无线自组织网络的联合安全路由选择和功率优化算法

惠 鏸* 张晓静

(西安理工大学自动化与信息工程学院 西安 710048)

摘 要：针对无线自组织网络在窃听环境中的安全传输问题，该文提出了一种无线多跳自组织网络的联合安全路由和功率优化算法。首先，在窃听者服从泊松簇过程(PCP)这一假设下推导得到了系统安全中断概率(SOP)和连接中断概率(COP)的表达式；然后以安全中断概率约束下的连接中断概率最小为准则，针对给定路径推导得到了源与各跳中继的最优传输功率，并进一步获得了源与目的节点间的最优路由。仿真结果表明，该文所提系统安全中断概率和连接中断概率的表达式与蒙特卡洛仿真结果相符，所提算法可获得与穷举搜索方法接近的安全性能，显著优于传统方法。

关键词：多跳自组织网络；泊松簇过程；安全路由；功率优化

中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2020)12-2923-08

DOI: 10.11999/JEIT190909

Joint Secure Routing and Power Optimization Algorithm for Wireless Ad Hoc Networks

HUI Hui ZHANG Xiaojing

(*School of Automation and Information Engineering, Xi'an University of Technology, Xi'an* 710048, *China*)

Abstract: A joint security routing and power optimization algorithm for wireless multi-hop Ad hoc network is proposed in an eavesdropping environment. Firstly, the Secrecy Outage Probability (SOP) and expressions of Connection Outage Probability (COP) are derived under the assumption that the distribution of the eavesdroppers follows the Poisson Cluster Process (PCP). Then, in view of minimizing COP with the constraint of SOP, the optimal transmission power of each hop is derived for any given path. Based on that, the optimal route from the source to the destination is obtained. The simulations on COP and SOP show that the derived theoretical results agree well with the Monte-Carlo simulations. It is also shown that the security performance of the proposed algorithm is close to that of exhaustive searching, and also outperforms the traditional method.

Key words: Multi-hop Ad hoc network; Poisson Cluster Process (PCP); Security routing; Power optimization

1 引言

近年来无线通信技术迅猛发展，各种新型网络形态不断涌现。其中无线自组织网络以无中心、自组织、无需基础设施等特点被广泛应用于军事、交通、救援等各领域[1]。但其自组织的部署特性使窃听节点的广泛存在成为可能，多跳传输的特点则带来更多的窃听机会。鉴于此，迫切需要对其传输安全性展开研究。

物理层安全技术通过利用无线信道的本质特征来保障信息的安全传输而成为近年来的研究热点。为提高系统安全性能，常采用多天线[2,3]、协作通信[4,5]、波束赋型[6,7]以及人工加噪[8,9]等手段。针对无线多跳自组织网络，除以上手段外还可以通过功率分配和路由选择来提高安全性能。文献[10]针对无线多跳自组织网络以保密速率最大化为目标提出了一种路由选择方案。文献[11]在给定路由的情况下研究了无线多跳网络的功率分配问题。文献[12]以安全中断概率(Secrecy Outage Probability, SOP)和连接中断概率(Connection Outage Probability, COP)为性能指标，考虑了网络安全性和服务质量之间的权衡。

收稿日期：2019-11-13；改回日期：2020-06-07；网络出版：2020-07-17
*通信作者： 惠鏸 huihui@xaut.edu.cn
基金项目：国家重点研发计划(2018YFB1201500)，国家自然科学基金(61873201)，陕西省教育厅科学基金(19JS051)

Foundation Items: The National Key R&D Program of China (2018YFB1201500), The National Natural Science Foundation of China(61873201), The Science Foundation of Shaanxi Provincial Education Department (19JS051)

上述研究均假设已知合法和窃听节点的信道状态信息，而在实际情况中窃听节点的相关信息往往很难获得。针对该情况，文献[13]将窃听者建模为PPP(Poisson Point Process)分布，研究了无线多跳自组织网络保密速率最大化的安全路由方案。文献[14]在窃听者服从PPP分布的前提下研究了无线多中继网络的安全路由和功率优化问题。然而由于地理等因素的影响，节点可能是聚类的，例如移动用户常聚集在人口密集的城市周围，或者窃听节点虽服从PPP分布，但参与窃听活动的节点子集却不是均匀分布的。为此，文献[15]提出使用泊松簇过程(Poisson Cluster Process, PCP)对窃听者的位置进行建模。文献[16]将窃听者建模为PCP分布，研究了无线多跳自组织网络中安全连接概率最大化的安全路由选择问题，但未考虑系统的可靠性，亦未讨论功率分配对系统性能的影响。总体而言，目前对于窃听者服从PCP分布的无线自组织网络安全传输的研究尚处于初期阶段，很多问题有待解决。

本文在上述工作的基础上提出了一种面向物理层安全的联合功率优化和路由选择算法，其创新之处在于：首先，采用了与实际情况更为吻合的泊松簇过程对窃听者的位置进行建模；其次，综合考虑了系统传输的安全性和可靠性，在安全中断概率满足给定阈值的条件下使连接中断概率达到最小；最终，将传输功率和安全路由进行联合优化设计，从而寻求最佳的解决方案。

