中国科学: 信息科学 2016 年 第 46 卷 第 7 期: 925–936
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

非理想 CSI 下 DF 与 RF 中继 SIMO 系统保密中断性能分析

王丹阳, 赵辉, 潘高峰*

西南大学电子信息工程学院, 重庆 400715
* 通信作者. E-mail: gfpan@swu.edu.cn

收稿日期: 2016–04–14; 接受日期: 2016–05–10; 网络出版日期: 2016–06–27
国家自然科学基金 (批准号: 61401372, 61531016)、教育部高校博士点新教师基金 (批准号: 20130182120017)、重庆市基础与前沿研究计划 (批准号: cstc2013jcyjA40040) 和中央高校基本科研业务经费 (批准号: XDJK2015B023, XDJK2016A011) 资助项目

摘要 本文研究了非理想信道状态信息 (channel state information, CSI) 下经典 4 点 (信源、信宿、中继、窃密者) 模型的物理层保密中断性能. 在此模型中, 考虑窃密信道为单输入多输出, 也就是信源、中继均为单天线, 信宿、窃密者均为多天线. 信宿和窃密者均采用最大比合并分集策略处理接收到的多径信号, 中继分别采用解码放大转发 (decode-and-forward, DF) 和随机放大转发 (randomize-and-forward, RF) 两种方式向信宿转发信息. 信源通过中继向信宿发送信息时, 信源与中继、中继与信宿两跳通信过程均遭到窃密者的窃听. 在非理想 CSI 下, 本文分别推导出了 DF 与 RF 中继转发下保密中断概率的闭式表达式及渐近表达式, 并通过 Monte Carlo 仿真验证了理论模型的正确性.

关键词 CSI Gauss 估计误差 保密中断概率 单输入多输出系统 最大比合并 解码放大转发 随机放大转发 物理层保密通信

1 引言

由于无线信道的开放性、复杂性, 使得无线通信过程中的信息安全受到了威胁. 物理层作为开放式系统互联 (open system interconnection, OSI) 模型的底层, 它的安全对整个通信过程有着至关重要的作用, 因此受到了广泛的关注. 物理层安全由 Wyner [1] 于 1975 年提出, 其基本理念是利用无线信道的不相关特性实现信息的安全传输, 同时, 他还建立了窃密信道模型, 即在没有密钥情况下安全的通信链路.

近年来, 研究人员在 Wyner 窃密信道模型的基础上对无线信道模型作了补充与改进. 文献 [2] 研究了 Nakagami-m 衰落信道下基于认知无线电的物理层保密性能, 分别推导出了非零保密容量 (probability of non-zero secrecy capacity, PNSC) 以及保密中断概率 (secrecy outage probability, SOP). 文献 [3] 对非小尺度衰落信道下的物理层保密性能进行了研究, 当主信道和窃听信道服从独立/相关的 log-normal 衰落信道以及独立复合衰落信道时, 分别分析了该系统的平均保密容量, PNSC 以及 SOP, 并推导出了闭式表达式.

引用格式: 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, doi: 10.1360/N112015-00265

信号在空间进行传输时会受到衰落带来的损耗, 为了克服这种损耗, 研究人员提出了以中继协作系统和多天线系统为主的分集技术 [4~6]. 文献 [7] 研究了两路无线中继网络中以放大转发 (amplify-and-forward, AF) 与解码放大转发 (decode-and-forward, DF) 为策略的各种中继选择方案, 包括最佳中继选择, 最好的和最糟糕的信道选择以及最大谐波均值选择. 文献 [8] 对解码放大转发以及随机放大转发 (randomize-and-forward, RF) 在经典的 4 点模型的情况下最优功率分配问题和蜂窝网络中中继位置问题作了研究. 为改善存在被动窃听者的无线传输的安全性, 文献 [9] 在 AF 中继网络下提出了一种联合协作波束成形, 干扰以及功率分配方案, 将中继模型进一步扩展. 另外, 文献 [10~12] 对多天线的分集技术进行了研究. 文献 [10] 中研究了合法用户 (信源与信宿) 采用单天线, 窃密者采用多天线, 合法/非法信道分别为 Rayleigh/Nakagami-m 及 Nakagami-m/Rayleigh 衰落信道, 且窃密者使用最大比合并 (maximal ratio combining, MRC)、选择式合并 (selection combining, SC) 来改善窃听质量的物理层保密性能. 文献 [11] 推导出了双分支 MRC 分集系统以及各种自适应传输技术在非理想两波弥漫功率 (two wave diffuse power) 衰落信道下的信道容量. 在文献 [12] 中, 作者研究了 Nakagami-m 衰落信道下天线采用 MRC 与 SC 策略来改善分集技术的 PNSC, 在对比两种分集技术的性能后得到了 MRC 优于 SC 的结论.

综上, 可以看出这些研究均是基于发送节点或接收节点拥有理想信道状态信息 (channel state information, CSI) 的前提, 实现分集增益. 然而, 在现实的无线通信系统中获取理想的 CSI 是十分困难的 [13]. 信道估计误差对 MRC 系统性能的影响最早由 Bello 和 Nelin 提出 [14]. 他们分析了选择性 Rayleigh 衰落信道下使用导频音 (pilot tone) 为 MRC 系统提供加权因子的影响, 其中 pilot tone 是从数据信号中分离出来的频率, 所得到的信道估计误差被证明是服从 Gauss 分布的. Gans [15] 用复 Gauss 信道估计误差在实际的 MRC 系统中进行建模, 得出了输出信噪比的概率密度函数.

文献 [16] 对合法用户和窃密者信道都存在 Gauss 误差的单输入多输出 (single input multiple output, SIMO) 系统进行研究分析, 得出了在采用 MRC 分集技术时的 SOP. 文献 [17] 对 Gauss 信道估计误差下 DF 与 RF 中继 SIMO 系统的 PNSC 进行了研究. 考虑到物理层保密性能包括: 非零保密容量、保密中断概率以及遍历保密容量, 仅研究非零保密容量不能完整地描述该系统的保密性能.

在文献 [17] 的基础上, 本文研究了非理想 CSI 下 SIMO 系统的物理层保密中断性能, 分别分析了 DF 与 RF 中继策略下的 SOP, 并推导出了闭式表达式及渐近表达式; 最后, 通过 Monte Carlo 仿真对理论模型进行了验证.

2 系统模型

2.1 中继转发描述

如图 1 所示, 整个系统由信源 S、中继 R [1)]、信宿 D (拥有 M 根天线并采用 MRC 分集技术) 和窃密者 E (拥有 N 根天线并采用 MRC 分集技术) 组成. 通信过程分为两跳, 第 1 跳中 S 将信息编码后发给 R, 第 2 跳中 R 将来自 S 的信息重新编码后转发给 D. 假设 E 对 S 及 R 传输的信息均窃密, S 与 D 距离较远, 信号存在严重衰落, S 与 D 之间不存在直接信号链路 [8]. 假设本文前后两跳的信道均为互相独立的平坦 Rayleigh 衰落信道, 衰落系数在一个符号传输周期内保持不变, 且衰落过程是各态历经的 [17].

