文章编号：2095-4980(2020)05-0826-05

多跳协同中继网络的安全性评估与仿真

盛 国[1]，党红飞[2]，韦林昌[2]，黎成中[2]，舒新文[3]

(1.浙江邮电职业技术学院 电子与通信工程学院，浙江 绍兴 312366；2.广西华南通信股份有限公司 研发部，广西 南宁 530007；3.安徽师范大学 物理与电子信息学院，安徽 芜湖 241000)

摘 要：为适应 5G 通信的发展与现实通信系统的需求，假设一个更为通用的多跳协同无线通信网络场景，并分析了在该场景下的系统安全容量，得出该指标的积分解析解。同时，通过基于蒙特卡洛算法的计算机数值仿真实验，安全容量的积分解析解的正确性得到验证。最后，通过对数值仿真的观察与讨论，可以得到一系列关于多跳协同中继无线通信网络的安全性能的结论。

关键词：物理层安全；多跳中继协同系统；安全容量；解码转发；数值仿真

中图分类号：TN911.6 **文献标志码：**A **doi：**10.11805/TKYDA2019168

Security assessment and simulation of multi-hop cooperative relay networks

SHENG Guo[1]，DANG Hongfei[2]，WEI Linchang[2]，LI Chengzhong[2]，SHU Xinwen[3]

(1.Department of Telecommunication Engineering，Zhejiang Post and Telecommunication College，Shaoxing Zhejiang 312000，China；
2.R & D Department，Guangxi South China Communications Co.，Ltd.，Nanning Guangxi 530007，China；
3.College of Physics and Electronic Information，Anhui Normal University，Wuhu Anhui 241000，China)

Abstract：To meet the requirements of 5G communication systems，the traditional scenarios are extended by assuming a general multi-hop cooperative wireless transmission scenario，and security analysis is performed in this scenario. The security capacity of the proposed scenario is derived and the key performance evaluation metric in integral form is obtained. The simulations based on Monte Carlo method are carried out to verify the correctness of the analytical results regarding security capacity. Through the observation and discussion on numerical simulations，a series of conclusions pertaining to the proposed multi-hop cooperative relay wireless communication network are given.

Keywords：physical security；multi-hop cooperative relay system；security capacity；decode-and-forward；numerical simulation

随着 5G 通信、物联网技术的发展以及移动端互联网技术的普及，信息变得触手可及，这使得信息加密愈发重要。基于大数质因分解的非对称加密体系 RSA(Rivest-Shamir-Adleman)的传统信息加密算法，随着科技的发展，其安全性受到挑战，能够使用的破解、遍历算法越来越多，破解效率也越来越高[1]。与 RSA 加密体系相对的是物理层安全体系。该体系基于香农提出的绝对安全概念和信息熵的理论研究成果。具体来说，信息论的研究成果和在 Wire-tap 信道模型下的相关计算已经证明，只要合法接收端的信道容量大于窃听端的信道容量，即一定存在某种传输方式，可以使得信息被绝对安全、保密地传输，无法被窃听端窃取。这一性质不依赖于复杂的信息传输加密算法，而是利用随机信道的衰落与自然波动进行安全通信，系统复杂度较低，也不需要繁琐的密钥分配、解码过程[2-4]。

绝大多数分析物理层安全的文献都聚焦于端到端的直传通信场景，而随着 5G 通信的发展与要求，通信场景愈发多样化，其中基于中继转发机制的多跳协同网络由于其快速的组网特性和高覆盖、高稳定、低能耗等优良特点，逐步被各种通信标准和协议采纳，成为常见的无线通信与信号传输场景[5]。但目前大多数文献只分析了两跳协同中继无线通信网络的安全性能[6-9]。

收稿日期：2019-05-17；**修回日期：**2019-07-12

基金项目：国家自然科学基金资助项目(11573001)