2 系统模型及性能指标

2.1 系统模型

考虑一个无线多跳自组织网络如图1所示。该网络包含1个源节点S、1个目的节点D、多个备选中继节点和多个窃听节点。假设所有节点均配备单根天线，在半双工模式下工作。网络中S和D通过$K-1$个中继节点的信息转发完成信息传输。将第k跳表示为$l_k(k=1,2,\cdots,K)$，则整个传输路径可表示为$\Pi=\{l_1,l_2,\cdots,l_K\}$。将第$l_k$跳的合法发送和接收节点分别表示为$T_k$和$R_k$，则$S$可表示为$T_1$，$D$可表示为$R_K$。将第$l_k$跳中$T_k-R_k$和$T_k-E_{n,i}$链路的信道衰落系数分别表示为$h_{T_k,R_k}$和$h_{T_k,E_{n,i}}$，假设其均服从均值为零、方差为1的复高斯分布。不失一般性，假设所有链路的接收端噪声为均值为零，方差为σ^2的加性高斯白噪声。

假设窃听者服从PCP分布，将第n个窃听者簇表示为$C_n(n=1,2,\cdots,N)$，其半径为r_{C_n}，将簇C_n中的窃听者表示为$E_{n,i}$，本文将分别针对父节点位置已知和未知两种情况展开研究。当父节点位置未知时，假设窃听者簇的父节点分布是一个密度为λ_{C_n}的齐次泊松点过程，用Φ_{C_n}表示，子节点则是以父节点为圆心，在半径为r_{C_n}的圆内均匀分布，在每个圆内平均产生N_{E_n}个点，因此窃听者的密度是$\lambda_{E_n}=\lambda_{C_n}N_{E_n}$，窃听者是在$r_{C_n}^2$上各向同性的泊松簇过程$\Phi_{E_n}$。当父节点位置已知时簇$C_n$是半径为$r_{C_n}$，平均数量为$N_{C_n}$的各向同性的泊松过程$\Phi_{C_n}$，窃听者簇的中心是已知的，本簇的窃听者在半径为$r_{C_n}$的圆内遵循均匀分布。窃听节点的概率密度函数可表示为$f(x_{E_{n,i}})=\dfrac{1}{\pi r_{C_n}^2},\left\|x_{E_{n,i}}\right\|\le r_{C_n}$。其中，$x_{E_{n,i}}$是父节点的坐标，$\|\cdot\|$代表欧氏范数。

2.2 性能指标

保密信息的传输分K跳完成，每一跳合法接收节点在接收信息的同时窃听节点也在窃听信息。为提高系统安全性，本文采用随机转发策略，并假设多个窃听者之间不能合作。在第k跳，节点R_k和$E_{n,i}$的接收信噪比分别为

$$\gamma_{R_k}=\frac{P_{T_k}|h_{T_k,R_k}|^2}{d_{T_k,R_k}^{\alpha}\sigma^2} \tag{1}$$

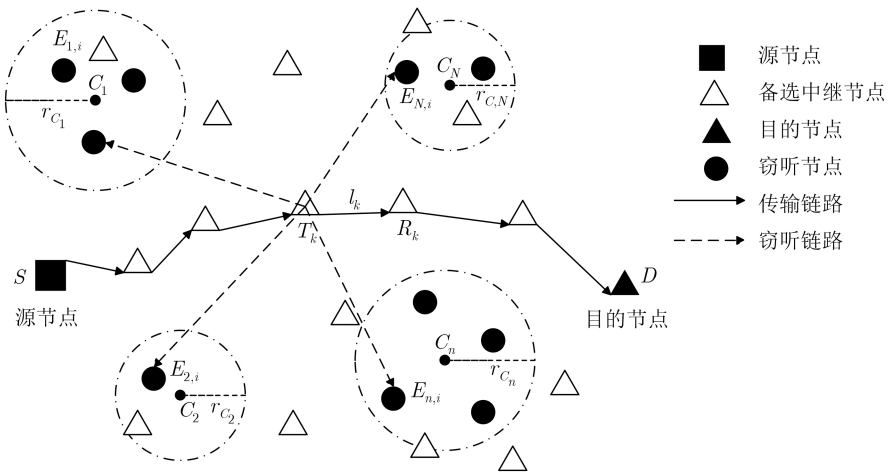

图 1 存在非均匀窃听者簇的无线自组织网络

$$\gamma_{T_k,E_{n,i}}=\frac{P_{T_k}|h_{T_k,E_{n,i}}|^2}{d^{\alpha}_{T_k,E_{n,i}}\sigma^2} \tag{2}$$

其中，P_{T_k}为第k跳节点T_k的发送功率，d_{T_k,R_k}和$d_{T_k,E_{n,i}}$为T_k-R_k和$T_k-E_{n,i}$之间的距离，α为路径损耗指数。

