中国科学: 信息科学 2016 年 第 46 卷 第 3 期: 350–360
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

Gauss 信道估计误差下 DF 与 RF 中继 SIMO 系统保密通信性能分析

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: 2015–04–14; 接受日期: 2015–06–23; 网络出版日期: 2015–08–04
国家自然科学基金 (批准号: 61401372)、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)、重庆市科技人才培养计划 (新产品创新青年科技人才培养) (批准号: cstc2013kjrc-qnrc40011) 和中央高校基本科研业务经费 (批准号: XDJK2015B023, 2362014xk12) 资助项目

摘要 本文研究了经典的四点 (信源、中继、信宿、窃密者) 协作模型的物理层保密性能. 在此协作模型中, 信源通过中继向信宿发送信息, 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) 两种中继方式向信宿转发信息. 同时, 信源与中继、中继与信宿两跳通信中均遭到窃密者的窃听. 考虑信源和中继均为单天线, 信宿和窃密者为多天线的单输入多输出窃密信道模型. 信宿和窃密者采用最大比合并策略处理多径信号. 在考虑 Gauss 信道估计误差下, 首先推导出 DF 协议下信噪比的概率密度分布和累积概率密度分布的闭式表达式, 然后分别推导出 DF 与 RF 中继协作的非零保密容量概率的闭式表达式. 最后, 通过 Monte Carlo 仿真验证了理论模型的正确性.

关键词 物理层保密通信 解码放大转发 随机放大转发 单输入多输出系统 最大比合并 Gauss 误差 非零保密容量概率

1 引言

由于无线通信的开放性, 物理层保密通信已被广泛地认为是一种可有效保护信息而不被窃密的技术 [1]. 物理层保密通信的目的主要是通过利用无线信道的不相关特性尽可能地实现信息的完全保密. 完全保密意味着对于所有的消息 X 和窃密者对消息的获取 Y, 满足 $\mathrm{H}(X|Y) = \mathrm{H}(X)$.

Wyner 等 [2] 最早开展了物理层保密通信领域的研究, 建立了窃密信道模型, 并提出了保密容量的概念. 这些研究奠定了物理层保密通信领域研究的基础. 近些年来, 文献 [3∼5] 对 Wyner 的窃密信道模型进行了扩展, 在衰落环境中, 分别研究了在独立的/相关的 Rayleigh, log-normal, Rayleigh-log-normal 衰落信道下的保密性能.

为了改善保密性能, 分集技术受到了越来越多学者的关注. 目前, 分集的实现方式主要有多天线系统和中继系统. 文献 [6] 研究了多输入多输出 (multiple input multiple output, MIMO) 系统在

引用格式: 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, doi: 10.1360/N112015-00074

© 2015《中国科学》杂志社

Nakagami-m 衰落信道下采用发射天线选择, 最大比合并 (maximal ratio combining, MRC) 和接收天线选择式合并 (selection combining, SC) 分集技术的非零保密容量的概率 (probability of non-zero secrecy capacity, PNSC) 等保密性能, 证明了多天线的分集技术可以有效地提高通信的保密性能, 并且 MRC 保密分集性能明显高于 SC 保密分集性能. 另外, 文献 [7∼11] 等在中继协作系统也开展了一些研究工作. 文献 [7] 研究了在中继协作系统中保密通信的两种中继策略 — 解码放大转发 (decode-and-forward, DF) 和随机放大转发 (randomize-and-forward, RF) 在经典的四点模型 (信源、中继、信宿、窃密者) 中最优功率分配问题和在蜂窝网络中中继物理位置放置的问题. 针对多中继保密通信系统, 文献 [8] 提出了一个两阶段协作方案来改善保密性能. 在双向中继网络中, 文献 [9] 提出了分布式模拟网络编码和分布式波束形成两种策略, 并且通过功率分配来提高数据交换的保密速率. 文献 [10] 在经典的四点模型中, 分别研究了阻塞直接传输和中继传输方案的物理层保密通信性能. 文献 [11] 系统地讨论了 DF 中继传输方案的设计, 并且比较了相同码字、不同码字 (码书)、不同码率等情况下的保密性能.

文献 [12, 13] 指出: 因为 MRC 的平均合并输出信噪比是最高的, 所以对于所有的线性合并系统, MRC 是最理想的分集方式. 但是, 由于分集支路上的加权因子要时刻与衰落信道矢量的复共轭成比例, 那么, 当 pilot 的频谱范围与信道的相关带宽相近时, 就很容易出现 Gauss 信道估计误差, 从而导致 MRC 分集不理想, 降低了输出信噪比. 另外, 为了及时地从信号中分离出 pilot, 一般采用信号与 pilot 交替发送. 而当这个分离时间与衰落速率的倒数相近时, 从 pilot 中获得的加权因子也会出现 Gauss 信道估计误差. 文献 [14, 15] 将 Gans 和 Tomiuk 等的工作拓展到物理层保密通信中, 分别研究了单输入多输出 (single input multiple output, SIMO) 和 MIMO 窃密信道中接收者和窃密者同时出现 Gauss 信道估计误差时, MRC 合并的保密中断概率, 并给出了近似分析.

基于 Rayleigh 衰落信道, 在采用 MRC 分集技术的 SIMO 系统中, 研究了 Gauss 信道估计误差对 DF 与 RF 中继策略物理层保密通信性能的影响. 本文的主要创新点可以归纳为以下两点:

(1) 在文献 [12∼14] 的基础上, 根据 DF 中继的特点, 推导出了非理想 MRC 合并得到的信号信噪比的概率密度分布 (probability density function, PDF) 和累积概率密度分布 (cumulative distribution function, CDF);

(2) 在 (1) 的基础上, 分别研究了 DF 与 RF 的 PNSC 性能并推导出其闭式表达式.

