



研究与开发

相关衰落信道上 WCDMA 系统的安全性能分析

李光球, 王占湾, 任婷洁, 刘帅帅

(杭州电子科技大学通信工程学院, 浙江 杭州 310018)

摘要: 对多输入多输出(MIMO)相关衰落信道上宽带码分多址接入(WCDMA)的安全性能进行评估, 一种省时高效的解决方案是理论分析法。推导了相关 Nakagami 衰落信道上采用空时分组码和二维瑞克接收机(2D-Rake)的 WCDMA 系统的非零安全容量概率和安全中断概率的精确解析表达式。利用上述表达式, 可以快速地评估收发天线数、天线相关系数、Nakagami 衰落系数、平均路径衰减系数等参数对 WCDMA 系统安全性能造成的影响。数值计算和仿真结果相吻合, 证明了以上理论分析的正确性。推导了 WCDMA 系统渐近安全中断概率的解析表达式。结果表明, WCDMA 系统的安全分集增益为主信道各个可分离路径上的分集增益之和, 与窃听信道无关; 对于恒定多径强度轮廓的同分布 Nakagami 衰落信道, WCDMA 系统的安全分集增益为主信道的收/发天线数、多径个数以及 Nakagami 衰落系数四者之积。

关键词: 物理层安全; 宽带码分多址接入; 相关 Nakagami 衰落信道; 二维瑞克接收机; 安全中断概率

中图分类号: TN918.1

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018190

Secure performance analysis of WCDMA systems over correlated Nakagami fading channels

LI Guangqiu, WANG Zhanwan, REN Tingjie, LIU Shuaishuai

School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: In order to evaluate the security performance of wideband code division multiple access (WCDMA) over multiple-input and multiple-output fading channels, a time-saving and efficient solution is theoretical analysis. The exact analytical expressions of the non-zero security capacity probability and the security outage probability of WCDMA systems using space-time block codes and 2D Rake receivers (2D-Rake) on the relevant Nakagami fading channels was deduced. Using the above expressions, the effects of parameters such as the number of transmit and receive antennas, antenna correlation coefficient, Nakagami fading coefficient, and average path attenuation coefficient on the security performance of the WCDMA system could be quickly evaluated. The numerical calculation was in good agreement with the simulation results, which proved the correctness of the above theoretical analysis. The analytical expression of the asymptotic safety outage probability of WCDMA system was deduced. The results show that the security diversity gain of WCDMA system is the sum of the diversity gains on the separable paths of the main channel, and has nothing to do with the eavesdropping channel; the same for the constant multipath intensity profile. The Nakagami fading channel is distributed, and the security diversity gain of the WCDMA system is the product of the number of received and transmitted antennas of the primary channel, the number of multipaths, and the Nakagami fading coefficient.

Key words: physical layer security, wideband code division multiple access, correlated Nakagami fading channel, two-dimension Rake receiver, secrecy outage probability

收稿日期: 2018-04-02; 修回日期: 2018-06-06



1 引言

近年来, 物理层安全^[1-2]逐渐成为通信领域的研究热点, 其中光通信和无线通信领域的码分多址接入 (code division multiple access, CDMA) 系统的物理层安全研究已受到广泛关注^[3-6]。参考文献[3]研究了多用户光 CDMA 系统的安全容量, 分析了用户数、输入信号功率和移位寄存器级数对其安全性能的影响。参考文献[4]建立了相干光 CDMA 系统的物理层安全模型并分析其安全性能。在无线通信领域, 参考文献[5]通过对 CDMA 系统的扩频码进行设计, 在保证合法用户服务质量的前提下, 使窃听者的输出信干噪比 (signal-to-interference-plus-noise ratio, SINR) 达到最小, 以此来提升瑞利 (Rayleigh) 衰落信道上单用户 CDMA 系统的安全性能。参考文献[6]研究了 CDMA 系统下行链路在单用户和多用户应用场景下的安全传输问题, 对单用户传输场景, 设计了一种二进制签名方案, 其目标是使合法接收者的 SINR 维持在期望的水平, 同时使窃听者的 SINR 达到最小。参考文献[7]研究了伪装干扰下的 CDMA 系统设计并给出其容量分析。参考文献[8]研究了采用低密度奇偶校验码的方案来提升 CDMA 系统的安全性能。由于可采用盲检测算法在没有信号先验信息的情况下对 CDMA 系统传输的信息符号进行提取^[9-10], 宽带码分多址接入 (wideband-CDMA, WCDMA) 系统作为 3G 移动通信技术标准之一^[11], 其本身虽然具有一定的保密传输能力, 然而, 关于 WCDMA 系统的物理层安全性能分析却并未像光 CDMA 那样受到关注。为此, 下面对 WCDMA 系统的物理层安全性能进行研究, 推导相关 Nakagami 衰落信道上采用空时分组码^[12]和二维瑞克 (two-dimension Rake, 2D-Rake) 接收机的 WCDMA 系统的非零安全容量概率和安全中断概率等性能指标的精确解析表达式, 并利用上述表达式对系统的安全性

能进行分析与评估。

2 系统模型

考虑相关 Nakagami 衰落信道上 WCDMA 系统下行链路的物理层安全模型, 如图 1 所示, 由发送端 (或基站) Alice、合法移动接收端 Bob、被动窃听者 Eve 组成, 各个节点上的天线数分别为 N_A 、 N_B 和 N_E 。假定: Alice 采用空时分组码发送信号, 发射功率在 N_A 根天线间平均分配, 信道衰落至少在两个符号间隔上保持恒定; Bob 和 Eve 具有理想的信道估计且采用最大比合并 2D-Rake 接收机进行分集接收; 窃听者 Eve 能够获得 Alice 发送信号的参数^[3], 如数据速率、编码类型以及码字结构等, 且可以通过盲估计算法对接收信号进行解扩和解调^[10]; Alice、Bob 和 Eve 上的天线阵之间相互独立, 合法接收端 Bob 和窃听者 Eve 的接收天线均经历相同的衰落, 每对发射天线和接收天线间的各个可分离路径上的衰落相互独立。主信道和窃听信道均可由多径抽头延时线模型来模拟, 其等效低通矢量信道可分别表示为^[13-14]:

$$\mathbf{H}_x(\tau) = \sum_{l=0}^{L_x-1} \delta(\tau - \tau_l) \mathbf{h}_x^{(l)}, x \in \{B, E\} \quad (1)$$

