



信道预测天线选择的空时分组码物理层安全增强

钱 辉, 李光球, 汪玲波, 蔡建辉

(杭州电子科技大学 通信工程学院, 杭州 310018)

摘 要: 针对延时发射天线选择(TASD)/正交空时分组码(OSTBC)无线通信系统, 基于最小均方误差(MMSE)信道预测器, 提出一种系统物理层安全增强方案。将 MMSE 信道预测方案应用于 TASD/OSTBC 无线通信系统, 构成信道预测发射天线选择(TASP)/OSTBC 无线通信系统, 并对其推导瑞利块衰落信道上安全中断概率、非零安全容量概率以及渐近安全中断概率的解析表达式。在此基础上, 分析主信道收发天线数、窃听者天线数和信道的归一化延时等参数对系统物理层安全性能的影响。数值计算和仿真结果表明, 采用 TASP 可以提高 OSTBC 编码无线通信系统的物理层安全性能。

关键词: 物理层安全; 信道预测; 发射天线选择; 正交空时分组码; 安全中断概率

开放科学(资源服务)标志码(OSID):



中文引用格式: 钱辉, 李光球, 汪玲波, 等. 信道预测天线选择的空时分组码物理层安全增强[J]. 计算机工程, 2020, 46(2): 141-147, 153.

英文引用格式: QIAN Hui, LI Guangqiu, WANG Lingbo, et al. Physical layer security enhancement of space-time block code using channel prediction for antenna selection[J]. Computer Engineering, 2020, 46(2): 141-147, 153.

Physical Layer Security Enhancement of Space-Time Block Code Using Channel Prediction for Antenna Selection

QIAN Hui, LI Guangqiu, WANG Lingbo, CAI Jianhui

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

[Abstract] Aiming at Transmit Antenna Selection with Delay (TASD)/Orthogonal Space-Time Block Code (OSTBC) wireless communication system, this paper proposes a system physical layer security enhancement scheme based on the Minimum Mean Square Error (MMSE) channel predictor. The MMSE channel prediction scheme is applied to the TASD/OSTBC wireless communication system to form a channel Transmit Antenna Selection with Prediction (TASP)/OSTBC wireless communication system. The analytical expressions of secrecy outage probability, non-zero secrecy capacity probability and asymptotic secrecy outage probability over the Rayleigh block fading channel are derived. On this basis, the effects of parameters such as the number of transmit and receive antennas on the main channel, the number of eavesdropper antennas, and the normalized delay of the channel on the security performance of the system physical layer are analyzed. Numerical calculations and simulation results show that using TASP can improve the physical layer security performance of OSTBC wireless communication system.

[Key words] physical layer security; channel prediction; Transmit Antenna Selection (TAS); Orthogonal Space-Time Block Code (OSTBC); secrecy outage probability

DOI: 10.19678/j.issn.1000-3428.0053779

0 概述

在衰落信道上的被动窃听场景下, 多输入多输出 (Multiple-Input Multiple-Output, MIMO) 无线通信系统的物理层安全受到广泛关注^[1]。常用的三节点

被动窃听信道模型包括发射端 (Alice)、合法接收端 (Bob) 和窃听者 (Eve), 针对三者采用不同技术的情形, 研究人员分别研究了无线通信系统的物理层安全。

文献[2]研究瑞利衰落信道上 Alice 采用发射天

基金项目: 浙江省自然科学基金 (LY12F01008)。

作者简介: 钱 辉 (1994—), 男, 硕士研究生, 主研方向为无线通信安全; 李光球 (通信作者), 教授、博士; 汪玲波、蔡建辉, 硕士研究生。

收稿日期: 2019-01-22 **修回日期:** 2019-03-13 **E-mail:** gqli@hdu.edu.cn

线选择 (Transmit Antenna Selection, TAS) 在多天线 Eve 场景下的物理层安全问题。文献 [3] 比较 Nakagami 衰落信道上 Alice 采用 TAS、Bob 和 Eve 分别采用最大比合并 (Maximal Ratio Combining, MRC) 或选择合并 (Selection Combining, SC) 分集接收 4 种组合情形下的物理层安全性能。文献 [4] 推导相关衰落信道上 Alice 采用正交空时分组码 (Orthogonal Space-Time Block Code, OSTBC) 编码无线通信系统的安全中断概率和渐近安全中断概率的解析表达式。文献 [5] 研究 Nakagami 衰落信道上 Alice 采用 TAS、Bob 采用人工噪声方案的多入单出无线通信系统的物理层安全性能。文献 [6] 提出发射端多天线选择方案来保障 MIMO 无线通信系统的物理层安全传输。文献 [7] 推导瑞利衰落信道上 Alice 采用组合 TAS 和 Alamouti 码的方案、Bob 和 Eve 采用 MRC 分集接收无线通信系统的安全中断概率和非零安全容量概率的解析表达式。文献 [8] 研究人工噪声辅助 OSTBC 编码的多用户多入单出中继网络的物理层安全问题。