2 系统模型

2.1 中继协作描述

如图 1 所示, 保密协作 SIMO 系统中包含信源 S, 中继 R, 信宿 D, 窃密者 E. 整个协作通信过程分为两个阶段 (参见文献 [7]): 在第 1 阶段, S 在编码后将信息发送给 R (采用 DF/RF 转发策略, 与信源采用相同的码书/与信源不同的码书); 在第 2 阶段中, R 重新编码来自信源 S 的信息, 并发送给 D (拥有 M 根天线并采用 MRC 分集技术). 假设 E (拥有 N 根天线并采用 MRC 分集技术) 对 S 和 R 传输的信息均窃密. 本文还假设从 S 到 D 之间没有直接信号路径 (在 D 距离信源比较远时, 由于衰落严重, 可以认为没有直接信号路径 [7]).

2.2 信噪比分析

2.2.1 信道估计误差分析

为了贴近实际环境, 考虑 D 和 E 的信道估计存在 Gauss 误差 (参见文献 [14, 15]), 造成 MRC 合

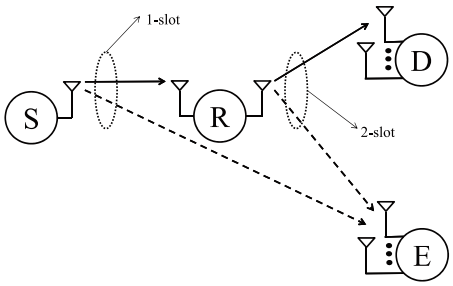

图 1　系统模型图

Figure 1　System model

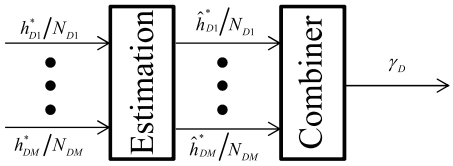

图 2　接收原理图

Figure 2　The principle diagram of the receiving

并时各个信道权重不准确, 导致输出信噪比下降.

如图 2 所示, 在 D 处, 第 u 个子信道接收信号为

$$y_{Du} = \sqrt{P_R} h_{Du} x + n_{Du}, u = 1, 2, ..., M, \tag{1}$$

其中, h_{Du} 为 R–D 链路中第 u 个子信道的信道衰落系数, x 为 R 发送的信息, n_{Du} 为复 Gauss 噪声, P_R 是 R 的平均发射功率.

合并信号为

$$y_D = \sum_{u=1}^{M} \frac{h_{Du}^*}{N_{Du}} y_{Du}, \tag{2}$$

其中, h_{Du}^* 为 h_{Du} 的共轭, N_{Du} 为 Gauss 噪声功率.

在实际情况中, 由于存在 Gauss 信道估计误差, 合并权重 h_{Du}^*/N_{Du} 很难被准确获得. 令 $\widehat{h}_{Du}^*/N_{Du}$ 为 h_{Du}^*/N_{Du} 的估计值, 那么第 2 跳中 D 处接收信号的瞬时信噪比可以表示为

$$\gamma_D = \sum_{u=1}^{M} \frac{P_R \left|\widehat{h}_{Du}\right|^2}{N_{Du}}.$$

根据文献 [15], 真实信道增益与估计误差信道增益的关系为

$$h_{Du} = \sqrt{\rho_D} \widehat{h}_{Du} + \sqrt{1-\rho_D} g_{Du}, \tag{3}$$

其中, $\rho_D \in [0, 1]$ 为文献 [12] 中 (58) 式定义的 R–D 链路的信道功率相关系数[1)], g_{Du} 是与 h_{Du} 独立同分布的随机变量.

同理, 可以得到 E 在前后两跳的瞬时信噪比分别为 $\gamma_{1E} = \sum_{v_1=1}^{N} \frac{P_S \left|\widehat{h}_{Ev_1}\right|^2}{N_{Ev_1}}$, $\gamma_{2E} = \sum_{v_2=1}^{N} \frac{P_R \left|\widehat{h}_{Ev_2}\right|^2}{N_{Ev_2}}$, 其中, P_S 为 S 平均发射功率, $\widehat{h}_{Ev_1}$ 与 N_{Ev_1} 和 $\widehat{h}_{Ev_2}$ 与 N_{Ev_2} 分别为第 1 跳和第 2 跳中 E 处第 v_1 和 v_2 $(v_1, v_2 = 1, 2, ..., N)$ 子信道的信道衰落系数的估计值与 Gauss 噪声功率.

2.2.2　中继信号分析

本文假设前后两跳的信道均为相互独立的平坦 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.

1) ρ_D 是衡量信道估计好坏的一个重要参数, ρ_D 越大, 信道估计越准确, 当 $\rho_D = 1$ 时, 代表理想 MRC 合并.

在第 1 阶段, R 处接收信号的信噪比的 PDF 和 CDF 可以分别写为

$$f_{\gamma_R}(x)=\frac{1}{\overline{\gamma}_R}\exp\left(-\frac{x}{\overline{\gamma}_R}\right), \tag{4}$$

$$F_{\gamma_R}(x)=1-\exp\left(-\frac{x}{\overline{\gamma}_R}\right), \tag{5}$$

其中, $\overline{\gamma}_R$ 为 R 接收信噪比的均值.

