中国科学: 信息科学 2017 年 第 47 卷 第 9 期: 1242–1254
SCIENTIA SINICA Informationis
论文

解码转发中继选择系统的安全性能分析

雷宏江[1*], 张环[1], 刘俊杰[1], 潘高峰[2]

1. 重庆邮电大学移动通信技术重庆市重点实验室, 重庆 400065
2. 西南大学非线性电路与智能信息处理重庆市重点实验室, 重庆 400715
* 通信作者. E-mail: leihj@cqupt.edu.cn

收稿日期: 2017–03–21; 接受日期: 2017–06–09; 网络出版日期: 2017–08–23
国家自然科学基金 (批准号: 61471076, 61401372)、重庆市教委科学技术研究项目 (批准号: KJ1600413) 和重庆市基础科学与前沿技术研究项目 (批准号: cstc2017jcyjAX0204) 资助

摘要 本文研究源节点与中继节点发送的信号均能被窃听时, 多中继自适应解码转发 (decode-and-forward, DF) 系统的安全性能. 根据信道状态信息是否可知, 分析最优中继选择 (optimal relay selection, ORS)、传统中继选择 (conventional relay selection, CRS) 和多中继选择 (multiple relays selection, MRS) 3 种方案的安全性能, 推导出 3 种方案安全中断概率的解析表达式. 通过渐进性能分析, 得到了 3 种方案的安全分集增益和安全分集阶数. 仿真结果验证了理论研究的正确性, 并分析得到不同参数对系统安全性能的影响. 结果表明多中继场景中, ORS 方案对系统的安全性能提升最为明显, 3 种方案的安全分集阶数相同且均与中继个数有关, 窃听信道参数只对系统安全分集增益有影响. 最后, 给出了系统最佳功率分配方法.

关键词 物理层安全, 解码转发, 中继选择, 安全中断概率, 功率分配

1 引言

由于传输信道的开放性和广播性, 无线通信较有线通信面临更加严峻的可靠性和安全性挑战. 传统的保密通信主要利用密钥通过复杂的加密算法保证信息的安全传输, 但随着计算机运算速度的不断提升, 这种加密方式变得容易破解. 建立在 Shannon 信息论基础上的物理层安全 (physical layer security, PLS) 利用无线信道的时变性和随机性来实现安全通信 [1], 近年来逐渐成为无线通信的研究热点 [2].

早期的物理层安全研究主要是分析不同衰落信道下三节点 Wiretap 模型的安全性能 [3~5]. 近些年来, 利用人工噪声、波束成形、多天线分集、多用户分集等技术提升系统安全性能逐渐成为 PLS 领域的研究热点. 文献 [6,7] 提出将波束成形和人工干扰相结合的方案增强 PLS 性能; 文献 [8] 指出利用多天线技术能够很好提升系统的安全性和可靠性; 文献 [9] 提出发射天线选择 (transmit antenna selection,

引用格式: 雷宏江, 张环, 刘俊杰, 等. 解码转发中继选择系统的安全性能分析. 中国科学: 信息科学, 2017, 47: 1242–1254, doi: 10.1360/N112017-00002
Lei H J, Zhang H, Liu J J, et al. Security performance analysis of DF relay selection systems (in Chinese). Sci Sin Inform, 2017, 47: 1242–1254, doi: 10.1360/N112017-00002

TAS) 方案, 分析了接收端分别采用选择合并 (selection combining, SC) 和最大比值合并 (maximal ratio combining, MRC) 时系统的安全性能, 推导出安全中断概率 (secrecy outage probability, SOP) 和渐近 SOP 的闭式解析表达式. 然而, 由于移动终端体积和功率的限制, 很多设备上难以配备多根天线, 通过空间上不同位置的中继节点形成虚拟的多天线阵列, 协同无线终端收发信号的协作网络, 也能很好地提升系统的安全性能 [10].

在协作网络中根据某种合适的策略选择合适的中继发送信号可以有效提升网络安全性能 [11]. 文献 [12] 通过考虑中继和窃听信道状态信息 (channel state information, CSI), 提出了两种提升 PLS 的有效中继选择方案, 推导出系统 SOP 的闭式解析表达式. 文献 [13] 提出了一种广义多中继选择方案提升系统的 PLS 性能, 并推导出系统 SOP 的闭式解析表达式. 文献 [14] 研究了可发送人工噪声的认知无线电协作网络中选择不同中继节点和干扰节点的 PLS 安全性能, 推导出系统 SOP 的闭式解析表达式. 文献 [15] 在分析协作系统的安全性能时, 考虑放大转发 (amplify-and-forward, AF) 和解码转发 (decode-and-forward, DF) 两种协作协议, 分析了最优中继选择 (optimal relay selection, ORS)、传统中继选择 (conventional relay selection, CRS) 和多中继选择 (multiple relay selection, MRS) 3 种方案的系统中断概率 (outage probability, OP) 和截获概率 (intercept probability, IP).

本文的创新点可以归纳如下:

(1) 本文研究分析了源节点与中继节点发送的信号均被窃听时, 自适应 DF 协作系统 (即当信源到中继的信道容量大于设定的阈值时, 中继节点可以成功解码信源信号 [16,17]) 的物理层安全性能. 成功解码的中继节点根据主信道和窃听信道瞬时 CSI 是否可知, 采用相应的中继选择方案发送信息, 提升系统安全容量, 保证信息安全传输. 本文推导出 3 种不同中继选择方案下 SOP 的闭式解析表达式, 分析了各项参数对系统安全性能的影响. 为了更加直观地分析系统的安全性能, 本文还推导出不同中继选择方案的渐近 SOP 闭式解析表达式, 分析得到了系统的安全分集阶数和安全分集增益. 最后, 给出了一种简单的最佳功率分配方案的设计方法.

(2) 文献 [12~15] 的系统模型均假设因为严重的路径损耗和阴影衰落, 源节点与窃听节点间无直传链路. 在实际应用中, 窃听节点位置往往是任意的. 因此, 文献 [12~15] 的假设具有局限性. 本文考虑更加实际的情况，即源节点与中继节点发出的信号均能被窃听的情况.

(3) 文献 [15] 分析解码转发协议时, ORS 和 CRS 采用固定 DF 协议 [17], MRC 采用自适应 DF 协议, 对比不具有公平性. 此外, 评价系统安全性能的 OP 和 IP 均为 SOP 的特殊形式. 本文考虑更加一般的情况, 研究了不同的中继选择策略中均采用自适应 DF 协议时系统的物理层安全性能，并推导出 SOP 的准确和渐进闭式解析式.

(4) 文献 [18, 19] 研究了含窃听直传中继单输入多输出 (single input multiple output, SIMO) 系统的物理层安全性能, 但都只考虑单个中继节点的情况. 本文考虑存在多个中继节点时的场景, 根据中继节点上拥有的不同 CSI 的情况, 分析了 3 种不同的中继选择策略的安全中断概率.

