doi:10.11959/j.issn.1000-436x.2017011

解码转发协作通信网中能效最优的物理层安全传输机制研究

王东[1,2,3,4]，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，河南 洛阳 471003；2. 清华大学电子工程系，北京 100084；
3. 新星技术研究所，安徽 合肥 230031；4. 北京邮电大学网络与交换技术国家重点实验室，北京 100876)

摘 要：针对物理层安全信息传输过程中的功率和能量制约，研究解码转发中继网络中的能量高效利用问题，基于分式规划和 DC(difference of convex functions)规划理论，提出一种迭代的发送功率分配算法。该算法在满足节点峰值功率约束和系统最小保密速率要求下，联合进行源和中继的功率分配，实现高能效的物理层安全传输。仿真结果表明，与传统的最大化保密速率相比，该安全能效最大化算法能显著提高系统的能量利用效率。

关键词：能量效率；功率分配；物理层安全；中继网络

中图分类号：TN918.91 **文献标识码**：A

Research on energy-efficient physical-layer secure transmission mechanism in decode-and-forward cooperative networks

WANG Dong[1,2,3,4], LI Yong-cheng[1], BAI Bo[2], WANG Man-xi[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;
4. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The maximization problem of secure energy efficiency (EE) in decode-and-forward relay networks was investigated considering the power and energy constraints in physical-layer secure transmission. An iterative algorithm for power allocation was proposed based on fractional programming and DC (difference of convex functions) programming. This algorithm jointly allocated power for source and relay nodes to achieve energy-efficient secure transmission, subject to the peak power constraint of each node and the minimum secrecy rate requirement of the system. Simulation results demonstrate that the propose algorithm can improve the secure EE significantly compared with the conventional secrecy rate maximization strategy.

Key words: energy efficiency, power allocation, physical layer security, relay networks

1 引言

随着通信技术的发展和业务需求的变化，各种分布式协作网络和异构网络都将融入移动互联网。这使网络节点变得复杂多样，信息安全显得尤为重要。如何保证信息安全可靠传输而不被窃听，成为非常值得关注的问题[1]。传统的以密码学为基础的信息安全技术主要应用于物理层以上层次，以计算量为代价，需要高性能的硬件支持。物理层安全是一种信息论意义上的安全理论，主要是利用物理层信道的随机性以及合法信道和窃听信道之间的差异实现信息安全传输，具有复杂度低、计算量小、信道适应性好等特点[2]。然而，在物理层实现安全通信常常受限于实际的物理资源，如通信设备的峰值功率和能量供应等。因此，如何在保证信息安全的同时，提高系统的能量利用率成为一个非常值得研究的问题。

为了实现物理层安全通信，大量的文献主要是

收稿日期：2016-05-20；**修回日期**：2016-11-21

基金项目：CEMEE 国家重点实验室开放课题基金资助项目（No.CEMEE2015K0204B）

Foundation Item: The Open Project Foundation of CEMEE State Key Laboratory (No.CEMEE2015K0204B)

在有限的功率约束下最大化系统的保密速率[3~5]。类似地，文献[6]致力于提高 MIMO 中继网络的传输有效性和可靠性；文献[7]提出了联合源和中继的波束成形策略来最大化系统的保密速率；文献[8]探讨了噪声辅助预编码、目的节点协作干扰、特征波束成形等物理层安全传输方案可以达到的遍历保密速率。然而，从能量利用效率的角度来看，这些研究工作并不能保证能效最优。因此，一些研究者开始关注物理层安全的能效问题。文献[9]以单位保密比特的最小能耗为指标，研究低信噪比情况下的安全通信问题；文献[10]从信息论的角度揭示了保密性能和能量消耗之间的折中问题；文献[11]研究了典型的点对点窃听模型的安全能效问题，没有考虑中继协作传输。文献[12]重点考虑了放大转发中继网络的安全能效最大化问题。这里，安全能效定义为单位能量消耗所能传输的保密数据量，即保密速率与总功率的比值。

根据上述讨论，本文以安全能效为优化指标，研究在受到窃听威胁的解码转发(DF, decode-and-forward)中继网络中的高能效物理层安全传输技术，通过源和中继节点联合的功率分配实现安全能效最大化(SEEM, secure energy efficiency maximization)，同时满足每个通信节点的峰值功率约束和中继节点的最小解码速率要求。该问题是一个分数形式的非凸优化。本文基于分式规划和 DC 规划理论，把原始问题逐步转化为相对容易的一系列子问题进行逐层求解，并针对该问题提出一种嵌套迭代的优化算法。仿真结果表明，与传统的保密速率最大化(SRM, secrecy rate maximization)相比，本文提出的安全能效最大化算法能显著提高系统的能量利用效率。

2 系统模型与问题建模

2.1 DF 中继窃听模型

考虑如图 1 所示的 DF 中继窃听模型，包括一个源节点、一个目的节点、一个中继节点和一个窃听者。源节点在中继节点的帮助下向目的节点发送保密数据。本文考虑译码转发方式中的选择译码转发[13]。假设每个节点都是半双工的，且只有一个天线。由于窃听者的存在，数据传输过程可能会被窃听。由于能量限制和信息安全要求，系统设计应综合考虑能效性和安全性。

