一种全双工认知中继网络中实现能量高效的安全传输方法

张 培 张建明 王良民
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 在"绿色"安全通信背景下,提出了一种保证同时同频全双工认知中继网络物理层安全、不影响主用户性能且能量高效的中继簇功率分配方案,该网络包含两个认知源节点、多个认知中继节点、多个主用户节点以及多个主用户窃听节点。在考虑了自干扰消除率以及中继转发信息的公平性的基础上,分别针对中继节点选择放大转发与译码转发策略的情形,设计协作波束成形向量及人工噪声矩阵,并通过一种结合半定松弛技术的爬山算法来获取最优解。仿真结果与理论分析表明了方案的有效性与合理性,同时表明选择放大转发策略能够获取更高的总能量效率。

关键词 绿色通信,物理层安全,认知中继网络,能量效率,同时同频全双工,半定松弛
中图法分类号 TN929.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.09.033

Design for Improving Energy-efficiency and Ensuring Physical-layer Security in Full-duplex Cognitive Relay Networks

ZHANG Pei ZHANG Jian-ming WANG Liang-min
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract Under the "green" and secure communication background, we studied the co-time co-frequency full-duplex cognitive relay networks consisting of two secondary source nodes, multiple cognitive relay nodes, multiple primary nodes and multiple primary eavesdroppers. To improve the total energy efficiency on the premise of ensuring the physical-layer security and the primary node's performance whether the selection relay protocol is the amplify-and-forward or decode-and-forward, we proposed the power allocation schemes to obtain a cooperative beamforming coefficient and an artificial noise matrix after taking both self-cancellation and forwarding fairness into consideration. It is mainly optimized by the "hill climbing" algorithm that combines the semidefinite relaxation (SDR) technology. Simulation results and theoretical analysis show the effectiveness and rationality of our scheme. Moreover, the choice of amplify-and-forward relay protocol contributes to the higher total energy efficiency.

Keywords Green communication, Physical-layer security, Cognitive relay networks, Energy-efficiency, Co-time co-frequency full-duplex, SDR

1 引言

随着无线通信业的膨胀式发展,能耗问题正逐渐成为制约其发展的瓶颈。在通信领域,作为能源可持续发展的重要体现,绿色通信的研究越来越引人关注[1]。一些有效提高能量效率的技术[2-4]可以使通信"绿色",如协作中继、认知无线电、同时同频全双工等。

通常中继的功率分配策略采用放大转发(AF)、译码转发(DF)和混合转发(CC)等。在协作中继系统[2,5]中,所有中继节点共享天线,构成一个虚拟的多天线系统,在增加系统分集增益的同时能够提高通信的可靠性。认知无线电技术通过频谱感知来保证次用户不影响主用户性能,利用比较空闲的频谱资源进行通信,从而实现高可靠的通信质量。然而通信过程中次用户对主用户的功率干扰需要控制,产生干扰的功率大小称为干扰温度[3,6]。同时同频全双工[4]是指在上、下行链路使用同一频率、同一时间传输信号,将无线资源的利用率提升近一倍,从而显著提高系统吞吐量和容量,提高自干扰消除率是实现该技术的关键所在[7]。

无线通信由于广播和开放特性,使得容易受到窃听。一直以来,使用基于高层加密技术来保障安全性。然而随着计算能力的持续突破以及编码技术的快速发展,一种基于信息论的绝对安全技术——物理层安全[8]的研究变得必要且有意义。协作中继技术不仅能提高能量效率,同时可以有效保证通信的物理层安全[9]。此外,加入用于混淆传输信号的人工噪声、增加对窃听用户接收信号的干扰、减少信息泄露可以改善系统的安全性能[10]。文献[11-12]分别分析了存在一个窃听节点的AF与DF双向中继网络中,中继与阻塞联合机制下的最大安全速率问题。

到稿日期:2016-08-05 返修日期:2016-08-28 本文受国家自然科学基金项目(61272074,U1405255)资助。
张 培(1992-),男,硕士生,主要研究方向为无线通信物理层安全,E-mail:zhangpei.ujs@foxmail.com;**张建明**(1964-),男,博士,教授,硕士生导师,主要研究方向为图象处理、模式识别及安全协议;**王良民**(1977-),男,博士后,教授,博士生导师,CCF高级会员,主要研究方向为物联网、大数据及安全协议。

相对于其他无线网络，全双工认知中继网络在使通信“绿色”的同时，其所受到的安全威胁也随着主用户的接入而增加[13]。文献[14-15]考虑了多输入单输出(MISO)认知无线电网络中完全信道状态信息(CSIT)是否存在的情况，设计了一种在发射功率与干扰温度受限时，最大安全速率的功率分配方案。文献[16]研究了慢衰落信道环境中提高主用户的安全吞吐量的方案。F. Alavi 等人[17]比较了不同的环境参数对单工与双工认知中继网络的安全和容量的影响。文献[18]提出了一种机会中继方案，在特定中继节点传输人工噪声，以提升系统的抗窃听性。

本文主要研究了同时同频全双工认知中继网络中一种保证物理层安全以及提高系统能量效率的中继簇功率分配方法。这里考虑的能量效率 $\eta=SINR/P$ 是指各个次用户源节点的接收信噪比(SINR)与认知中继簇所提供的总发射功率之比。本文主要贡献可总结如下：

针对认知中继簇选择放大转发与译码转发策略的两种情形，在考虑自干扰消除率及中继转发公平性的基础上，通过设计协作波束成形向量与人工噪声矩阵，实现物理层安全，同时保证主用户通信性能以及提高系统能量效率。

针对此功率分配方案，提出了一种结合半定松弛技术[20]的爬山算法来获取最优解，同时证明了半定松弛的合理性。仿真结果表明了该算法的有效性，以及本方案中基于放大转发策略的情形能获取更高的系统性能。

2　网络模型与传输策略

2.1　网络模型

本文提出的同时同频全双工认知中继网络模型如图 1 所示。该网络中存在两个次用户源节点 SA 和 SB，K 个次用户中继节点簇 $SR=\{SR_1,SR_2,\cdots,SR_K\}$，$T$ 个主用户节点 $PU=\{PU_1,PU_2,\cdots,PU_T\}$ 以及 M 个行为不端的主用户窃听节点 $PE=\{PE_1,PE_2,\cdots,PE_M\}$。该模型中的所有节点均配置单天线。