2 系统模型

本文考虑如图 1 所示的系统模型, 包含源节点 S, N 个自适应译码转发中继节点 $\mathrm{R}_i\,(i=1,\ldots,N)$, 目的节点 D, 以及窃听节点 E, 图中所有的节点只配置一根天线并且在半双工模式下工作. 假设由于严重的多径和阴影衰落 S 和 D 之间无直传链路, 只能通过 R_i 的协同经过两个时隙才能完成通信 [20], E 能通过 $\mathrm{S}\to\mathrm{E}$ 链路窃取 S 发送的合法信号. 各个节点之间的信道可以分成 $\mathrm{S}\to\mathrm{R}_i$, $\mathrm{S}\to\mathrm{E}$, $\mathrm{R}_i\to\mathrm{E}$, $\mathrm{R}_i\to\mathrm{D}$ 4 组, 每组信道均为独立同分布准静态 Rayleigh 信道, 平均信道增益为 ρ_j, 信道系数为 h_j, 这里

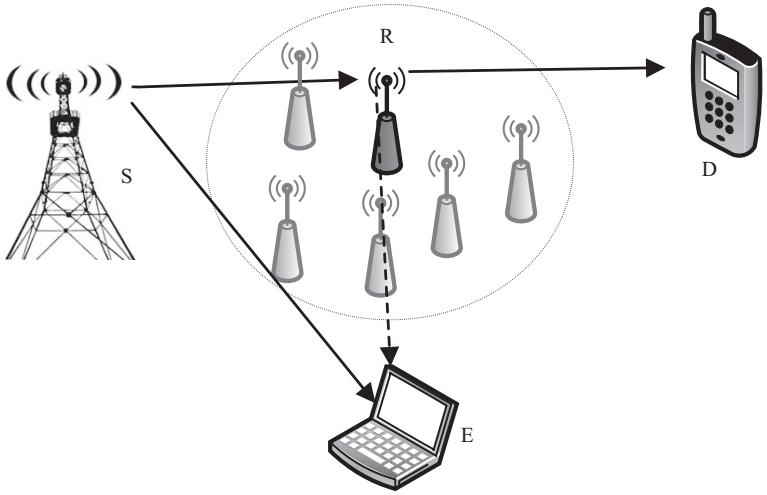

图 1　系统模型

Figure 1　System model

的 $j \in \{\mathrm{SR}, \mathrm{SE}, \mathrm{RD}, \mathrm{RE}\}$ 用于区分不同的信道. 各组信道增益 $Y_j = |h_j|^2$ 的概率密度函数 (probability density function, PDF) 和累计分布函数 (cumulative distribution function, CDF) 如下所示:

$$f_{Y_j}(y) = \lambda_j \exp(-\lambda_j y), \tag{1}$$

$$F_{Y_j}(y) = 1 - \exp(-\lambda_j y), \tag{2}$$

其中 $\lambda_j = 1/\rho_j$.

在第 1 个时隙, S 发送的信号被中继节点和窃听节点接收, R_i 和 E 的接收信号可以分别表示为

$$y_{\mathrm{SR}_i} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}_i} x + n_{\mathrm{SR}}, \tag{3}$$

$$y_{\mathrm{SE}} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SE}} x + n_{\mathrm{SE}}, \tag{4}$$

其中 P_{S} 为源节点的发射功率, n_{SR}, n_{SE} 是均值为 0 方差为 N_0 的加性 Gauss 白噪声. S 到 R_i 的信道容量可以表示为

$$C_{\mathrm{SR}_i} = \frac{1}{2} \log(1 + \alpha Y_{\mathrm{SR}_i}), \tag{5}$$

其中 $\frac{1}{2}$ 表示由中继节点协同完成从 S 到 D 的信息传输需要两个时隙, $\alpha = P_{\mathrm{S}}/N_0$.

由文献 [17] 中关于自适应 DF 协议的定义可知, 当 C_{SR_i} 大于给定的目标信息速率 R_{th} 时, 中继节点能够成功解码 S 发送的信号, 成功解码的中继集合用 Φ 表示, 成功解码的中继个数满足 $0 \leqslant |\Phi| = L \leqslant N$ 条件. 在第 2 个时隙, 将从 Φ 中选出一个最佳中继节点 $\mathrm{R_b}$ 转发 S 信号. 此时, D 和 E 的接收信号可以分别表示为

$$y_{\mathrm{R_bD}} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{R_bD}} x + n_{\mathrm{RD}}, \tag{6}$$

$$y_{\mathrm{R_bE}} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{R_bE}} x + n_{\mathrm{RE}}, \tag{7}$$

其中 P_{R} 为中继节点的发射功率, n_{RD}, n_{RE} 是均值为 0, 方差为 N_0 的加性 Gauss 白噪声, 当中继节点 $\mathrm{R_b}$ 转发信号时, 节点 D 接收的瞬时信噪比表示为 $\gamma_{\mathrm{D}}^{\mathrm{b}} = \beta Y_{\mathrm{R_bD}}$, 其中 $\beta = P_{\mathrm{R}}/N_0$.

为了最大化接收信噪比, 窃取更多的合法信息, 节点 E 采用 MRC 合并方式接收两个时隙的信号. 节点 E 的瞬时信噪比表示为 $\gamma_{\mathrm{E}}^{b}=\alpha Y_{\mathrm{SE}}+\beta Y_{\mathrm{R_bE}}$. 因此系统的瞬时安全容量 [21] 可以表示为

$$\begin{aligned}C_{\mathrm{s}}&=\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{D}}^{b}\right)-\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}^{b}\right)\\&=\frac{1}{2}\log_2\left(1+\beta Y_{\mathrm{R_bD}}\right)-\frac{1}{2}\log_2\left(1+\alpha Y_{\mathrm{SE}}+\beta Y_{\mathrm{R_bE}}\right).\end{aligned}\tag{8}$$

由式 (8) 可以看出 $\mathrm{R_b}$ 到 D/E 的瞬时信道增益对系统瞬时安全容量有很大的影响, 结合相应的信道参数从 Φ 中选出一个最佳中继节点能够很好地提升系统瞬时安全容量. 接下来将分别讨论 R 到 D 或 E 的信道状态信息是否可知的 3 种情形, 依次分析相应中继选择方案的系统瞬时安全容量.

2.1 ORS 方案

当 R 到 D 和 E 的 CSI 均能被 R 获知, 这种场景称为主动窃听 (active eavesdropping) [22]. 此时, 以系统安全容量最大作为中继选择的依据, 记为 ORS 方案 [15]. 被选中的中继可表示为

$$\begin{aligned}b&=\arg\max_{k\in\Phi}\left[\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{D}}^{k}\right)-\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}^{k}\right)\right]^{+}\\&=\arg\max_{k\in\Phi}\left(\frac{1+\beta Y_{\mathrm{R}_k\mathrm{D}}}{1+\alpha Y_{\mathrm{SE}}+\beta Y_{\mathrm{R}_k\mathrm{E}}}\right).\end{aligned}\tag{9}$$

ORS 方案下, 系统的瞬时安全容量可表示为

$$C_{\mathrm{s}}^{\mathrm{ORS}}=\frac{1}{2}\log_2\left(\gamma_{\mathrm{eq}}\right),\tag{10}$$

其中 $\gamma_{\mathrm{eq}}=\max\limits_{k\in\Phi}(\gamma_{\mathrm{eq}}^{k})=\max\limits_{k\in\Phi}(\frac{1+\beta Y_{\mathrm{R}_k\mathrm{D}}}{1+\alpha Y_{\mathrm{SE}}+\beta Y_{\mathrm{R}_k\mathrm{E}}})$.

