个 DC 函数，即两个凸函数相减。因此，根据 DC 规划理论[19,20]，问题 $\min_{\boldsymbol{p}\in\overline{\mathcal{D}}}\{-L(\lambda_n,\boldsymbol{p})\}$ 的最优解可以通过迭代地求解如式(30)所示的凸的子问题进行逼近：

$$\min_{\boldsymbol{p}\in\overline{\mathcal{D}}}\left\{f(\boldsymbol{p})\triangleq L_1(\boldsymbol{p})-L_2\left(\boldsymbol{p}_k\right)-\left\langle\nabla L_2\left(\boldsymbol{p}_k\right),\boldsymbol{p}-\boldsymbol{p}_k\right\rangle\right\} \tag{30}$$

其中，$\boldsymbol{p}_k$ 表示 DC 规划第 $k-1$ 次迭代得到的解，被应用于第 k 次迭代。$\nabla L_2\left(\boldsymbol{p}_k\right)$ 表示函数 $L_2(\boldsymbol{p})$ 在 $\boldsymbol{p}_k$ 的梯度。由式(8)和式(28)，可以得到 $\nabla L_2\left(\boldsymbol{p}\right)$ 为

$$\nabla L_2(\boldsymbol{p})=\left(\frac{\partial L_2}{\partial p_{\mathrm{r}_1}},\frac{\partial L_2}{\partial p_{\mathrm{r}_2}},\cdots,\frac{\partial L_2}{\partial p_{\mathrm{r}_M}}\right) \tag{31}$$

其中，$\dfrac{\partial L_2}{\partial p_{\mathrm{r}_j}}$，$j=1,2,\cdots,M$，表示为

$$\frac{\partial L_2}{\partial p_{\mathrm{r}_j}}=\frac{-\dfrac{1}{\ln 2}\alpha_{\mathrm{r}_j}\beta_{\mathrm{e}_j}p_{\mathrm{s}}(\lambda_n+1)\left(1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}\right)}{\left(1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{e}_j}p_{\mathrm{r}_j}\right)^2\left(1+\sum\limits_{j=1}^{M}\dfrac{\alpha_{\mathrm{r}_j}\beta_{\mathrm{e}_j}p_{\mathrm{s}}p_{\mathrm{r}_j}}{1+\alpha_{\mathrm{r}_j}p_{\mathrm{s}}+\beta_{\mathrm{e}_j}p_{\mathrm{r}_j}}\right)} \tag{32}$$

事实上，DC 规划通过反复迭代求解问题式(30)来逼近问题 $\min\limits_{\boldsymbol{p}\in\mathcal{D}}\{-L(\lambda_n,\boldsymbol{p})\}$ 的最优解[19]。当给定收敛精度 $\epsilon>0$，这个迭代过程会终止于 $|-L(\lambda_n,\boldsymbol{p}_k)+L(\lambda_n,\boldsymbol{p}_{k-1})|\le\epsilon$，这时会得到一个单调递减序列 $\{L_1(\boldsymbol{p}_k)-L_2(\boldsymbol{p}_k)\}$，如定理 2 所述。

定理 2　序列 $\{L_1(\boldsymbol{p}_k)-L_2(\boldsymbol{p}_k)\}$ 是单调递减的。

证明　根据函数 $L_2(\boldsymbol{p})$ 的凸性，$\forall\boldsymbol{p}_k,\boldsymbol{p}_{k+1}\in\overline{\mathcal{D}}$，可以得到

$$L_2(\boldsymbol{p}_{k+1})\ge L_2(\boldsymbol{p}_k)+\langle\nabla L_2(\boldsymbol{p}_k),\boldsymbol{p}_{k+1}-\boldsymbol{p}_k\rangle \tag{33}$$

在 DC 规划的第 k 次迭代，我们知道 $\boldsymbol{p}_{k+1}$ 是问题式(30)的最优解，而 $\boldsymbol{p}_k$ 仅是其一个可行解，故可得

$$L_1(\boldsymbol{p}_k)-L_2(\boldsymbol{p}_k)\ge L_1(\boldsymbol{p}_{k+1})-L_2(\boldsymbol{p}_k)-\langle\nabla L_2(\boldsymbol{p}_k),\boldsymbol{p}_{k+1}-\boldsymbol{p}_k\rangle \tag{34}$$