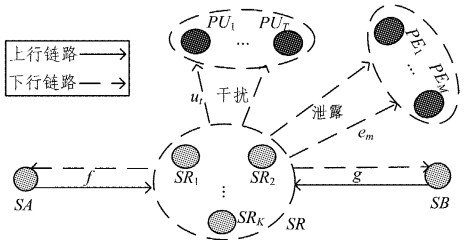

图 1　同时同频全双工认知中继网络模型

不失一般性，假定所有信道均为准静态平坦衰落信道，且 SA 与 SB 无直接的通信链路。其中 f_k，g_k，$u_{k,t}$ 及 $e_{k,m}$ 表示 SA，SB，PU_t，PE_m 到中继簇 SR 中第 k 个中继节点的信道衰落参数，各节点 SA，SB，SR_k，PU_t 以及 PE_M 处的加性高斯白噪声分别记为 $n_{SA}\sim\mathcal{CN}(0,\delta_A^2)$，$n_{SB}\sim\mathcal{CN}(0,\delta_B^2)$，$n_{r,k}\sim\mathcal{CN}(0,\delta_r^2)$，$n_{u,t}\sim\mathcal{CN}(0,\delta_{u,t}^2)$ 以及 $n_{e,m}\sim\mathcal{CN}(0,\delta_{e,m}^2)$。

为方便运算，定义符号 $\mathbb{C}$ 为复数集合，0 为全零矩阵，$(\cdot)^{\mathrm{T}}$，$(\cdot)^{\mathrm{H}}$，$(\cdot)^{\dagger}$ 分别表示转置、共轭转置、伪逆运算，$D(\partial)$ 为以 ∂ 中元素为对角元素的对角矩阵，$Tr(\cdot)$ 为矩阵的迹，$Rank(\cdot)$ 表示矩阵的秩，$norm(x)$ 表示向量 x 的 2-范数，$x\sim\mathcal{CN}(\bar{\omega},\Delta)$ 中随机向量 x 服从平均值为 $\bar{\omega}$、方差为 Δ 的复高斯分布，$X\succeq 0$ 为埃尔米特半定矩阵。

2.2　传输策略

在上行链路中，SA 与 SB 分别在次用户频段上发送信号 $\sqrt{P_A}s_A$，$\sqrt{P_B}s_B$，其中 P_A 与 P_B 为各自的发射信号功率，s_A，s_B 为能量归一化的源信息。则次用户中继簇 SR 的接收信号为：

$$Y_R=\sqrt{P_A}s_Af+\sqrt{P_B}s_Bg+n_R \tag{1}$$

其中，$f_k=[f_1,f_2,\cdots,f_K]\in\mathbb{C}^{K\times 1}$，$g_k=[g_1,g_2,\cdots,g_K]\in\mathbb{C}^{K\times 1}$。

针对下行链路，值得注意的是，我们假设 SR 中各节点基于源节点的发射功率公平地分配功率转发 s_A 及 s_B。同时 SA 与 SB 能够进行一定程度上的自干扰消除，自干扰消除因子记为 $\gamma\in(0,1)$。

2.2.1　AF 策略

中继簇 SR 中的各中继节点对接收的信号进行能量归一，归一化因子 $l_k^{AF}=1/\sqrt{|f_k|^2P_A+|g_k|^2P_B+\delta_{r,k}^2}$，归一化向量 $L^{AF}=[l_1^{AF},l_2^{AF},\cdots,l_K^{AF}]^{\mathrm{T}}$。然后通过协作波束成形技术，对归一化后的信号进行加权，加权因子 $\alpha^{AF}\in\mathbb{C}^{K\times 1}$，同时用一定形式的人工噪声 z^{AF} 来混淆加权信号，$z^{AF}\sim\mathcal{CN}(0,\boldsymbol{\Sigma}^{AF})$。

SR 提供总发射功率 P_{tot}，在主用户的授权频段上广播源信息与人工噪声组成的混合信号 $\boldsymbol{D}(\alpha^{AF})\boldsymbol{D}(L^{AF})Y_R+z^{AF}$，且发射功率 $(\alpha^{AF})^H\alpha^{AF}+\boldsymbol{\Sigma}^{AF}\leqslant P_{tot}$。

各接收节点 SA，SB，PE_m 及 PU_t 接收到的信号如下：

$$Y_{SA}^{AF}=f^{\mathrm{T}}(\boldsymbol{D}(\alpha^{AF})\boldsymbol{D}(L^{AF})Y_R+z^{AF})+n_{SA} \tag{2}$$

$$Y_{SB}^{AF}=g^{\mathrm{T}}(\boldsymbol{D}(\alpha^{AF})\boldsymbol{D}(L^{AF})Y_R+z^{AF})+n_{SB} \tag{3}$$

$$Y_{e,m}^{AF}=e_m^{\mathrm{T}}(\boldsymbol{D}(\alpha^{AF})\boldsymbol{D}(L^{AF})Y_R+z^{AF})+n_{e,m} \tag{4}$$

$$Y_{u,t}^{AF}=u_t^{\mathrm{T}}(\boldsymbol{D}(\alpha^{AF})\boldsymbol{D}(L^{AF})Y_R+z^{AF})+n_{u,t} \tag{5}$$

其中，$e_m=[e_{1,m},e_{2,m},\cdots,e_{K,m}]\in\mathbb{C}^{K\times 1}$，$u_t=[u_{1,t},u_{2,t},\cdots,u_{K,t}]\in\mathbb{C}^{K\times 1}$。

则 SA 和 SB 各自的能量效率分别为：

$$\eta_{SA}^{AF}=\frac{(\alpha^{AF})^H\boldsymbol{W}^{AF}(A)\alpha^{AF}}{((\alpha^{AF})^H\boldsymbol{V}^{AF}(A)\alpha^{AF}+Tr(\boldsymbol{F}^{AF}(A)\boldsymbol{\Sigma}^{AF})+\delta_A^2)P_{tot}} \tag{6}$$

$$\eta_{SB}^{AF}=\frac{(\alpha^{AF})^H\boldsymbol{W}^{AF}(B)\alpha^{AF}}{((\alpha^{AF})^H\boldsymbol{V}^{AF}(B)\alpha^{AF}+Tr(\boldsymbol{F}^{AF}(B)\boldsymbol{\Sigma}^{AF})+\delta_B^2)P_{tot}} \tag{7}$$

各窃听节点 PE_m 处关于 SA 和 SB 的接收信噪比及 PU_t 处的干扰温度为：

$$SINR_{e,m}^{AF}(SB)=\frac{(\alpha^{AF})^H\boldsymbol{X}_m^{AF}(B)\alpha^{AF}}{(\alpha^{AF})^H\boldsymbol{H}_m^{AF}(B)\alpha^{AF}+Tr(\boldsymbol{Z}_m^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{e,m}^2} \tag{8}$$

$$SINR_{e,m}^{AF}(SA)=\frac{(\alpha^{AF})^H\boldsymbol{X}_m^{AF}(A)\alpha^{AF}}{(\alpha^{AF})^H\boldsymbol{H}_m^{AF}(A)\alpha^{AF}+Tr(\boldsymbol{Z}_m^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{e,m}^2} \tag{9}$$

$$IN_t^{AF}=(\alpha^{AF})^H\boldsymbol{Q}_t^{AF}\alpha^{AF}+Tr(\boldsymbol{S}_t^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{u,t}^2 \tag{10}$$