本文旨在研究如何在安全中断概率满足给定阈值的情况下使连接中断概率达到最小。将源节点到目的节点的所有可行路径的集合定义为S_{Π}，并将ζ定义为SOP的阈值，则该优化问题可以表示为

$$\min_{\Pi\in S_{\Pi},P_{T_k}} P_{\rm co}(\Pi) \tag{3}$$

$$\text{s.t. } P_{\rm so}(\Pi)\le\zeta \tag{4}$$

3　功率优化和路由选择算法

本节分别针对父节点位置未知和已知两种情况研究上述优化问题。

3.1　安全中断概率和连接中断概率

3.1.1　父节点位置未知

对于父节点位置未知的情况，根据安全中断概率的定义可得第l_k跳的SOP为

$$P^{(1)}_{\rm so}(l_k)=\Pr\left\{\max_{E_{n,i}\in\Phi_E}(\gamma_{T_k,E_{n,i}})>\gamma_{\rm e}\right\}=1-{\rm E}_{\Phi_C}\left\{\prod_{n=1}^{N}{\rm E}_{\Phi_E}\left[\prod_{E_{n,i}\in\Phi_E}\left[1-\exp\left(-\frac{\gamma_{\rm e}\sigma^2 d^{\alpha}_{T_k,E_{n,i}}}{P_{T_k}}\right)\right]\right]\right\} \tag{5}$$

其中，${\rm E}_{\Phi_E}[\cdot]$表示概率生成函数${\rm E}_{\Phi_E}\left[\prod_{E_n\in\Phi_E}f(x_{E_n})\right]=\exp\left[-\lambda_E\int_{R^2}1-f(x_{E_n}){\rm d}x_{E_n}\right]$。将其代入式(5)中可得

$$P^{(1)}_{\rm so}(l_k)=1-{\rm E}_{\Phi_C}\left\{\prod_{n=1}^{N}\exp\left[-N_E\int_{R^2}\exp\left(-\frac{\gamma_{\rm e}\sigma^2 d^{\alpha}_{T_k,E_{n,i}}}{P_{T_{\rm k}}}\right){\rm d}x_{E_{n,i}}\right]\right\} \tag{6}$$

式(6)可进一步转化为

$$P^{(1)}_{\rm so}(l_k)=1-{\rm E}_{\Phi_C}\left\{\prod_{n=1}^{N}\exp\left[-N_E(1-z(d_{T_k,E_{n,i}}))\right]\right\} \tag{7}$$

其中，

$$z(d_{T_k,E_{n,i}})=\int_{R^2}\left(1-\exp\left(-\frac{\gamma_e\sigma^2 d^{\alpha}_{T_k,E_{n,i}}}{P_{T_k}}\right)\right)f(x_{E_{n,i}}){\rm d}x_{E_{n,i}} \tag{8}$$

利用奈曼-斯科特(Neyman-Scott)簇过程[17] $M(z)=\exp(-N_E(1-z))$和概率生成函数，式(8)可转化为

$$P^{(1)}_{\rm so}(l_k)=1-\exp\left\{-\lambda_C\int_{R^2}[1-M(z)]{\rm d}x_C\right\} \tag{9}$$

式(9)进一步化简可得SOP的上界为

$$P^{(1)}_{\rm so}(l_k)\le 1-\exp\left[-\frac{\lambda_E 2\pi\Gamma(2/\alpha)}{\alpha}\left(\frac{\gamma_{\rm e}\sigma^2}{P_{T_k}}\right)^{-\frac{2}{\alpha}}\right] \tag{10}$$

其中，$\Gamma(\cdot)$为伽马函数。

令$v=\frac{2\pi\lambda_E}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\left(\gamma_{\rm e}\sigma^2\right)^{-\frac{2}{\alpha}}$，可得在父节点位置未知的情况下，整个路径的SOP为

$$P^{(1)}_{\rm so}(\Pi)=1-\prod_{l_k\in\Pi}(1-P^{(1)}_{\rm so}(l_k))\le 1-\exp\left(-v\sum_{l_k\in\Pi}(P_{T_k})^{2/\alpha}\right) \tag{11}$$

根据连接中断概率的定义，此时整个路径的COP为

$$P_{\rm co}(\Pi)=1-\prod_{l_k\in\Pi}\Pr(\gamma_{R_k}>\gamma_c)=1-\exp\left(-\sum_{l_k\in\Pi}\frac{\gamma_c\sigma^2 d^{\alpha}_{T_k,R_k}}{P_{T_k}}\right) \tag{12}$$

3.1.2　父节点位置已知

对于父节点位置已知的情况，可得第l_k跳的SOP为

$$P^{(2)}_{\rm so}(l_k)=\Pr\left\{\max_{n=1,2,\cdots,N}\max_{E_{n,i}\in\Phi_{C_n}}(\gamma_{T_k,E_{n,i}})>\gamma_{\rm e}\right\}=1-\prod_{n=1}^{N}\exp\left[-\frac{N_{C_n}}{\pi r^2_{C_n}}\int_0^{2\pi}\int_0^{r_{C_n}}\exp\left(-\frac{\gamma_{\rm e}\sigma^2 d^{\alpha}_{T_k,E_{n,i}}}{P_{T_k}}\right){\rm d}r{\rm d}\theta\right] \tag{13}$$

其中，$d_{T_k,E_{n,i}}$及该边的对角θ分别为$d_{T_k,E_{n,i}}=\sqrt{d^2_{T_k,C_n}+r^2-2\cos(\theta)rd_{T_k,C_n}}$和$\theta=\arccos\left(\frac{d^2_{T_k,C_n}+r^2-d^2_{T_k,E_{n,i}}}{2rd_{T_k,C_n}}\right)$。