文献 [2-8] 均假定 Alice 可以获得理想的主信道状态信息 (Channel State Information, CSI), 然而在实际情况由于反馈链路存在延时, 使得 Alice 使用过期的 CSI 进行 TAS, 严重降低了无线通信系统的物理层安全性能。文献 [9-10] 分别研究了瑞利和 Nakagami 衰落信道上 Eve 采用 MRC 分集接收、主信道采用反馈延时发射天线选择 (TAS with Feedback Delay, TASD)/MRC 分集接收无线通信系统的物理层安全性能, 其渐近分析结果均表明反馈延时使得系统只能获得 Bob 的接收分集增益, 无法获得发射天线增益。文献 [11] 推导了瑞利衰落信道上接收端天线相关场景下, Eve 采用 MRC 分集接收、主信道采用 TASD/MRC 分集接收无线通信系统的安全中断概率和非零安全容量概率。文献 [12-13] 研究 Nakagami 衰落信道上中继协作系统在过期 CSI 下的物理层安全性能, 推导了遍历安全容量和安全中断概率的表达式, 理论分析结果表明, 过期 CSI 会降低中继协作系统的物理层安全性能。

上述研究仅分析了过期 CSI 下的无线通信系统物理层安全性能, 未提出提高其安全性能的解决方案。最小均方误差 (Minimal Mean Square Error, MMSE) 信道预测器可以减小反馈延时对无线通信系统误码性能的影响^[14-15], 文献 [16] 将其应用于 TAS/MRC 无线通信系统, 改善系统在多窃听场景下的物理层安全性能。受此启发, 本文将 MMSE 信道预测方案应用于 TAS/OSTBC 无线通信系统, 以改善其在过期 CSI 下的物理层安全性能。

1 系统模型

1.1 系统描述

本文研究对象为时间选择性瑞利衰落信道上采用组合信道预测发射天线选择 (TAS with Prediction, TASP) 和 OSTBC 的 MIMO 无线通信系统, 其信道增益服从同一分布并且互相独立。如图 1 所示, 在此系统中, 三节点被动窃听模型由 Alice、Bob 和 Eve 组成, 其分别配有 N_A 、 N_B 、 N_E 根天线, Alice 采用 TAS/OSTBC 编码发送安全信息符号, Bob 和 Eve 均采用 MRC 分集接收。Alice 与 Bob 之间的信道通过导频信号辅助调制技术和 MMSE 维纳信道预测器来获得主信道的 CSI。由于是被动窃听攻击, 因此 Alice 无法获得窃听信道的 CSI。

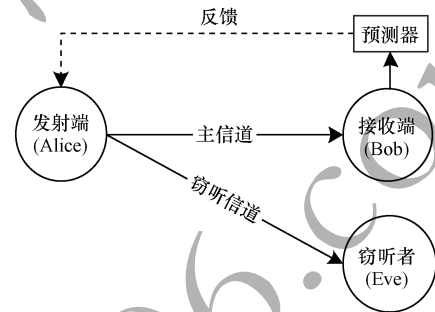


图 1 TASP/OSTBC 无线通信系统的物理层安全模型

Fig. 1 Physical layer security model of TASP/OSTBC wireless communication system

1.2 信道模型

主信道和窃听信道增益均按块变化 (块长为 L_b), 主信道第 α 个衰落块的信道矩阵为 $\mathbf{H}_{AB}(\alpha) \in \mathbb{C}^{N_B \times N_A}$, 其元素 $h_{jm}(\alpha)$ 表示第 m 根发射天线与第 j 根接收天线之间的信道增益, 服从均值为 0、方差为 1 的复高斯分布, 记为 $h_{jm}(\alpha) \sim CN(0, 1)$ 。