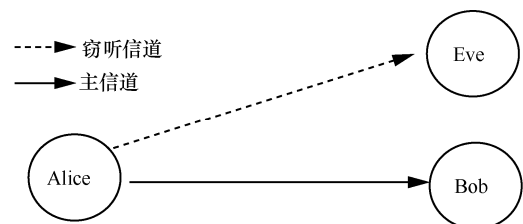


图 1 WCDMA 系统的物理层安全模型

其中, $\delta(\tau)$ 为冲激函数, $x \in \{B, E\}$ 分别表示主信道和窃听信道, L_x 表示主信道或窃听信道的可分离路径数; $\mathbf{h}_x^{(l)} = [\mathbf{h}_{1,l,x}, \mathbf{h}_{2,l,x}, \dots, \mathbf{h}_{N_A,l,x}]$, $\mathbf{h}_{i,l,x}$ 为第 i 根发射天线以时延 τ_l 到达 N_x 根接收天线的信道衰落矢量, 其元素 $h_{i,j,l,x}$ 分别为主信道或窃听信道第 l 条可分离路径上第 i 根发射天线到第 j 根接

收天线之间的信道衰落系数, 衰落幅度 $\gamma_{l,x} = |h_{i,j,l,x}|$ 的概率密度函数 (probability density function, PDF) 服从 Nakagami 分布^[13]:

$$f(\gamma_{l,x}) = \frac{2}{\Gamma(m_l)} (m_l / \Omega_{l,x})^{m_l} \gamma_{l,x}^{2m_l-1} \exp(-m_l / \Omega_{l,x} \gamma_{l,x}^2), \quad l=1, \dots, L_x \quad (2)$$

其中, $\Gamma(\cdot)$ 为伽马函数, m_l 为第 l 条可分离路径上的 Nakagami 衰落系数且 $m_l \geq 1/2$, 当 $m_l = 1$ 时表示瑞利衰落, $\Omega_{l,x}$ 为 Bob 或 Eve 第 l 条可分离路径上的平均功率, 多径强度轮廓 (multipath intensity profile, MIP) 服从指数分布^[13], 即 $\Omega_{l,x} = \Omega_{1,x} e^{-(l-1)\delta_x}$, $\Omega_{1,x}$ 为主信道或窃听信道第一条到达路径的平均信号强度, δ_x 为平均路径衰减系数, $\delta_x = 0$ 时对应恒定 MIP 情形。每个可分离路径上组成的多输入多输出衰落信道的协方差矩阵可表示为 $\mathbf{R}_{H,x} = \mathbf{R}_A \otimes \mathbf{R}_x$, 其中 $\otimes$ 为 Kronecker (克罗内克) 积^[15-16], $\mathbf{R}_A$ 为 Alice 发送天线阵的 $N_A \times N_A$ 维相关矩阵, $\mathbf{R}_x$ 为 Bob 或 Eve 接收天线阵的 $N_x \times N_x$ 维相关矩阵, $\mathbf{R}_{H,x}$ 为 $M_x \times M_x$ 维矩阵, $M_x = N_A \times N_x$, $x \in \{B, E\}$ 。多址干扰近似为加性高斯白噪声 (additive white Gaussian noise, AWGN)^[13]。

当 Alice 采用空时分组码时, N_A 根天线平均分配发射功率, 由参考文献[14]可得主信道或窃听信道 2D-RAKE 接收机的瞬时输出 SINR 为:

$$\gamma_x = \sum_{l=1}^{L_x} \gamma_{l,x} = \frac{1}{N_A} \sum_{l=1}^{L_x} \sum_{i=1}^{N_A} \sum_{j=1}^{N_x} \gamma_{i,j,l}, \quad x \in \{B, E\} \quad (3)$$

其中, $\gamma_{l,x}$ 为 Bob 或 Eve 第 l 条可分离路径上的瞬时输出 SINR, $\gamma_{i,j,l}$ 为 Alice 第 i 根发射天线到第 j 根接收天线间第 l 条可分离路径上的瞬时输出 SINR。由于假定所有可分离路径相互独立, 由参考文献[14]可得合法接收端或窃听者 2D-Rake 接收机瞬时输出 SINR γ_x 的矩生成函数 (moment generating function, MGF) 为:

$$\phi_x(s) = \prod_{l=1}^{L_x} \left(\mathbf{I}_{M_x} + s \frac{\bar{\gamma}_{l,x}}{N_A m_l} \mathbf{R}_{H,x} \right)^{-m_l}, \quad x \in \{B, E\} \quad (4)$$

其中, $\mathbf{I}_{M_x}$ 为 $M_x \times M_x$ 维单位阵, $\bar{\gamma}_{l,x} = (E_s / N_0) \Omega_{l,x}$ 为主信道或窃听信道第 l 条可分离路径上的平均接收 SINR, E_s 为发送符号能量, N_0 表示包括 AWGN 和高斯近似多址干扰的总等效噪声功率谱密度^[13]。

令 $\{\lambda_i\}_{i=1}^{K_x}$ 为协方差矩阵 $\mathbf{R}_{H,x}$ 的 K_x ($K_x \leq M_x$) 个不同特征根, μ_i 为特征根 λ_i 的重数, $\sum_{i=1}^{K_x} \mu_i = M_x$; 记 $\mathbf{A}_x$ 、 $\mathbf{B}_x$ 、 $\mathbf{C}_x$ 、 $\mathbf{P}_x$ 均为 $K_x \times L_x$ 维矩阵, 对应元素为 $a_{ij,x} = m_j$ 、 $b_{ij,x} = \lambda_i$ 、 $c_{ij,x} = \bar{\gamma}_{j,x}$ 、 $p_{ij,x} = \mu_i$, $i=1, \dots, K_x$, $j=1, \dots, L_x$ 。分别对矩阵 $\mathbf{A}_x$ 、 $\mathbf{B}_x$ 、 $\mathbf{C}_x$ 、 $\mathbf{P}_x$ 作 $\text{vec}(\cdot)$ 运算^[17], 即矩阵各列依次竖排得到 $K_x L_x$ 维列向量, 其第 k 个元素分别记为 $a_{k,x}$ 、 $b_{k,x}$ 、 $c_{k,x}$ 、 $p_{k,x}$, $k=1, \dots, K_x L_x$ 。利用特征值分解, 式 (4) 可重写为:

$$\phi_x(s) = \prod_{j=1}^{L_x} \prod_{i=1}^{K_x} \left(1 + s \frac{\bar{\gamma}_{j,x}}{N_A m_j} \lambda_i \right)^{-m_j \mu_i} = \prod_{k=1}^{K_x L_x} (1 + s \eta_{k,x})^{-\pi_{k,x}} \quad (5)$$