1) 中继 R 分别采用 DF 与 RF 转发策略, 其中, DF 中继转发策略指中继与信源采用相同的码书进行转发, RF 中继转发策略指中继与信源采用不同的码书进行转发.

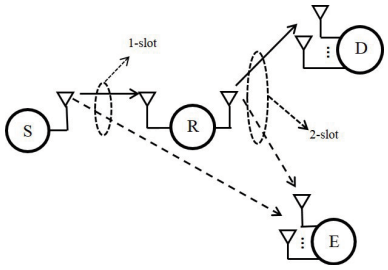

图 1 系统模型图

Figure 1 System model

2.2 信噪比分析

2.2.1 信道估计误差分析

D 与 E 均采用 MRC 信号合并技术, 在 D 处, 第 m 个子信道接收的信号为 $y_{D_m}=\sqrt{P_{\rm R}}h_{D_m}x_1+n_{D_m}, m=1,2,\ldots,M$, 其中, h_{D_m} 为 R–D 链路中第 m 个子信道的信道衰落系数, x_1 为 R 发送的信息, n_{D_m} 为复 Gauss 噪声, $P_{\rm R}$ 是 R 的平均发射功率.

在 E 处, 第 1 跳中第 n 个子信道及第 2 跳中第 p 个子信道接收的信号为 $y_{E_n}=\sqrt{P_{\rm S}}h_{E_n}x_1+n_{E_n}, n=1,2,\ldots,N$, $y_{E_p}=\sqrt{P_{\rm R}}h_{E_p}x_2+n_{E_p}, p=1,2,\ldots,N$, 同样, h_{E_n} 为 S–E 链路中第 n 个子信道的信道衰落系数, h_{E_p} 为 R–E 链路中第 p 个子信道的信道衰落系数, x_1, x_2 分别为 R 及 S 发送的信息, n_{E_n} 与 n_{E_p} 为复 Gauss 噪声, $\sqrt{P_{\rm S}}$ 是 S 的平均发射功率.

合并信号为 $y_{\rm D}=\sum_{m=1}^{M}\frac{h_{D_m}^*}{N_{D_m}}y_{D_m}$, $y_{1{\rm E}}=\sum_{n=1}^{N}\frac{h_{E_n}^*}{N_{E_n}}y_{E_n}$, $y_{2{\rm E}}=\sum_{p=1}^{N}\frac{h_{E_p}^*}{N_{E_p}}y_{E_p}$, 其中, h_u^* 为 h_u 的共轭, N_u 为 Gauss 噪声功率 ($u\in\{D_m,E_n,E_p\}$). 在现实情况下, 考虑到存在 Gauss 信道估计误差, 获得合并权重 h_u^*/N_u 的准确值比较困难. 因此, 令 $\widehat{h}_u^*/N_u$ 为 h_u^*/N_u 的估计值, 根据文献 [18], 二者关系如下 $h_u=\sqrt{\rho_u}\widehat{h}_u+\sqrt{1-\rho_u}g_u$, 其中, $\rho_u\in[0,1]$ 为信道功率相关系数[2)], g_u 是 h_u 独立同分布的随机变量. 第 1 跳中 E 处接收信号的瞬时信噪比可以表示为 $\gamma_{1{\rm E}}=\sum_{n=1}^{N}\frac{P_{\rm S}\left|\widehat{h}_{E_n}\right|^2}{N_{E_n}}$, 第 2 跳中 D 处, E 处接收信号的瞬时信噪比分别为 $\gamma_{\rm D}=\sum_{m=1}^{M}\frac{P_{\rm R}\left|\widehat{h}_{D_m}\right|^2}{N_{D_m}}$, $\gamma_{2{\rm E}}=\sum_{p=1}^{N}\frac{P_{\rm R}\left|\widehat{h}_{E_p}\right|^2}{N_{E_p}}$.

2.2.2 中继信号分析

第 1 跳, R 处接收信号的信噪比的 PDF 与 CDF 分别为 $f_{\gamma_{\rm R}}(x)=\frac{1}{\overline{\gamma}_{\rm R}}\exp(-\frac{x}{\overline{\gamma}_{\rm R}})$, $F_{\gamma_{\rm R}}(x)=1-\exp(-\frac{x}{\overline{\gamma}_{\rm R}})$, 其中, $\overline{\gamma}_{\rm R}$ 为 R 接收信噪比的均值. 根据文献 [17], E 处在存在信道估计误差的情况下接收的信号信噪比的 PDF 和 CDF 分别为 $f_{\gamma_{1{\rm E}}}(x)=\sum_{m=1}^{N}B(m)\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1{\rm E}})}{\Gamma(m)\overline{\gamma}_{1{\rm E}}^m}$, $F_{\gamma_{1{\rm E}}}(x)=\sum_{m=1}^{N}B(m)\{1-\frac{\Gamma(m,x/\overline{\gamma}_{1{\rm E}})}{\Gamma(m)}\}$, $\overline{\gamma}_{1{\rm E}}$ 为第 1 跳 E 每个子信道接收信号的信噪比[3)], $\Gamma(d)=\int_0^\infty\exp(-t)\times t^{d-1}{\rm d}t$, $d\in\{m,i,j\}$ 为 Gamma 函数, $\Gamma(d,x)=\int_x^\infty\exp(-t)\,t^{d-1}{\rm d}t$ 为不完全 Gamma 函数, $B(m)$ 定义为 $B(m)=\binom{N-1}{m-1}(1-\rho_{1{\rm E}})^{N-m}\rho_{1{\rm E}}^{m-1}$, $\rho_{1{\rm E}}\in[0,1]$ 为第 1 跳 E 的信道估计与真实信道之间的功率相关系数.

2) ρ_u 是衡量信道估计情况的一个重要参数, ρ_u 越大, 信道估计越准确, 当 $\rho_u=1$ 时, 代表理想 MRC 合并.

3) 指接收端进行 MRC 合并之前的接收信噪比. 另外, 每个子信道接收的平均信噪比不同时, 处理起来较复杂, 为方便处理, 采用与文献 [19] 相同的方法进行简化.

