研究与开发

随机位置窃听场景下 SWIPT 系统的物理层安全性能

钱辉，李光球，丁一凡
（杭州电子科技大学通信工程学院，浙江 杭州 310018）

摘　要：鉴于窃听者的位置会对采用发射天线选择（TAS）和功率分割（PS）策略的无线携能通信（SWIPT）系统的物理层安全性能产生严重影响，考虑将其建模为泊松点过程（PPP）。利用 PPP 的概率生成函数分别推导了采用 TAS 和 PS 策略的 SWIPT 系统在非合谋（独立）与合谋两种窃听场景下的安全中断概率（SOP）闭合表达式。数值计算和仿真结果均表明，发射天线数越大，发射端与信息接收者之间的距离越小，PS 因子越小，SWIPT 系统在非合谋与合谋两种窃听场景下的 SOP 均越小；合谋窃听会进一步恶化 SWIPT 系统的物理层安全性能。

关键词：物理层安全；无线携能通信；泊松点过程；功率分割；发射天线选择；安全中断概率
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020147

Physical layer security performance of SWIPT system in the presence of randomly located eavesdroppers

QIAN Hui, LI Guangqiu, DING Yifan
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: The locations of the eavesdroppers have serious impact on the physical layer security performance of simultaneous wireless information and power transfer (SWIPT) systems with transmit antenna selection (TAS) and power split (PS) strategy, which can be considered to be modeled as Poisson point process (PPP). The closed-form expressions for secrecy outage probability (SOP) of SWIPT system with TAS and PS strategy under non-colluding and colluding eavesdropping scenarios were derived by using probability generation function of PPP, respectively. Numerical and simulation results show that, the larger the number of transmit antennas, the smaller the distance between the transmitter and the information receiver, and the smaller the PS factor, the smaller SOP of SWIPT system under non-colluding and colluding eavesdropping scenarios. Colluding eavesdropping will further deteriorate the physical layer security performance of SWIPT systems.

Key words: physical layer security, simultaneous wireless information and power transfer, Poisson point process, power split, transmit antenna selection, secrecy outage probability

收稿日期：2019−12−13；修回日期：2020−03−24
通信作者：李光球，gqli@hdu.edu.cn

1 引言

采用功率分割（power split，PS）或时间切换策略的无线携能通信（simultaneous wireless information and power transfer，SWIPT）是解决节点在复杂环境（如海洋、太空等）中无法架设供电线路和需要频繁更换电池等应用场景问题的有效方法[1-2]，然而当能量收集器（energy-harvesting receiver，ER）要进行恶意窃听时，SWIPT 系统的物理层安全将面临严重威胁[3-13]。参考文献[3-4]分别推导了考虑路径损耗的瑞利衰落信道上目的节点发送人工噪声的SWIPT 系统和广义K衰落信道上 SWIPT 系统的安全中断概率（secrecy outageprobability，SOP）闭合表达式。参考文献[5]推导了源节点采用最大比发射的 SWIPT 系统的 SOP 闭合表达式。参考文献[6]推导了中继节点采用 SWIPT 技术的无线解码转发中继系统在线性、非线性两种能量收集模式下的 SOP 闭合表达式。参考文献[7]研究了大气湍流、指向误差、检测技术、信道衰落系数等参数对两跳混合射频－自由空间光 SWIPT 系统下行链路 SOP 性能的影响。

参考文献[3-7]研究的均为单窃听场景，参考文献[8-13]研究了多窃听场景下 SWIPT 系统的物理层安全性能。参考文献[8]推导了信息接收者（information receiver，IR）采用最大比合并分集接收、ER 为单天线的 SWIPT 系统在非合谋（即独立）窃听场景下的 SOP、渐近 SOP 和平均安全容量的闭合表达式。参考文献[9]推导了参考文献[8]的 SWIPT 系统在 Nakagami 衰落信道上的 SOP 和平均安全容量的解析表达式并研究了 Nakagami 衰落系数和 PS 因子对其物理层安全性能的影响。参考文献[10]推导了采用发射天线选择（transmit antenna selection，TAS）、IR 和 ER 均为单天线的 SWIPT 系统在瑞利衰落信道上和反馈时延下的 SOP、渐近 SOP 和平均安全容量的闭合表达式。参考文献[11]研究了大规模天线 SWIPT 系统的安全速率。参考文献[12]研究了多组合谋窃听场景下 SWIPT 多播系统的可达安全容量优化问题。参考文献[13]提出了一种异构携能通信网络中采用人工噪声辅助的稳健能量与信息安全传输方案。