其中, $\eta_{k,x} = b_{k,x} c_{k,x} / (N_A a_{k,x})$, $\pi_{k,x} = a_{k,x} p_{k,x}$ 。当所有的 $\pi_{k,x}$ 为正整数时, 对式 (5) 进行部分分式分解^[18], 可推得:

$$\phi_x(s) = \sum_{k,r} \beta_x(k,r) (1 + s \eta_{k,x})^{-r}, \quad x \in \{B, E\} \quad (6)$$

其中, $\sum_{k,r} (\cdot) = \sum_{k=1}^{K_x L_x} \sum_{r=1}^{\pi_{k,x}} (\cdot)$ 。

$$\beta_x(k,r) = \begin{cases} \eta_{k,x}^{r-\pi_{k,x}} \sum_{S_{k,x} \in \mathcal{S}_x} \prod_{u=1, u \neq k}^{K_x L_x} \binom{\pi_{u,x} + n_u - 1}{n_u} \frac{(-\eta_{u,x})^{n_u}}{(1 - \eta_{u,x} / \eta_{k,x})^{\pi_{u,x} + n_u}}, & 1 \leq r < \pi_{k,x} \\ \prod_{u=1, u \neq k}^{K_x L_x} (1 - \eta_{u,x} / \eta_{k,x})^{-\pi_{u,x}}, & r = \pi_{k,x} \end{cases} \quad (7)$$

其中, $\mathcal{S}_x = \{S_{k,x} | \sum_{u=1, u \neq k}^{K_x L_x} n_u = \pi_{k,x} - r\}$ 且 n_u 为非负整数。

对式 (6) 进行反拉普拉斯变换, 可推得主信道



2D-Rake 接收机瞬时输出 SINR 的 PDF 为:

$$f_{\gamma_B}(\gamma_B) = \sum_{k,r} \beta_B(k,r) p(\gamma_B, k, r) \quad (8)$$

其中:

$$p(\gamma_B, k, r) = \frac{\gamma_B^{r-1}}{\Gamma(r) \eta_{k,B}^r} e^{-\gamma_B/\eta_{k,B}} \quad (9)$$

由式 (8) 可推得 γ_B 的累积分布函数 (cumulative distribution function, CDF):

$$F_{\gamma_B}(\gamma) = \sum_{k,r} \frac{\beta_B(k,r)}{\Gamma(r) \eta_{k,B}^r} \int_0^\gamma \gamma_B^{r-1} e^{-\gamma_B/\eta_{k,B}} d\gamma_B \quad (10)$$

参照参考文献[20]中的式 (3.351.1), 可得:

$$\int_0^\gamma \gamma_B^{r-1} e^{-\gamma_B/\eta_{k,B}} d\gamma_B = \frac{\Gamma(r)}{(1/\eta_{k,B})^r} - \exp\left(-\frac{\gamma}{\eta_{k,B}}\right) \sum_{t=0}^{r-1} \frac{\Gamma(r) \gamma^t}{t! (1/\eta_{k,B})^{r-t}} \quad (11)$$

将式 (11) 代入式 (10), 令 $\gamma \rightarrow \infty$, 可得

$$F_{\gamma_B}(\infty) = \sum_{k,r} \beta_B(k,r) = 1。于是有:$$

$$F_{\gamma_B}(\gamma) = 1 - \sum_{k,r} \beta_B(k,r) \sum_{t=0}^{r-1} \frac{\gamma^t}{t! \eta_{k,B}^r} \exp\left(-\frac{\gamma}{\eta_{k,B}}\right) \quad (12)$$

采用与式 (8) ~ 式 (12) 相同的推导过程, 可得窃听信道 2D-Rake 接收机瞬时输出 SINR 的 PDF 和 CDF 的表达式分别为:

$$f_{\gamma_E}(\gamma_E) = \sum_{l,j} \beta_E(l,j) p(\gamma_E, l, j) \quad (13)$$

$$F_{\gamma_E}(\gamma) = 1 - \sum_{l=1}^{K_E L_E} \sum_{j=1}^{\pi_{l,E}} \beta_E(l,j) \sum_{t=0}^{j-1} \frac{\gamma^t}{t! \eta_{l,E}^r} \exp\left(-\frac{\gamma}{\eta_{l,E}}\right) \quad (14)$$

3 安全性能分析指标

3.1 非零安全容量概率

安全容量的表达式为 $C_s = \max\{0, C_B - C_E\}$, 其中 $C_B = \text{lb}(1 + \gamma_B)$ 、 $C_E = \text{lb}(1 + \gamma_E)$ 分别为主信道和窃听信道的容量, $\max\{a, b\}$ 表示取 a 和 b

的最大值。根据参考文献[19], 相关 Nakagami 衰落信道上 WCDMA 系统的非零安全容量概率可写为:

$$\Pr(C_s > 0) = \Pr(\gamma_B > \gamma_E) = \int_0^\infty F_{\gamma_E}(\gamma_B) f_{\gamma_B}(\gamma_B) d\gamma_B \quad (15)$$

其中, $\Pr(C_s > 0)$ 和 $\Pr(\gamma_B > \gamma_E)$ 分别表示 $C_s > 0$ 和 $\gamma_B > \gamma_E$ 时的概率。

$$\text{令 } \beta_{BE} = \beta_B(k,r) \beta_E(l,j), \quad \sum_{l,j,k,r} (\cdot) = \sum_{l=1}^{K_E L_E} \sum_{j=1}^{\pi_{l,E}}$$

