Journal of System Simulation

Volume 33 | Issue 1 Article 24

1-18-2021

Modeling and Simulation of Physical Layer Security Strategy in Two-Way Cognitive Networks

Pan Lei
1. State Key Lab of ISN, Xidian University, Xi'an 710071, China; ;2. Rocket Force University of Engineering, Xi'an 710025, China;

Li Zan
1. State Key Lab of ISN, Xidian University, Xi'an 710071, China; ;

Zhili Zhang
2. Rocket Force University of Engineering, Xi'an 710025, China;

Xiangyang Li
2. Rocket Force University of Engineering, Xi'an 710025, China;

Modeling and Simulation of Physical Layer Security Strategy in Two-Way Cognitive Networks

Abstract

Abstract: In order to improve the performance of the mobile communication system, *the physical layer security transmission models of a two-way cognitive relay network with the primary network and eavesdropper are established, and a joint optimization strategy for relay selection and power allocation is proposed* to protect the source-destination transmission against the eavesdropper. It can be seen from the simulation analysis that this non-convex optimization problem has many restrictions, and it is difficult to guarantee the feasibility of the initial solution generated randomly by the PSO algorithm, resulting in the difficulty of obtaining solution. Therefore, *a hybrid optimization algorithm based on variable mesh optimization (VMO) and particle swarm optimization (PSO) is proposed.* Simulation results show that this algorithm improves the security rate and performance of the secondary network.

Keywords

physical layer security, relay selection, power allocation, hybrid optimization, secrecy rate

第 33 卷第 1 期 系统仿真学报© Vol. 33 No. 1
2021 年 1 月 Journal of System Simulation Jan. 2021

双向认知网络物理层安全策略建模及仿真研究

潘蕾[1,2]，李赞[1]，张志利[2]，李向阳[2]
(1. 西安电子科技大学 综合业务网国家重点实验室，陕西 西安 710071；2. 火箭军工程大学，陕西 西安 710025)

摘要：为提高移动通信系统的性能，*构建了一个存在主网络干扰和窃听者的双向认知中继网络的物理层安全传输模型，设计了一种中继选择和功率分配的联合优化策略，*用于对抗窃听者，保护收发节点的信息传输。通过仿真分析得出，此非凸优化问题限制条件较多，难以保证粒子群优化算法随机生成的初始解的可行性，从而造成求解困难。*提出了一种基于可变网格优化和粒子群优化算法的混合优化算法。*仿真结果表明此算法提高了次级网络的保密速率，提升了次级网络的安全性能。

关键词：物理层安全；中继选择；功率分配；混合优化；保密速率
中图分类号：TN92 文献标志码：A 文章编号：1004-731X (2021) 01-0222-09
DOI: 10.16182/j.issn1004731x.joss.19-0179

Modeling and Simulation of Physical Layer Security Strategy in Two-Way Cognitive Networks

Pan Lei[1,2], *Li Zan*[1], *Zhang Zhili*[2], *Li Xiangyang*[2]
(1. State Key Lab of ISN, Xidian University, Xi'an 710071, China; 2. Rocket Force University of Engineering, Xi'an 710025, China)

Abstract: In order to improve the performance of the mobile communication system, *the physical layer security transmission models of a two-way cognitive relay network with the primary network and eavesdropper are established, and a joint optimization strategy for relay selection and power allocation is proposed* to protect the source-destination transmission against the eavesdropper. It can be seen from the simulation analysis that this non-convex optimization problem has many restrictions, and it is difficult to guarantee the feasibility of the initial solution generated randomly by the PSO algorithm, resulting in the difficulty of obtaining solution. Therefore, *a hybrid optimization algorithm based on variable mesh optimization (VMO) and particle swarm optimization (PSO) is proposed.* Simulation results show that this algorithm improves the security rate and performance of the secondary network.

Keywords: physical layer security; relay selection; power allocation; hybrid optimization; secrecy rate

引言

随着无线移动通信技术的飞速发展，人们对无线多媒体业务的需求不断增长。提高无线通信系统的信息传输速率和频谱利用率，扩大通信覆盖范围，提升安全可靠的传输性能，已成为无线通信领域的研究重点。协作中继技术应运而生[1-3]，在多用户通信网络中，每个单天线用户终端之间通过相互协作，共享彼此天线来实现信息的传输。与非协作终端相比，协作终端可以获得更高的空间分集增益，能够对抗信道衰落、扩大通信覆盖范围、提升无线链路通信质量及提高信息传输速率，比较容易在现有的单天线移动通信系统中实现，因此，被认为是第 5 代移动通信系统(5G)的关键技术之一。

随着各种新无线业务的不断涌现，更多的频谱资源被消耗，可用的频谱资源已经非常紧缺。而固定分配的授权频谱资源利用率较低，大量宝贵的授权频谱得不到充分的利用。根据美国联邦通信委员

收稿日期：2019-04-24 修回日期：2019-05-09
作者简介：潘蕾(1980-)，女，博士生，副教授，研究方向为协作通信技术等。E-mail：pl_528@163.com

会的调查[4]显示，在实际无线通信环境中，无线频谱资源利用率只有 15%~85%。造成了可用频谱资源匮乏和频谱资源利用率过低之间的矛盾。认知无线电技术(Cognitive Radio，CR)[5-7]已成为解决这一矛盾的有效途径。CR 是一种动态频谱接入技术，认知用户(次级用户)可以在不干扰主网络用户正常通信的情况下，通过频谱感知技术与主网络用户共享授权的频谱资源。大幅提高系统的频谱利用率，有效缓解频谱资源紧缺的问题。但是，认知无线电通信本身会受到功率限制、阴影效应、多径衰落等因素的影响，而导致通信性能的恶化。协作中继技术可以有效地对抗信道衰落，提升系统性能。因此，将认知无线电技术巧妙的应用到协作通信领域中，形成的认知协作中继技术[8-10]可有效克服认知无线电系统的弊端，充分发挥协作通信的优势，进一步提高系统的频谱利用率、提升系统性能，已受到国内外研究学者的广泛关注。