作者简介：盛 国(1979-)，男，硕士，教授，主要研究方向为通信系统信号处理。email:sg@zptc.edu.cn

1　系统模型

本文所假设的通信系统模型中，仅存在一对信源与信宿作为信号的发送端与接收端，分别标记为 S 与 D。假设一个从信源发送的信号总共需要 L 跳转发，各跳中继节点记为 R_i。所有中继采用解码转发(Decode-and-Forward，DF)协议，且采纳半双工转发机制。一个完整的从信源到信宿的信号传输过程需要 L 个正交时隙。各节点之间实现时域与频域的完美同步，实时信道状态信息(Channel State Information，CSI)完全可知。所有中继节点皆假设为可信中继节点，除此之外，只存在一个窃听节点，记为 E，该节点能够感知所有信号传输端的传输信号，包含信源与 $L-1$ 个中继。为了便于讨论与分析，假设该窃听节点采用选择接收(Selection Combining，SC)的方式来合并各路窃听信号，且所有节点都只配备有一根天线，为单线系统；所有无线信道的多径衰落都服从独立不同分布参数的准静态瑞利(Rayleigh)信道模型。

根据以上系统模型与假设，可以得到 L 个时隙在 $L-1$ 个中继节点和信宿的信号输入输出关系式 $y_i=\sqrt{P_\mathrm{t}}h_i x_i+n_i$，其中，$P_\mathrm{t}$ 为所有节点的共同发送功率；h_i 为第 i 跳合法信道的信道系数；x_i 为归一化后的第 i 跳合法信道的发送端发送符号，有 $|x_i|^2=1$；n_i 为第 i 跳合法信道接收端的加性高斯白噪声(Additive White Gaussian Noise，AWGN)，其噪声平均功率为 N_0。由于本文采用瑞利信道模型，其合法信道的每跳的信道增益 $H_i=|h_i|^2$ 服从指数分布，概率密度函数与累积分布函数分别为 $f_i(\xi)=1/\mu_i\exp(-\xi/\mu_i)$ 与 $F_i(\xi)=1-\exp(-\xi/\mu_i)$，其中 μ_i 为第 i 跳合法信道的平均信道增益[10]。

相似地，对于窃听节点来说，其在 L 个时隙中，也可以分别收到 L 个独立的畸变传输信号，有如下的输入输出关系 $z_i=\sqrt{P_\mathrm{t}}g_i x_i+\eta_i$，其中 g_i 为第 i 跳窃听信道的信道系数；η_i 为第 i 跳合法信道接收端的加性高斯白噪声，其噪声平均功率为 N_E(考虑到人工噪声干扰作为一个常见的窃听反制手段，特别假设窃听节点与合法接收节点处于不同的背景噪声环境中[11])。同理，由于本文采用瑞利信道模型，其窃听信道的每跳的信道增益 $G_i=|g_i|^2$ 也服从指数分布，并拥有概率密度函数与累积分布函数分别为 $t_i(\xi)=1/\sigma_i\exp(-\xi/\sigma_i)$ 与 $T_i(\xi)=1-\exp(-\xi/\sigma_i)$，其中 σ_i 为第 i 跳窃听信道的平均信道增益。

2　安全容量分析

安全容量是物理层安全性能的重要指标之一，它衡量了合法信道与窃听信道之间的差值，表征了通信系统的安全性。当安全容量为正值时，即合法信道接收效率高于窃听信道时，系统可认为是绝对安全的。安全容量越大，说明系统在绝对安全的前提下传输效率越高[12]。鉴于安全容量的重要性，本文中对其进行详细分析，并给出了它的积分解析解。为获得安全容量的积分解析解，首先要分别求得合法信道和窃听的信道容量。由于解码转发中继的误差传递(error propagation)效应，可以很容易获得其端到端等效信噪比(Signal-to-Noise Ratio，SNR)[13]：$R_{\mathrm{SN,SD}}=P_\mathrm{t}\min_{i\in L}\{H_i\}/N_0, L=\{1,2,\cdots\}$。根据信道容量的定义和半双工协同转发策略，合法信道的信道容量可以通过最大流最小割定理求知[14] $C_\mathrm{SD}=1/L\log(1+R_{\mathrm{SN,SD}})$。