$\sum_{k=1}^{K_B L_B} \sum_{r=1}^{\pi_{k,B}} (\cdot)$, $\varepsilon = 1/\eta_{l,E} + 1/\eta_{k,B}$, 将式 (8) γ_B 的 PDF

和式 (14) γ_E 的 CDF 代入式 (15), 可得:

$$\Pr(C_s > 0) = 1 - \sum_{l,j,k,r} \sum_{t=0}^{j-1} \frac{\beta_{BE}}{t! \eta_{l,E}^r \Gamma(r) \eta_{k,B}^r} \int_0^\infty \gamma_B^{t+r-1} \exp(-\varepsilon \gamma_B) d\gamma_B \quad (16)$$

利用参考文献[20]中的式 (3.326.2), 可得:

$$\int_0^\infty \gamma_B^{t+r-1} \exp(-\varepsilon \gamma_B) d\gamma_B = \Gamma(r+t) / \varepsilon^{r+t} \quad (17)$$

经过化简整理, 可推得相关 Nakagami 衰落信道上 WCDMA 系统非零安全容量概率的表达式为:

$$\Pr(C_s > 0) = 1 - \sum_{l,j,k,r} \sum_{t=0}^{j-1} \frac{\beta_{BE}}{t! \eta_{l,E}^r \Gamma(r) \eta_{k,B}^r} \frac{\Gamma(r+t)}{\varepsilon^{r+t}} \quad (18)$$

3.2 安全中断概率

假定 WCDMA 系统的目标安全速率为 R_s , 由参考文献 [19] 可得其安全中断概率 $P_{\text{out}}(R_s) = \Pr(C_s < R_s)$ 的计算包含以下两种情况: 当主信道质量比窃听信道质量好时, 安全容量 $C_s > 0$ 且小于目标安全速率 R_s 的概率 $\Pr(C_s < R_s | \gamma_B > \gamma_E)$; 当主信道质量比窃听信道质量差时, 安全容量 C_s 为 0 且小于目标安全速率 R_s 的概率 $\Pr(C_s < R_s | \gamma_B < \gamma_E)$ 。因此, 相关 Nakagami 衰落信道上 WCDMA 系统的安全中断概率为:

$$P_{\text{out}}(R_s) = \int_0^\infty \int_{\gamma_E}^{\gamma_w} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E + \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E \quad (19)$$

$$= \int_0^\infty F_{\gamma_B} \left((2^{R_s} - 1) + 2^{R_s} \gamma_E \right) f_{\gamma_E}(\gamma_E) d\gamma_E$$

将式(13) γ_E 的 PDF 和式(12) γ_B 的 CDF 代入式(19), 经化简整理可得:

$$P_{\text{out}}(R_s) = 1 - \sum_{l,j,k,r} \sum_{t=0}^{r-1} \frac{\beta_{BE}}{t! \eta_{k,B}^t \Gamma(j) \eta_{l,E}^j} \int_0^\infty \left[(2^{R_s} - 1) + 2^{R_s} \gamma_E \right]^t \gamma_E^{j-1} \exp\left(-\frac{2^{R_s} - 1}{\eta_{k,B}}\right) \exp(-\xi \gamma_E) d\gamma_E \quad (20)$$

其中, $\xi = 2^{R_s}/\eta_{k,B} + 1/\eta_{l,E}$ 。令:

$$S(\eta_{k,B}, \eta_{l,E}, j) = \exp\left(-\frac{2^{R_s} - 1}{\eta_{k,B}}\right) \cdot \int_0^\infty \left[(2^{R_s} - 1) + 2^{R_s} \gamma_E \right]^t \gamma_E^{j-1} \exp(-\xi \gamma_E) d\gamma_E \quad (21)$$

利用二项式展开定理及式(17), 可推得:

$$S(\eta_{k,B}, \eta_{l,E}, j) = \exp\left(-\frac{2^{R_s} - 1}{\eta_{k,B}}\right) \sum_{v=0}^t \binom{t}{v} (2^{R_s} - 1)^{t-v} 2^{R_s v} \int_0^\infty \gamma_E^{v+j-1} \exp(-\xi \gamma_E) d\gamma_E$$

$$= \exp\left(-\frac{2^{R_s} - 1}{\eta_{k,B}}\right) \sum_{v=0}^t \binom{t}{v} (2^{R_s} - 1)^{t-v} 2^{R_s v} \cdot \Gamma(j+v)/\xi^{j+v} \quad (22)$$

将式(22)代入式(20), 经化简整理可得, 相关 Nakagami 衰落信道上 WCDMA 系统的安全中断概率为:

$$P_{\text{out}}(R_s) = 1 - \sum_{l,j,k,r} \sum_{t=0}^{r-1} \frac{\beta_{BE} S(\eta_{k,B}, \eta_{l,E}, j)}{t! \eta_{k,B}^t \Gamma(j) \eta_{l,E}^j} \quad (23)$$

当主信道和窃听信道的收、发天线阵均相互独立时, 此时 $\mathbf{R}_A$ 、 $\mathbf{R}_B$ 和 $\mathbf{R}_E$ 均退化为单位阵, $\mathbf{R}_{H,x}$ 的特征根全为 1, 即 $K_x = 1$ 、特征根重数为 M_x , 此时有 $\eta_{k,x} = c_{k,x}/(N_A a_{k,x})$ 、 $\pi_{k,x} = a_{k,x} M_x$, 则主信道或窃听信道 2D-Rake 接收机瞬时输出 SINR 的 PDF 为:

$$f_{\gamma_x}(\gamma_x) = \sum_{k=1}^{L_x} \sum_{r=1}^{\pi_{k,x}} \frac{\beta_x(k, r)}{\Gamma(r)} \frac{\gamma_x^{r-1}}{\eta_{k,x}^r} e^{-\gamma_x/\eta_{k,x}}, \quad x \in \{B, E\} \quad (24)$$