联合上面两个不等式，则有

$$L_1(\boldsymbol{p}_k)-L_2(\boldsymbol{p}_k)\ge L_1(\boldsymbol{p}_{k+1})-L_2(\boldsymbol{p}_{k+1}) \tag{35}$$

由式(35)可见，$\{L_1(\boldsymbol{p}_k)-L_2(\boldsymbol{p}_k)\}$ 是递减的。　证毕

3.4 算法总结

为了便于深入理解问题求解过程，算法 1(表 1)总结了本文算法的运行步骤。原始问题式(14)基于分式规划被转化成关于 μ 的参数规划式(16)，并通过迭代方法求进行求解。在求解参数规划的每一次迭代过程中，运用前一次迭代得到的 μ 的值，求解一个参数化的二次问题式(18)。接着，通过对偶理论，该参数化的二次问题被分解为两层子问题进行交替求解：内层子问题式(23)是已知对偶变量的功率优化，而外层子问题式(24)是已知功率的对偶变量优化。外层子问题通过梯度下降法求解。对于内层子问题，运用 DC 规划，通过求解该问题的一系列凸近似问题式(30)来逼近其最优解。算法 1 包括 3 层循环：最内层是 DC 规划求解问题式(23)。中间层是梯度下降法，运用内层得到的功率求解问题式(24)。最外层是分式规划，求解的是原始问题对应的参数规划问题式(16)。

根据上述讨论，算法 1 将原问题逐层转化为一系列凸的子问题式(30)进行迭代求解。所以，算法 1 的复杂度很大程度上取决于凸问题的求解复杂度。本文采用文献[21]提出的快速梯度法求解问题式(30)。这里定义 $\theta\ge 0$ 为一个 Lipschitz 常数，使得问题式(30)的目标函数 f 的梯度 ∇f 满足 Lipschitz 条件。另外，ρ 表示使得 f 满足强凸性的一个凸性参数。这样，由文献[21]可得快速梯度法在给定收敛精度 ξ 时的迭代次数为 $O(1)\min\left\{\sqrt{\dfrac{\theta}{\rho}}\ln\left(\dfrac{1}{\xi}\right),\sqrt{\dfrac{\theta}{\xi}}\right\}$。算法 1 包括 3 层循环，当各层的收敛精度 ϵ，δ，τ 达到时对应的循环次数分别为 N_ϵ，N_δ，N_τ。这时算法 1 总的计算复杂度可粗略表示为

$$O(1)\min\left\{\sqrt{\frac{\theta}{\rho}}\ln\left(\frac{1}{\xi}\right),\sqrt{\frac{\theta}{\xi}}\right\}N_\epsilon N_\delta N_\tau \tag{36}$$

表 1 安全能效最大化算法

算法 1：安全能效最大化算法

输入：a_j, h_j, g_j；

输出：$\boldsymbol{p}^*$, μ^*；

给定初始值 μ_0, $i:=0$；

Repeat

　给定初始值 λ_0, $n:=0$；

　Repeat

　　给定起始点 $\boldsymbol{p}_0$，计算 $-L(\lambda_n,\boldsymbol{p}_0)$, $k:=0$

　　Repeat

　　对既定的 $\boldsymbol{p}_k$，求解问题式(30)得到 $\boldsymbol{p}_{k+1}$；

　　计算 $-L(\lambda_n,\boldsymbol{p}_{k+1})$, $k:=k+1$；

　　Until $\left|-L(\lambda_n,\boldsymbol{p}_k)+L(\lambda_n,\boldsymbol{p}_{k-1})\right|\le\epsilon$；

　　$\boldsymbol{p}^*(\lambda_n):=\boldsymbol{p}_k$；

　　搜索最佳步长 ν_n，计算 λ_{n+1}，$n:=n+1$；

　Until $|\lambda_n-\lambda_{n-1}|\le\delta$

　$\boldsymbol{p}^*(\mu_i):=\boldsymbol{p}^*(\lambda_n)$；

　计算 μ_{i+1}, $i:=i+1$；

Until $\left|R_{\mathrm{s}}(\boldsymbol{p}^*(\mu_{i-1}))-\mu_{i-1}P_{\mathrm{sum}}(\boldsymbol{p}^*(\mu_{i-1}))\right|\le\tau$；