假设所有信道是统计独立的准静态平坦瑞利衰落信道。源节点到中继节点、目的节点和窃听者的信道增益分别用 h_{sr}、h_{sd} 和 g_{se} 表示。中继节点到目的节点和窃听者的信道增益分别用 h_{rd} 和 g_{re} 表示。假设发射机已知所有信道精确的信道状态信息(CSI, channel state information)。在一些实际场景中，精确的 CSI 是可以获得的。如文献[3]提到多用户进行联合的多播和单播传输，这时每个用户的角色是双重的，对一些信号来说，该用户是合法用户，而对另一些信号来说，该用户就是窃听者，但是从网络的角度，这些用户都是合法的，都能够将自己的 CSI 反馈给发送端。文献[14]也提到，有些所谓的窃听者也是网络内的合法用户，只是它和目的节点的通信业务不同。对于私密业务，目的节点以外的用户都应该当作窃听者。对于这种情况，窃听者可以说是一种半信任的用户，即在服务级是可以相信的，而在数据级是不可以相信的。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 CSI 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。

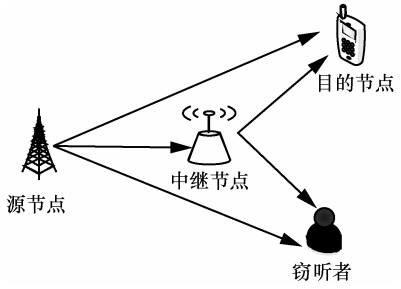


图 1 DF 中继窃听模型

在第 1 阶段，源节点广播保密符号 x ($\mathbb{E}\{|x|^2\}=1$)。中继节点、目的节点和窃听者都可能接收到该信号。源节点的发送功率 p_{s} 必须确保中继节点能够正确解码。第 1 阶段中继节点、目的节点和窃听者的接收信号分别表示为

$$y_{\mathrm{r}}=\sqrt{p_{\mathrm{s}}}h_{\mathrm{sr}}x+z_{\mathrm{r}} \tag{1}$$

$$y_{\mathrm{d}}^{(1)}=\sqrt{p_{\mathrm{s}}}h_{\mathrm{sd}}x+z_{\mathrm{d}} \tag{2}$$

$$y_{\mathrm{e}}^{(1)}=\sqrt{p_{\mathrm{s}}}g_{\mathrm{se}}x+z_{\mathrm{e}} \tag{3}$$

其中，z_{r}、z_{d}、z_{e} 分别是中继节点、目的节点、窃听者的信道加性高斯白噪声，它们具有相同的分布 $\mathcal{CN}(0,\sigma_z^2)$。

在第 2 阶段，中继节点对接收到的信号解码后

重新编码，再转发出去。假设中继节点使用与源节点相同的码字，并以功率 p_{r} 发送。第 2 阶段目的节点和窃听者的接收信号分别表示为

$$y_{\mathrm{d}}^{(2)}=\sqrt{p_{\mathrm{r}}}h_{\mathrm{rd}}x+z_{\mathrm{d}} \tag{4}$$

$$y_{\mathrm{e}}^{(2)}=\sqrt{p_{\mathrm{r}}}g_{\mathrm{re}}x+z_{\mathrm{e}} \tag{5}$$

这样，中继节点、目的节点和窃听者的接收速率可以表示为

$$R_{\mathrm{r}}=\frac{1}{2}\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}\left|h_{\mathrm{sr}}\right|^2}{\sigma_{\mathrm{z}}^2}\right) \tag{6}$$

$$R_{\mathrm{d}}=\frac{1}{2}\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}\left|h_{\mathrm{sd}}\right|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}\left|h_{\mathrm{rd}}\right|^2}{\sigma_{\mathrm{z}}^2}\right) \tag{7}$$

$$R_{\mathrm{e}}=\frac{1}{2}\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}\left|g_{\mathrm{se}}\right|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}\left|g_{\mathrm{re}}\right|^2}{\sigma_{\mathrm{z}}^2}\right) \tag{8}$$

假设目的节点和窃听者都使用最大比合并进行信号接收。上面 3 个式子中的系数 $\frac{1}{2}$ 表示完整的信息传输经历了 2 个阶段。这样，系统的保密速率可以表示为[15]

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

其中，$[x]^{+}$ 表示 $\max\{x,0\}$。

在一次完整的传输过程中，总的功率消耗应是 2 个传输阶段消耗功率之和。每一个阶段消耗的功率包括功率放大器消耗的功率和发送接收电路消耗的功率[16,17]。假设一次完整的传输过程耗费 1 个单位时间。在第 1 阶段，源节点广播信号，同时中继节点保持接收。所以，第 1 阶段消耗的能量应为

$$E^{(1)}=\frac{1}{2}\left(\frac{p_{\mathrm{s}}}{\eta}+p_{c_{\mathrm{s}}}^{\mathrm{transmit}}+p_{c_{\mathrm{r}}}^{\mathrm{receive}}+p_{c_{\mathrm{d}}}^{\mathrm{receive}}\right) \tag{10}$$

其中，$p_{c_{\mathrm{s}}}^{\mathrm{transmit}}$、$p_{c_{\mathrm{r}}}^{\mathrm{receive}}$ 和 $p_{c_{\mathrm{d}}}^{\mathrm{receive}}$ 分别是源节点发送电路消耗的功率、中继节点接收电路消耗的功率以及目的节点接收电路消耗的功率。这些基础电路功耗主要由混频器、滤波器、A/D 或 D/A 转换器和计算单元等电路模块产生，一般在系统优化时当作常值对待的[16,17]。η 表示功率放大器的效率系数。在第 2 阶段，中继节点转发重新编码后的符号，这时源节点保持静默。因此，第 2 阶段消耗的能量为

$$E^{(2)}=\frac{1}{2}\left(\frac{p_{\mathrm{r}}}{\eta}+p_{c_{\mathrm{r}}}^{\mathrm{transmit}}+p_{c_{\mathrm{d}}}^{\mathrm{receive}}\right) \tag{11}$$