主信道和窃听信道均为独立 Nakagami 衰落信道时, 可推得 WCDMA 系统的非零安全容量概率和安全中断概率的表达式分别为:

$$\Pr(C_s > 0) = 1 - \sum_{l=1}^{L_E} \sum_{j=1}^{\pi_{l,E}} \sum_{k=1}^{L_B} \sum_{r=1}^{\pi_{k,B}} \sum_{t=0}^{j-1} \frac{\beta_{BE}}{t! \eta_{l,E}^t \Gamma(r) \eta_{k,B}^r} \frac{\Gamma(r+t)}{\varepsilon^{r+t}} \quad (25)$$

$$P_{\text{out}}(R_s) = 1 - \sum_{l=1}^{L_E} \sum_{j=1}^{\pi_{l,E}} \sum_{k=1}^{L_B} \sum_{r=1}^{\pi_{k,B}} \sum_{t=0}^{j-1} \frac{\beta_{BE} S(\eta_{k,B}, \eta_{l,E}, j)}{t! \eta_{k,B}^t \Gamma(j) \eta_{l,E}^j} \quad (26)$$

3.3 渐近安全中断概率

虽然可以利用非零安全容量概率和安全中断概率对 WCDMA 系统的安全性能进行评估, 但其表达式过于复杂且不能直观地反映收发天线数、天线相关系数、Nakagami 衰落系数等参数对 WCDMA 安全性能的影响, 为此, 下面研究高 SINR 下的渐近安全中断性能, 明确上述参数对 WCDMA 系统安全分集增益的影响。

当 $c_{k,B} = \bar{\gamma}_{k,B} \rightarrow \infty, k=1, \dots, K_B L_B$ 时, 有 $\bar{\gamma}_B \rightarrow \infty$ 。将式(12) γ_B 的 CDF 中的 $\exp(-\gamma/\eta_{k,B})$ 项进行麦克劳林级数展开, 经化简整理, 可推得相关 Nakagami 衰落信道上 WCDMA 系统主信道瞬时输出 SINR 的 CDF 的渐近表达式为:

$$F_{\gamma_B}^\infty(\gamma) = 1 - \sum_{k=1}^{K_B L_B} \sum_{r=1}^{\pi_{k,B}} \beta_B(k, r) \sum_{t=0}^{r-1} \frac{\gamma^t}{t! \eta_{k,B}^t} \sum_{n=0}^\infty \frac{(-1)^n}{n!} \left(\frac{\gamma}{\eta_{k,B}} \right)^n$$

$$= \sum_{k,r} D(k, r) (\gamma/\bar{\gamma}_{k,B})^{G_d} + o\left((\gamma/\bar{\gamma}_{k,B})^{G_d}\right) \quad (27)$$

其中, $o(\cdot)$ 表示高阶无穷小量, $G_d = \sum_{l=1}^{L_B} m_l N_A N_B$ 。

$$D(k, r) = \beta_B(k, r) \sum_{t=0}^{r-1} \binom{G_d}{t} \frac{(-1)^{G_d-t+1}}{G_d!} \left(\frac{N_A a_{k,B}}{b_{k,B}} \right)^{G_d} \quad (28)$$

将式(13) γ_E 的 PDF 和式(27)代入式(19), 可推得 WCDMA 系统渐近安全中断概率的表达式



式为:

$$P_{\text{out}}^{\infty}(R_s) = (G_a \bar{\gamma}_{k,B})^{-G_d} + o(\bar{\gamma}_{k,B}^{-G_d}) \quad (29)$$

其中, G_a 表示系统的安全阵列增益, 其表达式为:

$$G_a = \left\{ \sum_{k,r} D(k,r) \sum_{v=0}^{G_d} \binom{G_d}{v} (2^{R_s} - 1)^{G_d-v} \cdot 2^{R_s v} \sum_{l=1}^{K_E} \sum_{j=1}^{L_E} \frac{\beta_E(l,j) \eta_{l,E}^v \Gamma(d+j)}{\Gamma(j)} \right\}^{-1/G_d} \quad (30)$$

由式 (29) 可知: WCDMA 系统的安全分集增益为 G_d , 反映了安全中断概率曲线随 SINR 变化的斜率; 相关 Nakagami 衰落信道上 WCDMA 系统的安全分集增益完全由主信道决定, 且等于各可分离路径分集增益 $m_l N_A N_B$ 之和, 但与窃听信道的可分离路径数、天线数、Nakagami 衰落系数等参数无关; 当主信道各可分离支路的 Nakagami 衰落参数相等时, 即 $m_1 = m_2 = \dots = m_{L_B} = m$ 且 $\delta_B = 0$ 时, WCDMA 系统的安全分集增益 $G_d = L m N_A N_B$ 。

4 数值计算与仿真

$$\text{令 } \bar{\gamma}_B = (E_s/N_0) \sum_{l=1}^{L_B} \Omega_{l,B} \text{ 和 } \bar{\gamma}_E = (E_s/N_0) \sum_{l=1}^{L_E} \Omega_{l,E}$$

分别表示主信道和窃听信道的一维瑞克接收机的平均 SINR。利用 MATLAB 软件对相关 Nakagami 衰落信道上 WCDMA 系统的安全性能进行数值计算和计算机仿真, 研究收/发天线数、Nakagami 衰落系数、天线相关系数以及平均路径衰减系数 δ 对系统安全性能的影响, 结果如图 2~图 6 所示。为不失一般性, 仿真参数设置为: 主信道和窃听信道的可分离路径数均为 $L_B = L_E = L = 4$, 天线数 $N_A = N_B = N_E = 2$, $\bar{\gamma}_E = 5 \text{ dB}$, $R_s = 1 \text{ bit/(s}\cdot\text{Hz)}$; Alice、Bob、Eve 上天线阵的相关矩阵分别为 $\mathbf{R}_A = [1 \ \rho_A; \rho_A \ 1]$ 、 $\mathbf{R}_B = [1 \ \rho_B; \rho_B \ 1]$ 、 $\mathbf{R}_E = [1 \ \rho_E; \rho_E \ 1]$, 其中 $\rho_A = 0$, $\rho_B = 0$, $\rho_E = 0$ 分别表示相应的天线阵相互独立; 主信道和窃听信道经历相同的 Nakagami 衰落, L 条可分离路径上的 Nakagami