利用中心逼近法假设所有窃听节点都位于其簇的中心位置，则SOP可近似为

$$P^{(2)}_{\rm so}(l_k)=1-\prod_{n=1}^{N}\exp\left[-N_{C_n}\exp\left(-\frac{\gamma_{\rm e}\sigma^2 d^{\alpha}_{T_k,C_n}}{P_{T_k}}\right)\right] \tag{14}$$

由此可得在父节点位置已知的情况下整个路径的SOP为

$$P^{(2)}_{\rm so}(\Pi)=1-\exp\left[-N_{C_{\rm n}}\sum_{l_k\in\Pi}\sum_{n=1}^{N}\exp\left(-\frac{\gamma_{\rm e}\sigma^2 d^{\alpha}_{T_k,C_n}}{P_{T_k}}\right)\right] \tag{15}$$

与父节点位置未知的情况类似，给定路径下父节点位置已知时整个路径连接中断概率的表达式如式(12)所示。

3.2 最优传输功率

下面将首先求解给定路径下源与各跳中继节点的最优传输功率，然后进一步求解最优安全路由。

3.2.1 父节点位置未知的最优传输功率

首先，在给定路径下，针对父节点位置未知的情况，原优化问题可转化为

$$\min_{P_{T_k}} P_{\mathrm{co}}(\boldsymbol{\Pi}) \tag{16}$$

$$\text{s.t. } P_{\mathrm{so}}^{(1)}(\boldsymbol{\Pi}) \le \zeta \tag{17}$$

将式(11)代入式(17)的不等式约束并进行简化，该约束可表示为

$$v\sum_{l_k\in\Pi}(P_{T_k})^{2/\alpha} \le \varepsilon = \ln\frac{1}{1-\zeta} \tag{18}$$

由式(12)可知连接中断概率是关于功率的递减函数，而式(18)是关于功率的递增函数，因此不等式取等号时连接中断概率达到最小，此时优化问题可以转化为

$$\begin{aligned}&\min_{t_k}\sum_{l_k\in\boldsymbol{\Pi}}\frac{\varphi_k}{t_k^{\alpha/2}}\\ &\text{s.t.}\quad \sum_{l_k\in\boldsymbol{\Pi}} vt_k = \varepsilon\end{aligned} \tag{19}$$

其中，$\varphi_k=\gamma_c d_{T_k,R_k}^{\alpha}\sigma^2$, $t_k=P_{T_k}^{2/\alpha}$。

利用拉格朗日乘数法，可得第l_k跳的最优传输功率为

$$P_{T_k}=\varphi_k^{\frac{\alpha}{\alpha+2}}\left[\frac{v}{\varepsilon}\sum_{l_k\in\Pi}\varphi_k^{\frac{2}{\alpha+2}}\right]^{-\frac{\alpha}{2}} \tag{20}$$

3.2.2 父节点位置已知的最优传输功率

类似地，在给定路径下，针对父节点位置已知的情况，原优化问题可转化为

$$\begin{aligned}&\min_{t_k}\sum_{l_k\in\boldsymbol{\Pi}}\varphi_k t_k\\ &\text{s.t.}\quad \sum_{l_k\in\boldsymbol{\Pi}}\sum_{n=1}^{N}\exp(-w_n t_k)=\varepsilon\end{aligned} \tag{21}$$

其中，$w_n=\gamma_e\sigma^2 d_{T_k,C_n}^{\alpha}$, $t_k=P_{T_k}^{-1}$, $\varepsilon=\dfrac{1}{N_{C_n}}\ln\dfrac{1}{1-\zeta}$。对该优化问题进行求解可得第$l_k$跳的最优传输功率为

$$P_{T_k}=\frac{\sum\limits_{l_k\in\boldsymbol{\Pi}}\sum\limits_{n=1}^{N}\varphi_k w_n}{\sum\limits_{n=1}^{N}\varphi_k-\varepsilon\varphi_k} \tag{22}$$

3.3 最优路由

3.3.1 父节点位置未知的最优路由

针对父节点位置未知的情况，将式(20)求得的最优传输功率代入式(12)中，可得安全路由问题为

$$\boldsymbol{\Pi}^*=\arg\min_{\boldsymbol{\Pi}\in S_{\boldsymbol{\Pi}}}\left\{1-\exp\left(-\left(\frac{v}{\varepsilon}\right)^{\frac{\alpha}{2}}\left(\sum_{l_k\in\boldsymbol{\Pi}}(\varphi_k)^{\frac{2}{2+\alpha}}\right)^{\frac{\alpha}{2}+1}\right)\right\} \tag{23}$$

该问题等价于

$$\boldsymbol{\Pi}^*=\arg\min_{\boldsymbol{\Pi}\in S_{\boldsymbol{\Pi}}}\sum_{l_k\in\boldsymbol{\Pi}}(\varphi_k)^{\frac{2}{2+\alpha}} \tag{24}$$