参考文献[8-13]未考虑窃听者的数量与位置分布对无线系统的物理层安全性能产生的重要影响，在没有任何先验知识的情况下，参考文献[14-18]将窃听者的数量与位置分布建模为泊松点过程（Poisson point process，PPP）。参考文献[14]研究了面向物联网无线携能通信系统的机会安全传输方案，其中的资源中心、能量受限用户和被动窃听者均被建模为 PPP 过程。参考文献[15]推导了考虑路径损耗的瑞利衰落信道上合法用户与窃听者均服从 PPP 时无线网络下行多入单出（multiple-input single-output，MISO）无线链路的 SOP 表达式。参考文献[16]分别研究了考虑路径损耗的瑞利衰落信道上独立与合谋两种窃听场景下无线网络的下行 MISO 链路的 SOP。参考文献[17]分别推导了在独立与合谋两种窃听场景下广播系统的 SOP 表达式。参考文献[18]推导了 MISO 无线系统在独立窃听场景下的 SOP 积分表达式及上限和合谋窃听场景下的 SOP 闭合表达式。

综上可知，SWIPT 系统的物理层安全以及将多窃听者的位置建模为 PPP 过程的无线系统物理安全均有较深入的研究，然而将多窃听者的位置建模为PPP过程的SWIPT系统在独立与合谋两种窃听场景下的物理层安全性能尚未见有研究报道，下面分析其 SOP 性能。

2 系统模型

考虑如图 1 所示的采用 PS 策略的 SWIPT 系统的物理层安全模型，其中发射端 Alice 配备 N_{T} 根发射天线、信息接收者（IR）和能量收集器（ER）均配置单根接收天线。

假定：Alice 位于原点，ER 随机分布在以 Alice 为圆心、半径为 R 的二维空间区域内，且可建模

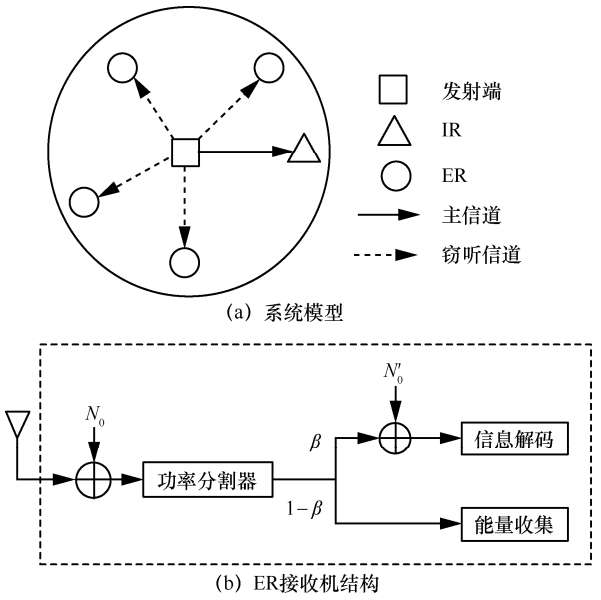

图 1　PS 策略下 SWIPT 系统的物理层安全模型

为密度为 ρ_{E} 的泊松点过程 Φ[16]；主信道和窃听信道均同时遭受大尺度路径损耗和小尺度衰落的干扰，Alice 的第 i 根发射天线与 IR 的接收天线之间的主信道增益为 $g_i = h_i d_{\mathrm{I}}^{-\alpha/2}$，其中，$d_{\mathrm{I}}$ 表示 Alice 与 IR 之间的距离，α 为路径损耗指数，h_i 服从复高斯 $\mathcal{CN}(0,1)$ 分布；Alice 第 i 根发射天线与第 k 个 ER 的接收天线之间的窃听信道增益为 $g_{ik} = h_{ik} d_k^{-\alpha/2}$，其中 d_k 表示 Alice 与第 k 个 ER 之间的距离，h_{ik} 服从 $\mathcal{CN}(0,1)$ 分布；主信道和每个窃听信道上的加性白高斯噪声相互独立，且均服从 $\mathcal{CN}(0,N_0)$ 分布，主信道和窃听信道均是准静态的，即信道衰落系数按块进行变化；Alice 采用 TAS 天线分集并按块发送信号，每个 ER 均采用相同的 PS 接收策略，即每个 ER 将收到的信号均以相同的 PS 因子 β 分为两部分，信息解码和能量收集的功率占比分别为 β 和 $1-\beta$，信息解码支路的加性白高斯噪声方差为 N_0'，ER 接收机结构如图 1（b）所示。研究 ER 独立与合谋两种被动窃听场景，即 Alice 无法获得 ER 窃听信道的信道状态信息。

3　安全中断概率

SWIPT 系统的安全容量 C_{S} 为：

$$C_{\mathrm{S}} = \begin{cases} C_{\mathrm{I}} - C_{\mathrm{E}}, \gamma_{\mathrm{I}} > \gamma_{\mathrm{E}} \\ 0 \quad , \gamma_{\mathrm{I}} \leqslant \gamma_{\mathrm{E}} \end{cases} \tag{1}$$