在第 2 跳中, D 处在存在信道估计误差的情况下接收到的信号信噪比的 PDF 与 CDF 分别有如下表示:

$$f_{\gamma_{\mathrm{D}}}(x)=\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)\overline{\gamma}_{\mathrm{D}}^{i}},\tag{1}$$

$$F_{\gamma_{\mathrm{D}}}(x)=\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)}\right\},\tag{2}$$

其中, $\overline{\gamma}_{\mathrm{D}}$ 为第 2 跳 D 处每个子信道接收信号的信噪比均值, $A(i)$ 定义为

$$A(i)=\binom{M-1}{i-1}(1-\rho_{\mathrm{D}})^{M-i}\rho_{\mathrm{D}}^{i-1}.\tag{3}$$

在第 2 跳中, E 处接收信号的信噪比的 PDF 与 CDF 分别为

$$f_{\gamma_{2\mathrm{E}}}(x)=\sum_{j=1}^{N}C(j)\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(j)\overline{\gamma}_{2\mathrm{E}}^{j}},\tag{4}$$

$$F_{\gamma_{2\mathrm{E}}}(x)=\sum_{j=1}^{N}C(j)\left\{1-\frac{\Gamma(j,x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(j)}\right\},\tag{5}$$

其中, $\overline{\gamma}_{2\mathrm{E}}$ 为第 2 跳中 E 处每个子信道接收信号的信噪比均值, $C(j)$ 定义为

$$C(j)=\binom{N-1}{j-1}(1-\rho_{2\mathrm{E}})^{N-j}\rho_{2\mathrm{E}}^{j-1},\tag{6}$$

其中, $\rho_{2\mathrm{E}}\in[0,1]$.

根据文献 [8] 中对 DF 中继转发策略的定义, 可得到 D 的瞬时等效信噪比为 $\gamma_1=\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}$, E 的瞬时等效信噪比为 $\gamma_2=\max\{\gamma_{1\mathrm{E}},\gamma_{2\mathrm{E}}\}$.

3 保密中断概率分析

3.1 求解 γ_1 和 γ_2 的 PDF 与 CDF

参照文献 [17], γ_1 和 γ_2 的 PDF 及 CDF 可以分别表示为

$$\begin{aligned}f_{\gamma_1}(x)=&\frac{1}{\overline{\gamma}_{\mathrm{R}}}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)+\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)\overline{\gamma}_{\mathrm{D}}^{i}}-\frac{1}{\overline{\gamma}_{\mathrm{R}}}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)}\right\}\\&-\left[1-\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)\right]\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)\overline{\gamma}_{\mathrm{D}}^{i}},\end{aligned}\tag{7}$$

$$\begin{aligned}F_{\gamma_1}(x)=&1-\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)+\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)}\right\}\\&-\left[1-\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)\right]\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)}\right\},\end{aligned}\tag{8}$$

$$f_{\gamma_2}(x)=\sum_{m=1}^{N}\sum_{j=1}^{N}B(m)C(j)\left\{\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(j)\overline{\gamma}_{2\mathrm{E}}^{j}}+\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1\mathrm{E}})}{\Gamma(m)\overline{\gamma}_{1\mathrm{E}}^{m}}\right.$$
$$\left.-\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2\mathrm{E}})\Gamma(m,x/\overline{\gamma}_{1\mathrm{E}})}{\Gamma(m)\Gamma(j)\overline{\gamma}_{2\mathrm{E}}^{j}}-\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1\mathrm{E}})\Gamma(j,x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(m)\Gamma(j)\overline{\gamma}_{1\mathrm{E}}^{m}}\right\},\tag{9}$$

$$F_{\gamma_2}(x)=\sum_{m=1}^{N}\sum_{j=1}^{N}B(m)C(j)\left\{1-\frac{\Gamma(m,x/\overline{\gamma}_{1\mathrm{E}})}{\Gamma(m)}-\frac{\Gamma(j,x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(j)}+\frac{\Gamma(m,x/\overline{\gamma}_{1\mathrm{E}})\Gamma(j,x/\overline{\gamma}_{2\mathrm{E}})}{\Gamma(m)\Gamma(j)}\right\}.\tag{10}$$

3.2 两种中继转发下的 SOP

DF 中继转发策略中, 中继 R 首先将接收到的信号进行解码, 其次对信号重新编码、调制, 然后转发给信宿 D. 如果中继节点能准确地接收到信源 S 的信息, 则可以避免 S–R 链路中噪声的引入, 反之, 如果中继节点接收到错误的信息, 就会导致错误的传播现象, 严重时系统的性能可能低于没有采用 DF 中继转发时系统的性能. RF 中继转发策略是指发射机每一跳使用独立的随机信号, 故对于窃密者而言, 在 S–R 链路与 R–D 链路接收到的信号不能进行分集合并, 因此, RF 中继转发策略优于 DF 中继转发策略 [17].

以下内容将分别推导 DF 及 RF 中继转发下 SOP 的闭式表达式.

3.2.1 DF 中继转发下的 SOP

保密中断概率被定义为瞬时保密容量 C_S 小于或等于目标保密容量 C_{th} 的概率, 文献 [8] 中对 DF 中继转发下的瞬时保密容量定义为

$$C_S(\gamma_1,\gamma_2)=\begin{cases}\frac{1}{2}\log_2(1+\gamma_1)-\frac{1}{2}\log_2(1+\gamma_2), & \gamma_1>\gamma_2;\\ 0, & \gamma_1\leqslant\gamma_2,\end{cases}\tag{11}$$

其中, $\frac{1}{2}\log_2(1+\gamma_1)$ 与 $\frac{1}{2}\log_2(1+\gamma_2)$ 分别为 D 与 E 的瞬时分集信道保密容量.

根据 DF 中继转发下瞬时保密容量的定义, SOP 可以写为

$$\mathrm{SOP}(C_{th})=\Pr\{C_S(\gamma_1,\gamma_2)\leqslant C_{th}\}=\Pr\left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_1}{1+\gamma_2}\right)\leqslant C_{th}\right\}=\Pr\left\{\frac{1+\gamma_1}{1+\gamma_2}\leqslant 2^{2C_{th}}\right\}.\tag{12}$$

令, $\alpha=2^{2C_{th}}$, 上式可以改写为

$$\mathrm{SOP}(C_{th})=\Pr\left\{\frac{1+\gamma_1}{1+\gamma_2}\leqslant\alpha\right\}=\Pr\{\gamma_1\leqslant\alpha\gamma_2+\alpha-1\}.\tag{13}$$

进一步, 式 (13) 可以写为

$$\begin{aligned}\mathrm{SOP}(C_{th})&=\int_0^{\infty}\int_0^{\alpha y+\alpha-1}f_{\gamma_1}(x)f_{\gamma_2}(y)\mathrm{d}x\mathrm{d}y=\int_0^{\infty}f_{\gamma_2}(y)F_{\gamma_1}(\alpha y+\alpha-1)\mathrm{d}y\\&=\int_0^{\infty}f_{\gamma_2}(y)\left\{1-\exp\left(-\frac{\alpha y+\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\right.\\&\quad\left.+\exp\left(-\frac{\alpha y+\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\sum_{i=1}^{M}A(i)\left[1-\frac{\Gamma(i,(\alpha y+\alpha-1)/\overline{\gamma}_{\mathrm{D}})}{\Gamma(i)}\right]\right\}\mathrm{d}y\end{aligned}$$

$$= \underbrace{\int_0^\infty f_{\gamma_2}(y)\mathrm{d}y}_{X_1} - \underbrace{\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha y+\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\mathrm{d}y}_{X_2}$$
$$+ \underbrace{\sum_{i=1}^{M} A(i)\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha y+\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\mathrm{d}y}_{X_3}$$
$$- \underbrace{\sum_{i=1}^{M} A(i)\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha y+\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\frac{\Gamma\left((i,\alpha y+\alpha-1)/\overline{\gamma}_{\mathrm{D}}\right)}{\Gamma(i)}\mathrm{d}y}_{X_4}, \tag{14}$$