主信道采用 Jakes 信道模型^[14], 信道增益之间的相关系数满足:

$$E[h_{jm}(\alpha)h_{jm}^*(\alpha - \tau)] = J_0(2\pi f_d \tau)$$

其中, $E[\cdot]$ 表示求期望, $h_{jm}^*(\alpha - \tau)$ 是 $h_{jm}(\alpha - \tau)$ 的复共轭, $J_0(\cdot)$ 为第一类零阶贝塞尔函数, f_d 为多普勒频移, $\tau = DL_b T_s$ 为反馈延时, D 为延时衰落块数, T_s 为发送的安全信息符号周期。

窃听信道第 α 个衰落块的信道矩阵为 $\mathbf{H}_{AE}(\alpha) \in \mathbb{C}^{N_E \times N_A}$, 其中, N_T 是选择天线数。

Bob 和 Eve 的每根接收天线上的加性白高斯噪声 (Additive White Gaussian Noise, AWGN) 相互独立, 均服从 $CN(0, N_0)$ 。

1.3 信道预测

Alice 采用如图 2 所示的传输帧结构, 每帧帧长均为 L_b 个符号, 每帧的前 N_A 个符号周期内发送正交导频序列, 用于 Bob 对主信道进行信道估计和预测。

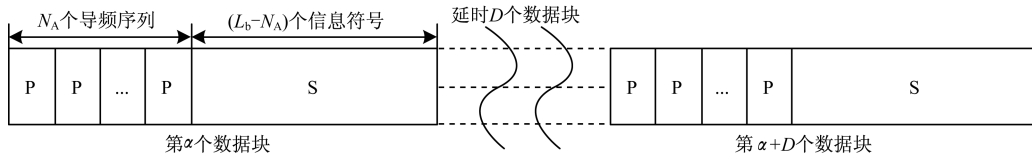


图2 TASP/OSTBC无线通信系统的安全传输帧结构

Fig. 2 Secure transmission frame structure of TASP/OSTBC wireless communication system

采用 K 阶 MMSE 维纳信道预测器, Bob 可得第 $\alpha + D$ 块的预测主信道系数为:

$$\hat{h}_{jm}(\alpha + D) = \mathbf{w}_{op}^H \tilde{\mathbf{h}}_{jm}$$

其中, \mathbf{w}_{op}^H 表示 \mathbf{w}_{op} 的共轭转置, $\mathbf{w}_{op} = \mathbf{R}^{-1} \mathbf{r}$ 表示最优加权复系数向量, $\tilde{\mathbf{h}}_{jm}$ 为主信道的估计矩阵。 \mathbf{R} 和 \mathbf{r} 中的元素分别为:

$$[\mathbf{R}]_{\varphi\vartheta} = J_0(2\pi f_d |\varphi - \vartheta| L_b T_s) + \sigma_v^2 \delta(\varphi - \vartheta)$$

$$\mathbf{r}_{\varphi} = J_0(2\pi f_d |D + \varphi - 1| L_b T_s)$$

其中, $\varphi, \vartheta = 1, 2, \dots, K, \sigma_v^2$ 为信道估计误差的方差。

由文献[14]可知, 预测的主信道增益与其真实值之间的关系为:

$$h_{jm}(\alpha + D) = \rho \hat{h}_{jm}(\alpha + D) + \sqrt{1 - \rho^2} n_{jm}(\alpha + D) \quad (1)$$

其中, $\rho = \sqrt{\mathbf{r}^H \mathbf{R}^{-1} \mathbf{r}}$ 为预测信道增益与真实值之间的归一化功率相关系数, $n_{jm}(\alpha + D)$ 为 AWGN 且服从 $CN(0, 1)$ 分布。

1.4 天线选择 OSTBC 编码

主信道的天线选择 OSTBC 编码过程如下:

1) Bob 通过观察导频符号并使用 MMSE 信道预测器得到预测的 $N_B \times N_A$ 维主信道矩阵:

$$\hat{\mathbf{H}}_{AB} = [\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2, \dots, \hat{\mathbf{h}}_{N_A}]$$

其中, $\hat{\mathbf{h}}_y (y = 1, 2, \dots, N_A)$ 表示矩阵 $\hat{\mathbf{H}}_{AB}$ 的第 y 列。