由于本文中假设各跳信道多径衰落独立且服从不同参数的瑞利分布，$R_{\mathrm{SN,SD}}$ 的累积分布函数 $P_\mathrm{SD}(\xi)$ 可以通过多跳分割的方法，并考虑多跳中断中的最坏情况来进行计算。换言之，只要端到端各跳信道中有一跳发生中断，整个信道即中断，因此，等效地，可以专注于研究最差一跳信道，只要该跳信道发生中断，整个端到端信道即发生中断。基于这一假设与转换，可以通过基本的顺序统计学原理求得[15]：

$$P_\mathrm{SD}(\xi)=P\{R_{\mathrm{SN,SD}}<\xi\}=P\{P_\mathrm{t}\min_{i\in L}\{H_i\}/N_0<\xi\}=P\{\min_{i\in L}\{H_i\}<N_0\xi/P_\mathrm{t}\}=1-\prod_{i=1}^{L}P\{H_i\geqslant N_0\xi/P_\mathrm{t}\}=1-\exp\left(-\frac{\xi N_0}{P_\mathrm{t}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right) \tag{1}$$

通过对式(1)求导，可以得到 $R_{\mathrm{SN,SD}}$ 的概率密度函数：

$$p_\mathrm{SD}(\xi)=\frac{\mathrm{d}P_\mathrm{SD}(\xi)}{\mathrm{d}\xi}=\left(\frac{N_0}{P_\mathrm{t}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right)\exp\left(-\frac{\xi N_0}{P_\mathrm{t}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right) \tag{2}$$

根据随机变量函数分布相关公式及 $R_{\mathrm{SN,SD}}$ 和 C_SD 的函数关系，可通过简单线性变换求 C_SD 的累积分布函数：

$$P_{C_\mathrm{SD}}(\xi)=P\{C_\mathrm{SD}<\xi\}=1-\exp\left(-\frac{\left(\exp(L\xi)-1\right)N_0}{P_\mathrm{t}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right) \tag{3}$$

同理，通过对上式进行求导，可以得到 C_{SD} 的概率密度函数：

$$p_{C_{\mathrm{SD}}}(\xi)=\left(\frac{LN_0}{P_{\mathrm{t}}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right)\exp\left(L\xi+\left(\frac{N_0}{P_{\mathrm{t}}}\sum_{i=1}^{L}\frac{1}{\mu_i}\right)\left(1-\exp(L\xi)\right)\right) \tag{4}$$

另一方面，对窃听信道进行分析。由于窃听节点采用选择合并的方式接收来自 L 个正交时隙的信息，根据选择合并原理，窃听节点的等效信噪比为 $R_{\mathrm{SN,E}}=P_{\mathrm{t}}\min_{i\in L}\{G_i\}/N_{\mathrm{E}}$。类似地，可以得到窃听信道的信道容量表达式 $C_{\mathrm{E}}=1/L\log\left(1+R_{\mathrm{SN,E}}\right)$。

同样根据各中继到窃听节点的信道也服从独立不同参数的瑞利分布假设，可以得到 $P_{\mathrm{E}}(\xi)$ 的累积分布函数：

$$P_{\mathrm{E}}(\xi)=P\left\{R_{\mathrm{SN,E}}<\xi\right\}\approx 1-\sum_{i=1}^{L}\exp\left(-\frac{\xi N_{\mathrm{E}}}{P_t\sigma_i}\right) \tag{5}$$

其中，最后一步近似在大信噪比条件下成立，即 $P_{\mathrm{t}}/N_{\mathrm{E}}\to\infty$。

根据莱布尼兹求导法则(Lebniz ruler)，可以对式(5)求导得到 $R_{\mathrm{SN,E}}$ 的概率密度函数以及其在大信噪比条件下的近似表达式：

$$p_{\mathrm{E}}(\xi)=\left[\prod_{i=1}^{L}\left(1-\exp\left(-\frac{\xi N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right)\right)\right]\left[\frac{N_{\mathrm{E}}}{P_{\mathrm{t}}}\sum_{i=1}^{L}\left(\frac{\frac{1}{\sigma_i}\exp\left(-\frac{\xi N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right)}{1-\exp\left(-\frac{\xi N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right)}\right)\right]\approx\left(\frac{N_{\mathrm{E}}}{P_{\mathrm{t}}}\right)\sum_{i=1}^{L}\frac{1}{\sigma_i}\exp\left(-\frac{\xi N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right) \tag{6}$$