显然, $X_1=1$, 利用 $\Gamma(n,x)=(n-1)!\exp(-x)\sum_{q=0}^{n-1}\frac{x^q}{q!}, n=1,2,\ldots$ (文献 [20, 式(8.352.4)]), 可以得到

$$X_2 = \exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}}y\right)\mathrm{d}y, \tag{15}$$

$$X_3 = \sum_{i=1}^{M} A(i)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}}y\right)\mathrm{d}y, \tag{16}$$

$$X_4 = \sum_{i=1}^{M}\sum_{q=0}^{i-1}\sum_{k=0}^{q}\binom{q}{k}A(i)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{D}}}\right)\frac{\alpha^k(\alpha-1)^{q-k}}{\overline{\gamma}_{\mathrm{D}}^q q!}$$
$$\cdot\int_0^\infty f_{\gamma_2}(y)\exp\left(-\frac{\alpha y}{\overline{\gamma}_{\mathrm{R}}}-\frac{\alpha y}{\overline{\gamma}_{\mathrm{D}}}\right)y^k\mathrm{d}y. \tag{17}$$

由附录 A 的积分公式得

$$X_2 = \exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},0\right), \tag{18}$$

$$X_3 = \sum_{i=1}^{M} A(i)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},0\right), \tag{19}$$

$$X_4 = \sum_{i=1}^{M}\sum_{q=0}^{i-1}\sum_{k=0}^{q}\binom{q}{k}A(i)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{D}}}\right)\frac{\alpha^k(\alpha-1)^{q-k}}{\overline{\gamma}_{\mathrm{D}}^q q!}I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}}-\frac{\alpha}{\overline{\gamma}_{\mathrm{D}}},k\right). \tag{20}$$

将式 (18), (19), (20), $X_1=1$ 代入到 式 (14), 可得到 DF 中继转发策略的 SOP.

在求得 SOP 的闭式表达式之后, 这里进一步求解当 $\overline{\gamma}_{\mathrm{D}}\to\infty$ 时, DF 转发策略下的保密中断概率 $\mathrm{SOP}_{\mathrm{DF}}^{\infty}$ 的渐近表达式.

式 (2) 中, $\Gamma\left(i,\frac{x}{\overline{\gamma}_{\mathrm{D}}}\right)=(i-1)!\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{D}}}\right)\sum_{q=0}^{i-1}\frac{x^i}{\overline{\gamma}_{\mathrm{D}}^i q!}$, $i=1,2,\ldots$, 把 $\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{D}}}\right)$ 展开为 Taylor 级数, 保留前两项, 因而, $F_{\gamma_{\mathrm{D}}}(x)$ 的渐近表达式 $F_{\gamma_{\mathrm{D}}}^{\infty}(x)$ 改写为

$$F_{\gamma_{\mathrm{D}}}^{\infty}(x) = \sum_{i=1}^{M} A(i)\left[\frac{x^i}{\overline{\gamma}_{\mathrm{D}}^i i!}+o\left(\overline{\gamma}_{\mathrm{D}}^{-i}\right)\right]. \tag{21}$$

进而, 式 (8) 中 $F_{\gamma_1}(x)$ 的渐近表达式 $F_{\gamma_1}^{\infty}(x)$ 为

$$F_{\gamma_1}^{\infty}(x) = 1-\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)+\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{R}}}\right)\sum_{i=1}^{M}\left[A(i)\frac{x^i}{\overline{\gamma}_{\mathrm{D}}^i i!}+o\left(\overline{\gamma}_{\mathrm{D}}^{-i}\right)\right]. \tag{22}$$

结合附录 A, $\mathrm{SOP}_{\mathrm{DF}}^{\infty}\left(C_{th}\right)$ 为

$$\begin{aligned}\mathrm{SOP}_{\mathrm{DF}}^{\infty}\left(C_{th}\right)&=1-\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},0\right)\\&\quad+\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\sum_{i=1}^{M}\left[\sum_{k=0}^{i}\binom{i}{k}\frac{A\left(i\right)\alpha^{k}\left(\alpha-1\right)^{i-k}}{\overline{\gamma}_{\mathrm{D}}^{i}i!}I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},k\right)+o\left(\overline{\gamma}_{\mathrm{D}}^{-i}\right)\right]\\&=1-\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},0\right)+\sum_{i=1}^{M}\left[\left(G_{1}\overline{\gamma}_{\mathrm{D}}\right)^{-i}+o\left(\overline{\gamma}_{\mathrm{D}}^{-i}\right)\right],\end{aligned}\tag{23}$$

其中, $G_{1}=\left[\exp\left(-\frac{\alpha-1}{\overline{\gamma}_{\mathrm{R}}}\right)\sum_{k=0}^{i}\binom{i}{k}\frac{A(i)\alpha^{k}(\alpha-1)^{i-k}}{i!}I\left(-\frac{\alpha}{\overline{\gamma}_{\mathrm{R}}},k\right)\right]^{-\frac{1}{i}}$.

3.2.2 RF 中继转发下的 SOP

文献 [21] 中指出, 只有当 S–R 以及 R–D 两跳的瞬时保密容量 C_{S_1} 与 C_{S_2} 分别小于或等于每跳的目标保密容量 C_{1th} 和 C_{2th} 时, 整个通信系统的保密容量 C_S 才能小于或等于系统的目标保密容量 C_{th}, 该系统才能实现保密传输. 因此, RF 中继转发下的 SOP 可以写为

$$\mathrm{SOP}\left(C_{th}\right)=\Pr\left\{C_{S_1}\left(\gamma_{\mathrm{R}},\gamma_{1\mathrm{E}}\right)\leqslant C_{1th}\right\}\Pr\left\{C_{S_2}\left(\gamma_{\mathrm{D}},\gamma_{2\mathrm{E}}\right)\leqslant C_{2th}\right\}.\tag{24}$$

第 1 跳中, 当 R 的信噪比大于 E 处的信噪比时, 此链路安全, 因此有

$$C_{S_1}\left(\gamma_{\mathrm{R}},\gamma_{1\mathrm{E}}\right)=\begin{cases}\frac{1}{2}\log_{2}\left(1+\gamma_{\mathrm{R}}\right)-\frac{1}{2}\log_{2}\left(1+\gamma_{1\mathrm{E}}\right), & \gamma_{\mathrm{R}}>\gamma_{1\mathrm{E}};\\0, & \gamma_{\mathrm{R}}\leqslant\gamma_{1\mathrm{E}}.\end{cases}\tag{25}$$