2) Bob 计算每一列的 Frobenius 范数并按降序排列得到矩阵 $\mathbf{H}'_{AB} = [\mathbf{h}'_1, \mathbf{h}'_2, \dots, \mathbf{h}'_{N_A}]$ 。采用 $\|\cdot\|_F$ 表示 Frobenius 范数, 则有 $\|\mathbf{h}'_1\|_F \geq \|\mathbf{h}'_2\|_F \geq \dots \geq \|\mathbf{h}'_{N_A}\|_F$ 。

3) Bob 将 \mathbf{H}'_{AB} 的前 N_T 列所对应的发射天线序号通过反馈链路反馈给 Alice。

4) Alice 根据收到的天线序号信息将对应的发射天线激活, 并对需要发送的安全信息符号进行天线数为 N_T 、码率为 R 的 OSTBC 编码。例如: 当 $N_T = 2$ 时, 可采用码率 $R = 1$ 的 G_2 码; 当 $N_T = 3$ 时, 可采用 $R = 1/2$ 的 G_3 码或 $R = 3/4$ 的 H_3 码^[17]。

5) Alice 将上述 OSTBC 码字安排在图 2 所示的每帧的后 $L_b - N_A$ 个符号周期内, 由选定的 N_T 根天线发送出去。

1.5 主信道和窃听信道 SNR 的 PDF

设主信道每根接收天线上的平均信噪比 (Signal-to-Noise Ratio, SNR) 为 $\bar{\gamma}_B$, 令 $c = 1/(RN_T)$, 根据文献[18]推导 TASP/OSTBC 无线通信系统输出 SNR 的矩生成函数 (Moment Generation Function, MGF) 的步骤, Bob 采用最大似然准则译码, 其 MRC 合并器输出的瞬时符号 SNR 的 MGF 为:

$$M_B(s) = \Sigma_1 [L_{N_T}! N_T^{-L_{N_T}-1} (1 + c \bar{\gamma}_B s)^{-N_T N_B} + \Sigma_2 (1 + c \bar{\gamma}_B s (1 - \rho))^{a_{ni}} (1 + c \bar{\gamma}_B s)^{-z} (1 + v_i s)^{-r}] \quad (2)$$

$$\Sigma_1 = N_T \binom{N_A}{N_T} \sum_l t(N_B; l) / (\Gamma(N_B))^{N_T} \prod_{u=1}^{N_T-1} \frac{l_u!}{u^{l_u}} \quad (3)$$

$$\Sigma_2 = \sum_{i=1}^{N_A - N_T} \binom{N_A - N_T}{i} (-1)^i \sum_{n \in \Omega} \frac{i! (a_{ni} + l_{N_T})!}{c_{ni} b_{ni} (N_T + i)^r} \quad (4)$$

其中, $t(N_B; l)$ 为多项式 $\left(\sum_{i=1}^{N_T} x_i\right)^{N_B-1} \left(\sum_{i=2}^{N_T} x_i\right)^{N_B-1} \dots x_{N_T}^{N_B-1}$ 中 $x_1^{l_1} x_2^{l_2} \dots x_{N_T}^{l_{N_T}}$ 的系数, $\Gamma(\cdot)$ 表示 gamma 函数, Ω 表示满足 $\sum_{k=0}^{N_B-1} n_k = i$ 的非负整数 $n_0, n_1, \dots, n_{N_B-1}$ 的集合, $d = \sum_{u=1}^{N_T-1} l_u$, $a_{ni} = \sum_{k=1}^{N_B-1} k n_k$, $b_{ni} = \prod_{k=1}^{N_B-1} (k!)^{n_k}$, $c_{ni} = \prod_{k=0}^{N_B-1} (k!)^{n_k}$, $r = a_{ni} + l_{N_T} + 1$, $z = d + N_T - 1$, $v_i = c \bar{\gamma}_B [N_T + i(1 - \rho)] / (N_T + i)$ 。

对式(2)中含有 s 的项进行部分分式展开:

$$\frac{[1 + c \bar{\gamma}_B s (1 - \rho)]^{a_{ni}}}{(1 + c \bar{\gamma}_B s)^z (1 + v_i s)^r} = \sum_{p=1}^z \frac{A_p}{(1 + c \bar{\gamma}_B s)^p} + \sum_{q=1}^r \frac{B_q}{(1 + v_i s)^q} \quad (5)$$

$$A_p = \frac{(c \bar{\gamma}_B)^{p-z} \partial^{z-p}}{(z-p)! \partial s^{z-p}} \left[\frac{(1 + c \bar{\gamma}_B s (1 - \rho))^{a_{ni}}}{(1 + v_i s)^r} \right]_{s = -1/(c \bar{\gamma}_B)} \quad (6)$$

$$B_q = \frac{((v_i)^{q-r} \partial^{r-q}}{(r-q)! \partial s^{r-q}} \left[\frac{(1 + c \bar{\gamma}_B s (1 - \rho))^{a_{ni}}}{(1 + c \bar{\gamma}_B s)^z} \right]_{s = -1/v_i} \quad (7)$$