Return $\mu^*=\mu_{i-1}$, $\boldsymbol{p}^*=\boldsymbol{p}^*(\mu_{i-1})$。

4　数值仿真

本小节通过仿真来验证算法的性能。我们比较了本文提出的安全能效最大化、保密速率最大化和发送总功率最小化等 3 种方案。在仿真中，各节点配置如图 2 所示，中继节点对称地分布于源和目的节点的连线上，窃听者非常接近于该直线移动。在仿真中，为了简单，忽略了窃听者到源和目的节点连线的距离，但并不意味着目的节点会和窃听者处于同一位置。用 d_{sr}，d_{sd}，d_{se} 分别表示源节点到中继节点、目的节点、窃听者的距离，用 d_{rd}，d_{re} 分别表示中继节点到目的节点和窃听者的距离。仿真参数

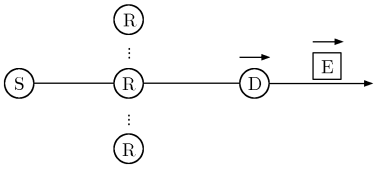

图 2 仿真节点配置示意图

设置如下： $M=5$ ， $P_{\mathrm{r}_j}^0=500$ mW， $\sigma^2=-100$ dBm/Hz， $r_0=1$ bit/(s·Hz)， $\eta=0.4$ ；路径损耗指数设为 3.5； p_{s} ， $p_{\mathrm{c_s}}$ ， $p_{\mathrm{c_r}}$ 和 $p_{\mathrm{c_d}}$ 都设为 10 mW。我们进行 1000 次蒙特卡洛仿真求取平均值。

首先，图 3 比较了当窃听者处于不同位置时 3 种方案的平均安全能效。设置 $d_{\mathrm{sr}}=200$ m， $d_{\mathrm{sd}}=700$ m； d_{se} 从 400 m 向 1000 m 变化。由图 3 可见，本文的安全能效最大值算法达到的平均安全能效明显优于保密速率最大化和发送总功率最小化的平均安全能效。当窃听者离源和中继节点越来越远时，合法信道相对于窃听信道越来越强，故安全能效最大化和保密速率最大化的平均能效曲线是递增的。然而，发送总功率最小化方案的平均能效曲线波动很小，这是由于该方案给中继节点分配的功率刚好达到最小目标保密速率要求。

采用和图 3 相同的仿真设置，图 4 比较了窃听者位置变化时 3 种方案的平均保密速率。对比图 3 和图 4 可见，相对于保密速率最大化，本文的安全能效优化会有一定的保密速率损失，这是因为安全能效和保密速率之间存在固有的折中。但是安全能效优化所能达到的保密速率依然远大于发送总功率最小化所达到的保密速率。我们知道，在不考虑安全约束的常规通信中，能效和数据速率之间存在固有的折中。类似的折中也存在于物理层安全中。由于安全能效是保密速率和发送总功率的比值，为了达到最大的安全能效，可能需要以相对较小的功率发送数据，这时达到的保密速率可能也会较小。从另一方面来说，为了达到更大的保密速率，必然需要消耗更高的功率，这可能会使二者的比值(即安全能效)降低。也就是说，与最大化保密速率相比，最大化安全能效会以“牺牲”一定的保密速率为代价。但是，本文提出的安全能效优化设计方案引入了保密速率约束，这使得本文提出的方案可以在保证信息保密传输速率的前提下，达到最佳的能量效率，即最佳的能效和保密性的折中。

在图 5 中，我们设置 $d_{\mathrm{sr}}=200$ m， $d_{\mathrm{se}}=700$ m； d_{sd} 从 400 m 向 1000 m 变化。由该图可见，和另外两个方案相比，本文的安全能效最大化可以产生明显的能效增益。当目的节点距离源和中继节点越来越远时，3 种方案的平均安全能效逐渐递减，这是因为合法信道相对于窃听信道变得越来越弱。与图 5 仿真设置一样，图 6 比较了目的节点位置变化时 3 种方案达到的保密速率。图 5 和图 6 对照起来看，由于安全能效和保密速率之间的固有折中，安全能效优化虽然有一定的保密速率损失，但其达到的平均保密速率仍然大于发送总功率最小化达到的平均保密速率，也要远大于系统要求的最小目标保密速率。