这时, 第 1 跳的保密中断概率 $\mathrm{SOP}_{1}\left(C_{th}\right)$ 为

$$\begin{aligned}\mathrm{SOP}_{1}\left(C_{1th}\right)&=\Pr\left\{C_{S_1}\left(\gamma_{\mathrm{R}},\gamma_{1\mathrm{E}}\right)\leqslant C_{1th}\right\}=\Pr\left\{\frac{1}{2}\log_{2}\left(\frac{1+\gamma_{\mathrm{R}}}{1+\gamma_{1\mathrm{E}}}\right)\leqslant C_{1th}\right\}\\&=\Pr\left\{\frac{1+\gamma_{\mathrm{R}}}{1+\gamma_{1\mathrm{E}}}\leqslant 2^{2C_{1th}}\right\}=\Pr\left\{\gamma_{\mathrm{R}}\leqslant\alpha_{1}\gamma_{1\mathrm{E}}+\alpha_{1}-1\right\},\end{aligned}\tag{26}$$

其中, $\alpha_{1}=2^{2C_{1th}}$, 结合文献 [20, 式(3.326.2)] 可以得到

$$\begin{aligned}\mathrm{SOP}_{1}\left(C_{1th}\right)&=\int_{0}^{\infty}\int_{0}^{\alpha_{1}y+\alpha_{1}-1}f_{\gamma_{\mathrm{R}}}\left(x\right)f_{\gamma_{1\mathrm{E}}}\left(y\right)\mathrm{d}x\mathrm{d}y\\&=\int_{0}^{\infty}f_{\gamma_{1\mathrm{E}}}\left(y\right)F_{\gamma_{\mathrm{R}}}\left(\alpha_{1}y+\alpha_{1}-1\right)\mathrm{d}y\\&=\sum_{m=1}^{N}B\left(m\right)\left[1-\frac{1}{\overline{\gamma}_{1\mathrm{E}}^{m}}\frac{1}{\left(1/\overline{\gamma}_{1\mathrm{E}}+\alpha_{1}/\overline{\gamma}_{\mathrm{R}}\right)^{m}}\exp\left(-\frac{\alpha_{1}}{\overline{\gamma}_{\mathrm{R}}}\right)\right].\end{aligned}\tag{27}$$

同理, 在第 2 跳中有

$$C_{S_2}\left(\gamma_{\mathrm{D}},\gamma_{2\mathrm{E}}\right)=\begin{cases}\frac{1}{2}\log_{2}\left(1+\gamma_{\mathrm{D}}\right)-\frac{1}{2}\log_{2}\left(1+\gamma_{2\mathrm{E}}\right), & \gamma_{\mathrm{D}}>\gamma_{2\mathrm{E}};\\0, & \gamma_{\mathrm{D}}\leqslant\gamma_{2\mathrm{E}},\end{cases}\tag{28}$$

$$\mathrm{SOP}_{2}\left(C_{2th}\right)=\Pr\left\{C_{S_2}\left(\gamma_{\mathrm{D}},\gamma_{2\mathrm{E}}\right)\leqslant C_{2th}\right\}=\Pr\left\{\frac{1}{2}\log_{2}\left(\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{2\mathrm{E}}}\right)\leqslant C_{2th}\right\}$$

$$= \Pr\left\{\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{2\mathrm{E}}} \leqslant 2^{2C_{2th}}\right\} = \Pr\left\{\gamma_{\mathrm{D}} \leqslant \alpha_2\gamma_{2\mathrm{E}} + \alpha_2 - 1\right\}, \tag{29}$$

其中, $\alpha_2 = 2^{2C_{2th}}$.

$$\begin{aligned}
\mathrm{SOP}_2\left(C_{2th}\right) &= \int_0^{\infty}\int_0^{\alpha_2 y+\alpha_2-1} f_{\gamma_{\mathrm{D}}}(x) f_{\gamma_{2\mathrm{E}}}(y)\,\mathrm{d}x\mathrm{d}y \\
&= \int_0^{\infty} f_{\gamma_{2\mathrm{E}}}(y) F_{\gamma_{\mathrm{D}}}\left(\alpha_2 y+\alpha_2-1\right)\mathrm{d}y \\
&= \sum_{i=1}^{M}\sum_{j=1}^{N} A(i) C(j) - \sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{q_3=0}^{i-1}\sum_{l=0}^{q_3}\binom{q_3}{l} A(i) C(j) \\
&\quad \cdot \frac{\alpha_2^l(\alpha_2-l)^{q_3-l}}{\Gamma(j)\, q_3!\overline{\gamma}_{2\mathrm{E}}^{j}\overline{\gamma}_{\mathrm{D}}^{q_3}} \frac{\Gamma(j+l)}{\left(1/\overline{\gamma}_{2\mathrm{E}}+\alpha_2/\overline{\gamma}_{\mathrm{D}}\right)^{j+l}} \exp\left(-\frac{\alpha_2-1}{\overline{\gamma}_{\mathrm{D}}}\right).
\end{aligned} \tag{30}$$

最后, 把式 (27) 和 (30) 代入式 (24) 中, 可得 RF 转发策略下的 SOP 为

$$\begin{aligned}
\mathrm{SOP}\left(C_{th}\right) &= \sum_{m=1}^{N} B(m)\left[1 - \frac{1}{\overline{\gamma}_{1\mathrm{E}}^{m}} \frac{1}{\left(1/\overline{\gamma}_{1\mathrm{E}}+\alpha_1/\overline{\gamma}_{\mathrm{R}}\right)^{m}} \exp\left(-\frac{\alpha_1}{\overline{\gamma}_{\mathrm{R}}}\right)\right] \\
&\quad \cdot \left[\sum_{i=1}^{M}\sum_{j=1}^{N} A(i) C(j) - \sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{q_3=0}^{i-1}\sum_{l=0}^{q_3}\binom{q_3}{l} A(i) C(j)\right. \\
&\quad \left. \cdot \frac{\alpha_2^l(\alpha_2-l)^{q_3-l}}{\Gamma(j)\, q_3!\overline{\gamma}_{2\mathrm{E}}^{j}\overline{\gamma}_{\mathrm{D}}^{q_3}} \frac{\Gamma(j+l)}{\left(1/\overline{\gamma}_{2\mathrm{E}}+\alpha_2/\overline{\gamma}_{\mathrm{D}}\right)^{j+l}} \exp\left(-\frac{\alpha_2-1}{\overline{\gamma}_{\mathrm{D}}}\right)\right].
\end{aligned} \tag{31}$$

在求得 SOP 的闭式表达式之后, 这里进一步求解当 $\overline{\gamma}_{\mathrm{D}} \to \infty$ 时, RF 转发策略下的保密中断概率 $\mathrm{SOP}_{\mathrm{RF}}^{\infty}$ 的渐近表达式, 由于第 1 跳中不含 $\overline{\gamma}_{\mathrm{D}}$ 这一项, 故只需求 $\mathrm{SOP}_2^{\infty}\left(C_{th}\right)$ 的渐近表达式

$$\mathrm{SOP}_2^{\infty}\left(C_{th}\right) = \sum_{i=1}^{M}\left[\left(G_2\overline{\gamma}_{\mathrm{D}}\right)^{-i} + o\left(\overline{\gamma}_{\mathrm{D}}^{-i}\right)\right], \tag{32}$$

其中, $G_2 = \left[\sum_{j=1}^{N}\sum_{r=0}^{i}\binom{i}{r}\frac{A(i)C(j)\alpha_2^r(\alpha_2-1)^{i-r}\overline{\gamma}_{2\mathrm{E}}^{r}\Gamma(j+r)}{i!\Gamma(j)}\right]^{-\frac{1}{i}}$.