协作中继技术通过网络中多个用户共享彼此天线进行信息传输，而认知协作中继技术允许非授权用户与授权用户共享频谱资源，这些都使得协作网络更容易受到窃听者的恶意窃听，信息安全受到很大的威胁。为了提高认知中继网络的安全性，学者们都普遍认为物理层安全技术[11-12]是一种有效的解决方案。它是利用无线信道的物理特征来构建无线通信的安全信道，从而阻止窃听者通过非法接收窃取信息。Wyner 等[13]提出了窃听信道的数学模型，定义了物理层安全意义下窃听信道的保密速率，即在保证窃听者无法窃取信息的情况下，发送端到合法接收端之间的最大信息传输速率。

本文针对双向认知中继网络构建了基于物理层安全的安全传输模型，提出了一种中继选择和功率分配的联合优化策略，用以对抗窃听者及信道衰落、提高次级网络的保密速率，从而提升系统的安全性能。然而，通过仿真分析可知这是一个非凸优化的问题，很难得到解析解。基于此，提出了一种基于可变网格优化(Variable Mesh Optimization，VMO)和粒子群优化(Particle Swarm Optimization，PSO)相结合的混合优化算法，提升了次级网络的安全传输性能。

1 系统模型

如图 1 所示，该系统由一个主网络(primary network)、一个次级网络(secondary network)和一个窃听者 E 构成。其中，主网络包括一个主用户发送节点 U 和一个主用户接收节点 V。次级网络包括 2 个收发源节点(S_1, S_2)和 L 个协作中继节点(R_1, R_2, …, R_L)。假设所有节点只配备单根天线，通过半双工模式传输信息，次级网络用户可以共享主网络用户的频谱资源。为了不影响主网络用户的正常通信，要求次级网络用户传输时，对主网络用户的干扰必须低于干扰门限。由于障碍物和路径损耗等因素的影响，次级网络中 2 个源节点 S_1 和 S_2 之间没有直达路径，必须借助于中继节点实现双向通信。而源节点 S_1 和 S_2 之间的双向信息传输过程需要通过 2 个时隙来完成。不失一般性，假设所有的数据链路、干扰链路和窃听链路均相互独立、服从平坦瑞利衰落、信道特性具有互易性，且窃听者 E 可以窃听到所有节点的信息。中继节点采用放大转发(Amplify and Forward，AF)协议处理其接收到的信号。

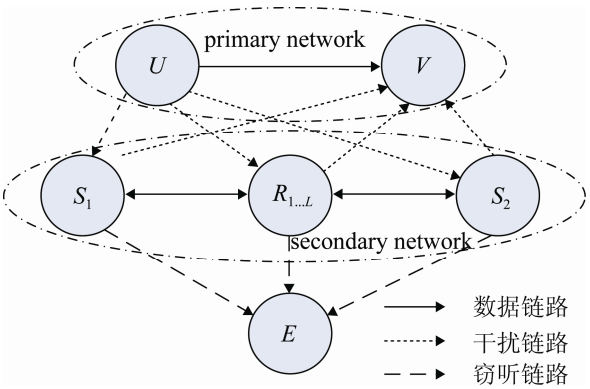

图 1 双向认知中继系统模型
Fig. 1 Two-way cognitive relay system model

在第 1 个时隙内，次级网络中的 S_1 和 S_2 节点分别广播其信号 x_1 和 x_2 到所有备选的中继节点。而主网络中的 U 节点发送信息 x_0 到 V 节点。假设

第 33 卷第 1 期 系统仿真学报 Vol. 33 No. 1
2021 年 1 月 Journal of System Simulation Jan. 2021

$E[|x_0|^2]=E[|x_1|^2]=E[|x_2|^2]=1$，其中 $E[\cdot]$表示数学期望，$|\cdot|$表示复数的模。在此阶段，窃听者可以监听到 S_1 和 S_2 节点发送的信息，则次级网络中的中继节点和窃听者的接收信号分别为

$$y_{R_i}=\sqrt{P_{1,i}}h_{S_1R_i}x_1+\sqrt{P_{2,i}}h_{S_2R_i}x_2+\sqrt{P_U}g_{UR_i}x_0+\mu_i,1\leqslant i\leqslant L \tag{1}$$

$$y_{E_1}=\sqrt{P_{1,i}}g_{S_1E}x_1+\sqrt{P_{2,i}}g_{S_2E}x_2+n_{E_1},\quad 1\leqslant i\leqslant L \tag{2}$$

式中：P_U，$P_{1,i}$ 和 $P_{2,i}$ 分别为主网络发送节点 U，次级网络源节点 S_1 和 S_2 的发送功率；$h_{S_1R_i}$ 和 $h_{S_2R_i}$ 分别表示次级网络中源节点 S_1 和 S_2 到中继节点 R_i 的信道衰落系数；g_{UR_i} 为主网络发送节点 U 到次级网络中继节点 R_i 的信道衰落系数；g_{S_1E} 和 g_{S_2E} 分别为次级网络中源节点 S_1 和 S_2 到窃听者 E 的信道衰落系数；μ_i 和 n_{E_1} 分别为在中继节点 R_i 和窃听者 E 处服从均值为 0、方差分别为 $\sigma_{\mu_i}^2$ 和 $\sigma_{E_1}^2$ 的加性高斯白噪声。从式(2)可以得到，窃听者 E 所接收到的对应于源节点 S_1 和 S_2 的接收信干比分别为

$$SINR_{E_{11}}=\frac{P_{1,i}\left|g_{S_1E}\right|^2}{P_{2,i}\left|g_{S_2E}\right|^2+\sigma_{E_1}^2} \tag{3}$$

$$SINR_{E_{12}}=\frac{P_{2,i}\left|g_{S_2E}\right|^2}{P_{1,i}\left|g_{S_1E}\right|^2+\sigma_{E_1}^2} \tag{4}$$