其中，$C_{\mathrm{I}} = \mathrm{lb}(1+\gamma_{\mathrm{I}})$ 和 $C_{\mathrm{E}} = \mathrm{lb}(1+\gamma_{\mathrm{E}})$ 分别为主信道和窃听信道容量，γ_{I} 和 γ_{E} 分别为主信道和窃听信道输出符号的瞬时信噪比（signal-to-noise ratio，SNR）。

主信道输出的瞬时符号 SNR 可表示为：

$$\gamma_{\mathrm{I}} = \frac{P}{N_0} \max_{i \in \{1,\cdots,N_{\mathrm{T}}\}} \left(|h_i|^2 / d_{\mathrm{I}}^{\alpha} \right) \tag{2}$$

其中，P 为 Alice 的发射功率，$|h_i|^2 / d_{\mathrm{I}}^{\alpha}$ 服从均值为 $d_{\mathrm{I}}^{-\alpha}$ 的指数分布。令 $\overline{\gamma} = P/N_0$，由参考文献[19]可得 γ_{I} 的概率密度函数（probability density function，PDF）和累积分布函数（cumulative distribution function，CDF）分别为：

$$f_{\mathrm{I}}(x) = \frac{N_{\mathrm{T}} d_{\mathrm{I}}^{\alpha}}{\overline{\gamma}} \sum_{m=0}^{N_{\mathrm{T}}-1} \binom{N_{\mathrm{T}}-1}{m} (-1)^m \cdot \exp\left(-\frac{(m+1) d_{\mathrm{I}}^{\alpha} x}{\overline{\gamma}} \right) \tag{3}$$

$$F_{\mathrm{I}}(x) = \sum_{m=0}^{N_{\mathrm{T}}} \binom{N_{\mathrm{T}}}{m} (-1)^m \exp\left(-\frac{m d_{\mathrm{I}}^{\alpha} x}{\overline{\gamma}} \right) \tag{4}$$

虽然 Alice 采用 TAS 天线分集，但是对于每个 ER 而言均是随机天线选择，因此每个窃听信道相当于一个单入单出系统。当 ER 独立窃听时，当且仅当主信道输出的瞬时符号 SNR 大于任意一个窃听信道输出的瞬时符号 SNR 时才可保证信息的安全传输，此时窃听信道的最大瞬时 SNR 可表示为[16]：

$$\gamma_{\mathrm{E}} = \frac{\beta P}{\beta N_0 + N_0'} \max_{k \in \Phi} \left(|h_{i^* k}|^2 / d_k^{\alpha} \right) \tag{5}$$

其中，i^* 表示 Alice 选择的最优发射天线序号。令 $N_0 = a N_0'$，$c = \beta/(\beta + a)$，则 ER 独立窃听场景下 γ_{E} 的 CDF 可表示为：

$$F_{\mathrm{E}}(x) = \Pr(\gamma_{\mathrm{E}} < x) = \Pr\left(\max_{k \in \Phi} \left(|h_{i^* k}|^2 / d_k^{\alpha} \right) < \frac{x}{c\overline{\gamma}} \right) \tag{6}$$

当 ER 合谋窃听时，每个 ER 可以共享各自窃听到的信息，因此能以最佳的方式合并信号并进行信息解码，此时窃听信道的瞬时 SNR 可表示为[16]：

$$\gamma_{\mathrm{E}}=\frac{\beta P}{\beta N_0+N_0'}\sum_{k\in\Phi}\left(\left|h_{i^*k}\right|^2/d_k^{\alpha}\right) \tag{7}$$

SWIPT 系统的 SOP 为 C_{S} 小于目标安全速率 R_{S} 的概率。当 Alice 的发射功率足够大时，SWIPT 系统的 SOP 可近似为[16]：

$$\begin{aligned}&P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)\simeq\Pr\left(\frac{\gamma_{\mathrm{I}}}{\gamma_{\mathrm{E}}}<2^{R_{\mathrm{S}}}\right)=\\&1-\int_0^{\infty}f_{\mathrm{I}}(x)F_{\mathrm{E}}\left(x/2^{R_{\mathrm{S}}}\right)\mathrm{d}x\end{aligned} \tag{8}$$