γ_{eq}^{k} 在 Y_{SE} 下的条件 CDF 可表示为

$$\begin{aligned}F_{\gamma_{\mathrm{eq}}^{k}|Y_{\mathrm{SE}}}(\gamma)&=\int_0^{\infty}F_{\mathrm{RD}}\left(\frac{\alpha\gamma}{\beta}Y_{\mathrm{SE}}+\gamma y+\frac{\gamma-1}{\beta}\right)f_{Y_{\mathrm{RE}}}(y)\,\mathrm{d}y\\&=1-\frac{\lambda_{\mathrm{RE}}}{\lambda_{\mathrm{RD}}\gamma+\lambda_{\mathrm{RE}}}\exp\left(-\lambda_{\mathrm{RD}}\left(\frac{\alpha\gamma}{\beta}Y_{\mathrm{SE}}+\frac{\gamma-1}{\beta}\right)\right),\end{aligned}\tag{11}$$

则 γ_{eq} 在 Y_{SE} 下的条件 CDF 可表示为

$$\begin{aligned}F_{\gamma_{\mathrm{eq}}|Y_{\mathrm{SE}}}(\gamma)&=\prod_{k\in\Phi}F_{\gamma_{\mathrm{eq}}^{k}|Y_{\mathrm{SE}}}(\gamma)\\&=\sum_{l=0}^{L}\frac{L!(-1)^l}{l!\,(L-l)!}\left(\frac{\lambda_{\mathrm{RE}}}{\lambda_{\mathrm{RD}}\gamma+\lambda_{\mathrm{RE}}}\right)^{l}\exp\left(-\lambda_{\mathrm{RD}}l\left(\frac{\alpha\gamma}{\beta}Y_{\mathrm{SE}}+\frac{\gamma-1}{\beta}\right)\right).\end{aligned}\tag{12}$$

因此, γ_{eq} 的 CDF 可以表示为

$$\begin{aligned}F_{\gamma_{\mathrm{eq}}}(\gamma)&=\int_0^{\infty}F_{\gamma_{\mathrm{eq}}|Y_{\mathrm{SE}}}(\gamma)\,f_{Y_{\mathrm{SE}}}(y)\,\mathrm{d}y\\&=\sum_{l=0}^{L}\frac{L!(-1)^l\beta\lambda_{\mathrm{SE}}}{l!\,(L-l)!\,(\lambda_{\mathrm{RD}}l\alpha\gamma+\beta\lambda_{\mathrm{SE}})}\left(\frac{\lambda_{\mathrm{RE}}}{\lambda_{\mathrm{RD}}\gamma+\lambda_{\mathrm{RE}}}\right)^{l}\exp\left(-\lambda_{\mathrm{RD}}l\frac{\gamma-1}{\beta}\right).\end{aligned}\tag{13}$$

2.2 CRS 方案

当 R 到 D 的 CSI 能被 R 获知, R 到 E 的 CSI 不能被 R 获知 (一般由窃听节点为被动通信节点或者恶意保持静默造成), 这种场景称为被动窃听 (passive eavesdropping) [22]. 此时, 以 D 接收到的信噪比最大作为中继选择的依据, 记为 CRS 方案 [23]. 被选中的中继可表示为

$$b = \arg\max_{k\in\Phi} \left(\beta Y_{\mathrm{R}_k\mathrm{D}}\right). \tag{14}$$

CRS 方案下, 系统的瞬时安全容量可表示为

$$C_{\mathrm{s}}^{\mathrm{CRS}} = \left[\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{D}}^{\mathrm{CRS}}\right) - \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}^{\mathrm{CRS}}\right)\right]^+, \tag{15}$$

其中 $\gamma_{\mathrm{D}}^{\mathrm{CRS}} = \max\limits_{k\in\Phi}\left(\beta Y_{\mathrm{R}_k\mathrm{D}}\right)$, $\gamma_{\mathrm{E}}^{\mathrm{CRS}} = \alpha Y_{\mathrm{SE}} + \beta Y_{\mathrm{R_bE}}$, $\gamma_{\mathrm{D}}^{\mathrm{CRS}}$ 的 CDF 可表示为

$$F_{\gamma_{\mathrm{D}}^{\mathrm{CRS}}}(\gamma) = \prod_{k\in\Phi} F_{Y_{\mathrm{R}_k\mathrm{D}}}\left(\frac{\gamma}{\beta}\right) = \left(1-\exp\left(-\lambda_{\mathrm{RD}}\frac{\gamma}{\beta}\right)\right)^L. \tag{16}$$

αY_{SE} 的矩母函数 (moment generating function, MGF) 为

$$M_{\alpha Y_{\mathrm{SE}}}(s) = \int_0^\infty f_{\alpha Y_{\mathrm{SE}}}(y)\exp(-sy)\mathrm{d}y = \frac{\lambda_{\mathrm{SE}}}{\lambda_{\mathrm{SE}}+\alpha s}, \tag{17}$$

$\beta Y_{\mathrm{R_bE}}$ 的 MGF 为

$$M_{\beta Y_{\mathrm{R_bE}}}(s) = \frac{\lambda_{\mathrm{RE}}}{\lambda_{\mathrm{RE}}+\beta s}. \tag{18}$$

由式 (17) 和 (18) 可得 $\gamma_{\mathrm{E}}^{\mathrm{CRS}}$ 的 MGF 为

$$M_{\gamma_{\mathrm{E}}^{\mathrm{CRS}}}(s) = M_{\alpha Y_{\mathrm{SE}}}(s)\, M_{\beta Y_{\mathrm{R_bE}}}(s) = \frac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{RE}}}{(\lambda_{\mathrm{SE}}+\alpha s)(\lambda_{\mathrm{RE}}+\beta s)}. \tag{19}$$

对式 (19) 求拉斯反变换可得 $\gamma_{\mathrm{E}}^{\mathrm{CRS}}$ 的 PDF 表达式为

$$f_{\gamma_{\mathrm{E}}^{\mathrm{CRS}}}(y) = \frac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{RE}}}{\alpha\lambda_{\mathrm{RE}}-\beta\lambda_{\mathrm{SE}}}\left(\exp\left(-\frac{\lambda_{\mathrm{SE}}}{\alpha}y\right) - \exp\left(-\frac{\lambda_{\mathrm{RE}}}{\beta}y\right)\right). \tag{20}$$

2.3 MRS 方案

当 R 到 D 和 R 到 E 的 CSI 均不能被 R 获知, 为了保证目的节点的接收信噪比, 确保主信道容量的最大化, Φ 中的所有中继均转发信号, 记为 MRS 方案 [15]. 由于 ORS 和 CRS 中均只选出一个中继发送信号, 为了保证对比的公平性, 这里假设 Φ 中每个中继的发送功率为 $\frac{P_{\mathrm{R}}}{L}$. 此时, 节点 D 和 E 的瞬时接收信噪比分别表示为

$$\gamma_{\mathrm{D}}^{\mathrm{MRS}} = \frac{\beta}{L}\sum_{k\in\Phi} Y_{\mathrm{R}_k\mathrm{D}}, \tag{21}$$

$$\gamma_{\mathrm{E}}^{\mathrm{MRS}} = \alpha Y_{\mathrm{SE}} + \frac{\beta}{L}\sum_{k\in\Phi} Y_{\mathrm{R}_k\mathrm{E}}. \tag{22}$$

MRS 方案下, 系统的瞬时安全容量可表示为

$$C_{\mathrm{s}}^{\mathrm{MRS}} = \left[\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{D}}^{\mathrm{MRS}}\right) - \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}^{\mathrm{MRS}}\right)\right]^+, \tag{23}$$

其中 $\gamma_{\mathrm{D}}^{\mathrm{MRS}}=\frac{\beta}{L}\sum_{k\in\Phi}Y_{\mathrm{R}_k\mathrm{D}}$, $\gamma_{\mathrm{E}}^{\mathrm{MRS}}=\alpha Y_{\mathrm{SE}}+\frac{\beta}{L}\sum_{k\in\Phi}Y_{\mathrm{R}_k\mathrm{E}}$.