综上所述, RF 转发策略下的保密中断概率 $\mathrm{SOP}_{\mathrm{RF}}^{\infty}$ 的渐近表达式为

$$\mathrm{SOP}_{\mathrm{RF}}^{\infty} = \mathrm{SOP}_1\left(C_{1th}\right)\mathrm{SOP}_2^{\infty}\left(C_{2th}\right). \tag{33}$$

4 仿真与分析

本节将用 Monte Carlo 仿真验证理论模型的正确性, 在 Monte Carlo 仿真中参照文献 [15, 式(23)] 构造接收端的瞬时合并信噪比.

当 $\overline{\gamma}_{\mathrm{R}} = 40$ dB, $\rho_{\mathrm{D}} = \rho_{1\mathrm{E}} = \rho_{2\mathrm{E}}$, $M = N = 2$ 时, 图 2 给出了 DF 中继策略下的 SOP 在组合 $(\overline{\gamma}_{1\mathrm{E}}, \overline{\gamma}_{2\mathrm{E}}) = (2,2), (4,4), (6,6), (8,8)$ dB 下随 $\overline{\gamma}_{\mathrm{D}}$ 的变化曲线. 从图中可以看出, 当 $\overline{\gamma}_{\mathrm{D}}$ 增大时, SOP 在减小, 这是因为 DF 中继策略下第 2 跳信道状况得到了改善. 另外, 随着组合 $(\overline{\gamma}_{1\mathrm{E}}, \overline{\gamma}_{2\mathrm{E}})$ 的增大, SOP 增大, 这是因为 E 处的分集信噪比在增大, 致使保密中断概率增大.

当 $\overline{\gamma}_{\mathrm{R}} = 15$ dB, $M = N = 4$, $\rho_{\mathrm{D}} = \rho_{1\mathrm{E}} = \rho_{2\mathrm{E}} = 0.8$ 时, 图 3 给出了 RF 中继的 SOP 在不同组合 $(\overline{\gamma}_{1\mathrm{E}}, \overline{\gamma}_{2\mathrm{E}}) = (8,4), (4,8), (8,8)$ dB 下随 $\overline{\gamma}_{\mathrm{D}}$ 的变化曲线. 可以看出, SOP 随着 $\overline{\gamma}_{\mathrm{D}}$ 的增大而减小, 这是

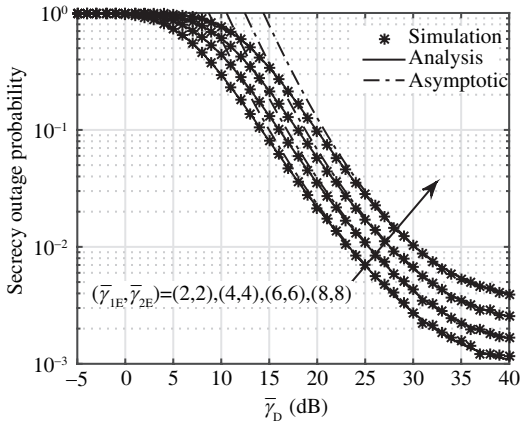

图 2 DF 中继下 SOP 随 $\overline{\gamma}_{\mathrm{D}}$ 以及 $(\overline{\gamma}_{\mathrm{1E}},\overline{\gamma}_{\mathrm{2E}})$ 的变化曲线

Figure 2 SOP versus $\overline{\gamma}_{\mathrm{D}}$ and $(\overline{\gamma}_{1\mathrm{E}},\overline{\gamma}_{2\mathrm{E}})$ of DF

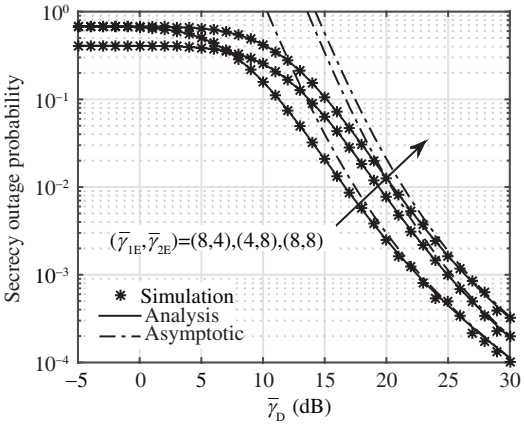

图 3 RF 中继下 SOP 随 $\overline{\gamma}_{\mathrm{D}}$ 的变化曲线

Figure 3 SOP versus $\overline{\gamma}_{\mathrm{D}}$ of RF

因为第 2 跳链路状况得到了改善. 另外, 当 $(\overline{\gamma}_{1\mathrm{E}},\overline{\gamma}_{2\mathrm{E}})=(8,4)$ dB 和 $(\overline{\gamma}_{1\mathrm{E}},\overline{\gamma}_{2\mathrm{E}})=(4,8)$ dB 时, SOP 的曲线大约在 7 dB 处有一个交汇点, 该交汇点与 γ_{D}, $\gamma_{1\mathrm{E}}$ 与 $\gamma_{2\mathrm{E}}$ 有关, 仅在本文所考虑的条件下, 交汇点出现在 7 dB 附近.

当 $\overline{\gamma}_{\mathrm{R}}=45$ dB, $M=N=2$, $\overline{\gamma}_{1\mathrm{E}}=\overline{\gamma}_{2\mathrm{E}}=4$ dB 时, 图 4 给出了 DF 中继的 SOP 在不同组合 $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})$ 下随 $\overline{\gamma}_{\mathrm{D}}$ 的变化曲线, ρ_u $(u\in\{\mathrm{D},1\mathrm{E},2\mathrm{E}\})$ 为信道功率相关系数, 分别来衡量信道 R–D, S–E 以及 R–E 的估计误差, 对比 $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(1,1,1)$, $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(0.8,0.8,0.8)$ 时的两条曲线, 可以看出, ρ_u 越大时, 该系统的 SOP 越好, 且当 $\rho_u=1$ 时, 为理想的 MRC 合并. 对比 $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(0.8,0.2,0.2)$, $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(0.8,0.8,0.8)$ 以及 $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(0.2,0.8,0.8)$, $(\rho_{\mathrm{D}},\rho_{1\mathrm{E}},\rho_{2\mathrm{E}})=(0.8,0.8,0.8)$ 可以得出当合法用户的信道功率相关系数大于窃听者的信道功率相关系数时该系统的保密中断性能要优于当窃听者信道功率相关系数大于合法用户的信道功率相关系数时的保密中断性能.