其中，$\Pr(\cdot)$ 表示求概率，$F_{\mathrm{E}}(\cdot)$ 表示 γ_{E} 的 CDF。

下面分别推导独立与合谋两种窃听场景下 SWIPT 系统的 SOP 表达式。

3.1 独立窃听

根据随机变量 $\left\{\left|h_{i^*k}\right|^2;k\in\Phi\right\}$ 的独立性，式（6）可化简为：

$$\begin{aligned}F_{\mathrm{E}}(x)&=\mathbb{E}_{\Phi}\left[\prod_{k\in\Phi}\Pr\left(\left|h_{i^*k}\right|^2<d_k^{\alpha}x/\left(c\bar{\gamma}\right)\middle|\Phi\right)\right]\\&=\mathbb{E}_{\Phi}\left[\prod_{k\in\Phi}\left(1-\exp\left(-d_k^{\alpha}x/\left(c\bar{\gamma}\right)\right)\right)\right]\end{aligned} \tag{9}$$

其中，$\mathbb{E}[\cdot]$ 表示求数学期望。由参考文献[18]的式(7)可知，泊松点过程的概率生成函数可表示为：

$$\mathbb{E}_{\Phi}\left[\prod_{x\in\Phi}f(x)\right]=\exp\left(-\rho_{\mathrm{E}}\int_0^{2\pi}\int_0^{R}r\left(1-f(x)\right)\mathrm{d}r\mathrm{d}\theta\right) \tag{10}$$

将 $f(x)=1-\exp\left(-d_k^{\alpha}x/\left(c\bar{\gamma}\right)\right)$ 代入式（10），并根据参考文献[20]的式（3.326.4）：

$$\begin{aligned}&\int_0^{u}(x-b)\exp\left(-\lambda(x-d)^{v}\right)\mathrm{d}x=\\&\frac{\Gamma\left(2/v,\lambda(-d)^{v}\right)-\Gamma\left(2/v,\lambda(u-d)^{v}\right)}{v\lambda^{2/v}}-\\&(b-d)\frac{\Gamma\left(1/v,\lambda(-d)^{v}\right)-\Gamma\left(1/v,\lambda(u-d)^{v}\right)}{v\lambda^{1/v}}\end{aligned} \tag{11}$$

其中，$\Gamma(\cdot,\cdot)$ 表示不完全伽马函数。可得 γ_{E} 的 CDF 为：

$$F_{\mathrm{E}}(x)=\exp\left(-\frac{2\pi\rho_{\mathrm{E}}}{\alpha}\left(\frac{c\bar{\gamma}}{x}\right)^{2/\alpha}\left(\Gamma\left(\frac{2}{\alpha}\right)-\Gamma\left(\frac{2}{\alpha},\frac{x}{c\bar{\gamma}}R^{\alpha}\right)\right)\right) \tag{12}$$

令 $n=(m+1)d_{\mathrm{I}}^{\alpha}/\bar{\gamma}$，$t=2\pi\rho_{\mathrm{E}}\Gamma(2/\alpha)\left(2^{R_{\mathrm{S}}}c\bar{\gamma}\right)^{2/\alpha}/\alpha$，假定 $\alpha=p/q$ 为有理数，即 p、q 为正整数，当窃听者分布半径很大时，将式(3)和式(12)代入式(8)，利用参考文献[16]中的式（30），可推导得 ER 独立窃听场景下 SWIPT 系统的 SOP 近似表达式为：

$$\begin{aligned}P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)\simeq1-&\sum_{m=0}^{N_{\mathrm{T}}-1}\binom{N_{\mathrm{T}}-1}{m}(-1)^m\frac{N_{\mathrm{T}}}{m+1}\cdot\frac{\sqrt{pq}}{2^{\frac{p+2q-3}{2}}\pi^{\frac{p+2q-2}{2}}}\cdot\\&G_{0,p+2q}^{p+2q,0}\left(\frac{n^{2q}t^{p}}{p^{p}4^{q}q^{2q}}\middle|\begin{matrix}-\\\frac{0}{p},\frac{1}{p},\cdots,\frac{p-1}{p},\frac{1}{2q},\frac{2}{2q},\cdots,\frac{2q}{2q}\end{matrix}\right)\end{aligned} \tag{13}$$

其中，$G(\cdot)$ 表示 Meijer G 函数[20]。

由式（13）可知：ER 独立窃听场景下 SWIPT 系统的 SOP 与发射端天线数、发射端与信息接收者之间的距离、PS 因子、路径损耗指数和窃听者密度等参数有关。

对于 $\alpha=2$ 的自由空间传播环境，利用参考文献[20]中的式（3.324.1），式（13）可简化为：

$$\begin{aligned}P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)\simeq1-&2N_{\mathrm{T}}d_{\mathrm{I}}\sum_{m=0}^{N_{\mathrm{T}}-1}\binom{N_{\mathrm{T}}-1}{m}(-1)^m\cdot\\&\sqrt{\frac{c\pi\rho_{\mathrm{E}}2^{R_{\mathrm{S}}}}{m+1}}K_1\left(2d_{\mathrm{I}}\sqrt{c\pi\rho_{\mathrm{E}}(m+1)2^{R_{\mathrm{S}}}}\right)\end{aligned} \tag{14}$$