其中，$p_{c_r}^{\mathrm{transmit}}$ 表示中继节点发送电路消耗的功率。上面 2 个式子中系数 $\frac{1}{2}$ 表示每个传输阶段耗费时间是总时间的一半。所以，一次完整传输消耗的总功率为

$$\begin{aligned}P_{\mathrm{tot}}&=E^{(1)}+E^{(2)}\\&=\frac{1}{2}\left(\frac{p_{\mathrm{s}}+p_{\mathrm{r}}}{\eta}+p_{c_{\mathrm{s}}}^{\mathrm{transmit}}+p_{c_{\mathrm{r}}}^{\mathrm{receive}}+p_{c_{\mathrm{r}}}^{\mathrm{transmit}}+2p_{c_{\mathrm{d}}}^{\mathrm{receive}}\right)\end{aligned} \tag{12}$$

定义安全能效为消耗单位能量传输的保密数据量，即是保密速率与总功率的比值，表达式为

$$\begin{aligned}\xi(p_{\mathrm{s}},p_{\mathrm{r}})&=\frac{R_{\mathrm{sec}}}{P_{\mathrm{tot}}}\\&=\frac{1}{\frac{p_{\mathrm{s}}+p_{\mathrm{r}}}{\eta}}\left[\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}\left|h_{\mathrm{sd}}\right|^2}{\sigma_z^2}+\frac{p_{\mathrm{r}}\left|h_{\mathrm{rd}}\right|^2}{\sigma_z^2}\right)-\right.\\&\quad\left.\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}\left|g_{\mathrm{se}}\right|^2}{\sigma_z^2}+\frac{p_{\mathrm{r}}\left|g_{\mathrm{re}}\right|^2}{\sigma_z^2}\right)\right]^{+}+\\&\quad p_{c_{\mathrm{s}}}^{\mathrm{transmit}}+p_{c_{\mathrm{r}}}^{\mathrm{receive}}+p_{c_{\mathrm{r}}}^{\mathrm{transmit}}+2p_{c_{\mathrm{d}}}^{\mathrm{receive}}\end{aligned} \tag{13}$$

2.2　问题建模

在实际的中继网络中，安全的信息传输常常受到功率以及能量的限制。所以，本文目的是在满足每个发送节点峰值功率约束和中继解码速率要求下，最大化 DF 中继网络的安全能效，尽可能提高系统的能量利用效率。该问题的数学表示为

$$\begin{aligned}&\max_{p_{\mathrm{s}},p_{\mathrm{r}}}\xi(p_{\mathrm{s}},p_{\mathrm{r}})\\&\text{s.t.}\begin{cases}0\leqslant p_{\mathrm{s}}\leqslant p_{\mathrm{s}}^{\max}\\0\leqslant p_{\mathrm{r}}\leqslant p_{\mathrm{r}}^{\max}\\R_{\mathrm{r}}\geqslant R_0\end{cases}\end{aligned} \tag{14}$$

在式(14)中，由于每个发送节点都有自己的峰值功率，故在问题建模时考虑单个节点的功率约束，其中，$p_{\mathrm{s}}^{\max}$ 和 $p_{\mathrm{r}}^{\max}$ 分别表示源节点和中继节点的最大允许功率。R_0 为中继节点进行解码的最小速率要求。约束条件 $R_{\mathrm{r}}\geqslant R_0$ 确保中继节点能够满足解码要求[13]。

3　SEEM 算法

式(14)的目标函数是非凸的分数形式，所以该

优化问题可以划归为非凸优化，求解比较困难。为了求解该问题，本节基于分式规划和 DC 规划，提出一种嵌套的迭代算法。该算法包括 2 层迭代过程，即基于分式规划的外层迭代过程和基于 DC 规划的内层迭代过程。

3.1 基于分式规划的问题转化

在第 1 个传输阶段，源节点的发送功率必须确保中继节点能够正确解码。所以中继节点的接收速率应该满足 $R_{\mathrm{r}} \geqslant R_0$。由式(6)可得

$$p_{\mathrm{s}} \geqslant \frac{\left(2^{2R_0}-1\right)\sigma_z^2}{|h_{\mathrm{sr}}|^2} \tag{15}$$

因此，式(14)的可行域可以写为

$$\mathcal{S}=\left\{\frac{\left(2^{2R_0}-1\right)\sigma_z^2}{|h_{\mathrm{sr}}|^2} \leqslant p_{\mathrm{s}} \leqslant p_{\mathrm{s}}^{\max}, 0 \leqslant p_{\mathrm{r}} \leqslant p_{\mathrm{r}}^{\max}\right\} \tag{16}$$

式(14)的目标函数是分数形式，可以转换成参数规划的形式，这样就可以根据分式规划理论进行求解[18,19]。问题转化过程描述如下所示。

形如 $\max\left\{\frac{R(\boldsymbol{x})}{P(\boldsymbol{x})}: \boldsymbol{x}\in\mathcal{S}\right\}$ 的优化问题称为分式规划，可以对应的参数规划为

$$\max\left\{R(\boldsymbol{x})-\xi P(\boldsymbol{x}): \boldsymbol{x}\in\mathcal{S}\right\}, \xi\in\mathbb{R} \tag{17}$$