在第 2 个时隙中，次级网络中的中继节点采用 AF 协议转发信息，即把在第 1 个时隙接收到的信号直接放大，然后发送至源节点 S_1 和 S_2。此时，窃听者 E 也接收到了此信号。则相应的源节点 S_1，S_2 和窃听者 E 的接收信号分别为

$$y_1=\sqrt{P_{1,i}}\omega_ih_{S_1R_i}h_{S_1R_i}x_1+\sqrt{P_{2,i}}\omega_ih_{S_1R_i}h_{S_2R_i}x_2+\sqrt{P_U}\omega_ih_{S_1R_i}g_{UR_i}x_0+\sqrt{P_U}g_{US_1}x_0+\omega_ih_{S_1R_i}\mu_i+n_1,\quad 1\leqslant i\leqslant L \tag{5}$$

$$y_2=\sqrt{P_{1,i}}\omega_ih_{S_2R_i}h_{S_1R_i}x_1+\sqrt{P_{2,i}}\omega_ih_{S_2R_i}h_{S_2R_i}x_2+\sqrt{P_U}\omega_ih_{S_2R_i}g_{UR_i}x_0+\sqrt{P_U}g_{US_2}x_0+\omega_ih_{S_2R_i}\mu_i+n_2,\quad 1\leqslant i\leqslant L \tag{6}$$

$$y_{E_2}=\sqrt{P_{1,i}}\omega_ig_{R_iE}h_{S_1R_i}x_1+\sqrt{P_{2,i}}\omega_ig_{R_iE}h_{S_2R_i}x_2+\sqrt{P_U}\omega_ig_{R_iE}g_{UR_i}x_0+\omega_ig_{R_iE}\mu_i+n_{E_2},1\leqslant i\leqslant L \tag{7}$$

式中：ω_i 为放大增益因子；g_{US_1} 和 g_{US_2} 分别为主网络发送节点 U 到源节点 S_1 和 S_2 的信道衰落系数；g_{R_iE} 为中继节点 R_i 到窃听者 E 的信道衰落系数；n_1，n_2 和 n_{E_2} 分别为在源节点 S_1，S_2 和窃听者 E 处服从均值为 0、方差分别为 $\sigma_{n_1}^2$，$\sigma_{n_2}^2$ 和 $\sigma_{E_2}^2$ 的加性高斯白噪声。

从式(5)~(6)可以看出，其第 3 项和第 4 项为主网络用户对次级网络用户的干扰。而式(5)的第一项和式(6)的第二项为相应源节点 S_1 和 S_2 的自干扰，因此可以在相应节点处将其消除，此时源节点 S_1 和 S_2 的接收信号分别变为

$$y_1'=\underbrace{\sqrt{P_{2,i}}\omega_ih_{S_1R_i}h_{S_2R_i}x_2}_{\text{信号}}+\underbrace{\sqrt{P_U}\omega_ih_{S_1R_i}g_{UR_i}x_0+\sqrt{P_U}g_{US_1}x_0}_{\text{主网络干扰}}+\underbrace{\omega_ih_{S_1R_i}\mu_i+n_1}_{\text{噪声}},\quad 1\leqslant i\leqslant L \tag{8}$$

$$y_2'=\underbrace{\sqrt{P_{1,i}}\omega_ih_{S_2R_i}h_{S_1R_i}x_1}_{\text{信号}}+\underbrace{\sqrt{P_U}\omega_ih_{S_2R_i}g_{UR_i}x_0+\sqrt{P_U}g_{US_2}x_0}_{\text{主网络干扰}}+\underbrace{\omega_ih_{S_2R_i}\mu_i+n_2}_{\text{噪声}},\quad 1\leqslant i\leqslant L \tag{9}$$

通过式(8)~(9)可以得到源节点 S_1 和 S_2 的信干比分别为

$$SINR_{1,i}=\frac{P_{2,i}\left|\omega_i\right|^2\left|h_{S_1R_i}\right|^2\left|h_{S_2R_i}\right|^2}{X_i} \tag{10}$$

$$SINR_{2,i}=\frac{P_{1,i}\left|\omega_i\right|^2\left|h_{S_1R_i}\right|^2\left|h_{S_2R_i}\right|^2}{Y_i} \tag{11}$$

其中，

$$X_i=P_U\left|\omega_i\right|^2\left|h_{S_1R_i}\right|^2\left|g_{UR_i}\right|^2+P_U\left|g_{US_1}\right|^2+\sigma_{\mu_i}^2\left|\omega_i\right|^2\left|h_{S_1R_i}\right|^2+\sigma_{n_1}^2,$$

$$Y_i = P_U |\omega_i|^2 |h_{S_2R_i}|^2 |g_{UR_i}|^2 + P_U |g_{US_2}|^2 + \sigma_{\mu_i}^2 |\omega_i|^2 |h_{S_2R_i}|^2 + \sigma_{n_2}^2。$$

同理，根据式(7)可以得到，窃听者 E 对应源节点 S_1 和 S_2 的接收信干比分别为

$$SINR_{E_{21}} = \frac{P_{1,i} |\omega_i|^2 |g_{R_iE}|^2 |h_{S_1R_i}|^2}{M_i} \tag{12}$$

$$SINR_{E_{22}} = \frac{P_{2,i} |\omega_i|^2 |g_{R_iE}|^2 |h_{S_2R_i}|^2}{N_i} \tag{13}$$