为获得最优路由$\boldsymbol{\Pi}^*$，将网络中任意两节点间的距离用$(\varphi_k)^{2/(2+\alpha)}$进行赋值，则该问题可通过Dijkstra算法求解。具体求解过程如表1所示。

3.3.2 父节点位置已知的最优路由

针对父节点位置已知的情况，将式(22)求得的最优传输功率代入式(12)中，该问题等价于

$$\boldsymbol{\Pi}^*=\arg\min_{\boldsymbol{\Pi}\in S_{\boldsymbol{\Pi}}}\sum_{l_k\in\boldsymbol{\Pi}}\sum_{n=1}^{N}\frac{\varphi_k}{w_n} \tag{25}$$

为寻找最佳路由，将备选中继节点集合表示为$\mathcal{M}$，其个数$|\mathcal{M}|=M$。不失一般性，将源节点、M个备选中继节点和目的节点依次编号为$1,2,\cdots,M+2$。建立矩阵$\boldsymbol{M}\in\mathbb{R}^{(M+2)\times(M+2)}$并将其第$i$行第$j$列元素用$\varphi_k\sum_{n=1}^{N}\dfrac{1}{w_n}=\dfrac{\gamma_c}{\gamma_e}d_{i,j}^{\alpha}\sum_{n=1}^{N}\dfrac{1}{d_{i,C_n}^{\alpha}}$赋值，由此可见，为获得最佳路由需要在$S-D$之间寻找一条路径，使得该路径上$\boldsymbol{M}(S,R_1)+\boldsymbol{M}(R_1,R_2)+\cdots+\boldsymbol{M}(R_{K-1},D)$的和最小。该最佳路由可通过遍历获得，但其计算复杂度较高，下面我们提出了一种简化算法：

初始状态下节点集合$\mathcal{R}$只包含S；接下来以$k=\arg\min(\boldsymbol{M}(S,R_k)+\boldsymbol{M}(R_k,D))$为目标，寻找$S-R_k-D$距离和最小的中继$R_k$加入集合$\mathcal{R}$；再以$\boldsymbol{M}(S,R_k)=\min\limits_{R_n,R_n\in\mathcal{M}}(\boldsymbol{M}(S,R_k),\boldsymbol{M}(S,R_n)+\boldsymbol{M}(R_n,R_k))$为依据，判断路径中是否存在其他备选中继使$S-R_k$的距离

表 1 父节点位置未知情况下的功率优化和路由选择算法

输入：信噪比阈值γ_c和γ_e，安全中断概率约束ζ；

输出：最优路由$\boldsymbol{\Pi}^*$，最优传输功率$P_{T_k}^*$；

(1) 计算$(\varphi_k)^{2/(2+\alpha)}$，并对传输距离进行赋值；

(2) 用Dijkstra算法获得最优路由$\boldsymbol{\Pi}^*$；

(3) 利用式(20)对最优路由上的各跳计算相应的最优传输功率$P_{T_k}^*$；

(4) 返回$\boldsymbol{\Pi}^*$, $P_{T_k}^*$。

缩短，若存在则将R_n加入集合$\mathcal{R}$，否则不变；重复上述操作，直到整条路由的距离不会因为纳入新的中继而减少时，遍历结束并得到最优路由Π^*。其具体过程如表2所示。

表1与2算法的计算复杂度等同于经典的Dijkstra算法，计算复杂度为$\mathcal{O}(M^2)$。因此父节点位置未知和已知两种情况下算法的计算复杂度都远低于穷举搜索$\mathcal{O}((M-2)!)$。

4　仿真验证

本节对系统性能进行了数值计算和蒙特卡罗仿真。与文献[12–14]类似，假设备选中继节点的个数为$M=10$，均匀地分布在20×20 m^{2}的正方形区域，给定阈值分别为$\gamma_c=0.8$ dB和$\gamma_e=0$ dB, $\sigma_n^2=1$, $\alpha=4$。

对于父节点位置未知的情况，与文献[16]仿真条件相同，假设所有簇具有相同的半径r和平均窃听者数量N_E。由图2可以看出，理论结果与仿真曲线相吻合，验证了文中推导结果的正确性。随着SOP给定阈值的增大COP减小，这说明通信服务质量的提高需要牺牲其传输安全性，反之亦然。还可看出随着M的增加COP减小，这是由于M增加意味着可以选取性能更好的节点作为中继加入路由，从而有效降低COP。

图3研究了窃听者密度λ_C和平均窃听者数量N_E的变化对系统性能的影响。从图3同样可以看出随着SOP给定阈值的增大COP减小。另外还可以

表 2　父节点位置已知情况下的功率优化和路由选择算法

输入：网络相关信息，信噪比阈值γ_c和γ_e，安全中断概率约束ζ；

输出：最优路由Π^*，最优传输功率$P_{T_k}^*$；

(1) 将网络中任意两合法节点间的距离赋值为φ_k，将各合法节点到各窃听者簇的距离用w_n进行赋值；

(2) 建立矩阵$\boldsymbol{M}\in\mathbb{R}^{(M+2)\times(M+2)}$，将矩阵$\boldsymbol{M}$的第$i$行第$j$列元素用$\dfrac{\gamma_c}{\gamma_e}d_{i,j}^{\alpha}\displaystyle\sum_{n=1}^{N}\frac{1}{d_{i,C_n}^{\alpha}}$进行赋值；