其中，$\boldsymbol{W}^{AF}(A)=norm(\sqrt{P_B}f^{\mathrm{T}}\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{Z}_m^{AF}=norm(e_m^{\mathrm{T}})^2$，$\boldsymbol{V}^{AF}(A)=norm((1-\gamma)\sqrt{P_A}f^{\mathrm{T}}\boldsymbol{D}(f)\boldsymbol{D}(L^{AF}))^2+norm(\delta_rf^{\mathrm{T}}\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{X}_m^{AF}(A)=norm(\sqrt{P_A}e_m^{\mathrm{T}}\boldsymbol{D}(f)\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{F}^{AF}(A)=norm(f^{\mathrm{T}})^2$，$\boldsymbol{F}^{AF}(B)=norm(g^{\mathrm{T}})^2$，$\boldsymbol{W}^{AF}(B)=norm(\sqrt{P_A}g^{\mathrm{T}}\boldsymbol{D}(f)\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{V}^{AF}(B)=norm(\delta_rg^{\mathrm{T}}\boldsymbol{D}(L^{AF}))^2+norm((1-\gamma)\sqrt{P_B}g^{\mathrm{T}}\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{X}_m^{AF}(B)=norm(\sqrt{P_B}e_m^{\mathrm{T}}\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{S}_t^{AF}=norm(u_t^{\mathrm{T}})^2$，$\boldsymbol{H}_m^{AF}(B)=norm(\delta_re_m^{\mathrm{T}}\boldsymbol{D}$

$(L^{AF}))^2+norm(\sqrt{P_A}e_m^{\mathrm{T}}\boldsymbol{D}(f)\boldsymbol{D}(L^{AF}))^2$，及 $\boldsymbol{H}_m^{AF}(A)=norm(\sqrt{P_B}e_m^{\mathrm{T}}\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^2+norm(\delta_r e_m^{\mathrm{T}}\boldsymbol{D}(L^{AF}))^2$，$\boldsymbol{Q}_t^{AF}=norm(\sqrt{P_B}u_t^{\mathrm{T}}\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^2+norm(\delta_r u_t^{\mathrm{T}}\boldsymbol{D}(L^{AF}))^2+norm(\sqrt{P_A}u_t^{\mathrm{T}}\boldsymbol{D}(f)\boldsymbol{D}(L^{AF}))^2$。

2.2.2 DF 策略

不同于 AF 中继策略，每个基于 DF 策略的中继需要先对接收到的信号进行解码，然后重新编码后转发。考虑到中继转发信息的公平性，能量归一化的信号为 $\lambda s_A+(1-\lambda)s_B$，其中 $\lambda=\sqrt{P_A}/(\sqrt{P_A}+\sqrt{P_B})$。

同样利用波束成形技术对 s_A 和 s_B 加权，人工噪声 z^{DF} 用于干扰窃听者，加权因子 $\alpha^{DF}\in\mathbb{C}^{K\times 1}$，$z^{DF}\sim CN(0,\boldsymbol{\Sigma}^{DF})$，$\boldsymbol{\Sigma}^{DF}\succeq 0$。

SR 利用主用户的频谱资源发送混合信号 $\alpha^{DF}(\lambda s_A+(1-\lambda)s_B)+z^{DF}$，且总发送功率 $(\alpha^{AF})^H\alpha^{AF}+\boldsymbol{\Sigma}^{AF}$ 不能超过 P_{tot}。

则 *SA*，*SB*，PE_m 及 PU_t 接收到的信号如下：

$$Y_{SA}^{DF}=f^{\mathrm{T}}(\alpha^{DF}(\lambda s_A+(1-\lambda)s_B)+z^{DF})+n_{SA} \tag{11}$$

$$Y_{SB}^{DF}=g^{\mathrm{T}}(\alpha^{DF}(\lambda s_A+(1-\lambda)s_B)+z^{DF})+n_{SB} \tag{12}$$

$$Y_{e,m}^{DF}=e_m^{\mathrm{T}}(\alpha^{DF}(\lambda s_A+(1-\lambda)s_B)+z^{DF})+n_{e,m} \tag{13}$$

$$Y_{u,t}^{DF}=u_t^{\mathrm{T}}(\alpha^{DF}(\lambda s_A+(1-\lambda)s_B)+z^{DF})+n_{u,t} \tag{14}$$

经过计算，得到中继簇 *SR* 关于 *SA* 和 *SB* 的能量效率：

$$\eta_{SA}^{DF}=\frac{(\alpha^{DF})^H\boldsymbol{W}^{DF}(A)\alpha^{DF}}{((\alpha^{DF})^H\boldsymbol{V}^{DF}(A)\alpha^{DF}+Tr(\boldsymbol{F}^{DF}(A)\boldsymbol{\Sigma}^{DF})+\delta_A^2)P_{tot}} \tag{15}$$

$$\eta_{SB}^{DF}=\frac{(\alpha^{DF})^H\boldsymbol{W}^{DF}(B)\alpha^{DF}}{((\alpha^{DF})^H\boldsymbol{V}^{DF}(B)\alpha^{DF}+Tr(\boldsymbol{F}^{DF}(B)\boldsymbol{\Sigma}^{DF})+\delta_B^2)P_{tot}} \tag{16}$$

同时得到窃听节点 PE_m 处关于 *SA* 和 *SB* 的接收信噪比及 PU_t 处的干扰温度为：

$$SINR_{e,m}^{DF}(SA)=\frac{(\alpha^{DF})^H\boldsymbol{X}_m^{DF}\alpha^{DF}}{(\alpha^{DF})^H\boldsymbol{H}_m^{DF}\alpha^{DF}+Tr(\boldsymbol{Z}_m^{DF}\boldsymbol{\Sigma}^{DF})+\delta_{e,m}^2} \tag{17}$$

$$SINR_{e,m}^{DF}(SB)=\frac{(\alpha^{DF})^H\boldsymbol{H}_m^{DF}\alpha^{DF}}{(\alpha^{DF})^H\boldsymbol{X}_m^{DF}\alpha^{DF}+Tr(\boldsymbol{Z}_m^{DF}\boldsymbol{\Sigma}^{DF})+\delta_{e,m}^2} \tag{18}$$

$$IN_t^{DF}=(\alpha^{DF})^H\boldsymbol{Q}_t^{DF}\alpha^{DF}+Tr(\boldsymbol{S}_t^{DF}\boldsymbol{\Sigma}^{DF})+\delta_{u,t}^2 \tag{19}$$