其中，

$$M_i = P_{2,i} |\omega_i|^2 |g_{R_iE}|^2 |h_{S_2R_i}|^2 + P_U |\omega_i|^2 |g_{R_iE}|^2 |g_{UR_i}|^2 + \sigma_{\mu_i}^2 |\omega_i|^2 |g_{R_iE}|^2 + \sigma_{E_2}^2,$$

$$N_i = P_{1,i} |\omega_i|^2 |g_{R_iE}|^2 |h_{S_1R_i}|^2 + P_U |\omega_i|^2 |g_{R_iE}|^2 |g_{UR_i}|^2 + \sigma_{\mu_i}^2 |\omega_i|^2 |g_{R_iE}|^2 + \sigma_{E_2}^2。$$

由于次级网络中的中继节点 R_i 的发送功率可表示为

$$P_{R_i} = E\{|\omega_i y_{R_i}|^2\} = P_{1,i} |\omega_i|^2 |h_{S_1R_i}|^2 + P_{2,i} |\omega_i|^2 |h_{S_2R_i}|^2 + P_U |\omega_i|^2 |g_{UR_i}|^2 + |\omega_i|^2 \sigma_{\mu_i}^2 \tag{14}$$

因此，可得

$$|\omega_i| = \frac{\sqrt{P_{R_i}}}{\sqrt{P_{1,i} |h_{S_1R_i}|^2 + P_{2,i} |h_{S_2R_i}|^2 + P_U |g_{UR_i}|^2 + \sigma_{\mu_i}^2}} \tag{15}$$

将其代入式(10)~(13)，可以得到 $SINR_{1,i}$，$SINR_{2,i}$，$SINR_{E_{21}}$ 和 $SINR_{E_{22}}$ 新的表达式。

此时，可以得到双向认知中继网络的保密速率[14]，即数据链路的信道容量与窃听链路的信道容量之差，其表达式为

$$R_{s_i} = \frac{1}{2}[\text{lb}(1+SINR_{1,i}) - \text{lb}(1+SINR_{E_1})]^+ + \frac{1}{2}[\text{lb}(1+SINR_{2,i}) - \text{lb}(1+SINR_{E_2})]^+ \tag{16}$$

式中：$SINR_{E_1} = SINR_{E_{12}} + SINR_{E_{22}}$，$SINR_{E_2} = SINR_{E_{11}} + SINR_{E_{21}}$，$[x]^+$为 $\max(x, 0)$。

另一方面，次级网络中的源节点 S_1，S_2 和中继节点 R_i 的发送功率将对主网络用户造成一定的干扰，其干扰分别为 $I_{1,i} = P_{1,i} |g_{S_1V}|^2$，$I_{2,i} = P_{2,i} |g_{S_2V}|^2$ 和 $I_{R_i} = P_{R_i} |g_{R_iV}|^2$。其中，$g_{S_1V}$，$g_{S_2V}$ 和 g_{R_iV} 分别表示次级网络中源节点 S_1，S_2 和中继节点 R_i 到主网络接收节点 V 的信道衰落系数。

2 基于混合优化的中继选择及功率分配问题建模及仿真分析

2.1 中继选择及功率分配联合优化策略

本文考虑了一种基于双向认知中继网络的中继选择和功率分配联合优化策略[15]，用于对抗窃听者。首先，以最大化次级网络保密速率为目标，得到最优功率分配方案。然后，根据最优功率分配结果选出最优中继节点。其表达式分别为

$$(P_{R_i}^*, P_{1,i}^*, P_{2,i}^*) = \arg \max_{P_{R_i}, P_{1,i}, P_{2,i}} R_{s_i}(P_{R_i}, P_{1,i}, P_{2,i}) \tag{17}$$

$$i^* = \arg \max_{i \in \{1,2,\cdots,L\}} R_{s_i}(P_{R_i}^*, P_{1,i}^*, P_{2,i}^*) \tag{18}$$

式中：$P_{1,i}^*$，$P_{2,i}^*$ 和 $P_{R_i}^*$ 分别为次级网络中 S_1，S_2 和 R_i 节点的最佳发射功率；i^*为所选出的最优中继节点的标号。

根据式(17)可以得出优化算法的目标函数为

$$\max_{P_{1,i}, P_{2,i}, P_{R_i}} [f(P)] = \max_{P_{1,i}, P_{2,i}, P_{R_i}} [R_{s_i}(P_{1,i}, P_{2,i}, P_{R_i})]$$

$$\text{subject to}: \begin{matrix} P_{1,i} + P_{2,i} + P_{R_i} \leqslant P_T \\ I_{1,i} + I_{2,i} \leqslant \theta, I_{R_i} \leqslant \theta \end{matrix} \tag{19}$$

$$\text{subject to}: \begin{matrix} P_{1,i} + P_{2,i} + P_{R_i} \leqslant P_T \\ I_{1,i} + I_{2,i} \leqslant \theta, I_{R_i} \leqslant \theta \end{matrix}$$

式中：$P = (P_{1,i}, P_{2,i}, P_{R_i})$；$P_T$ 为次级网络总发送功率的上限；θ 为次级网络用户传输时对主网络用户造成干扰的上限。