E 处接收信号的信噪比 (存在信道估计误差) 的 PDF 和 CDF 可以分别表示为 [13]

$$f_{\gamma_{1E}}(x)=\sum_{m=1}^{N}B(m)\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1E})}{\Gamma(m)\overline{\gamma}_{1E}^{m}}, \tag{6}$$

$$F_{\gamma_{1E}}(x)=\sum_{m=1}^{N}B(m)\left\{1-\frac{\Gamma(m,x/\overline{\gamma}_{1E})}{\Gamma(m)}\right\}, \tag{7}$$

其中, $\overline{\gamma}_{1E}$ 为第 1 阶段 E 处每个子信道接收信号的信噪比[2)] 的均值, $B(m)$ 定义为

$$B(m)=\binom{N-1}{m-1}(1-\rho_{1E})^{N-1}\rho_{1E}^{m-1}, \tag{8}$$

其中, $\rho_{1E}\in[0,1]$ 为第 1 跳 E 的信道估计与真实信道之间的功率相关系数.

在第 2 阶段, D 的接收信号的信噪比 (存在信道估计误差) 的 PDF 和 CDF 可以分别表示为

$$f_{\gamma_D}(x)=\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_D)}{\Gamma(i)\overline{\gamma}_D^{i}}, \tag{9}$$

$$F_{\gamma_D}(x)=\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_D)}{\Gamma(i)}\right\}, \tag{10}$$

其中, $\overline{\gamma}_D$ 为在第 2 阶段 D 处每个子信道接收信号的信噪比均值, $\Gamma(i)=\int_0^{\infty}\exp(-t)\,t^{i-1}\mathrm{d}t$ 为 Gamma 函数, $\Gamma(i,x)=\int_x^{\infty}\exp(-t)\,t^{i-1}\mathrm{d}t$ 为不完全 Gamma 函数, $A(i)$ 定义为

$$A(i)=\binom{M-1}{i-1}(1-\rho_D)^{M-1}\rho_D^{i-1}. \tag{11}$$

为了便于理解, 将 (9) 式改写为

$$f_{\gamma_D}(x)=\sum_{i=1}^{M}A(i)\,\widetilde{f}_{\gamma_D}(x,i), \tag{12}$$

其中, $\widetilde{f}_{\gamma_D}(x,i)$ 为 D 处 i 分集的 MRC 理想合并后输出信号的信噪比的 PDF [3)].

在第 2 阶段中, E 处接收信号的信噪比的 PDF 和 CDF 分别表示为

$$f_{\gamma_{2E}}(x)=\sum_{j=1}^{N}C(j)\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2E})}{\Gamma(j)\overline{\gamma}_{2E}^{j}}, \tag{13}$$

2) 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相同时, 处理起来非常的复杂. 为了便于分析, 本文采用了与文献 [12~15] 相同的方式进行简化.

3) 也就是说, 当信道权重不准确时, M 分集的 MRC 合并输出信噪比的 PDF 是 M 个理想 MRC 合并输出信噪比 PDF 的加权和.

$$F_{\gamma_{2E}}(x)=\sum_{j=1}^{N}C(j)\left\{1-\frac{\Gamma(j,x/\overline{\gamma}_{2E})}{\Gamma(j)}\right\}, \tag{14}$$

其中, $\overline{\gamma}_{2E}$ 为第 2 阶段中 E 处每个子信道接收信号的信噪比均值, 当 $\rho_{2E}\in[0,1]$ 时, $C(j)$ 的定义为

$$C(j)=\binom{N-1}{j-1}(1-\rho_{2E})^{N-1}\rho_{2E}^{j-1}. \tag{15}$$

根据 DF 中继转发策略, 可以分别得出 D [4] 和 E [5] 的瞬时等效信噪比

$$\gamma_1=\min\{\gamma_R,\gamma_D\},\quad \gamma_2=\max\{\gamma_{1E},\gamma_{2E}\}. \tag{16}$$

3 保密性能分析

3.1 求解 γ_1 和 γ_2 的 PDF 与 CDF

利用文献 [16] 的 (6-78) 式, 可以得到

$$F_{\gamma_1}(x)=F_{\gamma_R}(x)+F_{\gamma_D}(x)-F_{\gamma_R}(x)F_{\gamma_D}(x). \tag{17}$$

将 (5) 和 (10) 式带入 (17) 式, 可得 γ_1 的 CDF 为

$$\begin{aligned}F_{\gamma_1}(x)=&1-\exp\left(-\frac{x}{\overline{\gamma}_R}\right)+\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_D)}{\Gamma(i)}\right\}\\&-\left[1-\exp\left(-\frac{x}{\overline{\gamma}_R}\right)\right]\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_D)}{\Gamma(i)}\right\}.\end{aligned} \tag{18}$$

对 (17) 式进行求导, 可以得到

$$f_{\gamma_1}(x)=f_{\gamma_R}(x)+f_{\gamma_D}(x)-f_{\gamma_R}(x)F_{\gamma_D}(x)-F_{\gamma_R}(x)f_{\gamma_D}(x). \tag{19}$$

γ_1 的 PDF 可以表示为

$$\begin{aligned}f_{\gamma_1}(x)=&\frac{1}{\overline{\gamma}_R}\exp\left(-\frac{x}{\overline{\gamma}_R}\right)+\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_D)}{\Gamma(i)\overline{\gamma}_D^{i}}\\&-\frac{1}{\overline{\gamma}_R}\exp\left(-\frac{x}{\overline{\gamma}_R}\right)\sum_{i=1}^{M}A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_D)}{\Gamma(i)}\right\}\\&-\left[1-\exp\left(-\frac{x}{\overline{\gamma}_R}\right)\right]\sum_{i=1}^{M}A(i)\frac{x^{i-1}\exp(-x/\overline{\gamma}_D)}{\Gamma(i)\overline{\gamma}_D^{i}}.\end{aligned} \tag{20}$$

利用文献 [16] 的 (6-81) 式, 可以得到

$$F_{\gamma_2}(x)=F_{\gamma_{1E}}(x)F_{\gamma_{2E}}(x). \tag{21}$$

4) 出于简化的目的, 在 DF 中继策略中, 本文考虑 S 和 R 采用相同的码书, 且两者发送的码速率相同. 当然由于 DF 协作的特殊性, S 和 R 发送的码速率也可以不同 [11].