其中，$K_1(\cdot)$ 表示第二类一阶修正的贝塞尔函数[20]。

3.2 合谋窃听

将式（2）和式（7）代入式（8），可得 ER 合谋窃听场景下 SWIPT 系统的 SOP 为：

$$P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)=\Pr\left(\max_{i\in\{1,\cdots,N_{\mathrm{T}}\}}\left(\left|h_i\right|^2/d_{\mathrm{I}}^{\alpha}\right)<c2^{R_{\mathrm{S}}}\sum_{k\in\Phi}\left(\left|h_{i^*k}\right|^2/d_k^{\alpha}\right)\right) \tag{15}$$

令 $Z=\sum_{k\in\Phi}\left(\left|h_{i^*k}\right|^2/d_k^{\alpha}\right)$，$f_Z(\cdot)$ 表示随机变量 Z 的 PDF。利用参考文献[16]中的式（42），可将

式（15）化简为：

$$P_{\text{out}}\left(R_{\text{S}}\right)=\sum_{m=0}^{N_{\text{T}}}\binom{N_{\text{T}}}{m}(-1)^{m}\cdot \underbrace{\int_{0}^{\infty}\exp\left(-cmd_{\text{I}}^{\alpha}2^{R_{\text{S}}}x\right)f_{Z}\left(x\right)\text{d}x}_{\Delta} \tag{16}$$

其中的积分部分可转化为求数学期望的形式：

$$\begin{aligned}\Delta&=\mathbb{E}\left[\exp\left(-cmd_{\text{I}}^{\alpha}2^{R_{\text{S}}}Z\right)\right]\\&\overset{\text{(A)}}{=\!=}\mathbb{E}_{\Phi}\left[\prod_{k\in\Phi}\int_{0}^{\infty}\exp\left(-cmxd_{\text{I}}^{\alpha}2^{R_{\text{S}}}/d_{k}^{\alpha}\right)\exp\left(-x\right)\text{d}x\right]\\&\overset{\text{(B)}}{=\!=}\exp\left(-\rho_{\text{E}}\int_{0}^{2\pi}\int_{0}^{R}\left(1-\frac{1}{cm2^{R_{\text{S}}}\left(d_{\text{I}}/r\right)^{\alpha}}\right)r\text{d}r\text{d}\theta\right)\\&=\exp\left(-\pi\rho_{\text{E}}R^{2}{}_{2}F_{1}\left(1,\frac{2}{\alpha};1+\frac{2}{\alpha};-\frac{R^{\alpha}}{cmd_{\text{I}}^{\alpha}2^{R_{\text{S}}}}\right)\right)\end{aligned} \tag{17}$$

其中，等式 (A) 中的 $\exp\left(-x\right)$ 为变量 $\left|h_{i*k}\right|^{2}$ 的 PDF，等式 (B) 采用了概率生成函数进行化简，${}_{2}F_{1}\left(\cdot,\cdot;\cdot;\cdot\right)$ 表示高斯超几何函数[20]。

将式（17）代入式（16）可得 ER 合谋窃听场景下 SWIPT 系统的 SOP 闭合表达式，为：

$$P_{\text{out}}\left(R_{\text{S}}\right)=1-\sum_{m=1}^{N_{\text{T}}}\binom{N_{\text{T}}}{m}(-1)^{m+1}\cdot \exp\left(-\pi\rho_{\text{E}}R^{2}{}_{2}F_{1}\left(1,\frac{2}{\alpha};1+\frac{2}{\alpha};-\frac{R^{\alpha}}{cmd_{\text{I}}^{\alpha}2^{R_{\text{S}}}}\right)\right) \tag{18}$$

由式（18）可知：ER 合谋窃听场景下 SWIPT 系统的 SOP 与发射端天线数、发射端与信息接收者之间的距离、路径损耗指数和窃听者密度等参数有关。

对 $\alpha=2$ 的自由空间传播环境，式（18）可简化为：

$$P_{\text{out}}\left(R_{\text{S}}\right)=1-\sum_{m=1}^{N_{\text{T}}}\binom{N_{\text{T}}}{m}(-1)^{m+1}\cdot \left(1+R^{2}\Big/\left(cmd_{\text{I}}^{2}2^{R_{\text{S}}}\right)\right)^{-\pi\rho_{\text{E}}cmd_{\text{I}}^{2}2^{R_{\text{S}}}} \tag{19}$$

令 $\beta=1$、$N_{0}'=0$，即 ER 只进行信息解码不进行能量收集时，则图 1 中 SWIPT 系统的物理层安全模型即可转化为参考文献[16]中窃听者的空间位置服从泊松点过程时的无线网络下行链路的物理层安全模型，式（14）和式（19）可退变为参考文献[16]中的式（12）和式（19），由此可以看出参考文献[16]的结果为本文的特殊情况。