衰落参数矢量均用 $\mathbf{m}_B = \mathbf{m}_E = \mathbf{m} = [m_1, m_2, \dots, m_L]$ 来表示, $\mathbf{m}_a = [1, 1, 1, 1]$, $\mathbf{m}_2 = [2, 2, 2, 2]$ 。

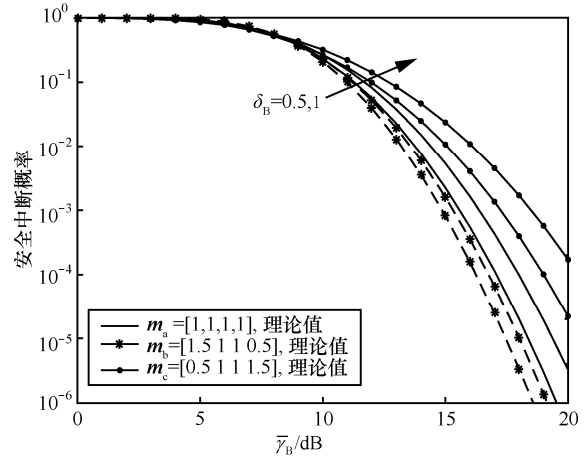


图 2 $\mathbf{m}$ 和 δ_B 对安全中断概率的影响

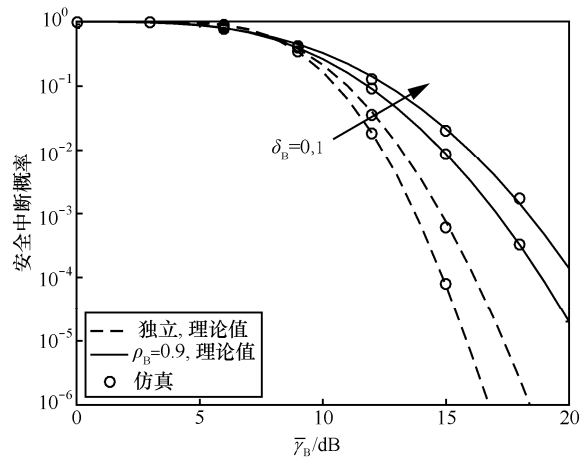


图 3 ρ_B 和 δ_B 对安全中断概率的影响

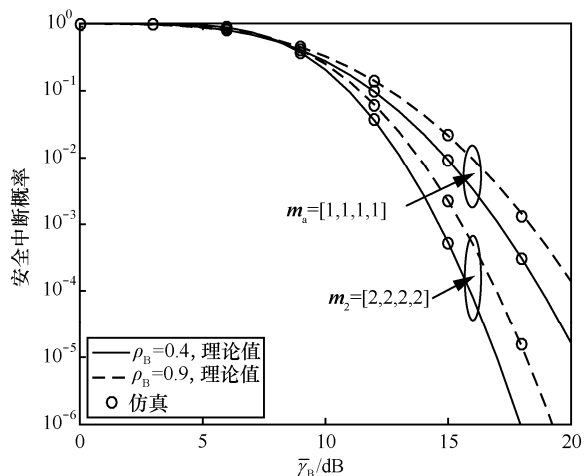


图 4 ρ_B 和 $\mathbf{m}$ 对安全中断概率的影响

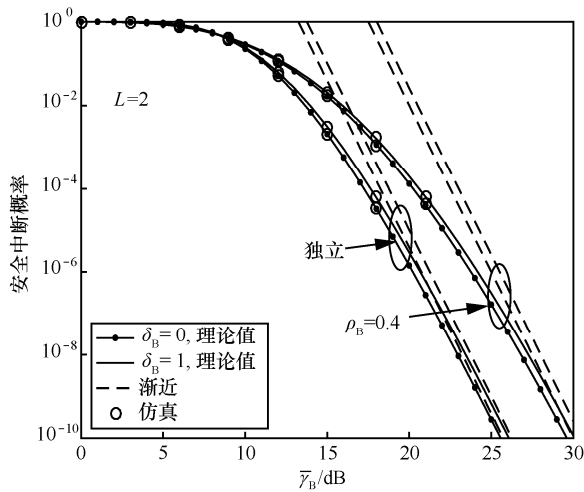
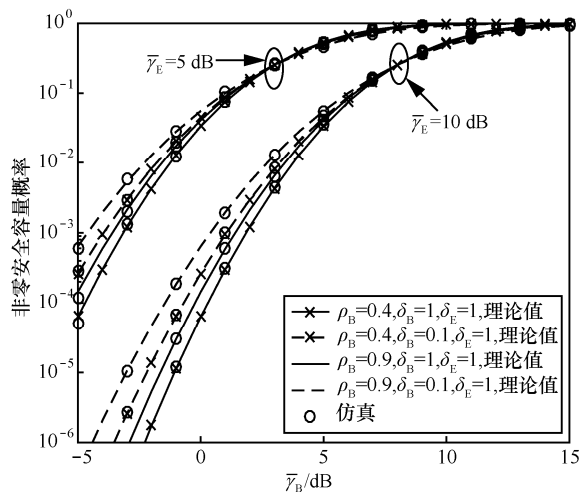
图5 不同 δ_B 对安全中断概率的影响图6 不同 $\gamma_{\bar{E}}$ 对非零安全容量概率的影响

图2给出了不同 m 和 δ 对 WCDMA 系统安全中断概率的影响, 其中 $\rho_A = 0$, $\rho_B = \rho_E = 0.8$, m_a 、 $m_b = [1.5, 1, 1, 0.5]$ 、 $m_c = [0.5, 1, 1, 1.5]$ 衰落系数矢量的均值均为 1, 窃听信道的平均路径衰减系数为 $\delta_E = 1$ 。由图 2 可知: 当衰落系数矢量 m 一定时, 主信道的 δ_B 越小, 系统的安全中断性能越好, 这是由于 δ_B 表征衰落信道的频率选择性, 且 δ_B 越小, 主信道的一维瑞克接收机的 SINR 越大, 系统所获得的安全性能越高; δ_B 一定时, m_b 安全性能最好, m_a 次之, m_c 性能最差, 如当安全中断概率为 10^{-3} 、 $\delta_B = 1$ 时, m_b 比 m_a 、 m_c 所对应的安全中断概率曲线约有 1.1 dB 和 3.1 dB