由文献 [24] 可得 $\gamma_{\mathrm{D}}^{\mathrm{MRS}}$ 的 CDF 为

$$F_{\gamma_{\mathrm{D}}^{\mathrm{MRS}}}(\gamma)=1-\exp\left(-\frac{\lambda_{\mathrm{RD}}L}{\beta}\gamma\right)\sum_{l=0}^{L-1}\frac{(\lambda_{\mathrm{RD}}L\gamma)^l}{l!\beta^l}. \tag{24}$$

定义 $Y_{\mathrm{E}}^{\Phi}=\frac{\beta}{L}\sum_{k\in\Phi}Y_{\mathrm{R}_k\mathrm{E}}$, 由文献 [24] 可得 Y_{E}^{Φ} 的 PDF 为

$$f_{Y_{\mathrm{E}}^{\Phi}}(y)=\frac{L}{\beta}f_{Y_{\mathrm{RE}}}\left(\frac{L}{\beta}y\right)=\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^L\frac{y^{L-1}}{(L-1)!}\exp\left(-\frac{\lambda_{\mathrm{RE}}L}{\beta}y\right), \tag{25}$$

计算可得 Y_{E}^{Φ} 的 MGF 为

$$M_{Y_{\mathrm{E}}^{\Phi}}(s)=\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^L\frac{1}{\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}+s\right)^L}. \tag{26}$$

由式 (17) 和 (26) 可得 $\gamma_{\mathrm{E}}^{\mathrm{MRS}}$ 的 MGF 为

$$M_{\gamma_{\mathrm{E}}^{\mathrm{MRS}}}(s)=\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^L\frac{\lambda_{\mathrm{SE}}}{\alpha}\left[\sum_{p=1}^{L}\frac{A_p}{\left(s+\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^p}+\frac{B}{s+\frac{\lambda_{\mathrm{SE}}}{\alpha}}\right], \tag{27}$$

其中

$$A_p=\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^L\frac{\lambda_{\mathrm{SE}}(-1)^{L-p}}{(p-1)!\alpha\left(\frac{\lambda_{\mathrm{SE}}}{\alpha}-\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^{L-p+1}},\quad B=\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}\right)^L\frac{\lambda_{\mathrm{SE}}}{\alpha\left(\frac{\lambda_{\mathrm{RE}}L}{\beta}-\frac{\lambda_{\mathrm{SE}}}{\alpha}\right)^L}.$$

对式 (27) 求拉斯反变换可得 $\gamma_{\mathrm{E}}^{\mathrm{MRS}}$ 的 PDF 表达式为

$$f_{\gamma_{\mathrm{E}}^{\mathrm{MRS}}}(y)=\sum_{p=1}^{L}A_p y^{p-1}\exp\left(-\frac{\lambda_{\mathrm{RE}}L}{\beta}y\right)+B\exp\left(-\frac{\lambda_{\mathrm{SE}}}{\alpha}y\right). \tag{28}$$

3 安全中断概率分析

安全中断概率定义为瞬时安全容量小于某一预定的目标安全速率 R_{s} 的概率 [21], 是系统安全性能分析的常用指标. 根据全概率公式, 图 1 所示系统的 SOP 可表示为

$$\begin{aligned}P_{\mathrm{out}}&=\Pr\left(C_{\mathrm{s}}\leqslant R_{\mathrm{s}}\right)\\&=\sum_{L=0}^{N}\frac{N!}{L!\,(N-L)!}\Pr\left(|\Phi|=L\right)\underbrace{\Pr\left(C_{\mathrm{s}}\leqslant R_{\mathrm{s}}\,||\Phi|=L\right)}_{P_{\mathrm{out}}^{L}},\end{aligned} \tag{29}$$

其中 $\Pr(|\Phi|=L)$ 为 L 个中继成功译码的概率, P_{out}^{L} 为 $|\Phi|=L$ 条件下的安全中断概率.

由式 (5) 和自适应译码转发协议可得

$$\begin{aligned}\Pr\left(|\Phi|=L\right)&=\Pr\left(\bigcap_{k\in\Phi}C_{\mathrm{SR}_k}\geqslant R_{\mathrm{th}},\bigcap_{i\notin\Phi}C_{\mathrm{SR}_i}<R_{\mathrm{th}}\right)\\&=\exp\left(-L\lambda_{\mathrm{SR}}\theta\right)\left[1-\exp\left(-\lambda_{\mathrm{SR}}\theta\right)\right]^{N-L},\end{aligned} \tag{30}$$

其中 $\theta=\left(2^{2R_{\mathrm{th}}}-1\right)/\alpha$, R_{th} 为中继节点能成功译码的门限值.

接下来依次分析不同选择方案下的 P_{out}^{L}.

3.1 ORS 方案

将式 (13) 带入 P_{out}^{L} 可得 ORS 方案下 P_{out}^{L} 的表达式为

$$P_{\text{out}}^{L,\text{ORS}}=\sum_{l=0}^{L}\frac{L!(-1)^{l}\beta\lambda_{\text{SE}}}{l!\,(L-l)!\,(\lambda_{\text{RD}}\Theta l\alpha+\beta\lambda_{\text{SE}})}\left(\frac{\lambda_{\text{RE}}}{\lambda_{\text{RD}}\Theta+\lambda_{\text{RE}}}\right)^{l}\exp\left(-\lambda_{\text{RD}}l\frac{\Theta-1}{\beta}\right), \tag{31}$$

其中 $\Theta=2^{2R_{\text{s}}}$. 将式 (30) 和 (31) 带入 (29) 可得 ORS 方案系统的安全中断概率为

$$\begin{aligned}P_{\text{out}}^{\text{ORS}}=&\sum_{L=0}^{N}\sum_{l=0}^{L}\frac{N!\exp\left(-L\lambda_{\text{SR}}\theta\right)}{(N-L)!l!\,(L-l)!}[1-\exp\left(-\lambda_{\text{SR}}\theta\right)]^{N-L}\\&\times\frac{(-1)^{l}\lambda_{\text{SE}}}{\lambda_{\text{RD}}l\frac{\alpha\Theta}{\beta}+\lambda_{\text{SE}}}\left(\frac{\lambda_{\text{RE}}}{\lambda_{\text{RD}}\Theta+\lambda_{\text{RE}}}\right)^{l}\exp\left(-\lambda_{\text{RD}}l\frac{\Theta-1}{\beta}\right).\end{aligned} \tag{32}$$