当 $\overline{\gamma}_R=40$ dB, $\overline{\gamma}_{1\mathrm{E}}=\overline{\gamma}_{2\mathrm{E}}=25$ dB, $\rho_{\mathrm{D}}=0.5$, $\rho_{1\mathrm{E}}=0.8$, $\rho_{2\mathrm{E}}=0.8$ 时, 图 5 给出了 DF 与 RF 中继转发的 SOP 在不同的 (M,N) 组合下, 随 $\overline{\gamma}_{\mathrm{D}}$ 的变化曲线. 从图中可以看出, RF 的 SOP 比 DF 的 SOP 明显小很多, 这是因为 RF 中继转发中要保证前后两跳都是保密的, 而在 DF 中继转发中, E 在前后两跳相当于一个信噪比最大的选择合并, 而 D 只能选择前后两跳中最小的信噪比作为自己的中继分集信噪比. 此外, 对于 DF 与 RF 系统均有 $(M,N)=(8,2)$ 的图线在 $(M,N)=(4,4)$ 及 $(M,N)=(2,8)$ 的图线下方, 表明当合法接收者的天线数目越多, 窃听者天线数目越少时, 该系统保密性能就越好.

最后, 从图 2∼5 还可以看出, 所有情况下的渐近曲线在 $\overline{\gamma}_{\mathrm{D}}\to\infty$ 时与仿真结果以及理论值拟合. 这是因为对 γ_{D}, 将其 CDF 中的 $\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{D}}}\right)$ 用 Taylor 级数展开并保留前两项后, 当 γ_{D} 过小时, $F_{\gamma_{\mathrm{D}}}^{\infty}(x)$ 不能准确描述 $F_{\gamma_{\mathrm{D}}}(x)$, 只有当 $\overline{\gamma}_{\mathrm{D}}\to\infty$ 时, $F_{\gamma_{\mathrm{D}}}^{\infty}(x)$ 才能无限逼近 $F_{\gamma_{\mathrm{D}}}(x)$, 故只有在大信噪比下渐近曲线才会与理论、仿真的曲线拟合.

5 结论

本文研究了非理想 CSI 下的 DF 与 RF 中继 SIMO 系统 MRC 分集的保密中断概率, 分别得出了

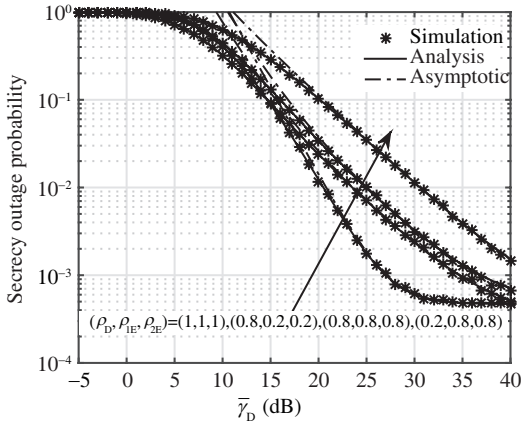

图 4 DF 中继下 SOP 随 $\overline{\gamma}_{\rm D}$ 以及 $(\rho_{\rm D},\rho_{\rm 1E},\rho_{\rm 2E})$ 的变化曲线

Figure 4 SOP versus $\overline{\gamma}_{\rm D}$ and $(\rho_{\rm D},\rho_{\rm 1E},\rho_{\rm 2E})$ of DF

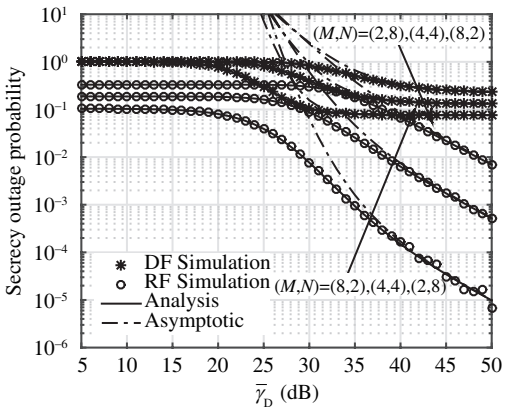

图 5 DF 与 RF 中继下 SOP 随 $\overline{\gamma}_{\rm D}$ 的变化曲线

Figure 5 SOP versus $\overline{\gamma}_{\rm D}$ of DF and RF

DF 与 RF 两种中继转发方式的 SOP 闭式表达式及渐近表达式, 最后通过 Monte Carlo 仿真验证了本文所提出的理论模型. 从仿真结果可以得到合法接收者的天线数量越多, 窃听者天线数目越少; MRC 合并权重向量估计值误差越小, 保密性能就越好; 信道功率相关系数越大, 信道的传输性能越好, 而且很明显可以看出 RF 比 DF 的保密性能要强.

参考文献

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

2 Tang C, Pan G, Li T. Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels. IEEE Wirel Commun Lett, 2014, 3: 609–612

3 Pan G, Tang C, Zhang X, et al. Physical layer security over non-small scale fading channels. IEEE Trans Veh Tech, 2016, 65: 1326–1339

4 Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays. IEEE Trans Sig Process, 2010, 58: 1975–1887

5 Zhong B, Wu M G, Li T, et al. Physical layer security via maximal ratio combining and relay selection over Rayleigh fading channels. Sci China Inf Sci, 2016, 59: 062305

6 Zhao H, Tan Y, Pan G, et al. Secrecy outage on transmit antenna selection/maximal ratio caombining in MIMO cognitive radio networks. IEEE Trans Veh Tech, in press. doi: 10.1109/TVT.2016.2529704

7 Ha X N, Ha H N, Tho L N. Diversity analysis of relay selection schemes for two-way wireless relay networks. Wirel Pers Commun 2011, 59: 173–189

8 Mo J, Tao M, Liu Y. Relay placement for physical layer security: a secure connection perspective. IEEE Commun Lett, 2012, 16: 878–881

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

10 Tran D D, Ha D B, Vu T H, et al. Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels. IETE J Res, 2015, 61: 363–371

11 Singh A D, Subadar R. Capacity of dual MRC with adaptive transmitters over non-identical TWDP fading channels. In: Proceedings of Computer Engineering and Applications, Ghaziabad, 2015. 93–97

12 Mohamed S A, Marvin K S. Performance of coherent receivers with hybrid SC/MRC over Nakagami- m fading channels. IEEE Trans Veh Tech, 1999, 48: 1155–1164