4　数值计算与仿真

下面利用 MATLAB 对采用 PS 接收策略的 SWIPT 系统在不同发射端天线数、发射端与信息接收者之间的距离、窃听者密度、功率分割因子等参数下的 SOP 进行数值计算与仿真实验。若无特殊说明，SWIPT 系统采用参考文献[16]的参数设置，见表 1。

表 1　PS 接收策略下 SWIPT 系统的参数设置

参数名称	参数值
噪声方差 N_{0}'	1
发射端输出信噪比 $\bar{\gamma}$ /dB	30
路径损耗指数 α	4
ER 分布半径 R/m	50
功率分割因子 β	0.5
目标安全速率 R_{S} /(bit· (s·Hz)$^{-1}$)	1
Alice 与 IR 之间的距离 d_{l}/m	10

图 2 给出了不同 N_{T} 下 SWIPT 系统的 SOP 性能曲线。由图 2 可知：在相同的窃听者密度下，SWIPT 系统的 SOP 在两种窃听场景下均随 N_{T} 的增加而减小，这是由于增加 Alice 的 N_{T} 相当于增大了主信道容量，而窃听信道容量保持不变，从而提高了 SWIPT 系统的安全容量，如当 $\rho_{\text{E}}=0.005\ \text{m}^{-2}$，$N_{\text{T}}$ 从 1 增加到 2 时，SWIPT 系统在独立窃听场景下的 SOP 从 0.74 降到 0.65；在合谋窃听场景下的 SOP 从 0.86 降到 0.78；在相同的系统参数配置下，合谋窃听场景下的 SOP 始终大于独立窃听场景下的 SOP，这是由于合谋窃

听场景下每个 ER 可以相互共享窃听到的信息，增加窃听信道的信噪比，因此更容易解码获得机密信息。

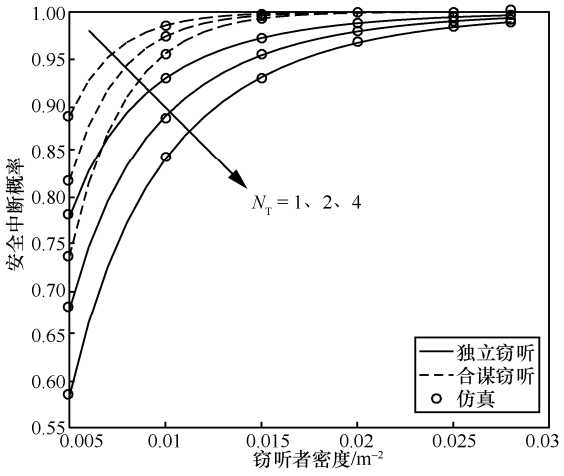

图 2　不同 N_T 下 SWIPT 系统的 SOP 性能曲线

图 3 给出了 SWIPT 系统的 SOP 随发射端与信息接收者之间距离 d_I 的变化曲线，其中 $N_T = 4$。由图 3 可知：SWIPT 系统在独立与合谋两种窃听场景下的 SOP 均随 d_I 的增大而增大，这是由于增大 d_I 减小了主信道容量，导致 SWIPT 系统的安全容量减小；ER 密度越大，则 ER 的数量越多，从而提高了窃听信道容量，因此 SWIPT 无线系统的 SOP 越大，如当 $d_I = 5\,\text{m}$，ρ_E 从 $0.01\,\text{m}^{-2}$ 增大到 $0.02\,\text{m}^{-2}$ 时，SWIPT 系统在独立窃听场景下的 SOP 从 0.35 增大到 0.58；合谋窃听场景下的 SOP 从 0.41 增大到 0.71。

图 4 给出了不同功率分割因子 β 下 SWIPT 系统的 SOP 性能曲线，其中 $N_T = 2$。由图 4 可知：在窃听者密度相同时，SWIPT 系统在独立与合谋两种窃听场景下的 SOP 均随 β 的增大而增大。这是由于增加 β 提高了 ER 信息解码过程的输出信噪比，从而提高了窃听信道容量，降低了 SWIPT 系统的安全容量。如当 $\rho_E = 0.01\,\text{m}^{-2}$ 时，$\beta = 0.5$ 较 $\beta = 0.2$ 在独立窃听与合谋窃听场景下的 SOP 分别增大约 0.07 和 0.03，因此若从 ER 进行窃听的角度考虑，其可设置合适的 PS 因子，在保证收集