将式(5)带入式(2),利用拉普拉斯反变换 $1/(1+\lambda s)^x \leftrightarrow 1/(x-1)! \lambda^{-x} t^{x-1} \exp(-t/\lambda)$,经化简整理后可得TASP/OSTBC无线通信系统的主信道输出信噪比 γ_B 的概率密度函数(Probability Density Function,PDF)为:

$$f_{\gamma_B}(\gamma_B) = \sum_l \left[\frac{l_{N_T}!}{N_T^{l_{N_T}+1}} g(N_T N_B, c \bar{\gamma}_B) + \sum_{p=1}^z A_p \cdot g(p, c \bar{\gamma}_B) + \sum_{q=1}^r B_q \cdot g(q, v_i) \right] \quad (8)$$

$$g(N, \mu) = \gamma_B^{N-1} / \Gamma(N) \mu^{-N} \exp(-\gamma_B / \mu) \quad (9)$$

设窃听信道每根接收天线上的平均 SNR 为 $\bar{\gamma}_E$, Eve 在 Alice 发送数据的过程中进行被动窃听, 由于主信道最佳 TAS 与窃听信道无关, 因此对 Eve 而言相当于随机天线选择, 则 Eve 瞬时输出信噪比 γ_E 的 PDF 为^[19]:

$$f_E(\gamma_E) = \frac{\gamma_E^{N_T N_E - 1}}{\Gamma(N_T N_E)} (c \bar{\gamma}_E)^{-N_T N_E} \exp\left(-\frac{\gamma_E}{c \bar{\gamma}_E}\right) \quad (10)$$

2 安全性能分析

设主信道的容量为 $C_B = R \log(1 + \gamma_B)$, 窃听信道的容量为 $C_E = R \log(1 + \gamma_E)$, 则瑞利块衰落信道上 TASP/OSTBC 无线通信系统的安全容量为:

$$C_S = \begin{cases} C_B - C_E, \gamma_B > \gamma_E \\ 0, \gamma_B \leq \gamma_E \end{cases} \quad (11)$$

$$F(N, \mu) = \frac{(c \bar{\gamma}_E)^{-N_T N_E}}{\Gamma(N_T N_E)} \exp\left(\frac{1-2^\theta}{\mu}\right) \sum_{k=0}^{N-1} \frac{\mu^{-k}}{k!} \sum_{w=0}^k \binom{k}{w} 2^{w\theta} (2^\theta - 1)^{k-w} (N_T N_E + w - 1)! [1/(c \bar{\gamma}_E) + 2^\theta / \mu]^{-N_T N_E - w} \quad (15)$$

$$P_{out}(R_S) = 1 - \binom{N_A}{N_T} \sum_l \frac{N_T t(N_B; l)}{(\Gamma(N_B))^{N_T}} \prod_{u=1}^{N_T-1} \frac{l_u!}{u^{l_u}} \left[\frac{l_{N_T}!}{N_T^{l_{N_T}+1}} F(N_T N_B, c \bar{\gamma}_B) + \sum_{i=1}^{N_A - N_T} \binom{N_A - N_T}{i} (-1)^i \sum_{n \in \Omega} \frac{i! (a_{ni} + l_{N_T})!}{c_{ni} b_{ni} (N_T + i)^r} \left(\sum_{p=1}^z A_p \cdot F(p, c \bar{\gamma}_B) + \sum_{q=1}^r B_q \cdot F(q, v_i) \right) \right] \quad (16)$$

由式(16)可知, TASP/OSTBC 无线通信系统的安全中断概率与主信道收发天线数、窃听者天线数、归一化反馈延时和目标安全速率等参数有关。本文考虑 2 种特殊情况:

1) 当 $N_T = 2, \tau = 0$ 时, 式(16)即为文献[7]中理想 CSI 下 TAS/MRC 无线通信系统的安全中断概率表达式。

2) 当 $N_T = N_A, \tau = 0$ 时, 式(16)即为文献[21]中理想 CSI 下 STBC 无线通信系统的安全中断概率表达式。

因此, 式(16)的结果更具一般性。

2.1 安全中断概率

TASP/OSTBC 无线通信系统的安全中断概率可定义为系统的安全容量小于目标安全速率 R_S 的概率。由式(11)可知, TASP/OSTBC 无线通信系统在以下 2 种情况下会发生安全中断:

1) 当 $\gamma_B \leq \gamma_E$ 时, 系统的安全容量为 0。

2) 当 $\gamma_B > \gamma_E$ 时, 系统的安全容量小于 R_S 。

因此, TASP/OSTBC 无线通信系统的安全中断概率可表示为^[9]:

$$P_{out}(R_S) = \Pr\{C_S < R_S | \gamma_B > \gamma_E\} \Pr\{\gamma_B > \gamma_E\} + \Pr\{\gamma_B < \gamma_E\} = 1 - \int_0^\infty \int_{2^{\theta(1+\gamma_E)}-1}^\infty f_B(\gamma_B) f_E(\gamma_E) d\gamma_B d\gamma_E \quad (12)$$

其中, $\Pr\{\cdot\}$ 表示概率, $\theta = R_S/R$ 。

定义积分公式:

$$F(N, \mu) = \int_0^\infty \int_{2^{\theta(1+\gamma_E)}-1}^\infty g(N, \mu) f_E(\gamma_E) d\gamma_B d\gamma_E \quad (13)$$

利用文献[20]中的式(3.351.2):

$$\int_a^\infty x^b e^{-\mu x} dx = e^{-a\mu} \sum_{v=0}^b \frac{b!}{v!} \frac{a^v}{\mu^{b-v+1}} \quad (14)$$

求解式(13), 经化简整理后可得式(15)。将式(8)、式(10)、式(15)代入式(12), 可得TASP/OSTBC 无线通信系统的安全中断概率如式(16)所示。

2.2 非零安全容量概率

TASP/OSTBC 无线通信系统的非零安全容量概率(安全容量大于 0 的概率)可表示为^[10]:

$$P_{non} = 1 - \int_0^\infty \int_{\gamma_B}^\infty f_B(\gamma_B) f_E(\gamma_E) d\gamma_E d\gamma_B \quad (17)$$

将式(8)和式(10)带入式(17), 并定义积分式:

$$G(N, \mu) = \int_0^\infty \int_{\gamma_B}^\infty g(N, \mu) \gamma_E^{N_T N_E - 1} \exp\left(-\frac{\gamma_E}{c \bar{\gamma}_E}\right) d\gamma_E d\gamma_B \quad (18)$$

采用与式(13)同样的推导过程, 经化简整理后可得:

$$G(N, \mu) = \sum_{k=0}^{N_T N_E - 1} \mu^{-N} (c \bar{\gamma}_E)^{-k} / [k! (N-1)! (N+k-1)!] \cdot [1/(c \bar{\gamma}_E) + (1/\mu)]^{-N-k} \quad (19)$$

将式(19)代入式(17),可得TASP/OSTBC无线通信系统的非零安全容量概率的表达式为:

$$P_{\text{non}} = 1 - \sum_1 \left[\frac{l_{N_T}!}{N_T^{l_{N_T}+1}} G(N_T N_B, c \bar{\gamma}_B) + \sum_{p=1}^{\infty} A_p G(p, c \bar{\gamma}_B) + \sum_{q=1}^r B_q \cdot G(q, v_i) \right] \quad (20)$$

将式(16)和式(20)中的 ρ 用 $J_0(2\pi f_d \tau)$ 代替,即可得到TASP/OSTBC无线通信系统的安全中断概率和非零安全容量概率的表达式。若某方法可以获得比其他方法更高的非零安全容量概率,即可认为该方法可以使无线通信系统获得更好的物理层安全性能。

2.3 渐近安全中断概率

由于式(16)的安全中断概率表达式在形式上过于复杂,无法直观地看出主信道收发天线数、窃听者天线数和归一化反馈延时等参数对TASP/OSTBC无线通信系统安全中断概率的影响,特别是无法直接反映安全中断概率随主信道平均信噪比的变化趋势。采用渐近安全中断概率进行性能评估,则可以解决上述问题。

由文献[9]可知,渐近安全中断概率公式如式(21)所示。

$$P_{\text{out}}^{\infty}(R_s) = (G_a \bar{\gamma}_B)^{-G_d} + o(\bar{\gamma}_B^{-G_d}) \quad (21)$$