13 Zhao H, Tan Y, Pan G, et al. Ergodic secrecy capacity of MRC/SC in SIMO wiretap systems with imperfect CSI. Front Inform Tech Electron Eng, in press. doi: 10.1631/FITEE.1500430
14 Bello P, Nelin B D. Predection diversity combining with selectively fading channels. IRE Trans Commun Syst, 1962, 10: 32–42
15 Gans M J. The effect of Gaussian error in maximal ratio combiners. IEEE Trans Commun Tech, 1971, 19: 492–500
16 Shrestha A P, Kwark K S. On maximal ratio diversity with weighting errors for physical layer security. IEEE Commun Lett, 2014, 18: 580–583
17 Zhao H, Pan G F. Analysis of secure communications for a DF and RF relaying SIMO system with Gauss errors. Sci Sin Inform, 2016, 46: 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]
18 Hu Y, Tao Y. Secrecy outage on transmit antenna selection with weighing errors at maximal-ratio combiners. IEEE Commun Lett, 2015, 4: 597–600
19 Tomiuk B R, Beaulieu N C, Abu-Dayya A A. General forms for maximal ratio diversity with weighting errors. IEEE Trans Commun, 1999, 47: 488–492
20 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products. 7th ed. London: Academic, 2007
21 Koyluoglu O O, Koksal C E, Gamal H E. On secrecy capacity scaling in wireless networks. IEEE Trans Inf Theory, 2012, 58: 3000–3015

附录 A

考虑如下积分等式

$$I\left(a,b\right)=\int_0^\infty f_{\gamma_2}\left(y\right)\exp\left(\alpha y\right)y^b\mathrm{d}y, \tag{A1}$$

其中, a 和 b 为非负实数. 将 γ_2 的 PDF 代入上式, 可以得到

$$I\left(a,b\right)=\sum_{m=1}^{N}\sum_{j=1}^{N}B\left(m\right)C\left(j\right)\left\{\underbrace{\int_0^\infty\frac{y^{j-1}\exp\left(-y/\overline{\gamma}_{2\mathrm{E}}\right)}{\Gamma\left(j\right)\overline{\gamma}_{2\mathrm{E}}^{j}}\exp\left(\alpha y\right)y^b\mathrm{d}y}_{I_1}+\underbrace{\int_0^\infty\frac{y^{m-1}\exp\left(-y/\overline{\gamma}_{1\mathrm{E}}\right)}{\Gamma\left(m\right)\overline{\gamma}_{1\mathrm{E}}^{m}}\exp\left(\alpha y\right)y^b\mathrm{d}y}_{I_2}\right.$$
$$\left.-\underbrace{\int_0^\infty\frac{y^{j-1}\exp\left(-y/\overline{\gamma}_{2\mathrm{E}}\right)\Gamma\left(m,y/\overline{\gamma}_{1\mathrm{E}}\right)}{\Gamma\left(m\right)\Gamma\left(j\right)\overline{\gamma}_{2\mathrm{E}}^{j}}\exp\left(\alpha y\right)y^b\mathrm{d}y}_{I_3}-\underbrace{\int_0^\infty\frac{y^{m-1}\exp\left(-y/\overline{\gamma}_{1\mathrm{E}}\right)\Gamma\left(j,y/\overline{\gamma}_{2\mathrm{E}}\right)}{\Gamma\left(m\right)\Gamma\left(j\right)\overline{\gamma}_{1\mathrm{E}}^{m}}\exp\left(\alpha y\right)y^b\mathrm{d}y}_{I_4}\right\}. \tag{A2}$$

利用文献 [20, 式(3.326.2)] 可以得到

$$I_1=\frac{1}{\Gamma\left(j\right)\overline{\gamma}_{2\mathrm{E}}^{j}}\frac{\Gamma\left(b+j\right)}{\left(1/\overline{\gamma}_{2\mathrm{E}}-\alpha\right)^{b+j}}, \tag{A3}$$

$$I_2=\frac{1}{\Gamma\left(m\right)\overline{\gamma}_{1\mathrm{E}}^{m}}\frac{\Gamma\left(b+m\right)}{\left(1/\overline{\gamma}_{1\mathrm{E}}-\alpha\right)^{b+m}}, \tag{A4}$$

$$I_3=\sum_{q_1=0}^{m-1}\frac{1}{\Gamma\left(j\right)\overline{\gamma}_{2\mathrm{E}}^{j}\overline{\gamma}_{1\mathrm{E}}^{q_1}q_1!}\frac{\Gamma\left(b+j+q_1\right)}{\left(1/\overline{\gamma}_{1\mathrm{E}}+1/\overline{\gamma}_{2\mathrm{E}}-\alpha\right)^{b+j+q_1}}, \tag{A5}$$

$$I_4=\sum_{q_2=0}^{j-1}\frac{1}{\Gamma\left(m\right)\overline{\gamma}_{1\mathrm{E}}^{m}\overline{\gamma}_{2\mathrm{E}}^{q_2}q_2!}\frac{\Gamma\left(b+m+q_2\right)}{\left(1/\overline{\gamma}_{1\mathrm{E}}+1/\overline{\gamma}_{2\mathrm{E}}-\alpha\right)^{b+m+q_2}}. \tag{A6}$$

最后, 根据式 (A2)∼(A6), 可以得到 $I(a,b)$ 的闭式表达式.

An analysis of secrecy outage performance of DF and RF relaying SIMO system with imperfect CSI

Danyang WANG, Hui ZHAO & Gaofeng PAN*

College of Electronic and Information Engineering, Southwest University, Chongqing 400715*, China*
*E-mail: gfpan@swu.edu.cn

Abstract This paper presents an investigation of the physical layer secrecy outage performance of the cooperative system in the typical four-node (source, relay, destination, and eavesdropper) scenario with imperfect channel state information (CSI). Specifically, we consider the single-input multiple-output wiretap channels, where the source (S) and the relay (R) are equipped with a single antenna, and the destination (D) and the eavesdropper (E) are equipped with multiple antennas. D and E adopt maximal ratio combining to process multiple copies of signals, and the relay adopts decode-and-forward (DF) and randomize-and-forward (RF) schemes to forward the received signal to the destination. E overhears the information transmitted over both the S-R and R-D links. We derive the closed-form and asymptotic expressions for the secrecy outage probability under both the DF and RF schemes with imperfect CSI, respectively, the accuracy of which is verified by simulation results.

Keywords CSI, Gauss errors, secrecy outage probability, single-input multiple-output, maximal ratio combining, decode-and-forward, randomize-and-forward, physical layer security

Danyang WANG was born in 1995. She is an undergraduate student with the School of Electronic and Information Engineering, Southwest University, Chongqing, China. Her main research interests include performance modeling and analysis of wireless systems, and physical layer security.

Hui ZHAO was born in 1993. He is an undergraduate student with the School of Electronic and Information Engineering, Southwest University, Chongqing, China. His main research interests include performance modeling and analysis of wireless systems, and physical layer security.