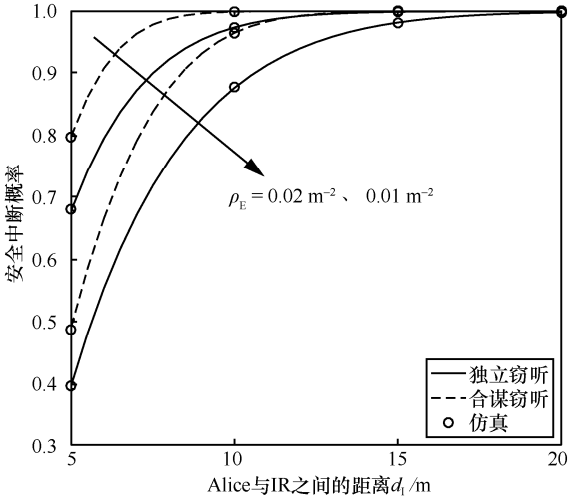

图 3　不同 d_I 下 SWIPT 系统的 SOP 性能曲线

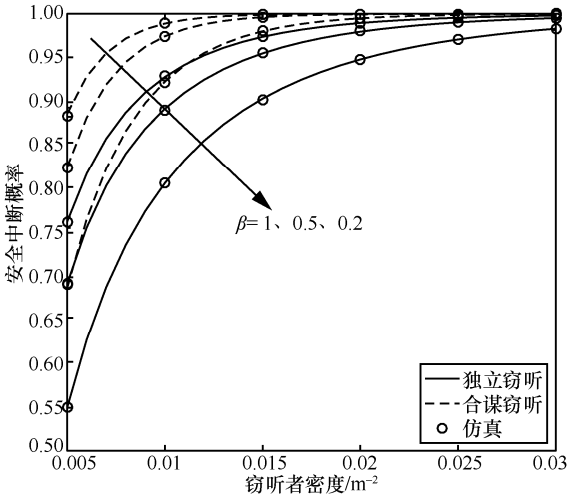

图 4　不同 β 下 SWIPT 系统的 SOP 性能曲线

的能量可以维持正常工作的情况下进行最大限度地窃听。当 $N_T = 1$、$\overline{\gamma} = 50\,\text{dB}$、$R = 100\,\text{m}$ 时，由式（13）获得的 $\beta = 1$ 时的 SOP 曲线即可退变为参考文献[16]的图 2 中的相应曲线。

图 5 给出了不同路径损耗指数 α 下 SWIPT 系统的 SOP 性能曲线，其中 $N_T = 2$。由图 5 可知：在相同窃听者密度下，随着 α 的增大，独立窃听场景下 SWIPT 系统的 SOP 逐渐增大，而合谋窃听场景下的 SOP 则逐渐减小。如当 α 从 2.5 增大到 3.5 时，独立窃听场景下 SWIPT 系统的 SOP 从 0.61 增大到 0.64，而合谋窃听场景下 SWIPT 系统的 SOP 从 0.91 减小到 0.81。

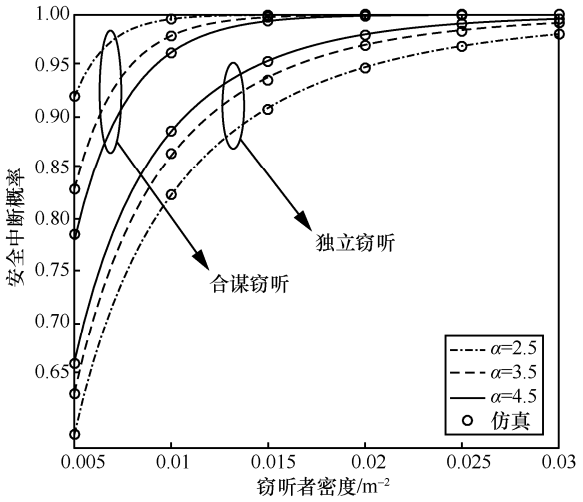

图 5　不同 α 下 SWIPT 系统的 SOP 性能曲线

在图 2~图 5 中，SWIPT 系统在独立与合谋两种窃听场景下的 SOP 数值计算均与仿真结果相吻合，从而验证了本文中理论推导的准确性。

5　结束语

本文将采用 PS 策略的 SWIPT 系统中 ER 视为恶意窃听者，并将其空间位置分布建模为泊松点过程，考虑主信道和窃听信道均遭受路径损耗和瑞利衰落的干扰，利用泊松点过程的概率生成函数分别推导了独立与合谋两种窃听场景下 SWIPT 系统的 SOP 表达式。通过数值计算与仿真实验研究了发射端天线数、发射端与 IR 之间的距离、PS 因子、ER 的密度以及路径损耗因子等参数在独立与合谋两种窃听场景下对 SWIPT 系统的 SOP 性能的影响。

参考文献：

[1] PERERA T D P, JAJAKODY D N K, SHARMA S K, et al. Simultaneous wireless information and power transfer (SWIPT): recent advances and future challenges[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 264-302.