的 SINR 增益。

图 3 给出了不同 ρ_B 和 δ_B 下相关 Nakagami 衰落信道上 WCDMA 系统的安全中断概率性能曲线, 其中 Nakagami 衰落系数矢量为 m_a , $\delta_E = 1$, $\rho_A = 0.8$, $\rho_B = 0.9$, $\rho_E = 0.6$, 而 $\rho_A = \rho_B = \rho_E = 0$ 表示独立情形。由图 3 可知: Bob 天线阵相关性恶化了 WCDMA 系统的安全性能。如安全中断概率为 10^{-3} 、 $\delta_B = 0$ 、 $\rho_B = 0.9$ 时, 其相对于独立同分布 Nakagami 衰落信道时所对应的安全中断概率曲线, 安全性能恶化了 3.4 dB; $\delta_B = 1$ 、 $\rho_B = 0.9$ 时, 其相对于独立同分布 Nakagami 衰落信道时所对应的安全中断概率曲线, 安全性能恶化了 3.5 dB; 当合法接收端和窃听者天线阵的相关系数一定时, δ_B 越小, 安全中断概率越小, 系统的安全性能越好, 这是由于到达各个可分离路径上的平均功率 Ω 越大, γ_B 越高, WCDMA 系统所获得的安全中断性能越好。如安全中断概率在 10^{-3} 且收发天线阵均独立时, $\delta_B = 0$ 比 $\delta_B = 1$ 所对应的曲线约有 0.8 dB 的 SINR 增益, 而在 $\rho_B = 0.9$ 时, 上述 SINR 增益为 0.9 dB。

图 4 给出了不同 ρ_B 和 m 下 WCDMA 系统安全中断概率的性能曲线, 其中 $\delta_B = \delta_E = 1$, $\rho_A = 0.8$, $\rho_E = 0.6$ 。由图 4 可知: 当衰落系数矢量一定时, 合法接收端 Bob 天线相关性恶化了 WCDMA 系统的安全中断性能。如当安全中断概率为 10^{-3} 、 $m = m_a$ 时, $\rho_B = 0.9$ 相对于 $\rho_B = 0.4$ 的安全中断性能恶化 1.3 dB; 当 $m = m_2$ 时, $\rho_B = 0.9$ 相对于 $\rho_B = 0.4$ 的安全中断性能恶化了 0.9 dB; 在天线相关系数 ρ_B 和平均路径衰减系数 δ_B 给定的前提下, Nakagami 衰落系数矢量越大, WCDMA 系统可以获得的安全中断性能越好, 这是由于 Nakagami 衰落系数越大, 信道质量越好; 同时 m 的增大也使得系统的安全分集增益增加, 以此来带来安全性能的提高。如安全中断概率为 10^{-3} 、 $\rho_B = 0.4$ 时, $m = m_2$ 对应的安全中断概率相对于



$m = m_a$ 时有 2.4 dB 的 SINR 增益；而 $\rho_B = 0.9$ 时上述 SINR 增益为 2.9 dB。

图 5 给出了不同 δ_B 对 WCDMA 系统安全中断性能的影响，并与其渐近安全中断概率进行对比，其中 $L=2$ ，所对应的各可分离路径上的衰落系数均为 1， $\rho_A = 0.8$ ， $\rho_B = 0.4$ ， $\rho_E = 0.6$ ， $\delta_E = 1$ 。由图 5 可知：SINR 一定时，利用式 (23)、式 (26) 得到的相关和独立情形下 WCDMA 系统的安全中断概率精确理论值与其对应的仿真值相吻合，从而证明了理论分析的正确性；在高 SINR 下，相关和独立情形下 WCDMA 系统的渐近结果与其精确理论结果非常接近，从而验证了渐近分析的准确性；从渐近线的斜率可以看出， δ_B 增加或减小时并不影响系统安全分集增益。

图 6 给出了窃听者接收 SINR 对 WCDMA 非零安全容量概率的影响，其中 $\rho_A = 0.8$ ， $\rho_E = 0.6$ ，衰落系数矢量为 m_a 。由图 6 可知：即使当窃听信道质量好于主信道时，即 $\bar{\gamma}_B < \bar{\gamma}_E$ ，依然存在 $\Pr(C_s > 0)$ ，且 $\Pr(C_s > 0)$ 随着 $\bar{\gamma}_B$ 的增大而增大； $\bar{\gamma}_E = 5$ dB 的安全性能明显优于 $\bar{\gamma}_E = 10$ dB，这是由于 $\bar{\gamma}_E$ 的增加使得窃听者获取信息的能力增强，造成非零安全容量概率的减小；与 $\bar{\gamma}_E$ 相比，当 $\bar{\gamma}_B$ 在小 SINR 时，如 $\bar{\gamma}_B < 2$ dB，非零安全容量概率随着 ρ_B 的增加而增加，这是由于在小 SINR 情况下，天线相关性降低了 Bob 的有效接收维数，从而使其接收的能量更加集中；当 $\bar{\gamma}_B$ 在中高 SINR 下，非零安全容量概率随着 ρ_B 的增加而减小，这是由于在中高 SINR 下，天线相关系数 ρ_B 的增加将对信道质量造成一定程度的恶化，因此导致非零安全容量概率的降低。

5 结束语

推导了相关 Nakagami 衰落信道上 WCDMA 系统的非零安全容量概率、安全中断概率的精确

解析表达式。数值计算结果和仿真结果相吻合，证明了上述理论分析的正确性。通过研究不同参数下 WCDMA 系统的安全性能，可得如下结果：主信道的 Nakagami 衰落系数愈大时，WCDMA 系统的安全分集增益愈大，从而系统获得的安全性愈好；与 $\bar{\gamma}_E$ 相比，当 $\bar{\gamma}_B$ 在中高 SINR 下，Bob 天线阵的相关系数增大时，将使主信道质量恶化，降低了 WCDMA 系统的安全性；相反地，在小 SINR 下，Bob 天线阵的相关系数增大将在一定程度上有助于 WCDMA 系统安全性能的提升；主信道平均路径衰减系数 δ_B 愈小时，WCDMA 系统的安全性愈好；通过对渐近安全中断概率的分析可知，系统的安全分集增益为 $\sum_{l=1}^{L_B} m_l N_A N_B$ ，且该安全分集增益与窃听信道的可分离路径数、窃听者天线数以及 Nakagami 衰落系数等参数无关。上述理论分析可以为相关 Nakagami 衰落信道上 WCDMA 系统安全性能的快速评估提供有力的理论分析工具。莱斯或 $\eta - \mu$ 衰落信道上 WCDMA 系统的物理层安全性能还有待进一步研究。