其中，$\boldsymbol{W}^{DF}(A)=norm((1-\lambda)f^{\mathrm{T}})^2$，$\boldsymbol{X}_m^{DF}=norm(\lambda e_m^{\mathrm{T}})^2$，$\boldsymbol{F}^{DF}(A)=norm(f^{\mathrm{T}})^2$，$\boldsymbol{S}_t^{AF}=norm(u_t^{\mathrm{T}})^2$，$\boldsymbol{W}^{DF}(B)=norm(\lambda g^{\mathrm{T}})^2$，$\boldsymbol{V}^{DF}(A)=norm((1-\gamma)\lambda f^{\mathrm{T}})^2$，$\boldsymbol{V}^{DF}(B)=norm((1-\gamma)(1-\lambda)g^{\mathrm{T}})^2$，$\boldsymbol{F}^{DF}(B)=norm(g^{\mathrm{T}})^2$，$\boldsymbol{H}_m^{DF}=norm((1-\lambda)e_m^{\mathrm{T}})^2$，$\boldsymbol{Z}_m^{DF}=norm(e_m^{\mathrm{T}})^2$ 及 $\boldsymbol{Q}_t^{AF}=norm(\lambda u_t^{\mathrm{T}})^2+norm((1-\lambda)u_t^{\mathrm{T}})^2$。

3 问题描述与优化方案

3.1 问题描述

本文的功率分配方案不仅需要实现物理层安全及保证干扰温度，同时还需要做到能量高效。当窃听节点的接收信噪比低于可容忍的窃听阈值时，则认为物理层安全得到实现。

类似于文献[19]的描述方式，式(20)给出了功率分配问题的数学描述：

$$\max_{\alpha,\boldsymbol{\Sigma}}\ \eta_{SA}+\eta_{SB} \tag{20(a)}$$

$$\text{s. t.}\ \max_{m=1,\cdots,M}(SINR_{e,m}(SA))\leqslant\Phi \tag{20(b)}$$

$$\max_{m=1,\cdots,M}(SINR_{e,m}(SB))\leqslant\Phi \tag{20(c)}$$

$$\max_{m=1,\cdots,T}(IN_t)\leqslant\Gamma \tag{20(d)}$$

$$\alpha^H\alpha+\boldsymbol{\Sigma}\leqslant P_{tot} \tag{20(e)}$$

此处目标函数要求最大化 *SR* 的总能量效率，约束条件式(20(b))、式(20(c))给出的 Φ 为最大可容忍窃听阈值，同时式(20(d))中要求主用户处的干扰温度不超过阈值 Γ，式(20(e))给出了中继簇的功率限制。

3.2 优化方案

显然，式(20)所述是 NP-hard 问题，很难直接对其进行求解。因此本文提出了一种结合半定松弛技术的爬山算法，将式(22(a))中的目标函数分解成子目标函数 $\max\limits_{\alpha,\boldsymbol{\Sigma}}\eta_{SA}$ 与一个新的约束条件 $\eta_{SB}\geqslant\Psi$，得到一个初始子问题。其中 Ψ 为 η_{SB} 需要满足的最小阈值。

本方案的关键是通过不断增长阈值 Ψ，更新求解子问题，直到子问题无法获取有效解。

3.2.1 AF 策略

针对 AF 中继情形，原问题转换为以下的子问题式(21)。

$$\max_{\alpha,\boldsymbol{\Sigma}}\frac{(\alpha^{AF})^H\boldsymbol{W}^{AF}(A)\alpha^{AF}}{((\alpha^{AF})^H\boldsymbol{V}^{AF}(A)\alpha^{AF}+Tr(\boldsymbol{F}^{AF}(A)\boldsymbol{\Sigma}^{AF})+\delta_A^2)P_{tot}} \tag{21(a)}$$

$$\text{s. t.}\ \frac{(\alpha^{AF})^H\boldsymbol{W}^{AF}(B)\alpha^{AF}}{((\alpha^{AF})^H\boldsymbol{V}^{AF}(B)\alpha^{AF}+Tr(\boldsymbol{F}^{AF}(B)\boldsymbol{\Sigma}^{AF})+\delta_B^2)P_{tot}}\geqslant\Psi \tag{21(b)}$$

$$\max_{m=1,\cdots,M}\frac{(\alpha^{AF})^H\boldsymbol{X}_m^{AF}(A)\alpha^{AF}}{(\alpha^{AF})^H\boldsymbol{H}_m^{AF}(A)\alpha^{AF}+Tr(\boldsymbol{Z}_m^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{e,m}^2}\leqslant\Phi \tag{21(c)}$$

$$\max_{m=1,\cdots,M}\frac{(\alpha^{AF})^H\boldsymbol{X}_m^{AF}(B)\alpha^{AF}}{(\alpha^{AF})^H\boldsymbol{H}_m^{AF}(B)\alpha^{AF}+Tr(\boldsymbol{Z}_m^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{e,m}^2}\leqslant\Phi \tag{21(d)}$$

$$\max_{t=1,\cdots,t}((\alpha^{AF})^H\boldsymbol{Q}_t^{AF}\alpha^{AF}+Tr(\boldsymbol{S}_t^{AF}\boldsymbol{\Sigma}^{AF})+\delta_{u,t}^2)\leqslant\Gamma \tag{21(e)}$$

$$(\alpha^{AF})^H\alpha^{AF}+\boldsymbol{\Sigma}^{AF}\leqslant P_{tot} \tag{21(f)}$$

为了求解此问题，定义 $\boldsymbol{E}^{AF}=(\alpha^{AF})^H\alpha^{AF}$，显然 $\boldsymbol{E}^{AF}\succeq 0$ 且 $Rank(\boldsymbol{E}^{AF})=1$。

$\boldsymbol{E}^{AF}$ 是半正定矩阵，因此利用半定松弛[20]的思想，忽略 $Rank(\boldsymbol{E}^{AF})=1$ 这一约束条件，同时定义 ξ^{AF} 满足 $(Tr(\boldsymbol{V}^{AF}(A)\boldsymbol{E}^{AF})+Tr(\boldsymbol{F}^{AF}(A)\boldsymbol{\Sigma}^{AF})+\delta_A^2)P_{tot}=1/\xi^{AF}$。这里进行以下转换 $\overline{\boldsymbol{E}}^{AF}=\xi^{AF}\boldsymbol{E}^{AF}$，$\overline{\boldsymbol{\Sigma}}^{AF}=\xi^{AF}\boldsymbol{\Sigma}^{AF}$，从而得到一个等价的凸优化问题式(22)，内点算法工具箱 CVX[21] 可用于求解这一问题。

$$\min_{\overline{\boldsymbol{E}}^{AF},\overline{\boldsymbol{\Sigma}}^{AF},\xi^{AF}}-Tr(\boldsymbol{W}^{AF}(A)\overline{E}^{AF}) \tag{22(a)}$$

$$\text{s. t.}\ P_{tot}\Psi Tr(\boldsymbol{F}^{AF}(B)\overline{\boldsymbol{\Sigma}}^{AF})+\xi^{AF}P_{tot}\Psi\delta_B^2-Tr((\boldsymbol{W}^{AF}(B)-P_{tot}\Psi\boldsymbol{V}^{AF}(B))\overline{E}^{AF})\leqslant 0 \tag{22(b)}$$

$$(Tr(\boldsymbol{V}^{AF}(A)\overline{E}^{AF})+Tr(\boldsymbol{F}^{AF}(A)\overline{\boldsymbol{\Sigma}}^{AF})+\xi^{AF}\delta_A^2)P_{tot}=1 \tag{22(c)}$$