同理，根据随机变量函数分布的相关概率论基本公式以及 $R_{\mathrm{SN,E}}$ 和 C_{E} 的函数关系，可以通过简单的线性变换求知 C_{E} 的累积分布函数及其在大信噪比条件下的近似表达式，有：

$$P_{C_{\mathrm{E}}}(\xi)=P\{C_{\mathrm{E}}<\xi\}=\prod_{i=1}^{L}\left(1-\exp\left(-\frac{\left(\exp(L\xi)-1\right)N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right)\right)\approx 1-\sum_{i=1}^{L}\exp\left(-\frac{\left(\exp(L\xi)-1\right)N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right) \tag{7}$$

利用莱布尼兹求导法则对式(7)求导，可得到 C_{E} 的概率密度函数及其在大信噪比条件下的近似表达式：

$$p_{C_{\mathrm{E}}}(\xi)=\left[\prod_{i=1}^{L}\left(1-\exp\left(-\frac{\left(\exp(L\xi)-1\right)N_{\mathrm{E}}}{P_{\mathrm{t}}\sigma_i}\right)\right)\right]\left(\frac{LN_{\mathrm{E}}}{P_{\mathrm{t}}}\sum_{i=1}^{L}\frac{\frac{1}{\sigma_i}\exp\left(L\xi+1-\exp(L\xi)\right)}{1-\exp\left(-\frac{\left(\exp(L\xi)-1\right)N_E}{P_{\mathrm{t}}\sigma_i}\right)}\right)\approx\frac{LN_{\mathrm{E}}}{P_{\mathrm{t}}}\sum_{i=1}^{L}\frac{1}{\sigma_i}\exp\left(L\xi+1-\exp(L\xi)\right) \tag{8}$$

基于以上的准备工作与计算，安全容量的定义表达式为：$C=\left(C_{\mathrm{SD}}-C_{\mathrm{E}}\right)^{+}$，其中，$(\bullet)^{+}$ 表示取正整数。根据相应的计算结果，可以很容易地得到遍历各态的安全容量表达式：

$$\overline{C}=\int_0^\infty\int_0^\infty C p_{C_{\mathrm{SD}}}(C_{\mathrm{SD}})p_{C_{\mathrm{E}}}(C_{\mathrm{E}})\mathrm{d}C_{\mathrm{SD}}\,\mathrm{d}C_{\mathrm{E}}=\int_0^\infty\int_0^\infty\left(C_{\mathrm{SD}}-C_{\mathrm{E}}\right)^{+}p_{C_{\mathrm{SD}}}(C_{\mathrm{SD}})p_{C_{\mathrm{E}}}(C_{\mathrm{E}})\mathrm{d}C_{\mathrm{SD}}\,\mathrm{d}C_{\mathrm{E}} \tag{9}$$

该物理量为衡量一个通信系统物理层安全性的最直接且重要的性能指标之一。为便于计算机计算分析以及进一步优化，利用梯形积分逼近法则中的复合求积公式和展开式原理以及二重积分的收敛性，对式(9)进行了进一步的化简，最终将积分式化简成连加式，从而避免因引入积分运算而导致较高的分析复杂度：

$$\overline{C}=\int_0^\infty\underbrace{\left(\int_{C_{\mathrm{E}}}^\infty C_{\mathrm{SD}}p_{C_{\mathrm{SD}}}(C_{\mathrm{SD}})\mathrm{d}C_{\mathrm{SD}}-C_{\mathrm{E}}\int_{C_{\mathrm{E}}}^\infty p_{C_{\mathrm{SD}}}(C_{\mathrm{SD}})\mathrm{d}C_{\mathrm{SD}}\right)}_{\Delta(C_{\mathrm{E}})}p_{C_{\mathrm{E}}}(C_{\mathrm{E}})\mathrm{d}C_{\mathrm{E}}=\frac{\delta}{M}\left(\frac{\Delta(\delta)p_{C_{\mathrm{E}}}(\delta)+\Delta(0)p_{C_{\mathrm{E}}}(0)}{2}+\sum_{m=1}^{M-1}\Delta\left(\frac{m\delta}{M}\right)p_{C_{\mathrm{E}}}\left(\frac{m\delta}{M}\right)\right) \tag{10}$$