5) 有别于文献 [7] 中窃听者处的信号处理方式, 为简化系统实现的复杂性, 本文假设 E 只对前后两次窃听到的信号中信噪比较高的进行解码, 这实质上相当于 SC 合并.

将 (7) 和 (14) 式带入 (21) 式, 可以得到 γ_2 的 CDF

$$F_{\gamma_2}(x)=\sum_{m=1}^{N}\sum_{j=1}^{N}B(m)C(j)\left\{1-\frac{\Gamma(m,x/\overline{\gamma}_{1E})}{\Gamma(m)}-\frac{\Gamma(j,x/\overline{\gamma}_{2E})}{\Gamma(j)}+\frac{\Gamma(m,x/\overline{\gamma}_{1E})\Gamma(j,x/\overline{\gamma}_{2E})}{\Gamma(m)\Gamma(j)}\right\}. \quad (22)$$

对 (21) 式进行求导, 可以得到

$$f_{\gamma_2}(x)=f_{\gamma_{1E}}(x)F_{\gamma_{2E}}(x)+F_{\gamma_{1E}}(x)f_{\gamma_{2E}}(x). \quad (23)$$

γ_2 的 PDF 可以表示为

$$f_{\gamma_2}(x)=\sum_{m=1}^{N}\sum_{j=1}^{N}B(m)C(j)\left\{\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2E})}{\Gamma(j)\overline{\gamma}_{2E}^{j}}+\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1E})}{\Gamma(m)\overline{\gamma}_{1E}^{m}}\right.$$
$$\left.-\frac{x^{j-1}\exp(-x/\overline{\gamma}_{2E})\Gamma(m,x/\overline{\gamma}_{1E})}{\Gamma(m)\Gamma(j)\overline{\gamma}_{2E}^{j}}-\frac{x^{m-1}\exp(-x/\overline{\gamma}_{1E})\Gamma(j,x/\overline{\gamma}_{2E})}{\Gamma(m)\Gamma(j)\overline{\gamma}_{1E}^{m}}\right\}. \quad (24)$$

3.2 非零保密容量概率

根据文献 [6], PNSC 被定义为保密容量不为零的概率, 是保密通信研究的热点和重点, 并与遍历保密容量和保密中断概率一起成为物理层保密的三大重要性能. 下面按照 PNSC 的定义以及 DF 与 RF 中继协作的特点, 分别求出了 DF 与 RF 中继协作下的 PNSC 的闭式表达式.

3.2.1 DF 中继转发的 PNSC

根据文献 [7], DF 中继协作下的瞬时保密容量可以定义为

$$C_S(\gamma_1,\gamma_2)=\begin{cases}\frac{1}{2}\log(1+\gamma_1)-\frac{1}{2}\log(1+\gamma_2), & \gamma_1>\gamma_2;\\ 0, & \gamma_1\leqslant\gamma_2,\end{cases} \quad (25)$$

其中, $\frac{1}{2}\log(1+\gamma_1)$ 和 $\frac{1}{2}\log(1+\gamma_2)$ 分别为 D 和 E 的瞬时分集信道容量.

根据 DF 中继协作下的瞬时保密容量的定义, PNSC 可以写为

$$\mathrm{PNSC}=\Pr\{C_S(\gamma_1,\gamma_2)>0\}=\Pr\{\gamma_1>\gamma_2\}. \quad (26)$$

(26) 式可以用积分形式表示为

$$\mathrm{PNSC}=\int_0^{\infty}\int_0^{\gamma_1}f_{\gamma_1}(\gamma_1)f_{\gamma_2}(\gamma_2)\,\mathrm{d}\gamma_2\mathrm{d}\gamma_1=\int_0^{\infty}f_{\gamma_1}(\gamma_1)F_{\gamma_2}(\gamma_1)\,\mathrm{d}\gamma_1. \quad (27)$$

将 γ_2 的 CDF 带入上式得到

$$\mathrm{PNSC}=\sum_{m=1}^{N}\sum_{j=1}^{N}B(m)C(j)\left\{\underbrace{\int_0^{\infty}f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1}_{I_1}-\underbrace{\int_0^{\infty}\frac{\Gamma(m,\gamma_1/\overline{\gamma}_{1E})}{\Gamma(m)}f_{\gamma_1}(\gamma_1)\mathrm{d}\gamma_1}_{I_2}\right.$$
$$\left.-\underbrace{\int_0^{\infty}\frac{\Gamma(j,\gamma_1/\overline{\gamma}_{2E})}{\Gamma(j)}f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1}_{I_3}+\underbrace{\int_0^{\infty}\frac{\Gamma(m,\gamma_1/\overline{\gamma}_{1E})\Gamma(j,\gamma_1/\overline{\gamma}_{2E})}{\Gamma(m)\Gamma(j)}f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1}_{I_4}\right\}. \quad (28)$$