通过仿真分析得出，该问题不是一个凸优化问题。当 $P_{1,i} + P_{2,i} + P_{R_i} = P_T$，假设 P_T=30 dB，且所有节点的功率≥0 时，在不同的信道衰落系数条件下，得到目标函数随 $P_{1,i}$，$P_{2,i}$ 的变化而变化的图形，如图 2 所示，目标函数既不是凸函数，又不是凹函数，因而该问题不是一个凸优化问题，不适合用凸优化方法求解。因此，本文拟采用 PSO 算法来求解这一优化问题。

https://dc-china-simulation.researchcommons.org/journal/vol33/iss1/24
DOI: 10.16182/j.issn1004731x.joss.19-0179

第 33 卷第 1 期 系统仿真学报 Vol. 33 No. 1
2021 年 1 月 Journal of System Simulation Jan. 2021

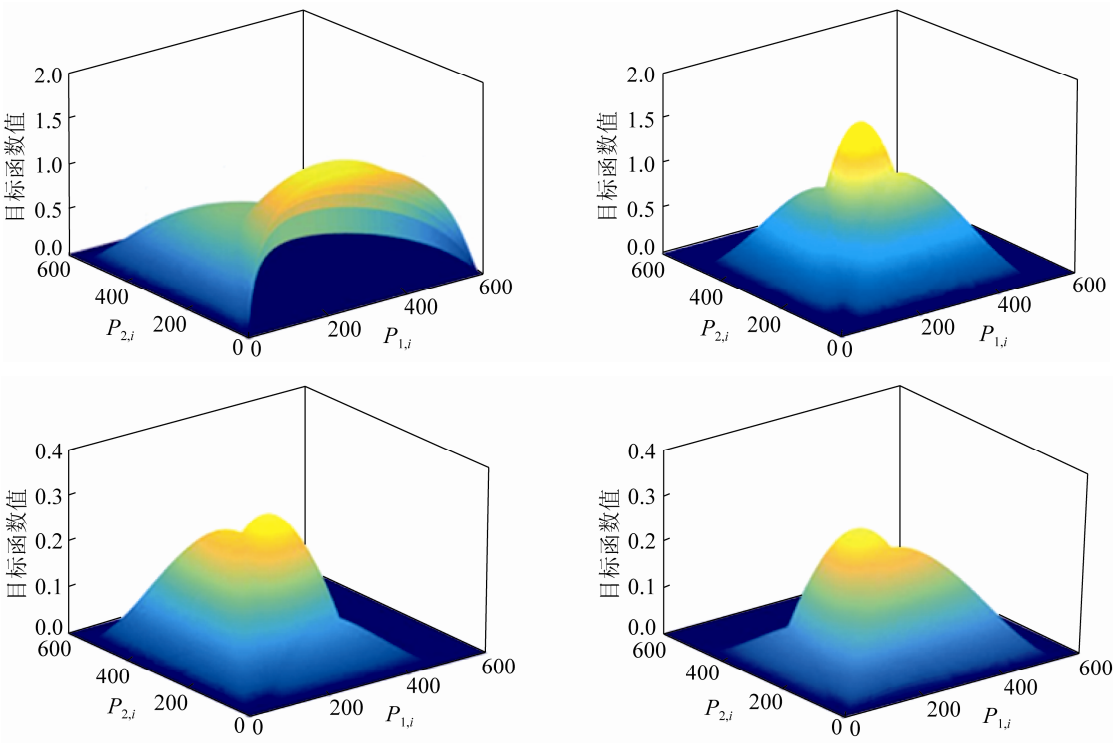

图 2 目标函数非凸优化证明

Fig. 2 Proof of objective function nonconvex optimization

进一步通过仿真分析得到 PSO 算法性能。仿真条件：种群中包括 30 个粒子(即潜在的可行解)，最大迭代次数为 50。通过各粒子之间的相互协作，每个粒子在解空间运动，并不断更新粒子的速度和位置来寻找全局最优解。双向认知协作中继网络利用 PSO 算法的功率分配结果，如表 1 所示。

表 1 直接利用 PSO 算法的功率分配结果

Tab. 1 Power distribution results of directly using PSO algorithm

序号	发送功率(1.0e+003)		
	源节点 S_1	源节点 S_2	中继节点
1	**–0.690 7**	**0.759 2**	**0.931 5**
2	**1.009 0**	**–0.549 5**	**0.540 5**
3	0.434 6	0.237 5	0.327 8
4	**1.387 3**	**–1.577 6**	**1.190 3**
5	0.388 6	0.263 5	0.347 8
6	**–0.173 3**	**1.096 3**	**0.077 1**
7	0.267 5	0.397 4	0.335 0
8	0.356 2	0.307 9	0.335 9
9	**–0.209 7**	**0.729 9**	**0.479 8**
10	**1.229 4**	**–1.069 7**	**0.840 3**

表 1 中总发送功率上限为 30 dB。通过表 1 的仿真结果可以看出，直接采用 PSO 算法求解此问题时，经常会出现粒子超出解空间范围，从而无法得到可行解的问题。这是因为优化问题本身限制条件较多，目标函数又相对比较复杂，而 PSO 算法的初始解是随机生成的，很难保证其可行性，即初始解不一定是可行解。因此，就可能造成求解失败。

2.2 基于 VMO 和 PSO 的混合优化

为了解决这一问题，提出了一种基于可变网格优化和粒子群优化的混合优化算法。首先，将解空间网格化，选取相对较大的网格步长，进行粗搜。若无法搜寻到可行解，则依次减小网格步长(一般采用将步长逐次减半的方式)，继续搜寻，直到获得一个初始的可行近似解；然后，以其为邻域中心，在邻域内产生 PSO 算法的初始种群；最后，利用 PSO 算法[16]获得最优可行解，如图 3 所示。