此处 δ 与 M 为人为设定的计算参量，和积分逼近精确度有关，其值越大，则用连加结果逼近积分结果的误差越小，相应的计算复杂度也就越大。

3 仿真验证与结果分析

为了便于讨论与仿真程序的架构，根据实际的无线通信与窃听场景，设置 $\mu_1=\mu_2=\cdots=\mu_L=1$，$\sigma_1=\sigma_2=\cdots=\sigma_L=0.2$ 并归一化 $N_0=N_{\mathrm{E}}=1$。采用 Matlab 软件进行仿真，计算机 CPU 为 Intel(R)CORE(TM)i7-4510U，主频为 2.0 GHz，内存为 8.0 GB，并对每个场景与数据点采样 10^5 次求平均，以统计出遍历各态的平均安全容量的数值解。仿真了 4 种不同的传输网络遍历各态的安全容量随合法信道传输信噪比 P_{t}/N_0 变化而变化的关系，分别是传统的端到端直传网络以及不同转发跳数的多跳中继转发网络，仿真结果如图 1 所示。

通过图 1 可发现通过蒙特卡洛算法得到的数值解曲线完美地贴合了通过式(9)算得的解析解曲线。因此，式(9)可以用来准确估计本文所提出的多跳协同中继无线网络模型的安全性能。

同时，通过图 1 还可以观察到，安全容量不同于普通的信道容量，该性能指标虽然随着合法信道的传输信噪比的提高而提高，但是会在大信噪比条件下达到饱和状态，之后不再随着合法信道的传输信噪比的提高而发生明显变化，这是因为随着传输信噪比的提高，虽然合法信道能够更有效率地大容量接收信号，但是同时所传输的信号也将更容易被窃听节点获知，因而合法信道和窃听信道的信道容量达到一个平衡状态，这是考虑窃听节点后的通信网络模型的一大特点。

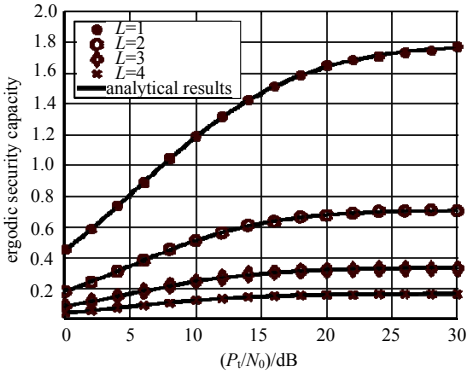

Fig.1 Ergodic security capacity $\overline{C}$ with P_t/N_0 of the legitimate channel

图 1 遍历各态安全容量 $\overline{C}$ 随合法信道信噪比 P_t/N_0 的变化趋势

在验证本文的主要核心计算贡献的同时，也通过基于蒙特卡洛算法的数值仿真来探究几个主要系统参数对多跳协同中继网络安全性能的影响。首先，在图 2 中呈现了遍历各态安全容量随着转发跳数 L 分别在大、中、小信噪比条件下的变化趋势。通过该图可以很清楚地看到，无论是在大信噪比、中信噪比还是小信噪比条件下，增加转发跳数都会极大地降低安全容量，严重破坏网络的安全性能。这一影响主要是由 3 个方面的原因造成的。其一，合法信道由于不存在网格式的跨跳连接，各跳解码转发中继需要串接转发，故存在误差传递效应，即解码转发瓶颈效应。也就是说，只要多跳转发信息中在任何一跳出错，整条合法信道即无法正确传输信号。因此，增多转发跳数无疑会增大信号不能被正确接收的概率，也就降低了合法信道的信道容量。第二，由于半双工转发协议机制，各跳发送端必须在正交时隙内发送信号，也就是说，当跳数增加时，需要的时隙增多，传输的平均时间越长，传输效率越低，这也降低了合法信道的信道容量。除了合法信道的信道容量被降低之外，增加转发跳数还会增加窃听信道的信道容量，这是因为由于窃听节点可以感知到各跳传输节点的信息，且采用选择合并方式接收窃听信号，因此越多的转发跳数，就给予了窃听节点更大的可能性来截获优质的窃听信号。这三个原因的综合作用，使得安全容量与转发跳数呈现反相关。