显然, $I_1=1$, 利用文献 [17] 中 (8.352.4) 式, 可得 $\Gamma(n,x)=(n-1)!\exp(-x)\sum_{q=0}^{n-1}\frac{x^q}{q!}, n=1,2,...,$ 可得

$$I_2=\sum_{q_1=0}^{m-1}\frac{1}{q_1!\overline{\gamma}_{1E}^{q_1}}\int_0^{\infty}\gamma_1^{q_1}\exp\left(-\frac{\gamma_1}{\overline{\gamma}_{1E}}\right)f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1, \tag{29}$$

$$I_3=\sum_{q_2=0}^{j-1}\frac{1}{q_2!\overline{\gamma}_{2E}^{q_2}}\int_0^{\infty}\gamma_1^{q_2}\exp\left(-\frac{\gamma_1}{\overline{\gamma}_{2E}}\right)f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1, \tag{30}$$

$$I_4=\sum_{q_3=0}^{m-1}\sum_{q_4=0}^{j-1}\frac{1}{q_3!q_4!\overline{\gamma}_{1E}^{q_3}\overline{\gamma}_{2E}^{q_4}}\int_0^{\infty}\gamma_1^{q_3+q_4}\exp\left[-\left(\frac{1}{\overline{\gamma}_{1E}}+\frac{1}{\overline{\gamma}_{2E}}\right)\gamma_1\right]f_{\gamma_1}(\gamma_1)\,\mathrm{d}\gamma_1. \tag{31}$$

由附录 A 中的积分等式, 可以得到

$$I_2=\sum_{q_1=0}^{m-1}\frac{1}{q_1!\overline{\gamma}_{1E}^{q_1}}I\left(q_1,\frac{1}{\overline{\gamma}_{1E}}\right), \tag{32}$$

$$I_3=\sum_{q_2=0}^{j-1}\frac{1}{q_2!\overline{\gamma}_{2E}^{q_2}}I\left(q_2,\frac{1}{\overline{\gamma}_{2E}}\right), \tag{33}$$

$$I_4=\sum_{q_3=0}^{m-1}\sum_{q_4=0}^{j-1}\frac{I\left(q_3+q_4,1/\overline{\gamma}_{1E}+1/\overline{\gamma}_{2E}\right)}{q_3!q_4!\overline{\gamma}_{1E}^{q_3}\overline{\gamma}_{2E}^{q_4}}. \tag{34}$$

因为 $I_1=1$, 再结合 (32)∼(34) 和 (28) 式, 最终可以得到 DF 中继转发的 PNSC.

3.2.2 RF 中继转发的 PNSC

根据文献 [18], 只有当两跳链路都是保密的时候, 才能实现保密传输. 因此, 可以定义 RF 策略的 PNSC 如下[6)]

$$\mathrm{PNSC}=\Pr\{\gamma_R>\gamma_{1E}\}\Pr\{\gamma_D>\gamma_{2E}\}. \tag{35}$$

将 $\Pr\{\gamma_R>\gamma_{1E}\}$ 写为积分形式

$$\Pr\{\gamma_R>\gamma_{1E}\}=\int_0^{\infty}\int_0^{\gamma_R}f_{\gamma_R}(\gamma_R)f_{\gamma_{1E}}(\gamma_{1E})\,\mathrm{d}\gamma_{1E}\mathrm{d}\gamma_R=\int_0^{\infty}f_{\gamma_R}(\gamma_R)F_{\gamma_{1E}}(\gamma_R)\,\mathrm{d}\gamma_R. \tag{36}$$

将 γ_R 的 PDF 和 γ_{1E} 的 CDF 带入上式得到

$$\begin{aligned}&\Pr\{\gamma_R>\gamma_{1E}\}\\&=\sum_{m=1}^{N}B(m)\frac{1}{\overline{\gamma}_R}\left\{\int_0^{\infty}\exp\left(-\frac{\gamma_R}{\overline{\gamma}_R}\right)\mathrm{d}\gamma_R-\sum_{q=0}^{m-1}\frac{(m-1)!}{q!\overline{\gamma}_{1E}^{q}}\int_0^{\infty}\gamma_R^{q}\exp\left[-\left(\frac{1}{\overline{\gamma}_{1E}}+\frac{1}{\overline{\gamma}_R}\right)\gamma_R\right]\mathrm{d}\gamma_R\right\}\\&=\sum_{m=1}^{N}B(m)\frac{1}{\overline{\gamma}_R}\left\{\overline{\gamma}_R-\sum_{q=0}^{m-1}\frac{1}{\overline{\gamma}_{1E}^{q}}\frac{1}{(1/\overline{\gamma}_{1E}+1/\overline{\gamma}_R)^{q+1}}\right\}.\end{aligned} \tag{37}$$

将 $\Pr\{\gamma_D>\gamma_{2E}\}$ 写成积分形式并计算得到

$$\Pr\{\gamma_D>\gamma_{2E}\}=\int_0^{\infty}f_{\gamma_D}(\gamma_D)F_{\gamma_{2E}}(\gamma_D)\,\mathrm{d}\gamma_D$$

6) 在 RF 中继策略中, 当 S 和 R 采用不同的码书发送信息时, 在窃密者的接收端将无法对两跳信号进行分集合并 [18], 这也正是 RF 策略在保密性能方面优于 DF 策略的原因 [7].