3.2 CRS 方案

将式 (16) 和 (20) 带入 P_{out}^{L}, 利用文献 [25] 中式 (3.326.2) 计算可得 CRS 方案下 P_{out}^{L} 的表达式为

$$P_{\text{out}}^{L,\text{CRS}}=\sum_{n=0}^{L}\frac{L!(-1)^{n}\lambda_{\text{SE}}\lambda_{\text{RE}}}{n!\,(L-n)!\,(\alpha\lambda_{\text{RE}}-\beta\lambda_{\text{SE}})}\exp\left(-\frac{n\lambda_{\text{RD}}\left(\Theta-1\right)}{\beta}\right)\left(\frac{\alpha\beta}{n\alpha\lambda_{\text{RD}}\Theta+\beta\lambda_{\text{SE}}}-\frac{\beta}{n\lambda_{\text{RD}}\Theta+\lambda_{\text{RE}}}\right). \tag{33}$$

将式 (30) 和 (33) 带入 (29) 可得 CRS 方案系统的安全中断概率为

$$\begin{aligned}P_{\text{out}}^{\text{CRS}}=&\sum_{L=0}^{N}\sum_{n=0}^{L}\frac{N!\exp\left(-L\lambda_{\text{SR}}\theta\right)}{(N-L)!n!\,(L-n)!}[1-\exp\left(-\lambda_{\text{SR}}\theta\right)]^{N-L}\\&\times\frac{(-1)^{n}\lambda_{\text{SE}}\lambda_{\text{RE}}}{\alpha\lambda_{\text{RE}}-\beta\lambda_{\text{SE}}}\exp\left(-n\lambda_{\text{RD}}\frac{(\Theta-1)}{\beta}\right)\left(\frac{\alpha\beta}{n\alpha\lambda_{\text{RD}}\Theta+\beta\lambda_{\text{SE}}}-\frac{\beta}{n\lambda_{\text{RD}}\Theta+\lambda_{\text{RE}}}\right).\end{aligned} \tag{34}$$

3.3 MRS 方案

将式 (24) 和 (28) 带入 P_{out}^{L}, 利用文献 [25] 中式 (3.326.2) 计算可得 MRS 方案下 P_{out}^{L} 的表达式为

$$P_{\text{out}}^{L,\text{MRS}}=1-\sum_{l=0}^{L-1}\sum_{m=0}^{l}\Lambda\left[\sum_{p=1}^{L}A_{p}\Xi+B\Psi\right], \tag{35}$$

其中 $\Lambda=\frac{(\lambda_{\text{RD}}L)^{l}\Theta^{m}}{m!(l-m)!\beta^{l}(\Theta-1)^{m-l}}\exp(-\frac{\lambda_{\text{RD}}L(\Theta-1)}{\beta})$, $\Xi=\frac{\Gamma(p+m)}{(\frac{\lambda_{\text{RE}}L+\lambda_{\text{RD}}L\Theta}{\beta})^{p+m}}$, $\Psi=\frac{\Gamma(m+1)}{(\frac{\lambda_{\text{RD}}L\Theta}{\beta}+\frac{\lambda_{\text{SE}}}{\alpha})^{m+1}}$.

将式 (30) 和 (35) 带入 (29) 可得 MRS 方案系统的安全中断概率为

$$P_{\text{out}}^{\text{MRS}}=\sum_{L=0}^{N}\frac{N!\exp\left(-L\lambda_{\text{SR}}\theta\right)}{L!\,(N-L)!}[1-\exp\left(-\lambda_{\text{SR}}\theta\right)]^{N-L}\left[1-\sum_{l=0}^{L-1}\sum_{m=0}^{l}\Lambda\left(\sum_{p=1}^{L}A_{p}\Xi+B\Psi\right)\right]. \tag{36}$$

4 渐近安全中断概率分析

第 3 节中推导出的不同选择方案 SOP 表达式较为复杂, 参考文献 [9], 本节考虑 ρ_{SR} 和 ρ_{RD} 趋于无穷大的特殊情况, 推导 SOP 的渐近表达式, 这种方法能够得到不同选择方案的安全分集增益和安全分集阶数, 便于更加直观地分析系统安全性能 [26].

当 $\rho_{\mathrm{SR}} \to \infty$, 由式 (5) 可得 $C_{\mathrm{SR}_i} \to \infty$. 此时所有中继均能成功译码 ($\Pr(|\Phi| = N) = 1$), 渐近 SOP 可表示为

$$P_{\mathrm{out}}^{\infty} = \Pr\left(C_{\mathrm{s}} \leqslant R_{\mathrm{s}} \,||\Phi| = N\right). \tag{37}$$

由文献 [9,26] 可知, 当 $\rho_{\mathrm{RD}} \to \infty$ 时渐近 SOP 还可表示为

$$P_{\mathrm{out}}^{\infty} = \left(G_a \rho_{\mathrm{RD}}\right)^{-G_d} + \mathcal{O}\left({\rho_{\mathrm{RD}}}^{-G_d}\right), \tag{38}$$

其中 G_d 为系统的安全分集阶数, G_a 为系统的安全分集增益, $\mathcal{O}(\cdot)$ 为高阶无穷小.

4.1 ORS 方案

当 $x \to 0$ 时有 $\mathrm{e}^{-x} \approx 1 - x$, 带入式 (2) 可得 $\beta Y_{\mathrm{R}_k\mathrm{D}}$ 的渐进 CDF 表达式为

$$F_{\beta Y_{\mathrm{R}_k\mathrm{D}}}(\gamma) = \frac{\lambda_{\mathrm{RD}}\gamma}{\beta}. \tag{39}$$

参考 γ_{eq} 的 CDF 推导过程 (式 (13)), 可得 γ_{eq} 近似 CDF 表达式为

$$F_{\gamma_{\mathrm{eq}}}^{\infty}(\gamma) = \sum_{n=0}^{N}\sum_{m=0}^{n} \frac{N!\alpha^m {\lambda_{\mathrm{RD}}}^N (\gamma-1)^{N-n}\gamma^n}{(N-n)!\,(n-m)!\beta^{2N+m-n}\lambda_{\mathrm{RE}}^{n-m}\lambda_{\mathrm{SE}}^{m}}, \tag{40}$$

因此, ORS 方案下 SOP 的渐近表达式为

$$P_{\mathrm{out}}^{\infty,\mathrm{ORS}} = \sum_{n=0}^{N}\sum_{m=0}^{n} \frac{N!\alpha^m {\lambda_{\mathrm{RD}}}^N (\Theta-1)^{N-n}\Theta^n}{(N-n)!\,(n-m)!\beta^{2N+m-n}\lambda_{\mathrm{RE}}^{n-m}\lambda_{\mathrm{SE}}^{m}}. \tag{41}$$

将式 (41) 带入 (38) 计算可得 ORS 方案的安全分集阶数和安全分集增益分别为

$$G_d^{\mathrm{ORS}} = N, \tag{42}$$

$$G_a^{\mathrm{ORS}} = \left[\sum_{n=0}^{N}\sum_{m=0}^{n} \frac{N!\alpha^m (\Theta-1)^{N-n}\Theta^n}{(N-n)!\,(n-m)!\beta^{2N+m-n}\lambda_{\mathrm{RE}}^{n-m}\lambda_{\mathrm{SE}}^{m}}\right]^{-\frac{1}{N}}. \tag{43}$$