其中，$\mathcal{S}$ 是非空的紧集，$R(\boldsymbol{x})$ 和 $P(\boldsymbol{x})$ 是连续函数且 $P(\boldsymbol{x})>0$。该分式规划的最大值是能够达到的，即

$$\xi^*=\frac{R(\boldsymbol{x}^*)}{P(\boldsymbol{x}^*)}=\max\left\{\frac{R(\boldsymbol{x})}{P(\boldsymbol{x})}: \boldsymbol{x}\in\mathcal{S}\right\} \tag{18}$$

当且仅当最大值 ξ^* 和最佳解 $\boldsymbol{x}^*$ 满足

$$\max\left\{R(\boldsymbol{x})-\xi^* P(\boldsymbol{x}): \boldsymbol{x}\in\mathcal{S}\right\}=0 \tag{19}$$

根据上述分式规划，式(14)可以重新等价描述为：找到最大能效 ξ^* 和最佳功率 $\boldsymbol{p}^*$ 满足

$$\max\left\{F(\xi,\boldsymbol{p})=R_{\mathrm{sec}}(\boldsymbol{p})-\xi^* P_{\mathrm{tot}}(\boldsymbol{p}): \boldsymbol{p}\in\mathcal{S}\right\}=0 \tag{20}$$

其中，$\boldsymbol{p}\triangleq(p_{\mathrm{s}}, p_{\mathrm{r}})$。在式(20)中，最大化问题 $\max\left\{F(\xi,\boldsymbol{p})=R_{\mathrm{sec}}(\boldsymbol{p})-\xi P_{\mathrm{tot}}(\boldsymbol{p}): \boldsymbol{p}\in\mathcal{S}\right\}$ 是关于 ξ 的参数规划。当给定 ξ 的初始值 ξ_0 时，该最大化问题可以通过迭代求解下面参数化的二次问题进行求解

$$\max\left\{F(\xi_i,\boldsymbol{p})=R_{\mathrm{sec}}(\boldsymbol{p})-\xi_i P_{\mathrm{tot}}(\boldsymbol{p}): \boldsymbol{p}\in\mathcal{S}\right\} \tag{21}$$

其中，i 是分式规划的迭代次数，ξ_i 表示第 i 次迭代得到的安全能效，$\boldsymbol{p}^*(\xi_i)$ 表示在给定 ξ_i 时求解式(21)得到的功率。在每一次迭代后 ξ_i 应该被更新为

$$\xi_{i+1}=\frac{R_{\mathrm{sec}}\left(\boldsymbol{p}^*(\xi_i)\right)}{P_{\mathrm{tot}}\left(\boldsymbol{p}^*(\xi_i)\right)} \tag{22}$$

实际上，式(14)是通过迭代求解参数化的二次问题式(21)而求解的。给定初始值 $\xi_0<\xi^*$，通过反复迭代，可以得到一个单调递增的序列 $\{\xi_i\}$。该序列至少是线性收敛的，当 $\xi_0<\xi^*$ 时，该序列是超线性收敛的。序列 $\{\xi_i\}$ 的递增性和收敛性证明可以参考文献[18]。当给定收敛精度 $\varepsilon>0$ 时，该迭代过程终止于 $\left|F\left(\xi_i,\boldsymbol{p}^*(\xi_i)\right)\right|\leqslant\varepsilon$。

3.2 给定 ξ_i 的内层子问题求解

在 3.1 节中，根据分式规划，原始问题可以转化为一系列参数化的二次问题，通过反复迭代进行求解。但是转化后的式(21)依然是非凸的。为了能够运用 DC 规划理论进行求解，还需对式(21)进行转化。首先，DC 规划简要描述如下所示[20,21]。

若函数 $B(\boldsymbol{x})$ 和 $D(\boldsymbol{x})$ 在凸集 $\mathcal{S}$ 上是可微的连续凸函数，则 $\min\left\{F(\boldsymbol{x})=B(\boldsymbol{x})-D(\boldsymbol{x}): \boldsymbol{x}\in\mathcal{S}\right\}$ 称作 DC 规划，可以通过下面凸的子问题迭代求解

$$\min\{B(\boldsymbol{x})-D(\boldsymbol{x}_k)-\langle\nabla D(\boldsymbol{x}_k), \boldsymbol{x}-\boldsymbol{x}_k\rangle: \boldsymbol{x}\in\mathcal{S}\} \tag{23}$$

其中，$\nabla D(\boldsymbol{x}_k)$ 是 $D(\boldsymbol{x})$ 在 $\boldsymbol{x}_k$ 的梯度，$\langle\nabla D(\boldsymbol{x}_k), \boldsymbol{x}-\boldsymbol{x}_k\rangle$ 表示 $\nabla D(\boldsymbol{x}_k)$ 和 $\boldsymbol{x}-\boldsymbol{x}_k$ 的内积。

在式(21)中 ξ_i 是给定的，该问题可以等价地写成如下最小化问题

$$\min\left\{-F(\xi_i,\boldsymbol{p})=-R_{\mathrm{sec}}(\boldsymbol{p})+\xi_i P_{\mathrm{tot}}(\boldsymbol{p}): \boldsymbol{p}\in\mathcal{S}\right\} \tag{24}$$