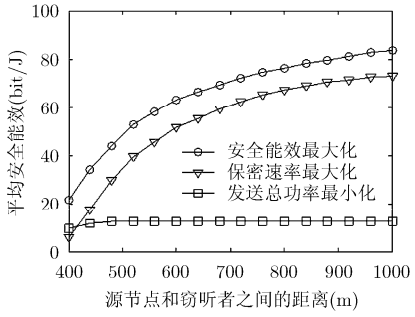

图 3 窃听者处于不同位置时的平均安全能效

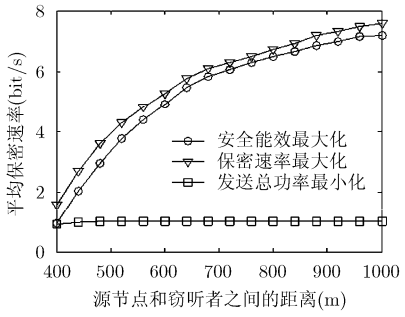

图 4 窃听者处于不同位置时的平均保密速率

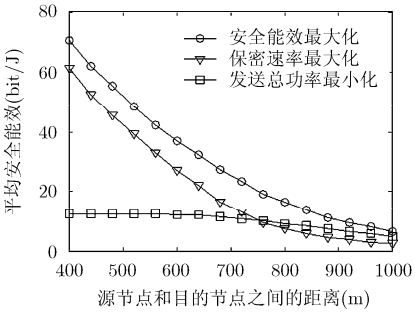

图 5 目的节点处于不同位置时的平均安全能效

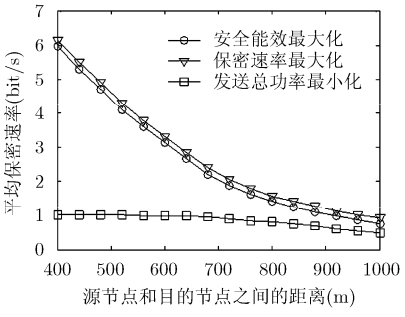

图 6 目的节点处于不同位置时的平均保密速率

5　结论

本文针对能量受限的 AF 中继网络中的信息安全问题，提出了一种高能效的物理层安全传输方案。该方案通过最优功率控制，在满足功率和保密速率约束条件下，实现系统的安全能效最大化。本文提出的功率分配算法以分式规划、对偶分解和 DC 规划为理论基础，将原始优化问题分层转化为更简单的一系列子问题，从而便于迭代求解。数值仿真表明，本文算法可以带来显著的能效增益。

参 考 文 献

[1] 黄开枝, 洪颖, 罗文宇, 等. 基于演化博弈机制的物理层安全协作方法[J]. 电子与信息学报, 2015, 37(1): 193–199. doi: 10.11999/JEIT140309.
HUANG Kaizhi, HONG Ying, LUO Wenyu, *et al*. A method for physical layer security cooperation based on evolutionary game[J]. *Journal of Electronics & Information Technology*, 2015, 37(1): 193–199. doi: 10.11999/JEIT140309.

[2] LIU J, DAI H, and CHEN W. Delay optimal scheduling for energy harvesting based communications[J]. *IEEE Journal on Selected Areas in Communications*, 2015, 33(3): 452–466. doi: 10.1109/JSAC.2015.2391972.

[3] CHEN W, DAI L, LETAIEF K B, *et al*. A unified cross-layer framework for resource allocation in cooperative networks[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(8): 3000–3012. doi: 10.1109/TWC. 2008.060831.

[4] 黄高勇, 方旭明, 陈煜. 基于速率约束的 OFDM 中继链路能效最优资源分配策略[J]. 电子与信息学报, 2014, 36(9): 2104–2110. doi: 10.3724/SP.J.1146.2013.01661.
HUANG Gaoyong, FANG Xuming, and CHEN Yu. Resource allocation for energy efficiency maximization based on rate constrains in OFDM DF relay link[J]. *Journal of Electronics & Information Technology*, 2014, 36(9): 2104–2110. doi: 10.3724/SP.J.1146.2013.01661.