4.2 CRS 方案

由式 (16) 和 (39) 可得 $\gamma_{\mathrm{D}}^{\mathrm{CRS}}$ 的 CDF 近似表达式为

$$F_{\gamma_{\mathrm{D}}^{\mathrm{CRS}}}^{\infty}(\gamma) = \left(\frac{\lambda_{\mathrm{RD}}\gamma}{\beta}\right)^N, \tag{44}$$

将式 (20) 和 (44) 带入 (37), 利用文献 [25] 中式 (3.326.2) 可得 CRS 方案下 SOP 的渐近表达式为

$$\begin{aligned} P_{\mathrm{out}}^{\infty,\mathrm{CRS}} &= \int_0^{\infty} F_{\gamma_{\mathrm{D}}^{\mathrm{CRS}}}^{\infty}(\Theta y + \Theta - 1)\, f_{\gamma_{\mathrm{E}}^{\mathrm{CRS}}}(y)\,\mathrm{d}y \\ &= \sum_{n=0}^{N}\left(\frac{\lambda_{\mathrm{RD}}}{\beta}\right)^N \frac{N!\lambda_{\mathrm{RE}}\Theta^n(\Theta-1)^{N-n}}{(N-n)!\,(\alpha\lambda_{\mathrm{RE}} - \beta\lambda_{\mathrm{SE}})}\left(\frac{\alpha^{n+1}}{\lambda_{\mathrm{SE}}^n} - \frac{\beta^{n+1}}{\lambda_{\mathrm{RE}}^n}\right). \end{aligned} \tag{45}$$

将式 (45) 带入 (38) 计算可得 CRS 方案的安全分集阶数和安全分集增益分别为

$$G_d^{\mathrm{CRS}} = N, \tag{46}$$

$$G_a^{\mathrm{CRS}} = \left[\sum_{n=0}^{N} \frac{N!\lambda_{\mathrm{RE}}\Theta^n(\Theta-1)^{N-n}}{\beta^N\,(N-n)!\,(\alpha\lambda_{\mathrm{RE}} - \beta\lambda_{\mathrm{SE}})}\left(\frac{\alpha^{n+1}}{\lambda_{\mathrm{SE}}^n} - \frac{\beta^{n+1}}{\lambda_{\mathrm{RE}}^n}\right)\right]^{-\frac{1}{N}}. \tag{47}$$

4.3 MRS 方案

根据 Taylor 级数展开式 $\mathrm{e}^x=\sum_{l=0}^{N-1}\frac{x^l}{l!}+\frac{x^N}{N!}+\mathcal{O}\left(x^N\right)$, 式 (24) 可以表示为

$$F_{\gamma_{\mathrm{D}}^{\mathrm{MRS}}}^{\infty}(\gamma)=\frac{\left(\lambda_{\mathrm{RD}}N\gamma\right)^N}{N!\beta^N}+\mathcal{O}\left(\gamma^N\right). \tag{48}$$

将式 (28) 和 (48) 带入 (37), 利用文献 [25] 中式 (3.326.2) 可得 MRS 方案下 SOP 的渐近表达式为

$$P_{\mathrm{out}}^{\infty,\mathrm{MRS}}=\sum_{n=0}^{N}\lambda_{\mathrm{RD}}^{N}C\left[\sum_{p=1}^{L}A_p\psi+BZ\right], \tag{49}$$

其中 $C=\frac{N^N\Theta^n(\Theta-1)^{N-n}}{n!(N-n)!\beta^N}$, $\psi=\Gamma(p+n)(\frac{\beta}{\lambda_{\mathrm{RE}}L})^{p+n}$, $Z=\Gamma(p+n)(\frac{\beta}{\lambda_{\mathrm{RE}}L})^{p+n}$.

将式 (49) 带入 (38) 计算可得 MRS 方案的安全分集阶数和安全分集增益分别为

$$G_d^{\mathrm{MRS}}=N, \tag{50}$$

$$G_a^{\mathrm{MRS}}=\left[\sum_{n=0}^{N}C\left(\sum_{p=1}^{L}A_p\psi+BZ\right)\right]^{-\frac{1}{N}}. \tag{51}$$

由 G_a 和 G_d 的表达式可以看出 3 种方案具有同样的安全分集阶数并且只与中继个数有关, 主信道和窃听信道的信道参数只对系统的安全分集增益有影响.

5 功率分配方案设计

本节假设系统的总发射功率为 P_{t}, S 的发送功率为 $P_{\mathrm{S}}=\eta P_{\mathrm{t}}$, R 的发送功率为 $P_{\mathrm{R}}=(1-\eta)P_{\mathrm{t}}$, $\eta\,(0<\eta<1)$ 为功率分配因子, 根据第 3 节中推出的准确 SOP 闭式解析表达式, 给出最优功率分配因子设计方法.

由文献 [27] 可知最优功率分配因子需满足

$$\eta^*=\begin{cases}\min\limits_{\eta}P_{\mathrm{out}}\quad \text{s.t.}\ \ 0<\eta<1,\\ \dfrac{\partial P_{\mathrm{out}}}{\partial\eta}=0.\end{cases} \tag{52}$$

分别对 3 种方案的 SOP 求二阶导数, 可以得到每种方案 $\partial^2P_{\mathrm{out}}/\partial\eta^2>0$ 均成立. 因此, SOP 在 $0<\eta<1$ 有极值, 利用数值寻根法 [28] 可以非常容易找到各个方案的最优功率分配因子 η^*.

6 仿真与分析

本节通过 Monte Carlo 仿真来验证理论分析, 解析曲线由第 3 节获得, 渐近曲线由第 4 节获得. 主要参数设置如下: $\rho_{\mathrm{SE}}=1$ dB, $N_0=1$ W, $R_{\mathrm{th}}=R_{\mathrm{s}}=0.1$ bps/Hz, 仿真次数为 10^6. 图 2∼5 中实线表示解析分析结果, 虚线表示渐近分析结果, "*" 表示 Monte Carlo 仿真分析结果. 从图中可以看出解析和仿真重合, 验证了理论分析结果的正确性.