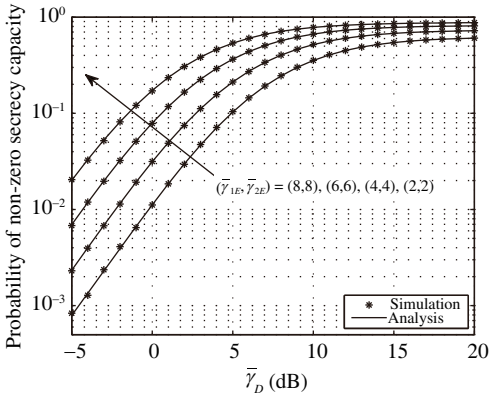

图 3 DF 中继下 PNSC 随 $\overline{\gamma}_D$ 的变化曲线

Figure 3 PNSC versus $\overline{\gamma}_D$ of DF

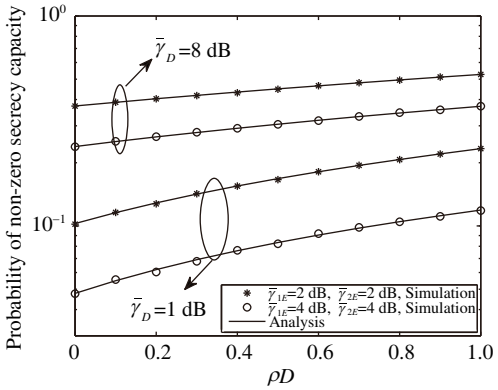

图 4 DF 中继下 PNSC 随 ρ_D 的变化曲线

Figure 4 PNSC versus ρ_D of DF

$$
\begin{aligned}
&= \sum_{i=1}^{M}\sum_{j=1}^{N} A(i)C(j)\frac{1}{\Gamma(i)\overline{\gamma}_D^i}\left\{\int_0^\infty \gamma_D^{i-1}\exp\left(-\frac{\gamma_D}{\overline{\gamma}_D}\right)\mathrm{d}\gamma_D\right.\\
&\quad\left.-\frac{1}{\Gamma(j)}\int_0^\infty \gamma_D^{i-1}\exp\left(-\frac{\gamma_D}{\overline{\gamma}_D}\right)\Gamma\left(j,\frac{\gamma_D}{\overline{\gamma}_{2E}}\right)\mathrm{d}\gamma_D\right\}\\
&= \sum_{i=1}^{M}\sum_{j=1}^{N} A(i)C(j)\frac{1}{\Gamma(i)\overline{\gamma}_D^i}\left\{\frac{(i-1)!}{(1/\overline{\gamma}_D)^i}-\sum_{p=0}^{j-1}\frac{(i+p-1)!}{p!\overline{\gamma}_{2E}^p}\frac{1}{(1/\overline{\gamma}_D+1/\overline{\gamma}_{2E})^{i+p}}\right\}. \qquad (38)
\end{aligned}
$$

最后, 结合 (35), (37) 和 (38) 式, 可以得到 RF 中继协作的 PNSC.

4 仿真与分析

本节将用 Monte Carlo 仿真法验证前面得到的 PNSC 闭式表达式. 在 Monte Carlo 仿真中, 参照文献 [12] 的 (23) 式构造接收端的瞬时合并信噪比[7)].

当 $\overline{\gamma}_R = 15$ dB, $\rho_D = \rho_{1E} = \rho_{2E} = 0.8$, $M = N = 2$ 时, 图 3 给出了 DF 中继策略下的 PNSC 在组合 $(\overline{\gamma}_{1E}, \overline{\gamma}_{2E}) = (2,2), (4,4), (6,6), (8,8)$ dB 下随 $\overline{\gamma}_D$ 的变化曲线. 可以很容易看出, 随着 $\overline{\gamma}_D$ 的增大, PNSC 也增大, 因为在 DF 中继策略下第 2 跳信道状况得到改善. 另外, 随着组合 $(\overline{\gamma}_{1E}, \overline{\gamma}_{2E})$ 的增大, PNSC 在下降. 这是因为 E 处的分集信噪比在增大, 导致保密容量变小.

当 $\overline{\gamma}_R = 8$ dB, $M = N = 2$, $\rho_{1E} = 0.8$, $\rho_{2E} = 0.5$ 时, 图 4 给出了 PNSC 在不同的 $\overline{\gamma}_D$, $\overline{\gamma}_{1E}$, $\overline{\gamma}_{2E}$ 下随 ρ_D 的变化情况. 可以看出, 随着 ρ_D 的增大, PNSC 也在增大, 因为 ρ_D 越大, D 处的信道加权因子的估计就越准确. 另外, 随着 $\overline{\gamma}_D$ 的减小和 $\overline{\gamma}_{1E}$, $\overline{\gamma}_{2E}$ 的增大, PNSC 在减小. 这是因为 D 处的第 2 跳链路状况变得恶劣, 而 E 处的分集信噪比得到了改善.

当 $\overline{\gamma}_R = 15$ dB, $M = N = 4$, $\rho_D = \rho_{1E} = \rho_{2E} = 0.8$ 时, 图 5 给出了 RF 中继下的 PNSC 在不同的组合 $(\overline{\gamma}_{1E}, \overline{\gamma}_{2E})$ 下随 $\overline{\gamma}_D$ 的变化曲线. 随着 $\overline{\gamma}_D$ 的增大, PNSC 在增大, 因为 D 的第 2 跳链路状况得到改善. 另外, $(\overline{\gamma}_{1E}, \overline{\gamma}_{2E}) = (5,10)$ dB 和 $(10,5)$ dB 时, PNSC 曲线在大约 10 dB 处有一个交汇点, 并且当 $\overline{\gamma}_D \to \infty$ 时, $(\overline{\gamma}_{1E}, \overline{\gamma}_{2E}) = (10,10)$ dB 和 $(10,5)$ dB 有相同的上限.

7) 也可以根据 (3) 式给出的真实信道和估计信道之间的相关关系构造信噪比.