(3) 初始时，路由节点集合$\mathcal{R}=\{S\}$；

(4) 依据$k=\arg\min(\boldsymbol{M}(S,R_k)+\boldsymbol{M}(R_k,D))$寻找$S-R_k-D$距离最小的中继$R_k$，并将其加入集合$\mathcal{R}$；

(5) 依据$\boldsymbol{M}(S,R_k)=\min\limits_{R_n,R_n\in\mathcal{M}}(\boldsymbol{M}(S,R_k),\boldsymbol{M}(S,R_n)+\boldsymbol{M}(R_n,R_k))$判断是否存在其他备选中继节点使得距离缩短，若存在则将R_n加入集合$\mathcal{R}$，否则不变；

(6) 与步骤(5)类似，依次判断整条链路中每一跳是否存在其他备选中继节点使得该跳距离缩短，若存在则将该中继加入集合$\mathcal{R}$，否则不变；

(7) 重复步骤(6)，直到整条路由的距离不再减少时，遍历结束并得到最优路由Π^*；

(8) 利用式(22)对最优路由上的每一跳计算相应的最优传输功率$P_{T_k}^*$；

(9) 返回Π^*, $P_{T_k}^*$。

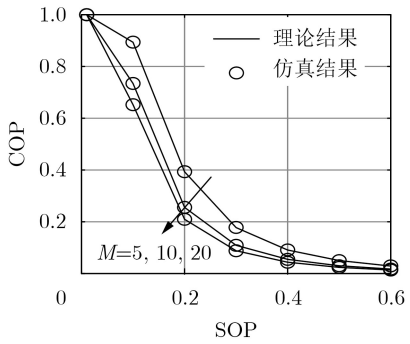

图 2 父节点位置未知下合法节点数量的变化

发现随着λ_C或N_E的增加COP增加。这是由于N_E的增加意味着单个窃听者具有良好信道条件的概率增加，那么保密信息被窃听的可能性就会增大。

对于父节点位置已知的情况，与文献[16]的仿真条件相同，假设3个窃听者簇的中心分别为$(-10,-30)$, $(10,-30)$和$(0,20)$，每个簇具有相同的半径。图4中的理论结果与仿真曲线相吻合，并且随着SOP给定阈值的增大COP减小，随着M的增加COP减小。由图5可以看出随着N_{C_n}的增加COP增加。

下面对不同路由选择算法的路由选择结果及其性能进行仿真。其中文献[16]在路由选择的过程中以安全连接概率最大化为目标，未考虑传输的可靠性及发送功率对系统性能的影响。穷举搜索算法可获得最佳的路由选择结果作为系统性能比较的依

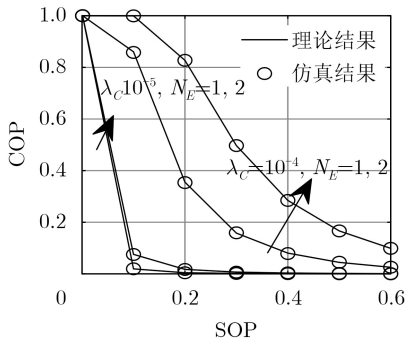

图 3 父节点位置未知下窃听者数量的变化

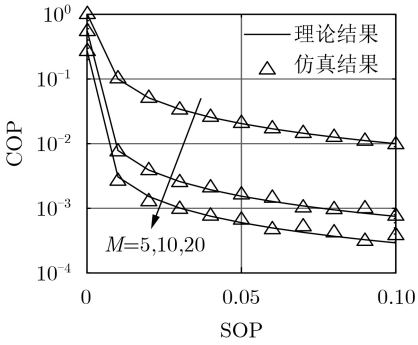

图 4 父节点位置已知下合法节点数量的变化

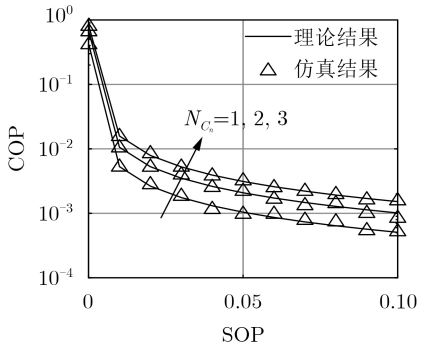

图 5 父节点位置已知下窃听者数量的变化

据。对于父节点位置未知的情况，不失一般性，假设$M=20$，均匀地分布在50×50 m^{2}的正方形区域，窃听者随机分布在2000×2000 m^{2}的正方形区域。

图6给出了父节点位置未知情况下的路由选择结果。由图7可以看出随着窃听者密度λ_E的增加SOP增加。由图8可以看出随着SNR的增加SOP减小。这两幅图均可得到本文在综合考虑无线自组织网络的安全性和可靠性的情况下进行的联合功率优化和路由选择算法，相比文献[16]只考虑安全性下进行的等功率分配的路由算法安全性能更优，且本文算法以显著低于穷举法的计算复杂度获得了与其近似的安全性能。