$$\max_{m=1,\cdots,M}Tr((\boldsymbol{X}_m^{AF}(A)-\Phi\boldsymbol{H}_m^{AF}(A))\overline{E}^{AF})-\Phi Tr(\boldsymbol{Z}_m^{AF}\overline{\boldsymbol{\Sigma}}^{AF})-\Phi\xi^{AF}\delta_{e,m}^2\leqslant 0 \tag{22(d)}$$

$$\max_{m=1,\cdots,M}Tr((\boldsymbol{X}_m^{AF}(B)-\Phi\boldsymbol{H}_m^{AF}(B))\overline{E}^{AF})-\Phi Tr(\boldsymbol{Z}_m^{AF}\overline{\boldsymbol{\Sigma}}^{AF})-\Phi\xi^{AF}\delta_{e,m}^2\leqslant 0 \tag{22(e)}$$

$$\max_{m=1,\cdots,M}Tr(\boldsymbol{Q}_t^{AF}\overline{E}^{AF})+Tr(\boldsymbol{S}_t^{AF}\overline{\boldsymbol{\Sigma}}^{AF})+\xi^{AF}\delta_{u,t}^2-\xi^{AF}\Gamma\leqslant 0 \tag{22(f)}$$

$$Tr(\overline{\boldsymbol{\Sigma}}^{AF})+Tr(\overline{E}^{AF})-\xi^{AF}P_{tot}\leqslant 0 \tag{22(g)}$$

设定初始值 $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}=0$，$\boldsymbol{E}_{\max}^{AF}=0$ 及 $\boldsymbol{\Sigma}_{\max}^{AF}=0$。计算式(22)，判断当前效率和 $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{cur}$ 是否大于 $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}$，若大于则更新 $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}=(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{cur}$，$\boldsymbol{E}_{\max}^{AF}=\boldsymbol{E}_{cur}^{AF}$ 及 $\boldsymbol{\Sigma}_{\max}^{AF}=\boldsymbol{\Sigma}_{cur}^{AF}$。

接下来迭代不断递增 Ψ 的值来更新式(22)，$\Psi=\mu\times(\eta_{SB}^{AF})_{cur}$，其中 μ 为递增系数。迭代计算新的式(22)，直到CVX求不出有效解。

值得注意的是，上述过程中忽略了 $Rank(\boldsymbol{E}^{AF})=1$ 这一条件，而在3.3节中我们也证明了半定松弛的合理性，即 $\boldsymbol{E}_{\max}^{AF}$ 的最优解的秩必为1。若秩为1，则其主特征矢量为式(22)所述问题的最优解；否则可通过随机化技术[24]获取 α^{AF} 的近似最优解。

算法1的伪代码给出了优化AF策略下的功率分配问题的详细过程。

算法 1　基于AF中继策略的一种结合半定松弛技术的爬山算法

输入：式(20)中除 α^{AF} 之外所有的变量

输出：α^{AF}，$\boldsymbol{\Sigma}^{AF}$

初始化：$(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}=0$，$\mathbf{E}_{\max}^{AF}=\mathbf{0}$ 及 $\boldsymbol{\Sigma}_{\max}^{AF}=\mathbf{0}$

1. 从式(20)到式(22)进行优化
2. while CVX 可以求解当前的式(22) do
3.　if $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{cur}>(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}$ then
4.　　$\Psi=\mu\times(\eta_{SB}^{AF})_{cur}$，$\mathbf{E}_{\max}^{AF}=\mathbf{E}_{cur}^{AF}$，$\boldsymbol{\Sigma}_{\max}^{AF}=\boldsymbol{\Sigma}_{cur}^{AF}$ 及 $(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{\max}=(\eta_{SA}^{AF}+\eta_{SB}^{AF})_{cur}$
5.　end if
6. end while
7. if Rank($\mathbf{E}^{AF}$)=1 then
8.　对 $\mathbf{E}_{\max}^{AF}$ 进行秩一分解，获取 $\mathbf{E}_{\max}^{AF}$ 的主特征向量
9. else
10.　通过随机化技术[22]获取 α^{AF} 的近似最优解
11. end if

3.2.2　DF 策略

为了解决基于DF中继策略情形下的功率分配问题，利用上节的半定松弛技术进行优化，得到一个凸优化形式(式(23))：

$$\min_{\overline{\boldsymbol{E}}^{DF},\overline{\boldsymbol{\Sigma}}^{DF},\xi^{DF}} -Tr(\boldsymbol{W}^{DF}(A)\overline{E}^{DF}) \tag{23(a)}$$

$$\text{s. t. } P_{tot}\,\Psi Tr(\boldsymbol{F}^{DF}(B)\overline{\boldsymbol{\Sigma}}^{DF})+\xi^{DF}P_{tot}\,\Psi\delta_B^2-Tr((\boldsymbol{W}^{DF}(B)-P_{tot}\,\Psi\boldsymbol{V}^{DF}(B))\overline{E}^{DF})\leqslant 0 \tag{23(b)}$$

$$(Tr(\boldsymbol{V}^{DF}(A)\overline{E}^{DF})+Tr(\boldsymbol{F}^{DF}(A)\overline{\boldsymbol{\Sigma}}^{DF})+\xi^{DF}\delta_A^2)P_{tot}=1 \tag{23(c)}$$

$$\max_{m=1,\cdots,M} Tr((\boldsymbol{X}_m^{DF}-\Phi\boldsymbol{H}_m^{DF})\overline{E}^{DF})-\Phi Tr(\boldsymbol{Z}_m^{DF}\overline{\boldsymbol{\Sigma}}^{DF})-\Phi\xi^{DF}\delta_{e,m}^2\leqslant 0 \tag{23(d)}$$

$$\max_{m=1,\cdots,M} Tr((\boldsymbol{X}_m^{DF}-\Phi\boldsymbol{H}_m^{DF})\overline{E}^{DF})-\Phi Tr(\boldsymbol{Z}_m^{DF}\overline{\boldsymbol{\Sigma}}^{DF})-\Phi\xi^{DF}\delta_{e,m}^2\leqslant 0 \tag{23(e)}$$

$$\max_{m=1,\cdots,M} Tr(\boldsymbol{Q}_t^{DF}\overline{E}^{DF})+Tr(\boldsymbol{S}_t^{DF}\overline{\boldsymbol{\Sigma}}^{DF})+\xi^{DF}\delta_{u,t}^2-\xi^{DF}\Gamma\leqslant 0 \tag{23(f)}$$

$$Tr(\overline{\boldsymbol{\Sigma}}^{DF})+Tr(\overline{E}^{DF})-\xi^{DF}P_{tot}\leqslant 0 \tag{23(g)}$$