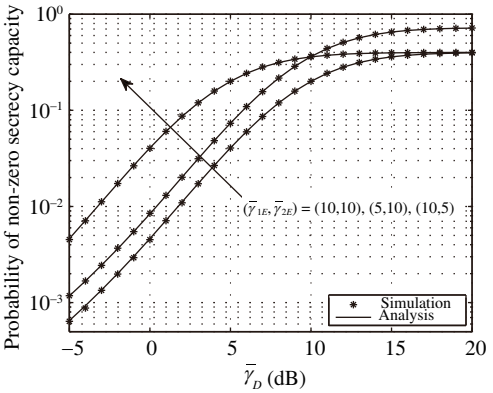

图 5 RF 中继下 PNSC 随 $\overline{\gamma}_D$ 的变化曲线
Figure 5 PNSC versus $\overline{\gamma}_D$ of RF

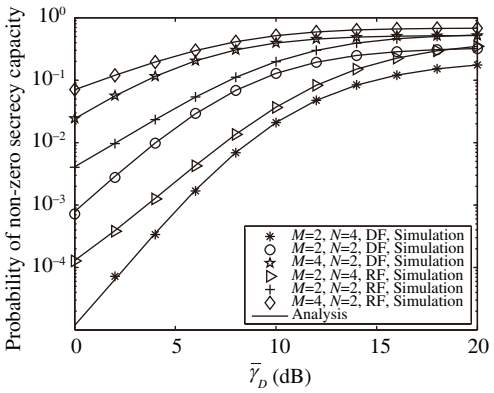

图 6 DF 与 RF 中继下 PNSC 随 $\overline{\gamma}_D$ 的变化曲线
Figure 6 PNSC versus $\overline{\gamma}_D$ of DF and RF

为了比较 DF 与 RF 中继协作的保密性能, 图 6 绘制了当 $\overline{\gamma}_R = 15$ dB, $\overline{\gamma}_{1E} = \overline{\gamma}_{2E} = 10$ dB, $\rho_D = 0.5$, $\rho_{1E} = 0.4$, $\rho_{2E} = 0.8$ 时, DF 与 RF 中继协作的 PNSC 在不同的 (M, N) 组合下随 $\overline{\gamma}_D$ 的变化曲线图. 从图中可以很容易看出随着 M 的增加和 N 的减小, DF 与 RF 中继协作的 PNSC 都增大, 原因在于 D 在第 2 跳的合并信噪比得到改善, E 前后两跳的合并信噪比都变小. 进一步, 可以看出在相同的 (M, N) 组合中, RF 中继协作的 PNSC 要明显高于 DF 中继协作的 PNSC, 因为 RF 中继协作中只需要保证前后两跳都是保密的, 而在 DF 协作中 E 在前后两跳相当于一个信噪比最大的选择合并, 同时 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. 另外, 还可以看出 DF 中继协作下 $(M, N) = (2, 2)$ 与 $(4, 2)$ 分别和 RF 中继协作下 $(M, N) = (2, 4)$ 与 $(2, 2)$ 在大信噪比时 PNSC 基本是一样的.

此外, 可以看出图 3∼6 中的 Monte Carlo 仿真与得到的理论结果吻合得非常好, 这充分证明了本文中得到的 DF 与 RF 中继协议下 PNSC 闭式表达式的正确性.

5 结论

本文研究了 Gauss 信道估计误差下的 DF 与 RF 中继 SIMO 系统 MRC 分集的保密通信性能, 并且得出了 DF 中继协作下接收者和窃密者信噪比的概率密度分布与累积概率密度分布的闭式表达式, 然后又分别得出了 DF 与 RF 两种中继协作方式的 PNSC 闭式表达式, 最后通过 Monte Carlo 仿真验证了本文所提出的理论分析模型的正确性, 从仿真中可以很明显看出 RF 的协作保密性能明显强于 DF 的协作保密性能, 并且随着接收者信道功率相关系数的增大, MRC 合并权重向量估计误差越小, 保密性能越好.

参考文献

1 Shiu Y S, Chang S Y, Wu H-C, et al. Physical layer security in wireless networks: a tutorial. IEEE Commun Mag, 2011, 18: 66–74
2 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
3 Gopala P K, Lai L, Gamal H El. On the secrecy capacity of fading channels. IEEE Trans Inf Theory, 2008, 54: 4687–4698

4 Sun X, Wang J, Xu W, et al. Performance of secure communications over correlated fading channels. IEEE Sig Process Lett, 2012, 54: 479–482

5 Pan G, Tang C, Zhang X, et al. Physical layer security over non-small scale fading channels. IEEE Trans Veh Tech, inpress. doi: 10.1109/TVT.2015.2412140

6 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

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

8 Yang B, Wang W, Yao B, et al. Destination assisted secret wireless communication with cooperative helpers. IEEE Sig Process Lett, 2013, 20: 1030–1033

9 Wang H M, Yin Q, Xia X G. Distributed beamforming for physical-layer security of two-way relay networks. IEEE Trans Sig Process, 2012, 60: 3532–3545

10 Deng H, Wang H M, Guo W, et al. Secrecy transmission with a helper: to relay or to jam. IEEE Trans Inf Foren Sec, 2015, 10: 293–307

11 Zheng T X, Wang H M, Liu F, et al. Outage constrained secrecy throughput maximization for DF relay networks. IEEE Trans Commun, 2015, 63: 1741–1755

12 Gans M J. The effect of Gaussian error in maximal ratio combiners. IEEE Trans Commun Technol, 1971, 19: 492–500

13 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

14 Shrestha A P, Kwark K S. On maximal ratio diversity with weighting errors for physical layer security. IEEE Commun Lett, 2014, 18: 580–583

15 Hu Y, Tao Y. Secrecy outage on transmit antenna selection with weighting errors at maximal-ratio combiners. IEEE Commun Lett, 2015, 4: 597–600

16 Papoulis A, Pillai S U. Probability, Random Variables and Stochastic Processes. 4th ed. New York: McGraw-Hill, 2001

17 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products. 7th ed. New York: Academic, 2007

18 Koyluoglu O O, Koksal C E, Gamal H El. On secrecy capacity scaling in wireless networks. IEEE Trans Inf Theory, 2012, 58: 3000–3015