其中: G_d 为安全分集增益,反映了安全中断概率随主信道平均信噪比变化的快慢,表现为曲线的斜率; G_a 为安全阵列增益,反映了相较于参考曲线 $\bar{\gamma}_B^{-G_d}$ 的SNR增益; $o(\cdot)$ 表示高阶无穷小项。下文将对 $\tau=0$ 和 $\tau \neq 0$ 两种情形分别进行分析。

情形1 $\tau=0$ 。将文献[22]中的式(21)和式(22)代入文献[18]中的式(8),令 $U=N_B(N_A-N_T)+l_{N_T}+1$,推导出理想CSI下TASP/OSTBC无线通信系统 γ_B 的MGF的渐近表达式为:

$$M_B^{\infty}(s) = \sum_1 \frac{\Gamma(U) (N_B!)^{N_T-N_A}}{N_T^U (c \bar{\gamma}_B s)^{N_A N_B}} + o(s^{-N_A N_B}) \quad (22)$$

利用拉普拉斯反变换 $1/(s-a)^{n+1} \leftrightarrow t^n e^{at}/n!$,求得 γ_B 的渐近PDF后代入式(12),经化简整理后可得理想CSI下TASP/OSTBC无线通信系统的安全分集增益 $G_d=N_A N_B$,安全阵列增益 $G_a=Y_1^{-1/G_d}$, Y_1 的表达式为:

$$Y_1 = \sum_1 \frac{\Gamma(U)}{N_T^U} (N_B!)^{N_T-N_A} \sum_{k=0}^{G_d} \binom{G_d}{k} \left(\frac{2^\theta - 1}{c} \right)^{G_d-k} 2^{k\theta} \cdot \frac{\bar{\gamma}_E^k \Gamma(N_T N_E + k)}{[G_d! \Gamma(N_T N_E)]} \quad (23)$$

情形2 $\tau \neq 0$ 。由文献[18]中的式(16)可得反馈延时下TASP/OSTBC无线通信系统 γ_B 的MGF与理想CSI下 γ_B 的MGF的关系式为:

$$\tilde{M}_B^{\infty}(s) = \frac{M_B^{\infty}(\rho s / [1 + c \bar{\gamma}_B s (1 - \rho)])}{[1 + c \bar{\gamma}_B s (1 - \rho)]^{N_T N_B}} \quad (24)$$

将式(22)代入式(24)可得反馈延时下TASP/OSTBC无线通信系统 γ_B 的渐近MGF。采用与 $\tau=0$ 同样的推导过程,经整理后可得反馈延时下TASP/OSTBC无线通信系统的安全分集增益 $G_d=N_T N_B$,安全阵列增益 $G_a=Y_2^{-1/G_d}$, Y_2 的表达式为:

$$Y_2 = \sum_1 \frac{\Gamma(U)}{N_T^U} \frac{(1-\rho)^{N_B N_A - G_d}}{(N_B!)^{N_A - N_T} \rho^{N_A N_B}} \sum_{k=0}^{G_d} \binom{G_d}{k} \left(\frac{2^\theta - 1}{c} \right)^{G_d-k} \frac{2^{k\theta} \bar{\gamma}_E^k \Gamma(N_T N_E + k)}{G_d! \Gamma(N_T N_E)} \quad (25)$$

经上述分析可知,在理想CSI下TASP/OSTBC无线通信系统的安全分集增益为发射端天线数与合法接收端天线数的乘积 $N_A N_B$ 。由于反馈延时的存在,使得系统的安全分集增益降为选择的发射天线数与合法接收端天线数的乘积 $N_T N_B$,且与窃听信道、归一化反馈延时等参数无关。安全阵列增益 G_a 反映了采用MMSE信道预测器对TASP/OSTBC无线通信系统物理层安全性能的影响。

将式(23)和式(25)中的 ρ 用 $J_0(2\pi f_d \tau)$ 代入即可得到TASP/OSTBC无线通信系统分别在上述2种情形下的安全阵列增益表达式。

3 数值计算与仿真

本文利用MATLAB软件,以表1所示的参数设置为例对TASP/OSTBC无线通信系统物理层安全性能进行数值计算和计算机仿真。如无特殊说明,Alice均选择2根天线发送信息符号,即Alice采用 G_2 空时分组码。