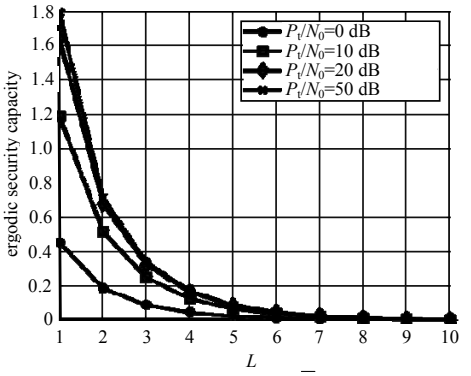

Fig.2 Ergodic security capacity $\overline{C}$ with the number of hops L

图 2 遍历各态安全容量 $\overline{C}$ 随转发跳数 L 的变化趋势

除了转发跳数以外，窃听信道的平均噪声功率 N_E 也是一个很重要的系统参数。它反映了人工噪声干扰反窃听技术对于增强通信系统安全性的作用。图 3 呈现了遍历各态安全容量随着窃听信道平均噪声功率 N_E 分别在不同的转发跳数和传输信噪比条件下的变化趋势。可以观察到，通过加强人工噪声干扰来增大系统安全性是可行的。因为这使得窃听信道的平均噪声功率增大，严重影响窃听效果与质量，因此随着窃听信道平均噪声功率 N_E 的上升，安全容量逐步增大。另外一方面，依靠人工噪声干扰反窃听技术也存在弊端，即其反窃听效果与合法信道传输信噪比高度相关，如果传输信噪比较小，则仅仅通过人工噪声干扰反窃听技术来增大窃听信道的平均噪声功率，很快会达到安全容量饱和，无法进一步提升安全容量，如图 3 中两个小信噪比得到的图线结果所示。因此，为了达到良好的反窃听效果，需确保合法信道的各发送节点拥有较高的传输功率，从而避免安全容量过早达到饱和态。另外，探究了合法信道与窃听信道平均信道增益对多跳协同中继网络安全性的影响，结果呈现在图 4 中。增大合法信道的平均信道增益 μ，意味着合法信道的传输效率更高，系统安全容量会得到提升。反之，增大窃听信道的平均信道增益 σ，则意味着窃听信道的传输效率更高，于是就造成了系统安全容量降低。

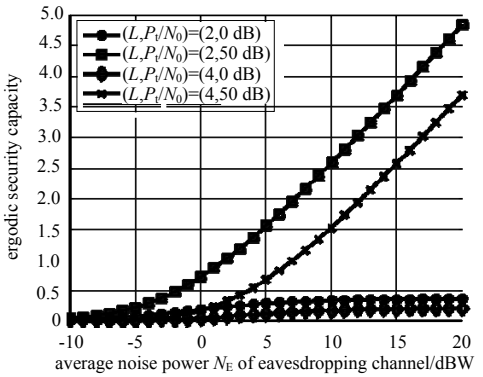

Fig.3 Security capacity $\overline{C}$ with the average noise power N_E of the eavesdropping channel

图 3 遍历各态安全容量 $\overline{C}$ 随窃听信道平均噪声功率 N_E 的变化趋势

4 结论

为应对新型高效的计算机破解算法对传统的RSA 加密算法体系的挑战，物理层安全利用信息论的基本理论实现绝对安全通信。随着当前 5G 网络的高速发展以及多跳异构网络的普及，本文分析了多跳协同中继无线通信网络的安全性能，获得了遍历各态的安全容量的积分解析解。并应用蒙特卡洛算法进行了数值仿真实验，验证了所求积分解析解的正确性。同时通过细致观察仿真结果，明晰了多个系统参数对网络安全性的影响机制，并得到一系列关于多跳协同中继无线通信网络的安全性能的结论与提升安全性的建议。