对于父节点位置已知的情况，与文献[16]的仿真条件相同，假设中继节点的个数$M=20$，均匀地分布在100×100 m^{2}的正方形区域。4个窃听者簇

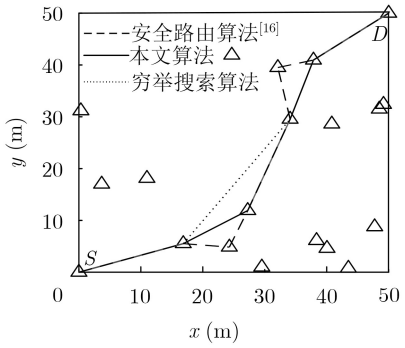

图 6 父节点位置未知下的路由选择算法

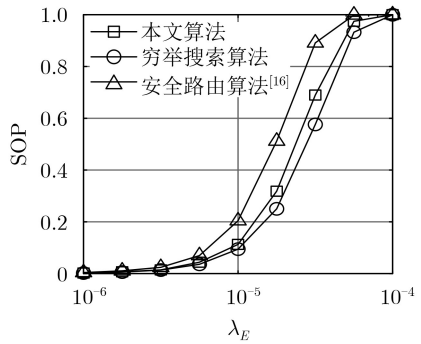

图 7 父节点位置未知下不同λ_E的SOP

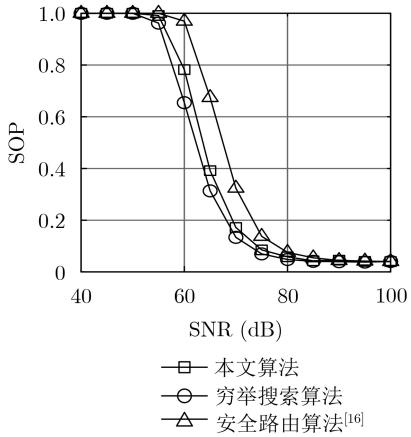

图 8 父节点位置未知下不同SNR的SOP

的中心位置分别在$(-30,-30)$, $(-20,30)$, $(10,-15)$和$(30,-5)$，其半径分别为$r_{C_1}=20$ m，$r_{C_2}=10$ m，$r_{C_3}=10$ m，$r_{C_4}=5$ m，各窃听者簇数量均为1。图9给出了不同路由选择算法的路由选择结果。图10和图11分别在不同λ_E和不同SNR下对不同路由选择算法的系统性能进行了仿真比较，可以看出本文提出的路由选择算法的安全性能优于安全路由算法[16]，并获得了与穷举搜索算法近似的安全性能。

5 结论

本文针对窃听者服从PCP分布的无线自组织网络提出了一种联合安全路由选择和功率优化算法。首先，针对窃听者分布服从泊松簇过程的场景进行了建模，并在该模型下推导得到了系统安全中断概率和连接中断概率的表达式。其次，综合考虑了系统传输的安全性和可靠性，提出了在安全中断概率约束下连接中断概率最小的优化问题。最后，将传输功率和安全路由进行联合优化设计，给出了在给定路径下源与各跳中继的最优传输功率，并进一步获得了源与目的节点间的最优路由。仿真结果表

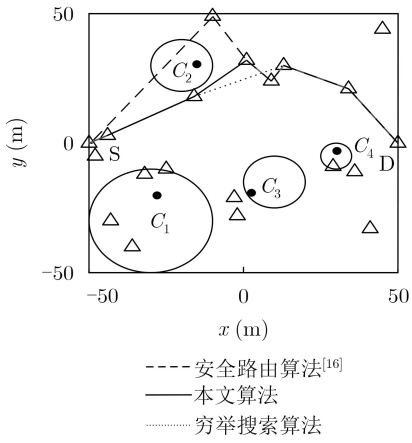

图 9 父节点位置已知下的路由选择结果

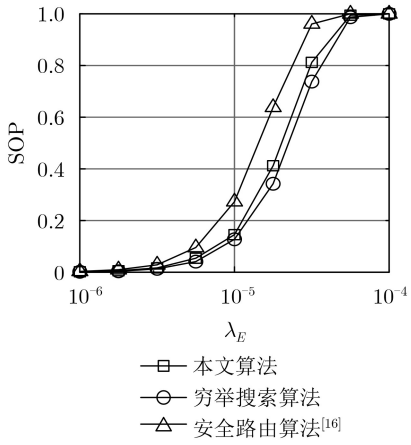

图 10 父节点位置已知下不同λ_E的SOP

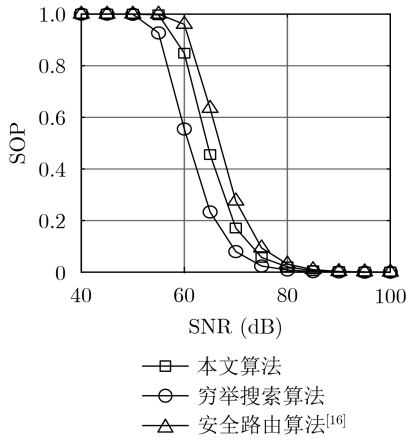

图 11 父节点位置已知下不同SNR的SOP

明，本文算法可获得与穷举搜索算法近似的安全性能，与传统方法相比可显著提高系统的安全性。

参 考 文 献

[1] BURMESTER M and YASINSAC A. Security Issues in Ad-Hoc Networks[M]. New York: Springer, 2008: 89–105.