其目标函数可以分解为

$$-F(\xi_i,\boldsymbol{p})=B(\boldsymbol{p})-D(\boldsymbol{p}) \tag{25}$$

其中，$B(\boldsymbol{p})$ 和 $D(\boldsymbol{p})$ 分别为

$$B(\boldsymbol{p})=\xi_i\left(\frac{p_{\mathrm{s}}+p_{\mathrm{r}}}{\eta}+p_{c_{\mathrm{s}}}^{\mathrm{transmit}}+p_{c_{\mathrm{r}}}^{\mathrm{receive}}+p_{c_{\mathrm{r}}}^{\mathrm{transmit}}\right)-\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}|h_{\mathrm{sd}}|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}|h_{\mathrm{rd}}|^2}{\sigma_{\mathrm{z}}^2}\right) \tag{26}$$

$$D(\boldsymbol{p})=-\mathrm{lb}\left(1+\frac{p_{\mathrm{s}}|g_{\mathrm{se}}|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}|g_{\mathrm{re}}|^2}{\sigma_{\mathrm{z}}^2}\right) \tag{27}$$

由式(26)、式(27)可以看出，$B(\boldsymbol{p})$ 和 $D(\boldsymbol{p})$ 关于 p_{s}、p_{r} 都是凸函数，$\mathcal{S}$ 是凸集。因此，式(24)是标准的 DC 规划，其解可以通过迭代求解下面凸的子问题得

$$\min\{f(\boldsymbol{p})=B(\boldsymbol{p})-D(\boldsymbol{p}_k)-\langle\nabla D(\boldsymbol{p}_k),\boldsymbol{p}-\boldsymbol{p}_k\rangle:\boldsymbol{p}\in\mathcal{S}\} \tag{28}$$

其中，k 是 DC 规划的迭代次数，$\boldsymbol{p}_k$ 是在第 k 次迭代时式(28)的最佳解，被用来进行第 $k+1$ 次迭代。梯度 $\nabla D(\boldsymbol{p})$ 表示为

$$\nabla D(\boldsymbol{p})=\left\{\frac{-\frac{|g_{\mathrm{se}}|^2}{\sigma_{\mathrm{z}}^2\ln 2}}{1+\frac{p_{\mathrm{s}}|g_{\mathrm{se}}|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}|g_{\mathrm{se}}|^2}{\sigma_{\mathrm{z}}^2}},\frac{-\frac{|g_{\mathrm{re}}|^2}{\sigma_{\mathrm{z}}^2\ln 2}}{1+\frac{p_{\mathrm{s}}|g_{\mathrm{se}}|^2}{\sigma_{\mathrm{z}}^2}+\frac{p_{\mathrm{r}}|g_{\mathrm{re}}|^2}{\sigma_{\mathrm{z}}^2}}\right\} \tag{29}$$

因为 $D(\boldsymbol{p})$ 是凸函数，$\forall\boldsymbol{p}\in\mathcal{S}$，可得

$$D(\boldsymbol{p})\geqslant D(\boldsymbol{p}_k)+\langle\nabla D(\boldsymbol{p}_k),\boldsymbol{p}-\boldsymbol{p}_k\rangle \tag{30}$$

所以，对于 $\boldsymbol{p}_{k+1}\in\mathcal{S}$ 可得

$$D(\boldsymbol{p}_{k+1})\geqslant D(\boldsymbol{p}_k)+\langle\nabla D(\boldsymbol{p}_k),\boldsymbol{p}_{k+1}-\boldsymbol{p}_k\rangle \tag{31}$$

由于 $\boldsymbol{p}_{k+1}$ 是式(28)的最佳解，而 $\boldsymbol{p}_k$ 只是其可行解，故

$$\begin{aligned}&B(\boldsymbol{p}_{k+1})-D(\boldsymbol{p}_{k+1})\\&\leqslant B(\boldsymbol{p}_{k+1})-D(\boldsymbol{p}_k)-\langle\nabla D(\boldsymbol{p}_k),\boldsymbol{p}_{k+1}-\boldsymbol{p}_k\rangle\\&\leqslant B(\boldsymbol{p}_k)-D(\boldsymbol{p}_k)\end{aligned} \tag{32}$$

实际上，DC 规划迭代时会产生一个单调递减的序列$\{B(\boldsymbol{p}_k)-D(\boldsymbol{p}_k)\}$。式(32)表明，每次迭代后式(24)的目标函数值都要小于前一次迭代后的目标函数值，所以每次迭代后得到的式(24)的解都要优于前一次得到的解，也就是说迭代是收敛的[20,21]。当给定收敛精度 $\tau>0$ 时，DC 规划迭代过程终止于 $|-F(\xi_i,\boldsymbol{p}_k)+F(\xi_i,\boldsymbol{p}_{k-1})|\leqslant\tau$。

3.3 SEEM 算法总结

为了能够清晰理解 SEEM 算法，算法 1 给出了程序的执行步骤。首先，根据分式规划理论，原始优化问题(式(14))被转化为一个以能效 ξ 为参数的参数规划。该参数规划可以通过迭代求解一系列参数化的二次问题(式(21))进行求解。对于参数化的二次问题，运用 DC 规划理论，把该二次问题再进一步转化为一系列凸的子问题(式(28))进行迭代求解。算法 1 中包含 2 层循环：内层循环是 DC 规划，求解的是式(21)，其中，每次迭代时 ξ_i 是既定的；外层循环是分式规划，求解的是原始问题式(14)的等价问题式(20)。