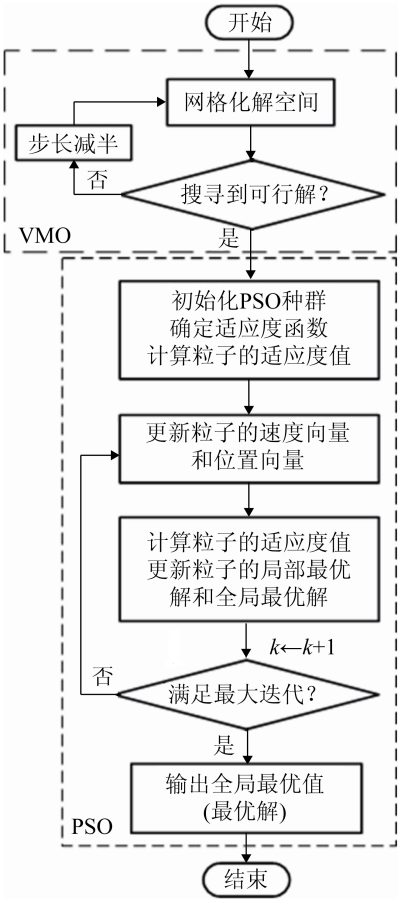

图 3 混合优化算法流程图

Fig. 3 Flowchart of hybrid optimization algorithm

具体步骤：

step 1：采用 VMO 算法确定最优可行解的邻域。首先，在区域 $Z=\{(P_{1,i},P_{2,i},P_{R_i})\big|P_{1,i}+P_{2,i}+P_{R_i}\leqslant P_T, P_{1,i}>0, P_{2,i}>0, P_{R_i}>0\}$ 内变间隔的划分网格，搜寻可行近似解。可变网格的步长确定方案如下：

(1) 假设初始步长为 $l=P_T/8$；

(2) 在区域 Z 内网格点处，依次判别约束条件 $I_{1,i}+I_{2,i}\leqslant\theta, I_{R_i}\leqslant\theta$ 是否满足？若满足，则为可行近似解；若不满足，则令 $l\leftarrow l/2$，返回(2)继续搜寻。

其次，比较所获得的可行近似解，得到最大近似解。

最后，将所得的解作为 PSO 算法初始化时的中心点。

step 2：在所得最大近似解的邻域内创建种群，并初始化该种群。以所得最大近似解为中心，假设初始半径为 $r=P_T/5$，在此范围内产生初始种群。在第一代种群中，j 粒子(j=1,2,…,n)的位置向量和速度向量分别为 $\boldsymbol{D}_j^{(0)}$ 和 $\boldsymbol{v}_j^{(0)}$。根据式(19)计算各粒子的适应度值，得到第一代种群的局部最优解 $L_j^{(0)}$ 和全局最优解 $G^{(0)}$。

step 3：更新各粒子的速度向量和位置向量。速度向量和位置向量更新公式分别为

$$\boldsymbol{v}_j^{(k+1)}=0.5\boldsymbol{v}_j^{(k)}+2r_1(L_j^{(k)}-\boldsymbol{D}_j^{(k)})+2r_2(G^{(k)}-\boldsymbol{D}_j^{(k)}) \tag{20}$$

$$\boldsymbol{D}_j^{(k+1)}=\boldsymbol{D}_j^{(k)}+\boldsymbol{v}_j^{(k)} \tag{21}$$

式中：$\boldsymbol{v}_j^{(k)}$，$\boldsymbol{D}_j^{(k)}$ 和 $L_j^{(k)}$ 分别为第 k 代种群中第 j 个粒子的速度向量、位置向量和局部最优解；$G^{(k)}$ 表示第 k 代种群的全局最优解；r_1 和 r_2 为介于[0, 1]之间相互独立的服从均匀分布的随机数。

step 4：更新局部最优解和全局最优解。通过式(19)计算各粒子的适应度值，从而更新局部最优解和全局最优解，其更新公式分别为：

$$L_j^{(k+1)}=\begin{cases}L_j^{(k)} & f(L_j^{(k)})\geqslant f(\boldsymbol{D}_j^{(k+1)})\\ \boldsymbol{D}_j^{(k+1)} & \text{other}\end{cases} \tag{22}$$

$$G^{(k+1)}=\begin{cases}G^{(k)} & f(G^{(k)})\geqslant\max\{f(L_j^{(k+1)})\big|j=1,2,\cdots,n\}\\ L_{j^*}^{(k+1)} & j^*=\arg\max\limits_{j\in\{1,2,\cdots,n\}}\{f(L_j^{(k+1)})\}\end{cases} \tag{23}$$

step 5：终止条件判定。判定优化结果是否达到最大迭代次数，若未达到，则返回 step 3；若达到，则终止程序，输出最优解，即为最优功率分配方案。根据式(18)选出最优中继节点。

3 双向认知中继网络物理层安全策略仿真结果及分析

本文使用 Matlab2010 进行仿真，仿真平台酷睿 i5-4590S CPU，内存 4 G。假设所有信道的瞬时信道状态信息是已知的，仿真参数设置如表 2 所示。仿真环境为瑞利分布的加性高斯白噪声信道，其均值为 0、方差为 1。

https://dc-china-simulation.researchcommons.org/journal/vol33/iss1/24
DOI: 10.16182/j.issn1004731x.joss.19-0179