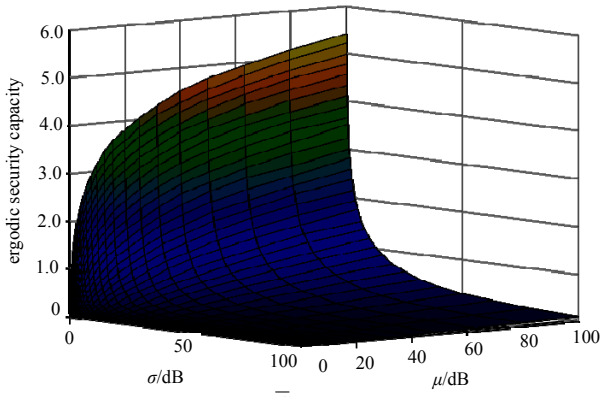

Fig.4 Ergodic security capacity $\overline{C}$ with the average channel gain μ of the legitimate channel and the average channel gain σ of the eavesdropping channel (P_t/N_0=20 dB, L=2)

图 4 遍历各态安全容量 $\overline{C}$ 随合法信道平均信道增益 μ 和窃听信道平均信道增益 σ 的变化趋势(P_t/N_0=20 dB, L=2)

参考文献：

[1] 向进. RSA 加密算法的安全性分析[J]. 吉首大学学报(自然科学版), 2011,32(1):42-43. (XIANG Jin. Security analysis of RSA encryption algorithm[J]. Journal of Jishou University(Natural Science Edition), 2011,32(1):42-43.)

[2] SHIU Y S,CHANG S Y,WU H C,et al. Physical layer security in wireless networks:a tutorial[J]. IEEE Wireless Communications, 2011,18(2):66-74.

[3] YANG N,WANG L,GERACI G,et al. Safeguarding 5G wireless communication networks using physical layer security[J]. IEEE Communications Magazine, 2015,53(4):20-27.

[4] BLOCH M,BARROS J. Physical-layer security: from information theory to security engineering[M]. Cambridge,United Kingdom:Cambridge University Press, 2011.

[5] 于欢,李云渊,溧欣,等. 高能效中继通信技术综述与展望[J]. 电信科学, 2017,29(3):111-116. (YU Huan,LI Yunyuan, LI Xin,et al. Overview and prospect of high energy efficiency relay communication technology[J]. Telecommunication Science, 2017,29(3):111-116.)

[6] ZHANG Jiliang,PAN Gaofeng,WANG Huiming. On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system[J]. IEEE Access, 2016(4):3887-3893.

[7] LEE K,HONG J,CHOI H,et al. Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication[J]. IEEE Internet of Things Journal, 2018,5(4):2793-2803.

[8] LI Q,YANG Y,MA W,et al. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks[J]. IEEE Transactions on Signal Processing, 2015,63(1):206-220.

[9] ATAPATTU S,ROSS N,JING Y,et al. Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection[J]. IEEE Transactions on Wireless Communication, 2019,18(2):1216-1232.

[10] 李成杰,裴峥. 无线信号服从瑞利分布的验证方法[J]. 通信技术, 2009,42(5):51-53. (LI Chengjie,PEI Zheng. Verification method of wireless signal obeying Rayleigh distribution[J]. Communication Technology, 2009,42(5):51-53.)

[11] ROMERO-ZURITA N,GHOGHO M,MCLERNON D. Outage probability based power distribution between data and artificial noise for physical layer security[J]. IEEE Signal and Processing Letters, 2012,19(2):71-74.

[12] 周伟伟. 线性网络编码研究[J]. 通信技术, 2008,41(2):97-99. (ZHOU Weiwei. Research on linear network coding[J]. Communication Technology, 2008,41(2):97-99.)

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

[14] 程卫军,李育红,胡健栋. 瑞利衰落信道下多跳合作分集系统的性能分析[J]. 北京邮电大学学报, 2004,27(3):93-97. (CHENGWeijun,LI Yuhong,HU Jiandong. Performance analysis of multi hop cooperative diversity system in Rayleigh fading channel[J]. Journal of Beijing University of Posts and Telecommunications, 2004,27(3):93-97.)

[15] 匡能晖. 关于两参数瑞利分布顺序统计量的分布性质[J]. 江西师范大学学报(自然科学版), 2009,33(6):648-651. (KUANG Nenghui. Distribution properties of two parameters Rayleigh distribution order statistics[J]. Journal of Jiangxi Normal University(Natural Science Edition), 2009,33(6):648-651.)