本文算法是将原始优化问题通过 2 层转化，最终转化为求解一系列凸的子问题。所以本文算法的复杂度很大程度上取决于凸问题的求解复杂度。对于凸的子问题，可以采用文献[22]中的快速梯度法。为了分析凸问题的计算复杂度，引入下面几个符号。用 $V\geqslant 0$ 表示 Lipschitz 常数使目标函数 f 的梯度 ∇f 满足 Lipschitz 条件。用 γ 表示一个凸性参数，使式(28)的目标函数 f 满足强凸性。根据文献[22]的分析，当给定收敛精度 $\varsigma>0$，快速梯度法的迭次数可以表示为

$$O(1)\min\left\{\sqrt{\frac{V}{\gamma}}\ln\left(\frac{1}{\varsigma}\right),\sqrt{\frac{V}{\varsigma}}\right\}$$

在算法 1 中，当达到收敛精度 ε 和 τ 时对应的迭代次数分别表示为 N_ε 和 N_τ。这时本文算法总的计算复杂度可粗略表示为

$$O(1)\min\left\{\sqrt{\frac{V}{\gamma}}\ln\left(\frac{1}{\varsigma}\right),\sqrt{\frac{V}{\varsigma}}\right\}N_\varepsilon N_\tau$$

算法 1　SEEM 算法

输入：h_{sr}，h_{sd}，h_{rd}，g_{se}，g_{re}

输出：$\boldsymbol{p}^*$，ξ^*

给定初始值 ξ_0，计算 $\boldsymbol{p}^*(\xi_0)$，$i:=0$；

while $\left|F\left(\xi_i,\boldsymbol{p}^*(\xi_i)\right)\right|>\varepsilon$ do

　$i:=i+1$;

　根据式(22)更新 ξ_i；

　对既定的 ξ_i，设定起始点 $\boldsymbol{p}_0$，$k:=1$；

　计算 $\boldsymbol{p}_1$、$-F(\xi_i,\boldsymbol{p}_0)$、$-F(\xi_i,\boldsymbol{p}_1)$；

　while $|-F(\xi_i,\boldsymbol{p}_k)+F(\xi_i,\boldsymbol{p}_{k-1})|>\tau$ do

　　$k:=k+1$；

　　对既定的 $\boldsymbol{p}_{k-1}$，求解式(28)得到 $\boldsymbol{p}_k$；

　　计算 $-F(\xi_i,\boldsymbol{p}_k)$；

　end while

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

end while

return $\xi^*=\xi_i$，$\boldsymbol{p}^*=\boldsymbol{p}^*(\xi_i)$。

4　数值仿真

为了验证算法性能，本节给出算法的仿真结果，主要是将SEEM与SRM这2种策略进行了对比。SRM是指在源节点和中继节点的最大功率约束下最大化保密速率。SRM 传输策略是物理层安全研究的一个传统方面。已有大量文献通过不同的传输策略设计，实现最大化保密速率的传输目的[3~8]。为了简单和公平性，在仿真中，所有的节点位于同一条直线上[3,4]。源节点固定于点(0,0)。仿真参数为 $\sigma_{\mathrm{z}}^2=-100$ dBm，

$\eta = 0.38$，$p_{\mathrm{s}}^{\max} = p_{\mathrm{r}}^{\max} = 500$ mW，$p_{c_{\mathrm{s}}}^{\mathrm{transmit}} = p_{c_{\mathrm{r}}}^{\mathrm{receive}} = p_{c_{\mathrm{r}}}^{\mathrm{transmit}} = p_{c_{\mathrm{d}}}^{\mathrm{receive}} = 15\,\mathrm{mW}$，$R_0 = 1\,\mathrm{bit\cdot s^{-1}\cdot Hz^{-1}}$，路径损耗指数 $\alpha = 3.5$。所有仿真结果是 1 000 次蒙特卡洛实验的平均值。

首先，图 2 比较了中继节点处于不同位置时 SEEM 和 SRM 所能达到的安全能效，其中，目的节点和窃听者分别位于(500, 0)和(550, 0)，而中继节点从(50, 0)向(450, 0)移动。很明显，无论中继节点位于何处，本文提出的 SEEM 算法的安全能效远大于 SRM 的安全能效。

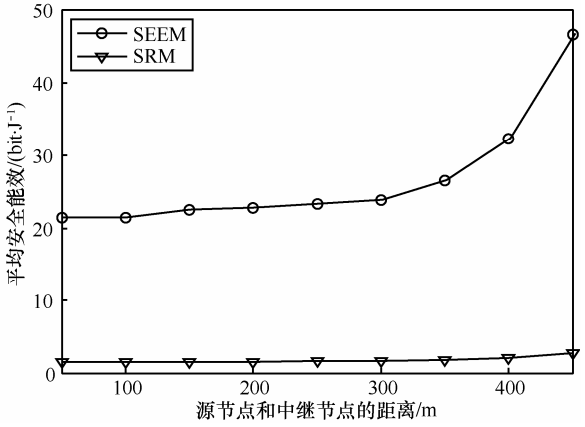


图 2 中继节点处于不同位置时的平均安全能效

在图 3 中，中继节点和窃听者分别固定于(250, 0)和(500, 0)，而目的节点从(250, 0)向(750, 0)移动。正如所料，SEEM 算法能达到的安全能效要优于 SRM 所能达到的安全能效。值得注意的是，随着源节点和目的节点间的距离增大，这 2 种方案的安全能效都逐渐递减，这是因为随着目的节点远离源和中继节点，合法信道和窃听信道间的差异越来越弱，窃听者对安全通信的威胁越来越大。