表 2 仿真参数设置
Tab. 2 Simulation parameter setting

中继节点个数	粒子数目	最大迭代次数	主用户功率
L=10	n=30	m=50	P_U=5 dB

在图 4 中，将本文所提算法与其他 3 种不同算法进行比较，分析了次级网络的保密速率与备选中继节点数量之间的关系。

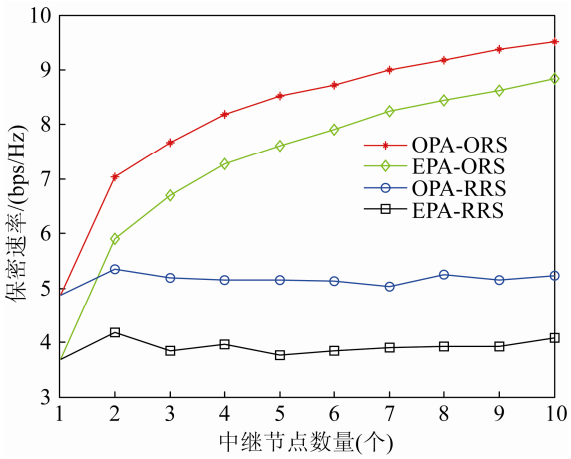

图 4 不同算法情况时保密速率与中继节点数量的关系
Fig. 4 Secrecy rate versus number of relays for different scheme

从图 4 可以看出本文所提的最优功率分配及中继选择(Optimal Power Allocation-Optimal Relay Selection，OPA-ORS)算法，保密速率最高($L\geqslant 2$)。在最优中继选择(ORS)情况下，随着备选中继数量的增加，次级网络的保密速率随之增大，且最优功率分配算法的保密速率高于等功率分配(Equal power allocation，EPA)算法。这是因为 EPA 不管信道状态如何变化，各节点的功率始终平均分配，这对于瞬时信道增益较高、信息传输量不大的信道来说，就会造成资源浪费，而 OPA 是根据信道状态信息的变化合理优化功率分配方案，从而提升了次级网络的保密速率。另一方面，从图 4 中还可以看出在随机中继选择(Random Relay Selection，RRS)情况下，随着备选中继数量的增加，次级网络的保密速率几乎不变。这是由于 RRS 算法是在所有备选中继中，随机挑选一个中继来实现信息转发的，分集增益并没有得到提高。而 ORS 则以最大化保密速率为目标，择优挑选中继节点，因此随着备选中继节点数量的增加，次级网络的空间分集增益将随之增大，从而提升了次级网络的系统性能。表 3 中分别给出了不同算法优化结果的对比数据。

表 3 不同算法优化结果对比
Tab. 3 Comparison of optimization results for different algorithms

中继节点个数	EPA-RRS	OPA-RRS	ERA-ORS	OPA-ORS
1	3.69	4.88	3.69	4.88
2	4.19	5.35	5.90	7.04
3	3.84	5.18	6.71	7.68
4	3.96	5.15	7.28	8.18
5	3.77	5.16	7.62	8.52

图 5 分析了在次级网络用户对主网络用户的干扰功率限制 θ=10 dB 和 θ=20 dB 情况下，次级网络的保密速率与主用户发送功率之间的对应关系。随着主用户发送功率的增大，次级网络的保密速率逐渐减小。这是由于在频谱共享环境下，当主用户发送功率变大时，其对次级网络中各节点的干扰将随之变大，这样会造成次级网络中各节点的信噪比下降，从而使得次级网络的保密速率变小。此外，还可以看出次级网络用户对主用户的干扰功率限制 θ 越大，次级网络的保密速率也越大。这是因为在认知中继网络中，当次级用户对主用户的干扰功率限制 θ 增大时，次级用户的发送功率就可以随之增大，从而提高了次级用户的发送信噪比，因此就增大了次级网络的保密速率。

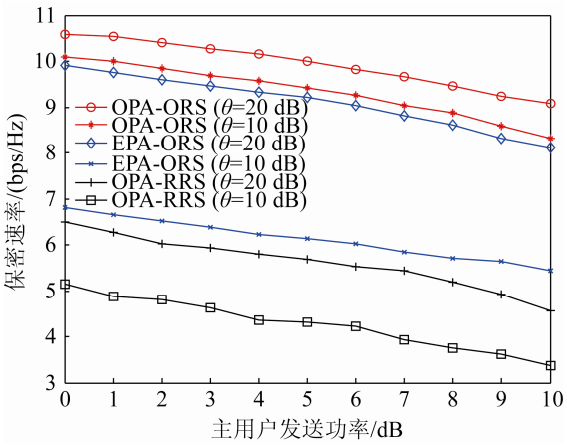

图 5 不同主网络干扰限制θ时保密速率与主用户发送功率的关系
Fig. 5 Secrecy rate versus transmit power of primary user for different interference limit θ of main network

图 6 给出了基于混合优化情况下，窃听者窃听范围不同时次级网络的保密速率与备选中继数量的对应关系。重点分析了以下 3 种情况：(1) 窃听者只能窃听到次级网络中所有中继节点的信息；(2) 窃听者可以窃听到次级网络中部分源节点和所有中继节点的信息；(3) 窃听者可以窃听到次级网络中所有节点的信息(本文所提算法)。从图 6 可以看出，当窃听者只能窃听到次级网络中所有中继节点的信息时，次级网络的保密速率最高、安全性相对最强；而当窃听范围扩大到能窃听到次级网络中部分源节点和所有中继节点的信息时，系统的保密速率随之降低；当窃听者进一步扩大窃听范围，能够窃听到次级网络中所有节点的信息时，系统的保密速率最低、安全性能最差。这是因为当窃听范围越大时，窃听者能够窃听到的信息就越多。这样就增大了窃听者的空间分集增益，从而造成系统安全传输的保密速率下降，次级网络的安全性能被降低。因此，在分析存在窃听者的物理层安全问题时，必须要考虑窃听者窃听的范围。为了缩小窃听者的窃听范围，移动通信系统可以在设备条件允许的情况下，采用定向天线去取代全向天线，从而提高系统的安全性能。