同样，使用爬山算法来解决式(23)。算法2给出了详细的优化过程。

算法 2　基于DF中继策略的一种结合半定松弛技术的爬山算法

输入：式(20)中除 α^{AF} 之外所有的变量

输出：α^{DF}，$\boldsymbol{\Sigma}^{DF}$

初始化：$(\eta_{SA}^{DF}+\eta_{SB}^{DF})_{\max}=0$，$\mathbf{E}_{\max}^{DF}=\mathbf{0}$ 及 $\boldsymbol{\Sigma}_{\max}^{DF}=\mathbf{0}$

1. 从式(20)到式(23)进行优化
2. while CVX 可以求解当前的式(23) do
3.　if $(\eta_{SA}^{DF}+\eta_{SB}^{DF})_{cur}>(\eta_{SA}^{DF}+\eta_{SB}^{DF})_{\max}$ then
4.　　$\Psi=\mu\times(\eta_{SB}^{DF})_{cur}$，$\mathbf{E}_{\max}^{DF}=\mathbf{E}_{cur}^{DF}$，$\boldsymbol{\Sigma}_{\max}^{DF}=\boldsymbol{\Sigma}_{cur}^{DF}$ 及 $(\eta_{SA}^{DF}+\eta_{SB}^{DF})_{\max}=(\eta_{SA}^{DF}+\eta_{SB}^{DF})_{cur}$
5.　end if
6. end while
7. if Rank($\mathbf{E}^{DF}$)=1 then
8.　对 $\mathbf{E}_{\max}^{DF}$ 进行秩一分解，获取 $\mathbf{E}_{\max}^{DF}$ 的主特征向量
9. else
10.　通过随机化技术[22]获取 α^{DF} 的近似最优解
11. end if

3.3　秩一性证明

我们可以得到式(22)的KKT(Karush-Kuhn-Tucker)条件(24)如下：

$$\boldsymbol{\Pi}^{AF}=\kappa_3 I+\kappa_1 P_{tot}\,\Psi\boldsymbol{V}^{AF}(B)+\kappa_2 P_{tot}\,\boldsymbol{V}^{AF}(A)+\sum_{m=1}^{M}\chi_{m,1}\boldsymbol{X}_m^{AF}(A)+\sum_{m=1}^{M}\chi_{m,2}\boldsymbol{X}_m^{AF}(B)+\sum_{t=1}^{T}\chi_{u,t}\boldsymbol{Q}_t^{AF}-\kappa_1\boldsymbol{W}^{AF}(B)-\sum_{m=1}^{M}\chi_{m,1}\Phi\boldsymbol{H}_m^{AF}(A)-\sum_{m=1}^{M}\chi_{m,2}\Phi\boldsymbol{H}_m^{AF}(B)-\boldsymbol{W}^{AF}(A) \tag{24(a)}$$

$$\boldsymbol{\Pi}^{AF}\overline{\boldsymbol{E}}^{AF}=0 \tag{24(b)}$$

$$\kappa_1\geqslant 0,\kappa_2\geqslant 0,\kappa_3\geqslant 0,\chi_{m,1}\geqslant 0,\chi_{m,2}\geqslant 0,\chi_{u,t}\geqslant 0,\boldsymbol{\Pi}^{AF}\geqslant 0 \tag{24(c)}$$

其中，κ_1，κ_2，$\chi_{m,1}$，$\chi_{m,2}$，$\chi_{u,t}$ 及 κ_3 分别是约束条件(22(b))－(22(g))相关的最优对偶变量，$\boldsymbol{\Pi}^{AF}$ 为 $\overline{\boldsymbol{E}}^{AF}$ 的最优对偶变量。

首先证明KKT条件(24(a))中 κ_3 的值不可能为0。假设 $\kappa_3=0$，式(24)表明 $\boldsymbol{\Pi}^{AF}\geqslant 0$ 且 $\sum_{m=1}^{M}\chi_{m,1}\Phi\boldsymbol{H}_m^{AF}(A)+\boldsymbol{W}^{AF}(A)+\kappa_1\boldsymbol{W}^{AF}(B)+\sum_{m=1}^{M}\chi_{m,2}\Phi\boldsymbol{H}_m^{AF}(B)>0$。

定义一个向量 q_Π 满足下式：

$$q_\Pi^H(\kappa_2 P_{tot}\boldsymbol{V}^{AF}(A)+\sum_{m=1}^{M}\chi_{m,1}\boldsymbol{X}_m^{AF}(A)+\sum_{m=1}^{M}\chi_{m,2}\boldsymbol{X}_m^{AF}(B)+\sum_{t=1}^{T}\chi_{u,t}\boldsymbol{Q}_t^{AF}+\kappa_1\Psi P_{tot}\boldsymbol{V}^{AF}(B))q_\Pi=0$$

结合上式与式(24(a))可知，

$$q_\Pi^H\boldsymbol{\Pi}^{AF}q_\Pi=-q_\Pi^H(\sum_{m=1}^{M}\chi_{m,1}\Phi\boldsymbol{H}_m^{AF}(A)+\kappa_1\boldsymbol{W}^{AF}(B)+\sum_{m=1}^{M}\chi_{m,2}\Phi\boldsymbol{H}_m^{AF}(B)+\boldsymbol{W}^{AF}(A))q_\Pi\geqslant 0$$

由上式可知，

$$\sum_{m=1}^{M}\chi_{m,1}\Phi\boldsymbol{H}_m^{AF}(A)+\kappa_1\boldsymbol{W}^{AF}(B)+\boldsymbol{W}^{AF}(A)+\sum_{m=1}^{M}\chi_{m,2}\Phi\boldsymbol{H}_m^{AF}(B)=0$$

这显然不成立，故 $\kappa_3=0$。

接下来，重写式(24(a))如下：

$$\boldsymbol{\Pi}^{AF}=\boldsymbol{O}_\Pi^{AF}-\boldsymbol{W}^{AF}(A)-\kappa_1\boldsymbol{W}^{AF}(B) \tag{25}$$

定义 $\boldsymbol{H}_M=[e_1^H,e_2^H,\cdots,e_M^H]$，并构建向量 x，且满足 $x=(\boldsymbol{I}-\boldsymbol{H}_M(\boldsymbol{H}_M^H\boldsymbol{H}_M)^\dagger\boldsymbol{H}_M^H)(f^T\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))\neq 0$。

对 $\forall m$，由于 $x^H\boldsymbol{H}_M=0$，可知 $x^He_m=0$。同样由于 $f^T\boldsymbol{D}(g)\boldsymbol{D}(L^{AF})\subset Range(e_1^H,e_2^H,\cdots,e_M^H)$，因此可以得到式(26)：

$$x^H(f^T\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))=(f^T\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))^H(\boldsymbol{I}-\boldsymbol{H}_M(\boldsymbol{H}_M^H\boldsymbol{H}_M)^\dagger\boldsymbol{H}_M^H)(f^T\boldsymbol{D}(g)\boldsymbol{D}(L^{AF}))>0 \tag{26}$$