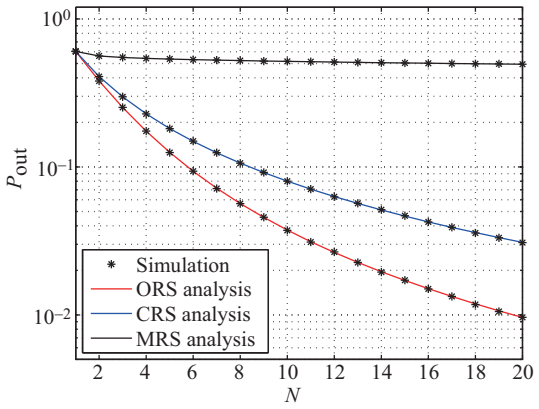

图 2 (网络版彩图) 安全中断概率随 N 变化趋势

Figure 2 (Color online) SOP versus N

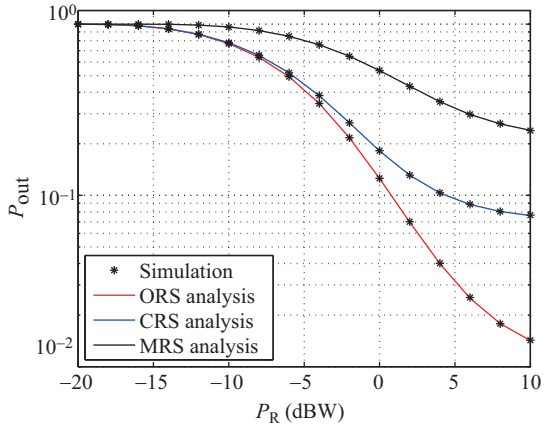

图 3 (网络版彩图) 安全中断概率随 P_{R} 变化趋势

Figure 3 (Color online) SOP versus P_{R}

图 2 中设定 $\rho_{\text{SR}} = \rho_{\text{RD}} = 5$ dB, $\rho_{\text{RE}} = 2$ dB, $P_{\text{S}} = P_{\text{R}} = 1$ dBW, 绘制出不同中继选择方案下安全中断概率 P_{out} 随中继个数 N 变化的曲线图. 从图中可以看出: 当 $N = 1$ 时, 3 种方案的 P_{out} 均相同, 这是由于仅有一个中继可以参与协作转发, 无法采用中继选择方案; 当 $N > 1$ 时, 随着中继个数的增加各个方案的 P_{out} 均不断降低, 这验证了通过增加中继节点个数, 可以增大系统安全分集阶数, 提升系统的安全性能. 此外, 从图 2 中可以看出当 $N > 1$ 时, ORS 方案的 P_{out} 始终最低, 因此采用 ORS 方案对提升系统安全性能最为有效.

图 3 中设定 $N = 5$, $\rho_{\text{SR}} = \rho_{\text{RD}} = 5$ dB, $\rho_{\text{RE}} = 2$ dB, $P_{\text{S}} = 1$ dBW, 绘制出不同中继选择方案下安全中断概率 P_{out} 随中继节点发送功率 P_{R} 变化的曲线图. 从图中可以看出, 随着 P_{R} 的增大, P_{out} 不断降低, 直至成为一个常数. 这是因为增大 P_{R} 可以在一定程度上增大系统的安全容量, 但是当发射功率无限增加时, 系统的安全容量趋于一个常数, 安全容量存在一个上界 [29], 安全中断概率存在一个下界.

图 4 中设定 $N = 5$, $\rho_{\text{SR}} = 100$ dB, $\rho_{\text{RE}} = 3$ dB, $P_{\text{R}} = P_{\text{S}} = 0$ dBW, 绘制出不同中继选择方案下安全中断概率 P_{out} 随 R $\to$ D 信道平均信道增益 ρ_{RD} 变化的曲线图. 从图中可以看出, 随着 ρ_{RD} 的增大, P_{out} 不断降低, 这是因为增大 ρ_{RD} 可以增大目的节点的接收信噪比, 从而提升系统安全性能. 此外, 图 4 中随着 ρ_{RD} 的增大, 渐近曲线逐渐逼近解析曲线, 最后趋于重合, 这验证了渐近分析的正确性. 各个方案的渐近曲线相互平行, 可以证明 3 种方案能够实现相同的安全分集阶数.

图 5 中设定 $N = 3$, $\rho_{\text{SR}} = \rho_{\text{RD}} = 2$ dB, $\rho_{\text{RE}} = 5$ dB, $P_{\text{t}} = 1$ dBW, 绘制出不同中继选择方案下安全中断概率 P_{out} 随功率分配因子 η 变化的曲线图, 并根据第 5 节设计方法, 找出不同方案的最优功率因子 η^* (精确到 0.01). 从图中可以看出, 当 $0 < \eta < \eta^*$ 时, 随着 η 的增大, 系统安全性能不断提升, 这是因为 η 增大了, 成功译码中继数量增加. 当 $\eta^* < \eta < 1$ 时, 随着 η 的增大, 系统安全性能不断降低, 这是由于 P_{R} 减小, 目的节点的接收信噪比降低. 因此 η 值体现了 P_{S} 与 P_{R} 对系统安全性能影响的权衡关系. 通过数值寻根法可以找到在图 5 的参数设定下, ORS 方案的 $\eta^* = 0.25$, CRS 方案的 $\eta^* = 0.24$, MRS 方案的 $\eta^* = 0.09$.

7 结论

本文针对多中继协作系统, 研究了源节点和中继节点发送的信号均能被窃听时, 不同中继选择方

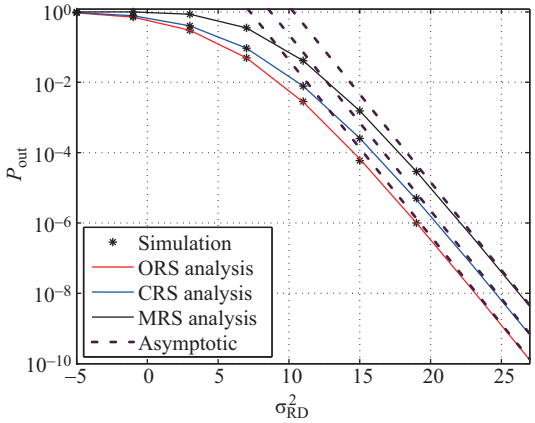

图 4 (网络版彩图) 安全中断概率随 $\rho_{\rm RD}$ 变化趋势

Figure 4 (Color online) SOP versus $\rho_{\rm RD}$

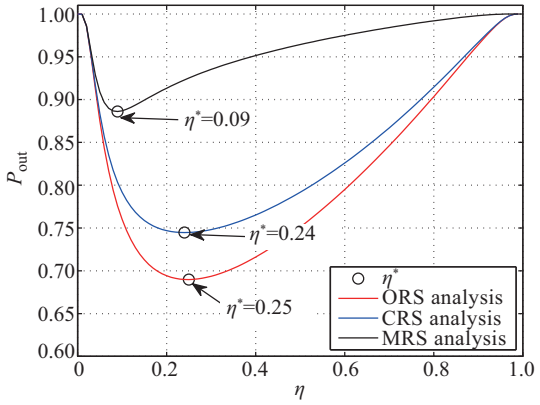

图 5 (网络版彩图) 安全中断概率随 η 变化趋势

Figure 5 (Color online) SOP versus η

案下采用自适应解码转发协议的物理层安全性能. 首先, 推导出不同中继选择方案下的安全中断概率闭式解析表达式, 得到系统参数与安全性能的关系; 其次, 推导出不同中继选择方案下的渐近安全中断概率闭式解析表达式, 能够更直观地研究系统安全性能. 通过对渐近安全中断概率的分析讨论得出 3 种选择方案具有同样的安全分集阶数, 并且只与中继个数有关, 主信道和窃听信道的信道参数只对系统的安全分集增益有影响; 最后给出了系统的最优功率分配方案. 仿真结果验证了理论分析的正确性, 研究结果能够为实际中考虑物理层安全的协作系统设计提供一定的参考价值.