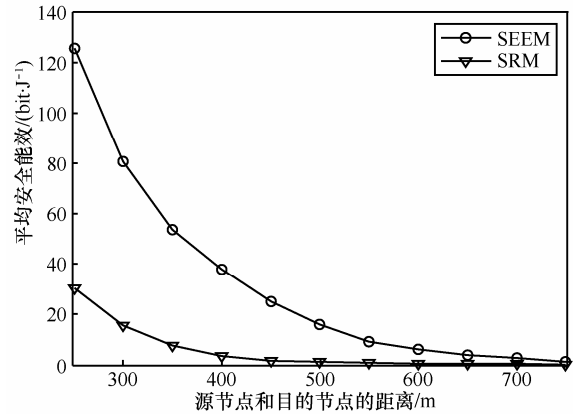


图 3 目的节点处于不同位置时的平均安全能效

为了观察安全能效优化对保密速率的影响，采用和图 3 相同的仿真设置，图 4 刻画了目的节点处于不同位置时 SEEM 和 SRM 所能达到的保密速率曲线。由图 4 可知，SEEM 算法能够达到的保密速率相比于 SRM 所能达到的保密速率有较小的损失，这是由于安全能效和保密速率之间本身存在折中。事实上，在原始问题求解过程中，通过分式规划将目标函数转化为相对应的参数规划，这时安全能效可以看成是对过高的功率消耗的惩罚。当能效优化使系统的安全能效达到最大值时，对功率消耗的惩罚最重；当安全能效置为 0 时，对功率消耗没有惩罚，这时最大化安全能效将转化为最大化保密速率。在实际应用中，可以通过调整系统的最小保密速率要求使系统在能效和安全性之间达到合理的平衡。

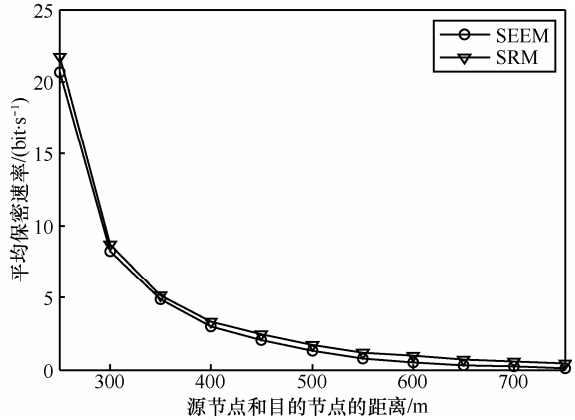


图 4 目的节点处于不同位置时的平均保密速率

在图 5 中，中继节点和目的节点分别固定于(250,0)和(500,0)，而窃听者从(250,0)向(750,0)移动。由图 5 可知，当合法信道和窃听信道的差异足够大时，保密通信才成为可能，这时 SEEM 算法的安全能效明显高于 SRM 的安全能效。

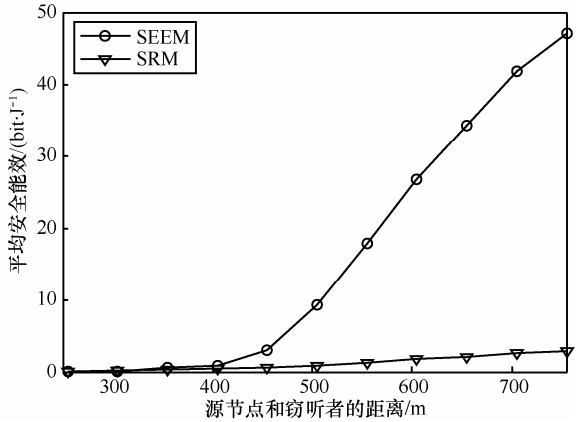


图 5 窃听者处于不同位置时的平均安全能效

采用与图 5 相同的仿真参数，图 6 给出了不同目标保密速率要求时的保密中断概率。保密中断概率定义为可达到的保密速率小于目标保密速率的概率。目标保密速率用 R_{out} 表示。保密中断概率即为 $\Pr(R_{\text{sec}} < R_{\text{out}})$。由图 6 可知，和 SRM 相比，SEEM 在提高安全能效的同时会带来微小的保密性能的损失。这也是由于安全能效和保密速率之间存在固有的折中。

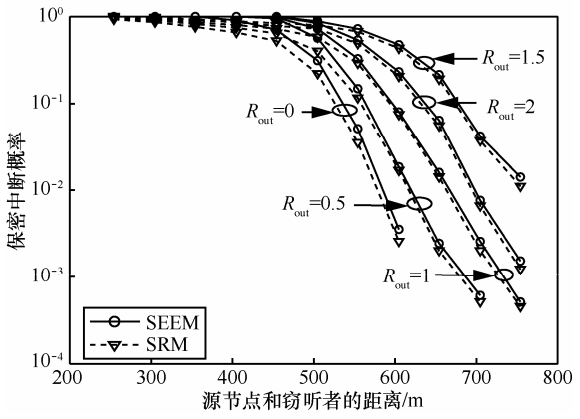


图 6　不同目标保密速率要求下的保密中断概率

5　结束语

本文针对解码转发中继网络中信息安全要求和能量受限问题，基于物理层安全理论，提出了一种高能效的功率分配算法。该算法基于分式规划和 DC 规划理论，通过 2 层循环迭代，联合进行源节点和中继节点的功率最优分配，达到安全能效最大化的传输要求。仿真结果表明，本文提出的算法能够明显提高系统的安全能效，同时有较小的保密性能损失，这是由于安全能效和保密速率之间存在固有的折中。

参考文献：

[1] 陈东华, 张秀秀, 谢维波. 窃听信道下认知多小区中的协同波束成形算法[J]. 通信学报, 2014, 35(11): 89-95.
CHEN D H, ZHANG X X, XIE W B. Coordinated beamforming for cognitive multi-cell networks with wiretap channels[J]. Journal on Communications, 2014, 35(11): 89-95.