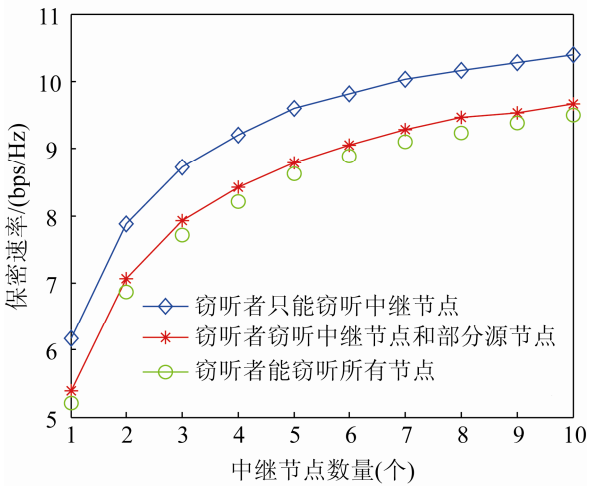

图 6 窃听者窃听不同范围情况下保密速率与中继节点数量的关系

Fig. 6 Secrecy rate versus number of relays for different eavesdropping area of eavesdropper

4 结论

本文研究了存在主网络用户干扰和窃听者窃听情况下的双向认知协作中继网络的物理层安全传输及中继选择和功率分配联合优化问题。通过仿真分析可以看出，此复杂的优化算法为非凸优化问题，且限制条件较多，难以保证 PSO 算法随机生成的初始解的可行性，从而造成求解困难。为此，本文提出了一种基于可变网格优化和粒子群优化相结合的混合优化算法。仿真结果表明此算法增大了系统的安全保密性，提升了系统的安全传输性能。然而，在本文的研究中，仅仅研究了存在单个主用户发射机、接收机及窃听者的双向认知中继网络模型。然而，在实际的网络环境中，通常存在多个主用户发射机、接收机及窃听者。因此，今后需要进一步研究存在多个主用户发射机干扰、次级用户对多个主用户接收机的干扰限制和多个窃听者窃听环境下的物理层安全问题。

参考文献：

[1] Kim Y G, Beaulieu N C. SEP of Decode-and-forward Cooperative Systems with Relay Selection in Nakagami-fading Channels[J]. IEEE Transactions on Vehicular Technology (S0018-9545), 2015, 64(5): 1882-1894.

[2] Sadek A K, Su W, Liu K J R. Multinode Cooperative Communications in Wireless Networks[J]. IEEE Transactions on Signal Processing (S1053-587X), 2007, 55(1): 341-355.

[3] Han Y, Pandharipande A, Ting S H. Cooperative decode-and-forward Relaying for Secondary Spectrum Access[J]. IEEE Transactions on Wireless Communications (S1536-1276), 2009, 8(10): 4945-4950.

[4] Force F S P T. Report of the Spectrum Efficiency Working group[R]. Spectrum Efficiency Working group, 2002.

[5] Mitola J, Maguire G Q. Cognitive Radio: Making Software Radios More Personal[J]. IEEE Personal Communications (S1070-9916), 1999, 6(4): 13-18.

[6] Vosoughi A, Cavallaro J R, Marshall A. Trust-Aware Consensus-Inspired Distributed Cooperative Spectrum Sensing for Cognitive Radio AD Hoc Networks[J]. IEEE Transactions on Cognitive Communications &

https://dc-china-simulation.researchcommons.org/journal/vol33/iss1/24
DOI: 10.16182/j.issn1004731x.joss.19-0179

第 33 卷第 1 期 系统仿真学报 Vol. 33 No. 1
2021 年 1 月 Journal of System Simulation Jan. 2021

Networking (S2332-7731), 2017, 2(1): 24-37.

[7] Xu D, Li Q. Resource Allocation for Cognitive Radio With Primary User Secrecy Outage Constraint[J]. IEEE Systems Journal (S1932-8184), 2016, 12(1): 893-904.

[8] Zou Y, Zhu J, Zheng B, et al. An Adaptive Cooperation Diversity Scheme With Best-Relay Selection in Cognitive Radio Networks[J]. IEEE Transactions on Signal Processing (S1053-587X), 2010, 58(10): 5438-5445.

[9] Jiang L, Tian H, Qin C, et al. Secure Beamforming in Wireless-Powered Cooperative Cognitive Radio Networks[J]. IEEE Communications Letters (S1089-7798), 2016, 20(3): 522-525.

[10] Bordon R, Sanchez S M, Mafra S B, et al. Energy Efficient Power Allocation Schemes for A Two-User Network-Coded Cooperative Cognitive Radio Network[J]. IEEE Transactions on Signal Processing (S1053-587X), 2016, 64(7): 1654-1667.

[11] Zou Y. Physical-Layer Security for Spectrum Sharing Systems[J]. IEEE Transactions on Wireless Communications (S1536-1276), 2017, 16(2): 1319-1329.

[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 (S1536-1276), 2016, 15(1): 329-340.

[13] Wyner A D. The Wire-Tap Channel[J]. The Bell System Technical Journal (S0005-8580), 1975, 54(8): 1355-1387.

[14] Alotaibi E R, Hamdi K A. Optimal Cooperative Relaying and Jamming for Secure Communication[J]. IEEE Wireless Communications Letters (S2162-2337), 2015, 4(6): 689-692.

[15] Li L, Zhou X, Xu H, et al. Simplified Relay Selection and Power Allocation in Cooperative Cognitive Radio Systems[J]. IEEE Transactions on Wireless Communications (S1536-1276), 2011, 10(1): 33-36.

[16] Javan M R, Mokari N, Alavi F, et al. Resource Allocation in Decode-and-Forward Cooperative Communication Networks With Limited Rate Feedback Channel[J]. IEEE Transactions on Vehicular Technology (S0018-9545), 2017, 66(1): 256-267.