由 $\boldsymbol{H}_m^{AF}(A)$ 及 $\boldsymbol{H}_m^{AF}(B)$ 的定义及 $x^He_m=0$ 可知，$x^H(\sum_{m=1}^{M}\chi_{m,1}\Phi\boldsymbol{H}_m^{AF}(A)+\sum_{m=1}^{M}\chi_{m,2}\Phi\boldsymbol{H}_m^{AF}(B))x=0$。

因此 $x^H\boldsymbol{O}_\Pi^{AF}x$ 可描述如下：

$$x^H(\kappa_3 I+\kappa_2 P_{tot}\boldsymbol{V}^{AF}(A)+\sum_{m=1}^{M}\chi_{m,1}\boldsymbol{X}_m^{AF}(A)+\sum_{m=1}^{M}\chi_{m,2}\boldsymbol{X}_m^{AF}(B)+\sum_{t=1}^{T}\chi_{u,t}\boldsymbol{Q}_t^{AF}+\kappa_1 P_{tot}\,\Psi\boldsymbol{V}^{AF}(B))x>0$$

这意味着 $\boldsymbol{O}_{\Pi}^{AF}\succ 0$，$\boldsymbol{O}_{\Pi}^{AF}$ 是个正定矩阵且 $Rank(\boldsymbol{O}_{\Pi}^{AF})=K$。

由式(25)、式(26)及 $\boldsymbol{W}^{AF}(A)$、$\boldsymbol{W}^{AF}(B)$ 的定义可知，$x^H\boldsymbol{\Pi}^{AF}x=x^H\boldsymbol{O}_{\Pi}^{AF}x-x^H(\boldsymbol{W}^{AF}(A)+\kappa_1\boldsymbol{W}^{AF}(B))x$。

上式表明 $Rank(\boldsymbol{\Pi}^{AF})\geqslant K-1$，同样式(24(b))表明 $Rank(\boldsymbol{\Pi}^{AF})+Rank(\overline{\boldsymbol{E}}^{AF})\leqslant K$，而 $Rank(\overline{\boldsymbol{E}}^{AF})=0$ 显然不成立，即 $Rank(\overline{\boldsymbol{E}}^{AF})=1$。

故 $Rank(\boldsymbol{E}^{AF})=\overline{\boldsymbol{E}}^{AF}/\xi^{AF}=1$。

4 仿真及性能分析

为证明功率分配方案的有效性，进行了实验仿真验证并分析结果。若不做特殊说明，则本系统包含 $M=2$ 个窃听节点，$T=2$ 个主用户节点以及 $K=10$ 个中继节点。方差、功率以及干扰温度均通过 dB 来标记，信道状态信息 f_k，g_k，$u_{k,t}$，$e_{k,m}\sim\mathcal{CN}(0,0\text{dB})$ 且相互独立，δ_A^2，δ_B^2，δ_r^2，$\delta_{u,t}^2$，$\delta_{e,m}^2=0\text{dB}$，递增系数 μ 取 1.05。其中 $P_A=10\text{dB}$，$P_B=10\text{dB}$，$P_{tot}=10\text{dB}$，窃听信噪比及干扰温度的阈值 Φ 和 Γ 分别记为 0dB 和 0dB，Ψ 取 0.5。仿真结果取 1000 次独立蒙特卡洛实验的平均值。

首先，我们给出爬山算法下总能量效率随 SR 提供的总发射功率 P_{tot} 以及包含的中继节点数目 K 变化的关系曲线图。如图 2 所示，总能量效率随着认知中继簇提供的发射功率线性增加；随着中继节点的增加，系统分集增益急剧增大，在同等发射功率条件下，系统可以获得更高的能量效率，中继节点数及可提供的总发射功率决定了网络的性能。

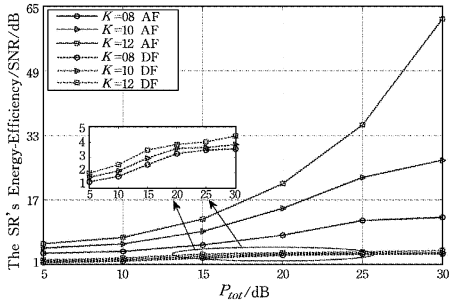

图 2 总能量效率随中继节点数目与中继簇提供的最大总发射功率变化的性能曲线

之后，我们研究了能量效率受干扰温度阈值 Γ 及网络中所存在的主用户节点个数 T 这两个因素影响的情况。如图 3 所示，在主用户具有较强抗干扰的背景下，干扰温度的约束不是影响系统性能的主要瓶颈，系统的总能量效率大幅增加；而随着主用户节点数目的增加，该功率分配方案设计过程中需要满足更多关于干扰温度的约束条件，需要牺牲一定的系统性能来保证系统的低干扰性。

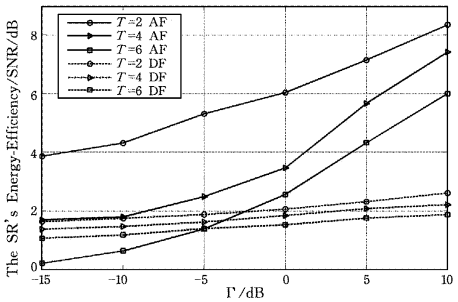

图 3 总能量效率随主用户节点数目及不影响其性能的干扰温度阈值的变化曲线

我们还给出了窃听容忍阈值 Φ 以及窃听节点数 M 对系统性能的影响。仿真结果如图 4 所示，随着对窃听可容忍程度的增加，物理层安全约束易得到保证，总能量效率随之增加。且在存在相同窃听容忍阈值 Φ 时，更多的窃听节点导致窃听能力增强，更多功率用于发射人工噪声，系统性能随之下降。

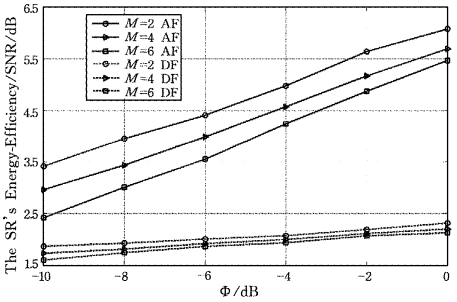

图 4 总能量效率随窃听节点数目及系统可容忍的最大窃听阈值的变化曲线

最后，从图 2—图 4 中可以看出，相对于采用 DF 中继策略，选择 AF 中继策略可以一定程度上利用传输过程中信号的衰落与白噪声干扰来干扰窃听者，可以更从容地设置加权向量及人工噪声矩阵，极大地提高系统的总能量效率。

结束语 本文研究了同时同频全双工认知中继网络中的一种可实现防窃听的安全技术——物理层安全。提出了一种能量高效的功率分配方案，不仅保证了主用户的通信性能，还实现了信号的安全传输。中继簇采用协作波速成形及人工噪声技术，设计了一种结合半定松弛方法的爬山算法来求解功率分配问题的数学表达。仿真结果和理论分析显示了该方案的有效性和合理性，此外方案表明基于 AF 中继策略能够使能量更加高效。

参 考 文 献

[1] CHEN Y, ZHANG S, XU S, et al. Fundamental trade-offs on green wireless networks[J]. IEEE Communications Magazine, 2011, 49(6): 30-37.