[5] LI J, PETROPULU A P, and WEBER S. On cooperative relaying schemes for wireless physical layer security[J]. *IEEE Transaction on Signal Processing*, 2011, 59(10): 4985–4996. doi: 10.1109/TSP.2011.2159598.

[6] DEHGHAN M, GOECKEL D L, GHADERI M, *et al*. Energy efficiency of cooperative jamming strategies in secure wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(9): 3025–3029. doi: 10.1109/TWC.2012.070912.110789.

[7] EL-HALABI M, LIU T, and GEORGHIADES C N. Secrecy capacity per unit cost[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1909–1920. doi: 10.1109/JSAC.2013.130922.

[8] NG D W K, LO E S, and SCHOBER R. Energy-efficient resource allocation for secure OFDMA systems[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(6): 2572–2585. doi: 10.1109/TVT.2012.2199145.

[9] COMANICIU C, POOR H V, and ZHANG R. An information theoretic framework for energy efficient secrecy [C]. IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, British Columbia, Canada, 2013: 2906–2910.

[10] CHEN W. CAO-SIR: Channel aware ordered successive relaying[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(12): 6513–6527. doi: 10.1109/TWC.2014.2363453.

[11] LIU J, CHEN W, ZHANG Y, *et al*. A utility maximization framework for fair and efficient multicasting in multicarrier wireless cellular networks[J]. *IEEE/ACM Transactions on Networking*, 2013, 21(1): 110–120. doi: 10.1109/TNET.2012.2192747.

[12] EKREM E and ULUKUS S. Capacity-equivocation region of the Gaussian MIMO wiretap channel[J]. *IEEE Transactions on Information Theory*, 2012, 58(9): 5699–5710. doi: 10.1109/TIT.2012.2204534.

[13] KHODAKARAMI H and LAHOUTI F. Link adaptation with untrusted relay assignment: design and performance analysis[J]. *IEEE Transactions on Communications*, 2013, 61(12): 4874–4883. doi: 10.1109/TCOMM.2013.111513.120888.

[14] LIU J, CHEN W, CAO Z, *et al*. Cooperative beamforming for cognitive radio networks: A cross-layer design[J]. *IEEE Transactions on Communications*, 2012, 60(5): 1420–1431. doi: 10.1109/TCOMM.2012.031712.100284A.

[15] CHEN W, LETAIEF K B, and CAO Z. Buffer-aware network coding for wireless networks[J]. *IEEE/ACM Transactions on Networking*, 2012, 20(5): 1389–1401. doi: 10.1109/TNET.2011.2176958.

[16] LIU J, CHEN W, CAO Z, *et al*. Delay optimal scheduling for cognitive radios with cooperative beamforming: A structured matrix-geometric method[J]. *IEEE Transactions on Mobile Computing*, 2012, 11(8): 1412–1423. doi: 10.1109/TMC.2011.153.

[17] DINKELBACH W. On nonlinear fractional programming[J]. *Management Science*, 1967, 13(7): 492–498.

[18] PALOMAR D P and CHIANG M. A tutorial on decomposition methods for network utility maximization[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(8): 1439–1451. doi: 10.1109/JSAC.2006.879350.

[19] AN L T H and TAO P D. The DC (difference of convex functions) programming and DCA revisited with DC models of real world nonconvex optimization problems[J]. *Annals of Operations Research*, 2005, 133(1/4): 23–46.

[20] NGO D T, KHAKUREL S, and LE-NGOC T. Joint subchannel assignment and power allocation for OFDMA femtocell networks[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(1): 342–355. doi: 10.1109/TWC.2013.111313.130645.

[21] RICHTER S, JONES C, and MORARI M. Computational complexity certification for real-time MPC with input constraints based on the fast gradient method[J]. *IEEE Transactions on Automatic Control*, 2012, 57(6): 1391–1403. doi: 10.1109/TAC.2011.2176389.

王　东：男，1980 年生，博士生，研究方向为协同通信、信息安全.

李永成：男，1978 年生，工程师，硕士，研究方向为复杂电磁环境效应.

白　铂：男，1982 年生，讲师、硕士生导师，研究方向为无线通信、物理层安全、组合优化.

王满喜：男，1979 年生，助理研究员，研究方向为无线通信与信道建模、复杂电磁环境效应.