[2] 洪鑫龙, 许晓荣, 姚英彪. 无线携能通信中一种能效优先的缓存队列机制中继选择方案[J]. 电信科学, 2018, 33(3): 67-75.
HONG X L, XU X R, YAO Y B. Energy-efficiency based buffer-aided relay selection scheme in SWIPT[J]. Telecommunication Science, 2018, 33(3): 65-75.

[3] YANG W W, MOU W F, XU X M, et al. Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques[J]. IET Communications, 2016, 10(14): 1712-1720.

[4] WANG Z J, ZHAO H, WANG S, et al. Secrecy analysis in SWIPT systems overgeneralized-K fading channels[J]. IEEE Communications Letters, 2019, 23(5): 834-837.

[5] TANG X X, CAI Y M, DENG Y S, et al. Energy-constrained SWIPT networks: enhancing physical layer security with FD self-jamming[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(1): 212-222.

[6] LIU X L, LI Z, WANG C. Secure decode-and-forward relay SWIPT systems with power splitting scheme[J]. IEEE Transactions on Vehicular Technology, 2018, 67(8): 7341-7354.

[7] LEI H J, DAI Z J, PARK K, et al. Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems[J]. IEEE Transactions on Communications, 2018, 66(12): 6384-6395.

[8] PAN G F, TANG C Q, LI T T, et al. Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems[J]. IEEE Transactions on Communications, 2015, 63(9): 3423-3433.

[9] 李婷婷, 雷宏江, 赵辉, 等. 独立不同分布 Nakagami-*m* 信道下选择合并分集信噪比的统计特性及其应用[J]. 中国科学: 信息科学, 2017, 47(4): 507-515.
LI T T, LEI H J, ZHAO H, et al. On the statistics of the outcome SNR of selective combiner over i.n.d. Nakagami-*m* channels and its applications (in Chinese)[J]. Scientia Sinica Informations, 2017, 47(4): 507-515.

[10] PAN G F, LEI H J, DENG Y S, et al. On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI[J]. IEEE Transactions on Communications, 2016, 64(9): 3831-3843.

[11] 鲍慧, 张敏敏, 姚亚青, 等. 大规模天线 SWIPT 的安全速率性能分析[J]. 电信科学, 2017, 32(9): 36-43.
BAO H, ZHANG M M, YAO Y Q, et al. Performance analysis of secrecy rate for SWIPT in massive antenna[J]. Telecommunications Science, 2017, 32(9): 36-43.

[12] XU W J, LI S Y, LEE C H, et al. Optimal secure multicast with simultaneous wireless information and power transfer in presence of multi-party eavesdropper-collusion[J]. IEEE Transactions on Vehicular Technology, 2016, 65(11): 9123-9137.

[13] 张波, 黄开枝, 钟州, 等. 异构携能通信网络中人工噪声辅助的顽健能量与信息安全传输方案[J]. 通信学报, 2019, 40(3): 60-72.
ZHANG B, HUANG K Z, ZHONG Z, et al. Artificial noise-aided robust secure information and power transmission scheme in heterogeneous networks with simultaneous wireless information and power transfer[J]. Journal on Communications, 2019, 40(3): 60-72.

[14] 马克明, 陈亚军, 胡鑫, 等. 面向物联网无线携能通信系统的机会安全传输方案[J]. 通信学报, 2019, 40(2): 70-81.
MA K M, CHEN Y J, HU X, et al. Opportunistic secure transmission scheme for simultaneous wireless information and power transfer[J]. Journal on Communications, 2019, 40(2): 70-81.
[15] CHEN G J, COON J P. Secrecy outage analysis in random wireless networks with antenna selection and user ordering[J]. IEEE Wireless Communications Letters, 2017, 6(3): 334-337.
[16] CHEN G J, COON J P, RENZO M D. Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(5): 1195-1206.
[17] GERACI G, SINGH S, ANDREWS J G. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers[J]. IEEE Transactions on Wireless Communications, 2014, 13(5): 2931-2943.
[18] ZHENG T X, WANG H M, YIN Q Y. On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers[J]. IEEE Communications Letter, 2014, 18(8): 1299-1302.
[19] YANG N, YEOH P L, ELKASHLAN M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels[J]. IEEE Transactions on Communications, 2013, 61(1): 144-154.
[20] GRADSHTEYN I S, RYZHIK I M. Table of integrals, series and products[M]. Pittsburgh: Academic Press, 2007.

[作者简介]

钱辉（1994– ），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。

李光球（1966– ），男，博士，杭州电子科技大学通信工程学院教授，主要研究方向为无线通信、信息论与编码等。

丁一凡（1996– ），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为无线通信。