[2] 钟州, 金梁, 黄开枝. 多载波系统随机子载波加权的物理层加密算法[J]. 通信学报, 2012, 33(10): 86-100.
ZHONG Z, JIN L, HUANG K Z. Using random subcarrier weighting for multi-carrier systems physical layer security[J]. Journal on Communications, 2012, 33(10): 86-100.

[3] DONG L, HAN Z, PETROPULU A, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Transaction on Signal Processing, 2010, 58(3): 1875-1888.

[4] LI J, PETROPULU A, WEBER S. On cooperative relaying schemes for wireless physical layer security[J]. IEEE Transaction on Signal Processing, 2011, 59(10): 4985-4996.

[5] WANG X, TAO M, MO J, et al. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks[J]. IEEE Transaction on Information Forensics and Security, 2011, 6(3): 693-702.

[6] HUANG J, SWINDLEHURST A. Cooperative jamming for secure communications in MIMO relay networks[J]. IEEE Transaction on Signal Processing, 2011, 59(10): 4871-4884.

[7] JEONG C, KIM I, KIM D. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system[J]. IEEE Transaction on Signal Processing, 2012, 60(1): 310-325.

[8] ZHAO R, HUANG Y, WANG W, et al. Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming[J]. IEEE Transactions on Wireless Communications, 2016, 15(4): 2537-2551.

[9] GURSOY M. Secure communication in the low-SNR regime[J]. IEEE Transaction on Communications, 2012, 60 (4): 1114-1123.

[10] COMANICIU C, POOR H. On energy-secrecy trade-offs for Gaussian wiretap channels[J]. IEEE Transaction on Information Forensics and Security, 2013, 8(2): 314-323.

[11] ZHANG H, HUANG Y, LI S, et al. Energy-efficient precoder design for MIMO wiretap channels[J]. IEEE Communications Letters, 2014, 18(9): 1559-1562.

[12] WANG D, BAI B, CHEN W, et al. Achieving high energy efficiency and physical-layer security in AF relaying[J]. IEEE Transactions on Wireless Communications, 2015, 15(1): 740-752.

[13] LANEMAN J, TSE D, WORNELL G. Cooperative diversity in wireless networks: efficient protocols and outage behavior[J]. IEEE Transaction on Information Theory, 2004, 50(12): 3062-3080.

[14] KHODAKARAMI H, LAHOUTI F. Link adaptation with untrusted relay assignment: design and performance analysis[J]. IEEE Transactions on Communications, 2013, 61(12):4874-4883.

[15] BLOCH M, BARROS J. Physical-layer security from information theory to security engineering[M]. New York: Cambridge University Press, 2011.

[16] ZHOU X, BAI B, CHEN W. Iterative antenna selection for decode-and-forward MIMO relay systems under a holistic power model[J]. IEEE Communications Letters, 2014, 18(12): 2237-2240.

[17] ZHOU X, BAI B, CHEN W. A low complexity energy efficiency maximization method for multiuser amplify-and-forward MIMO relay systems with a holistic power model[J]. IEEE Communications Letters, 2014, 18(8): 1371-1374.

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

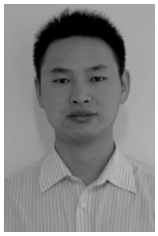
[19] NAEEM M, ILLANKO K, KARMOKAR A K, et al. Power allocation in decode and forward relaying for green cooperative cognitive radio systems[C]//IEEE Wireless Communications and Networking Conference (WCNC). 2013: 3806-3810.

[20] THI H A L, HUYNH V N, TAO P D. DC programming and DCA for general DC programs[C]//Advanced Computational Methods for Knowledge Engineering. 2014: 15-35.

[21] RASHID U, TUAN H, KHA H, et al. Joint optimization of source precoding and relay beamforming in wireless MIMO relay networks[J]. IEEE Transaction on Communications, 2014, 62(2): 488-499.

[22] RICHTER S, JONES C, MORARI M. Computational complexity certification for real-time MPC with input constraints based on the fast gradient method[J]. IEEE Transaction on Automatic Control, 2014, 57(6): 1391-1403.

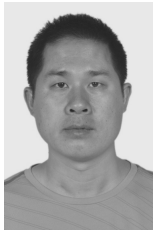
作者简介：



王东（1980-），男，陕西洛南人，清华大学博士生，主要研究方向为协同通信和信息安全等。

李永成（1978-），男，辽宁沈阳人，电子信息系统复杂电磁环境效应国家重点实验室工程师，主要研究方向为复杂电磁环境效应等。

白铂（1982-），男，陕西西安人，清华大学讲师、硕士生导师，主要研究方向为无线通信、物理层安全、组合优化等。



王满喜（1979-），男，河南驻马店人，电子信息系统复杂电磁环境效应国家重点实验室助理研究员，主要研究方向为无线通信与信道建模、复杂电磁环境效应机理等。