[2] NOSRATINIA A, HUNTER T E, Hedayat A. Cooperative communication in wireless networks[J]. IEEE Communications Magazine, 2004, 42(10): 74-80.

[3] HAYKIN S. Cognitive radio: brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(2): 201-220.

[4] ZHANG D D, WANG X, ZHANG Z S. Key techniques research on full duplex wireless communications[J]. Science in China Series F: Information Science, 2014, 44(8): 951-964. (in Chinese)
张丹丹，王兴，张中山. 全双工通信关键技术研究[J]. 中国科学：信息科学，2014，44(8)：951-964.

[5] COVER T, GAMAL A E L. Capacity theorems for the relay channel[J]. IEEE Transactions on Information Theory, 1979, 25(5): 572-584.

[6] WANG Q H, WANG H M, YIN Q Y. Distributed beamforming for multi-relay cognitive radio systems[J]. Science in China Series F: Information Sciences, 2014, 44(8): 980-992. (in Chinese)
王群欢，王慧明，殷勤业. 认知无线电系统中的多中继分布式波束成形方法[J]. 中国科学：信息科学，2014，44(8)：980-992.

[7] LI Y,SUN L,ZHAO C,et al. A digital self-interference cancellation algorithm based on spectral estimation in co-time co-frequency full duplex system[C]// 2015 10th International Conference on Computer Science & Education (ICCSE). IEEE,2015:412-415.

[8] MUKHERJEE A,FAKOORIAN S A A,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.

[9] LI L,HUANG C,CHEN Z. Cooperative secrecy beamforming in wiretap interference channels[J]. IEEE Signal Processing Letters,2015,22(12):2435-2439.

[10] GOEL S,NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications,2008,7(6):2180-2189.

[11] CHEN J,ZHANG R,SONG L,et al. Joint relay and jammer selection for secure decode-and-forward two-way relay networks[C]// IEEE International Conference Proc. of communications (ICC). 2011.

[12] CHEN J,ZHANG R,SONG L,et al. Joint relay and jammer selection for secure two-way relay networks[J]. IEEE Transactions on Information Forensics and Security,2012,7(1):310-320.

[13] FRAGKIADAKIS A G,TRAGOS E Z,ASKOXYLAKIS I G. A survey on security threats and detection techniques in cognitive radio networks[J]. IEEE Communications Surveys & Tutorials,2013,15(1):428-445.

[14] PEI Y,LIANG Y C,ZHANG L,et al. Secure communication over MISO cognitive radio channels[J]. IEEE Transactions on Wireless Communications,2010,9(4):1494-1502.

[15] PEI Y,LIANG Y C,TEH K C,et al. Secure communication in multiantenna cognitive radio networks with imperfect channel state information[J]. IEEE Transactions on Signal Processing,2011,59(4):1683-1693.

[16] WANG C,WANG H M. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels[J]. IEEE Transactions on Information Forensics and Security,2014,9(11):1814-1827.

[17] ALAVI F,SAEEDI H. Radio resource allocation to provide physical layer security in relay-assisted cognitive radio networks[J]. IET Communications,2015,9(17):2124-2130.

[18] ZOU Y,ZHU J,YANG L,et al. Securing physical-layer communications for cognitive radio networks[J]. IEEE Communications Magazine,2015,53(9):48-54.

[19] ZHU F,YAO M. Improving Physical-Layer Security for CRNs Using SINR-Based Cooperative Beamforming[J]. IEEE Transactions on Vehicular Technology,2016,65(3):1835-1841.

[20] LUO Z Q,MA W,SO A M C,et al. Semidefinite relaxation of quadratic optimization problems[J]. IEEE Signal Processing Magazine,2010,27(3):20.

[21] GRANT M,BOYD S,YE Y. CVX:Matlab software for disciplined convex programming[J]. Golbal Optimization,2008:155-210.

[22] SIDIROPOULOS N D,DAVIDSON T N,LUO Z Q. Transmit beamforming for physical-layer multicasting[J]. IEEE Transactions on Signal Processing,2006,54(6):2239-2251.

(上接第 171 页)

结束语　本文给出了快速寻找 MD4 算法有意义碰撞的通用方法,并给出了有意义碰撞的实例,为构造其他已经被破解的杂凑算法有意义的碰撞提供了思路。

参 考 文 献

[1] RIVEST R L. The MD 4 message-digest algorithm[C]// CPYPTO 1990. LNCS,1990:303-312.

[2] BOER B D,BOSSELAERS A. An attack on the last two rounds of MD4[C]//CRYPTO 1991. LNCS 576,1991:194-203.

[3] VAUDENAY S. On the need for multipermutations:Cryptanalsis of MD4 and SAFER[C]//FSE 1995. LNCS 1008,1995:286-297.

[4] DOBBERTIN H. Cryptanalysis of MD4[J]. Journal of Cryptology,1998,11(4):253-271.

[5] WANG X,FENG D,LAI X,et al. Collisions for hash functions MD4,MD5, HAVAL-128 and RIPEMD[OL]. http://eprint.iacr.org/2004/199.pdf.

[6] WANG X,YU H. How to break MD5 and other hash functions[C]//EUROCRYPT 2005,LNCS. 2005:19-35.

[7] WANG X,YIN Y L,YU H. Finding Collisions in the Full SHA-1[C] // International Cryptology Conference on Advances in Cryptology-CRYPTO. Springer-Verlag,2005:17-36.

[8] YU H B,WANG G L,ZHANG G Y,et al. The Second-Preimage Attack on MD4[C]//CANS 2005. LNCS 3810,2005:1-12.

[9] JIA K,WANG X. Meaningful Collision Attack on MD4[J]. Journal of Frontiers of Computer Science & Technology,2010,3:202-213.

[10] BAI D X. Safety analysis of some block cipher and hash function[D]. Beijing:Tsinghua University,2015. (in Chinese)
白东霞. 几个分组密码和杂凑函数的安全性分析[D]. 北京:清华大学,2015.

[11] LANDELLE F,PEYRIN T. Cryptanalysis of Full RIPEMD-128[J]. Journal of Cryptology,2015,7881:1-25.

[12] CHENG K,HAN W B. Automatic construction algorithm of MD4 differential path [J]. Journal of Information Engineering University,2014,15(2):129-133. (in Chinese)
程宽,韩文报. MD4 差分路径的自动化构造算法[J]. 信息工程大学学报,2014,15(2):129-133.

[13] WANG G L. Collision Attack on the Full Extended MD4 and Pseudo-Preimage Attack on RIPEMD[J]. Journal of Computer Science and Technology,2013,28(1):129-143.

[14] LI Q,TANG B,YANG J. Key Technology Research for Content Supervision Based on KAD Network[C]// International Conference on Multimedia & Image Processing. IEEE Computer Society,2016:72-77.