[2] 金梁, 宋昊天, 钟州, 等. 多用户大规模MIMO自适应安全传输策略[J]. 电子与信息学报, 2018, 40(6): 1468–1475. doi: 10.11999/JEIT170974.

JIN Liang, SONG Haotian, ZHONG Zhou, *et al*. Adaptive secure transmission strategy for multiuser massive MIMO[J]. *Journal of Electronics & Information Technology*, 2018, 40(6): 1468–1475. doi: 10.11999/JEIT170974.

[3] YOU Li, WANG Jiaheng, WANG Wenjin, *et al*. Secure multicast transmission for massive MIMO with statistical channel state information[J]. *IEEE Signal Processing Letters*, 2019, 26(6): 803–807. doi: 10.1109/LSP.2019.2900940.

[4] LUN Dong, ZHU Han, PETROPULU A P, *et al*. Improving wireless physical layer security via cooperating relays[J]. *IEEE Transactions on Signal Processing*, 2010, 58(3): 1875–1888. doi: 10.1109/TSP.2009.2038412.

[5] CHRAITI M, GHRAYEB A, ASSI C, *et al*. On the Achievable secrecy diversity of cooperative networks with untrusted relays[J]. *IEEE Transactions on Communication*, 2018, 66(1): 39–53. doi: 10.1109/TCOMM.2017.2755654.

[6] YANG Zilong and DONG Min. Low-complexity coordinated relay beamforming design for multi-cluster relay interference networks[J]. *IEEE Transactions on Wireless Communications*, 2019, 18(4): 2215–2228. doi: 10.1109/TWC.2019.2901477.

[7] SHENG Zhichao, TUAN H D, DUONG T Q, *et al*. Beamforming optimization for physical layer security in MISO wireless networks[J]. *IEEE Transactions on Signal Processing*, 2018, 66(14): 3710–3723. doi: 10.1109/TSP.2018.2835406.

[8] 洪涛, 张更新. 人工噪声辅助的物理层安全信号峰均功率比减低算法[J]. 电子与信息学报, 2018, 40(6): 1426–1432. doi: 10.11999/JEIT170739.

HONG Tao and ZHANG Gengxin. Peak-to-average power ratio reduction algorithm of artificial-noise-aided secure signal[J]. *Journal of Electronics & Information Technology*, 2018, 40(6): 1426–1432. doi: 10.11999/JEIT170739.

[9] ZHANG Wei, CHEN Jian, KUO Yonghong, *et al*. Artificial-noise-aided optimal beamforming in layered physical layer security[J]. *IEEE Communications Letters*, 2019, 23(1): 72–75. doi: 10.1109/LCOMM.2018.2881182.

[10] SAAD W, ZHOU Xiangyun, MAHAM B, *et al*. Tree formation with physical layer security considerations in wireless multi-hop networks[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(11): 3980–3991. doi: 10.1109/TWC.2012.091812.111923.

[11] LEE J H. Optimal power allocation for physical layer security in multi-hop DF relay networks[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(1): 28–38. doi: 10.1109/TWC.2015.2466091.

[12] XU Yang, LIU Jia, TAKAHASHI O, *et al*. SOQR: Secure optimal QoS routing in wireless ad hoc networks[C]. 2017 IEEE Wireless Communications and Networking Conference, San Francisco, USA, 2017: 1–6. doi: 10.1109/WCNC.2017.7925687.

[13] YAO Jianping and LIU Yuan. Secrecy rate maximization with outage constraint in multihop relaying networks[J]. *IEEE Communications Letters*, 2018, 22(2): 304–307. doi: 10.1109/LCOMM.2017.2768513.

[14] WANG Huiming, ZHANG Yan, NG D W K, *et al*. Secure routing with power optimization for Ad-Hoc networks[J]. *IEEE Transactions on Communications*, 2018, 66(10): 4666–4679. doi: 10.1109/TCOMM.2018.2835478.

[15] SAHA C, AFSHANG M, and DHILLON H S. Poisson cluster process: Bridging the gap between PPP and 3GPP HetNet models[C]. 2017 Information Theory and Applications Workshop, San Diego, USA, 2017: 1–9. doi: 10.1109/ITA.2017.8023448.

[16] CHEN Gaojie, COON J P, and TAJBAKHSH S E. Secure routing for multihop ad hoc networks with inhomogeneous eavesdropper clusters[J]. *IEEE Transactions on Vehicular Technology*, 2018, 67(11): 10660–10670. doi: 10.1109/TVT.2018.2866977.

[17] STOYAN D, CHIU S N, KENDALL W S, *et al*. Stochastic Geometry and Its Applications[M]. 3rd ed. Chichester: John Wiley & Sons, 2013: 171–175.

惠 鏸：女，1979年生，副教授，研究方向为智能无线通信与物联网关键技术等.

张晓静：女，1994年生，硕士生，研究方向为无线多跳网络优化问题.

责任编辑：马秀强