参考文献

1 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387

2 Yang N, Wang L F, Giovanni G, et al. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun Mag, 2015, 53: 20–27

3 Lei H J, Gao C, Guo Y C, et al. On physical layer security over generalized gamma fading channels. IEEE Commun Lett, 2015, 19: 1257–1260

4 Lei H J, Zhang H, Ansari I S, et al. Performance analysis of physical layer security over generalized-K fading channels using a mixture gamma distribution. IEEE Commun Lett, 2016, 20: 408–411

5 Liu X. Probability of strictly positive secrecy capacity of the Rician-Rician fading channel. IEEE Wirel Commun Lett, 2013, 2: 50–53

6 Wang H M, Luo M, Yin Q Y, et al. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. IEEE Trans Inf Foren Secur, 2013, 8: 2007–2020

7 Wang H M, Liu F, Yang M C. Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems. IEEE Trans Veh Technol, 2015, 64: 4893–4898

8 Khisti A, Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel. IEEE Trans Inf Theory, 2010, 56: 3088–3104

9 Yang N, Yeoh P L, Elkashlan M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans Commun, 2013, 61: 144–154

10 Zou Y L, Zhu J, Wang X B, et al. Improving physical-layer security in wireless communications using diversity techniques. IEEE Netw, 2015, 29: 42–48

11 Chen X M, Zhong C J, Yuen C, et al. Multi-antenna relay aided wireless physical layer security. IEEE Commun Mag, 2015, 53: 40–46

12 Krikidis I. Opportunistic relay selection for cooperative networks with secrecy constraints. IET Commun, 2010, 4:

1787–1791
13 Wang W, Teh K C, Li K H. Generalized relay selection for improved security in cooperative DF relay networks. IEEE Wirel Commun Lett, 2016, 5: 28–31
14 Liu Y W, Wang L F, Duy T T, et al. Relay selection for security enhancement in cognitive relay networks. IEEE Wirel Commun Lett, 2015, 4: 46–49
15 Zou Y L, Wang X B, Shen W M. Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J Sel Areas Commun, 2013, 31: 2099–2111
16 Zhao R, Lin H X, He Y C, et al. Secrecy performance analysis of MIMO decode-and-forward relay systems in Nakagami-m channels. J Electron Inf Technol, 2016, 38: 1913–1919 [赵睿, 林鸿鑫, 贺玉成, 等. Nakagami-m 信道下 MIMO 解码转发中继系统的安全性能分析. 电子与信息学报, 2016, 38: 1913–1919]
17 Laneman J N, Tse D N C, Wornell G W. Cooperative diversity in wireless networks: efficient protocols and outage behavior. IEEE Trans Inf Theory, 2004, 50: 3062–3080
18 Zhao H, Pan G F. Analysis of secure communications for a DF and RF relaying SIMO system with Gauss errors. Sci Sin Inform, 2016, 43: 350–360 [赵辉, 潘高峰. Gauss 信道估计误差下 DF 与 RF 中继 SIMO 系统保密通信性能分析. 中国科学: 信息科学, 2016, 46: 350–360]
19 Wang D Y, Zhao H, Pan G F. An analysis of secrecy outage performance of DF and RD relaying SIMO system with imperfect CSI. Sci Sin Inform, 2016, 46: 925–936 [王丹阳, 赵辉, 潘高峰. 非理想 CSI 下 DF 与 RF 中继 SIMO 系统保密中断性能分析. 中国科学: 信息科学, 2016, 46: 925–936]
20 Zhang X, Zhang Y, Yan Z, et al. Performance analysis of cognitive relay networks over Nakagami-m fading channels. IEEE J Sel Areas Commun, 2015, 33: 865–877
21 Bloch M, Barros J, Rodrigues M R, et al. Wireless information-theoretic security. IEEE Trans Inf Theory, 2008, 54: 2515–2534
22 Wang L F, Elkashlan M, Huang J, et al. Secure transmission with antenna selection in MIMO Nakagami-m fading channels. IEEE Trans Wirel Commun, 2014, 13: 6054–6067
23 Bletsas A, Khisti A, Reed D P, et al. A simple cooperative diversity method based on network path selection. IEEE J Sel Areas Commun, 2006, 24: 659–672
24 Zhao H, Tan Y Y, Pan G F, et al. Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks. IEEE Trans Veh Technol, 2016, 65: 10236–10242
25 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products. 7th ed. New York: Academic Press, 2007
26 Lei H J, Gao C, Ansari I, et al. Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels. IEEE Trans Veh Technol, 2017, 66: 2237–2250
27 Yang N, Elkashlan M, Yeoh P L, et al. Multiuser MIMO relay networks in Nakagami-m fading channels. IEEE Trans Commun, 2012, 60: 3298–3310
28 Boyd S, Vandenberghe L. Convex Optimization. Cambridge: Cambridge University Press, 2004
29 Lei H J, Ansari I S, Pan G F, et al. Secrecy capacity analysis over $\alpha-\mu$ fading channels. IEEE Commun Lett, 2017, 21: 1445–1448

Security performance analysis of DF relay selection systems

Hongjiang LEI[1*], Huan ZHANG[1], Junjie LIU[1] & Gaofeng PAN[2]

1. *Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065*, China*;
2. *Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Southwest University, Chongqing* 400715*, China*
* Corresponding author. E-mail: leihj@cqupt.edu.cn

Abstract In this work, we investigate the security performance of adaptive decode-and-forward cooperative networks when the signals transmitted from source and relay would be wiretapped. Based on whether the channel state information (CSI) of the wiretap link is available or not, optimal relay selection (ORS), conventional relay selection (CRS), and multiple relays selection (MRS) schemes are considered, and the exact closed-form expressions for security outage probability (SOP) are derived. Besides, we obtain the closed-form expressions for the secrecy diversity order and secrecy array gain of the three different selection schemes through asymptotic analysis. Simulations are presented to validate the accuracy of our proposed analytical results and illustrate that ORS is the best scheme. Furthermore, asymptotic analysis reveals that the secrecy diversity order of each scheme is the same and closely related to the number of relays. The impact of the wiretap channels is only reflected in the secrecy array gain. Finally, we determine the optimal power allocation between the source and relay.

Keywords physical layer security, decode-and-forward, relay selection, security outage probability, power allocation

Hongjiang LEI received the M.S. degree in computer application technology from Southwest Jiaotong University, China, in 2004, and the Ph.D. degree in instrument science and technology from Chongqing University, China, in 2015, respectively. Since 2004, he has been with the School of Communication and Information Engineering of Chongqing University of Posts and Telecommunications, where he is currently an associate professor. His research interest spans special topics in communications theory and signal processing, including secure communications and CR communications.

Huan ZHANG was born in 1992. He received the B.S. degree from Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China, in 2014. He is currently pursuing the M.S. degree in information and communication engineering at Chongqing University of Posts and Telecommunications. His research interests include cognitive radio networks, physical layer security, and cooperative communications.

Junjie LIU was born in 1996. He is an undergraduate student with the School of Information and Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. Her main research interests include performance modeling and analysis of wireless systems, and physical layer security.

Gaofeng PAN received the Ph.D. degree in communication and information systems from Southwest Jiaotong University, China, in 2011. He was with the Ohio State University, USA, from 2009 to 2011, as a joint-trained Ph.D. student. In 2012, he joined the School of Electronic and Information Engineering, Southwest University, as an associate professor. Since 2016, he has been with the School of Computing and Communications, Lancaster University, Lancaster, U.K., where he holds a post-doctoral position. His research interest spans special topics in communications theory, signal processing, and protocol design, including secure communications, CR/cooperative communications, and MAC protocols.