参考文献：

- [1] 韩帅, 台祥雪, 孟维晓. 空天地通信网络的物理层安全系统模型与关键技术[J]. 电信科学, 2018, 34(3): 23-31.
HAN S, TAI X X, MENG W X. Physical layer security for the air-space-ground communications networks[J]. Telecommunications Science, 2018, 34(3): 23-31.
- [2] 龙航, 袁广翔, 王静, 等. 物理层安全技术研究现状与展望[J]. 电信科学, 2011, 27(9): 60-65.
LONG H, YUAN G X, WANG J, et al. Physical layer security: survey and future[J]. Telecommunications Science, 2011, 27(9): 60-65.
- [3] TAN Y, PU T, XIANG P. Secrecy capacities of optical CDMA communication systems based on gold codes[C]//IEEE International Conference on Optical Communications and Networks, Sept 24-27, 2016, Hangzhou, China. Piscataway: IEEE Press, 2016: 1-3.
- [4] JI J, ZHANG G, LI W, et al. Performance analysis of physical-layer security in an OCDMA-based wiretap channel[J]. IEEE/OSA Journal of Optical Communications & Networking, 2017, 9(10): 813-818.

- [5] TI G, LI M, TIAN X, et al. Physical layer secure binary signature design for wiretap CDMA systems[C]//IEEE International Conference on Wireless Communications and Signal Processing, Oct 11-13, 2017, Nanjing, China. Piscataway: IEEE Press, 2017.
- [6] LI M, TI G, TIAN X, et al. QoS-based binary signature design for secure CDMA systems[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 1011-1023.
- [7] SONG T, ZHOU K, LI T. CDMA system design and capacity analysis under disguised jamming[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(11): 2487-2498.
- [8] SHOJAEZAND T, AZMI P, YADEGARI A M. Performance analysis of a LDPC coded CDMA system with physical layer security enhancement[C]//IEEE International Conference on Wireless Communication Network and Mobile Computing, Sept 23-25, 2010, Chengdu, China. Piscataway: IEEE Press, 2010: 1-4.
- [9] LI M, BATALAMA S N, PADOS D A, et al. Cognitive code-division links with blind primary-system identification[J]. IEEE Transactions on Wireless Communications, 2010, 10(11): 3743-3753.
- [10] 沈雷, 赵知劲. 多径信道中基于盲波束成形的 CDMA 多用户检测和伪码估计[J]. 信号处理, 2010, 26(11): 1730-1735.
SHEN L, ZHAO Z J. Multi-user detection and chip sequence estimation of multi-path CDMA signal based on blind beamforming[J]. Signal Processing, 2010, 26(11): 1730-1735.
- [11] 张平. WCDMA 移动通信系统(第 2 版)[M]. 北京: 人民邮电出版社, 2004.
ZHANG P. WCDMA mobile communication systems (2nd edition) [M]. Beijing: Posts & Telecom Press, 2004.
- [12] 蒋涉权, 王晶, 彭超. MIMO 系统中空时编码性能仿真和分析[J]. 电信科学, 2015, 31(2): 35-41, 51.
JIANG S Q, WANG J, PENG C. Simulation and analysis on performance of space-time coding in MIMO systems[J]. Telecommunications Science, 2015, 31(2): 35-41, 51.
- [13] LUO J, ZEIDLER J R, PROAKIS J G. Error probability performance for WCDMA systems with multiple transmit and receive antennas in correlated Nakagami fading channels[J]. IEEE Transactions on Vehicular Technology, 2002, 51(6): 1502-1516.
- [14] 李光球, 江虹. 相关 MIMO Nakagami 衰落信道上 MQAM WCDMA 系统的性能分析[J]. 电路与系统学报, 2009, 14(2): 12-17.
LI G Q, JIANG H. Performance analysis of MQAM WCDMA systems in correlated MIMO Nakagami fading channels[J]. Journal of Circuits and Systems, 2009, 14(2): 12-17.
- [15] SHIU D S, FOSCHINI G J, GANS M J, et al. Fading correlation and its effect on the capacity of multi-element antenna systems[J]. IEEE Transactions on Communications, 2002, 48(3): 502-513.
- [16] MUSAVIAN L, DOHLER M, NAKHAI M R, et al. Closed-form capacity expressions of orthogonalized correlated MIMO channels[J]. IEEE Communications Letters, 2004, 8(6): 365-367.
- [17] 张跃辉. 矩阵理论与应用[M]. 北京: 科学出版社, 2011.
ZHANG Y H. Matrix theory and applications[M]. Beijing: Science Press, 2011.
- [18] YU H, WEI G, JI F, et al. On the error probability of cross-QAM with MRC reception over generalized fading channels[J]. IEEE Transactions on Vehicular Technology, 2011, 60(6): 2631-2643.
- [19] BLOCH M, BARROS J, RODRIGUES M R D. Wireless information-theoretic security[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2515-2534.
- [20] GRADSHTEYN I S, RYZHIK I M. Table of integrals, series and products[M]. Pittsburgh: Academic Press, 2007.

[作者简介]



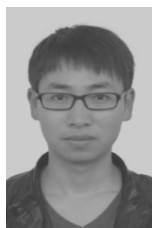
李光球 (1966-), 男, 博士, 杭州电子科技大学教授, 主要研究方向为无线通信、信息论与编码, 已主持完成 3 项国家自然科学基金项目和 3 项省部级基金项目, 发表学术论文 100 余篇。



王占湾 (1992-), 男, 杭州电子科技大学硕士生, 主要研究方向为无线通信。



任婷洁 (1994-), 女, 杭州电子科技大学硕士生, 主要研究方向为无线通信。



刘帅帅 (1994-), 男, 杭州电子科技大学硕士生, 主要研究方向为无线通信。