附录 A

考虑如下的积分等式

$$I(\alpha,\beta)=\int_0^\infty x^\alpha \exp(-\beta x) f_{\gamma_1}(x)\,\mathrm{d}x, \tag{A1}$$

其中, α 和 β 为非负实数. 将 γ_1 的 PDF 带入上式, 可以得到

$$\begin{aligned} I(\alpha,\beta)=&\underbrace{\int_0^\infty \frac{x^\alpha}{\overline{\gamma}_R}\exp\left[-\left(\beta+\frac{1}{\overline{\gamma}_R}\right)x\right]\mathrm{d}x}_{II_1}+\underbrace{\sum_{i=1}^M A(i)\int_0^\infty \frac{x^{\alpha+i-1}\exp\left[-\left(\beta+1/\overline{\gamma}_D\right)x\right]}{\Gamma(i)\,\overline{\gamma}_D^i}\mathrm{d}x}_{II_2}\\ &\underbrace{-\int_0^\infty \frac{1}{\overline{\gamma}_R}\exp\left[-\left(\beta+\frac{1}{\overline{\gamma}_R}\right)x\right]x^\alpha\sum_{i=1}^M A(i)\left\{1-\frac{\Gamma(i,x/\overline{\gamma}_D)}{\Gamma(i)}\right\}\mathrm{d}x}_{II_3}\\ &\underbrace{-\int_0^\infty\left[1-\exp\left(-\frac{x}{\overline{\gamma}_R}\right)\right]\sum_{i=1}^M A(i)\frac{x^{\alpha+i-1}\exp\left[-\left(\beta+1/\overline{\gamma}_D\right)x\right]}{\Gamma(i)\,\overline{\gamma}_D^i}\mathrm{d}x}_{II_4}. \end{aligned} \tag{A2}$$

利用文献 [17] 的 (3.326.2) 和 (6.455.1) 式, 可以计算得到

$$\mathrm{II}_1=\frac{1}{\overline{\gamma}_R}\frac{\Gamma(\alpha+1)}{(\beta+1/\overline{\gamma}_R)^{\alpha+1}}, \tag{A3}$$

$$\mathrm{II}_2=\sum_{i=1}^M A(i)\frac{1}{\Gamma(i)\,\overline{\gamma}_D^i}\frac{\Gamma(\alpha+i)}{(\beta+1/\overline{\gamma}_D)^{\alpha+i}}, \tag{A4}$$

$$\mathrm{II}_3=\sum_{i=1}^{M}A(i)\frac{1}{\overline{\gamma}_R}\left\{\frac{\Gamma(\alpha+1)}{(\beta+1/\overline{\gamma}_R)^{\alpha+1}}-\frac{1}{\Gamma(i)}\frac{(1/\overline{\gamma}_D)^i\Gamma(\alpha+i+1)}{(\alpha+1)(1/\overline{\gamma}_D+\beta+1/\overline{\gamma}_R)^{\alpha+i+1}}\right.$$
$$\left.\cdot\ {}_2F_1\left(1,\alpha+i+1;\alpha+2;\frac{\beta+1/\overline{\gamma}_R}{1/\overline{\gamma}_D+\beta+1/\overline{\gamma}_R}\right)\right\},\tag{A5}$$

$$\mathrm{II}_4=\sum_{i=1}^{M}\frac{A(i)}{\Gamma(i)\overline{\gamma}_D^i}\Gamma(\alpha+i)\left\{\frac{1}{(\beta+1/\overline{\gamma}_D)^{\alpha+i}}-\frac{1}{(1/\overline{\gamma}_R+\beta+1/\overline{\gamma}_D)^{\alpha+i}}\right\},\tag{A6}$$

其中, ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ 是 Gauss 超几何函数[17].

最后, 结合 (A2)∼(A6) 式, 可以得到 $I(\alpha,\beta)$ 的闭式表达式.

Analysis of secure communications for a DF and RF relaying SIMO system with Gauss errors

Hui ZHAO & Gaofeng PAN*

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

Abstract This paper investigates a cooperative system for the typical four-node (source, relay, destination, and eavesdropper) scenario in physical-layer security. In the cooperative system, the source transmits its message to the destination via the relay, which adopts decode-and-forward (DF) and randomize-and-forward (RF) schemes to forward the information from the source to the destination, respectively. However, the eavesdropper wants to overhear the information of the source-relay link and the relay-destination link over the two hops. We consider single-input, multiple-output (SIMO) wiretap channels, where the source and the relay are equipped with a single antenna and the destination and eavesdropper are equipped with M and N antennas, and adopt a maximal ratio combining to deal with multipath signals. Considering Gauss channel estimation errors, we first derive the closed-form expressions for the probability density function and cumulative distribution function of the received signal-to-noise ratio at the destination and the eavesdropper, respectively, under the DF scheme; then, the closed-form expressions for the probability of non-zero secrecy capacity are derived under the DF and RF schemes, respectively. Finally, the accuracy of our proposed expressions is verified by simulation results.

Keywords physical layer security, decode-and-forward, randomize-and-forward, single-input multiple-output, maximal ratio combining, Gauss errors, probability of non-zero secrecy capacity

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.

Gaofeng PAN was born in 1981. He received his B.S. in Communication Engineering from Zhengzhou University, Zhengzhou, China, in 2005, and the Ph.D. degree in Communication and Information Systems from Southwest Jiaotong University, Chengdu, China, in 2011. In May 2012, he joined the School of Electronic and Information Engineering, Southwest University, Chongqing, China, where he is currently an associate professor. His research interests span special topics in communications theory, signal processing, and resource scheduling, including secure communications and cooperative and CR communications.