表1 TASP/OSTBC无线通信系统仿真参数设置
Table 1 Simulation parameter setting of TASP/OSTBC wireless communication system

信道	参数	参数值
信道预测	信道预测阶数 K	5
	多普勒频移 f_d/Hz	100
	符号间隔 T_s/s	10^{-6}
	误差方差 σ_v^2/dB	-30
主信道	发射端天线数 N_A	4
	选择的天线数 N_T	2
	目标安全速率 $R_s/(\text{bit} \cdot \text{s}^{-1} \cdot \text{Hz}^{-1})$	1
窃听信道	窃听者平均信噪比 $\bar{\gamma}_E/\text{dB}$	5

当 $N_B=N_E=2$ 时,在不同 $f_d \tau$ 下TASP/OSTBC与TASP/OSTBC无线通信系统的安全阵列增益曲线如图3所示。由图3可知,在相同 $f_d \tau$ 下,TASP/OSTBC无线通信系统的安全阵列增益值始终

大于 TASP/OSTBC 无线通信系统。当 $f_d\tau = 10^{-1}$ 时, TASP 较 TASP 方案安全阵列增益高约 9.3 dB。由此表明, MMSE 信道预测器通过获得较大的安全阵列增益来改善反馈延时对无线通信系统物理层安全性能的影响。

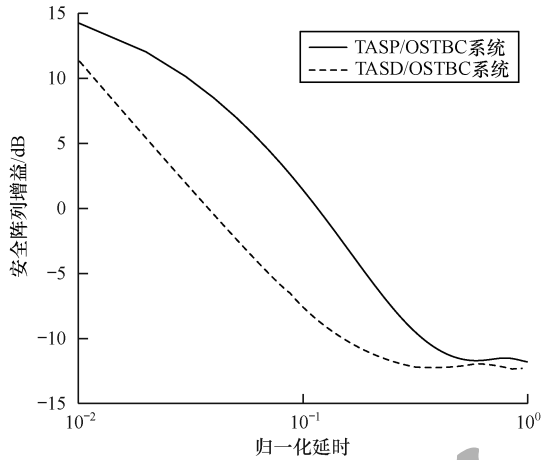


图 3 TASP/OSTBC 与 TASP/OSTBC 系统的安全阵列增益
Fig. 3 Security array gains between TASP/OSTBC and TASP/OSTBC systems

当 $N_B = 2$ 时, 不同 N_E 和 $f_d\tau$ 下 TASP/OSTBC 无线通信系统的非零安全容量概率曲线如图 4 所示。由图 4 可知, 在相同 $f_d\tau$ 下, 增加窃听者天线数提高了窃听者的接收分集增益, 导致 TASP/OSTBC 无线通信系统的非零安全容量概率变小, 降低了系统的安全性能。当 N_E 一定时, 非零安全容量概率随归一化延时 $f_d\tau$ 的减小而增大, 这是因为 $f_d\tau$ 越小越接近理想主信道 CSI 的情况, 所以可以获得更好的安全性能。如当非零安全容量概率为 10^{-2} , $N_E = 4$ 时, $f_d\tau = 0.4$ 较 $f_d\tau = 1.0$ 有约 0.3 dB 的 SNR 增益。

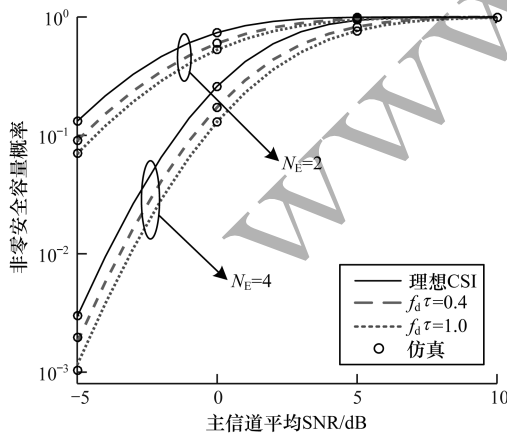


图 4 不同 N_E 和 $f_d\tau$ 下 TASP/OSTBC 的非零安全容量概率
Fig. 4 Non-zero secrecy capacity probability of TASP/OSTBC under different N_E and $f_d\tau$

当 $N_E = 2$ 时, 在不同 N_B 和 $f_d\tau$ 下 TASP/OSTBC 与 TASP/OSTBC 无线通信系统的安全中断概率曲线如图 5 所示。由图 5 可知, 安全中断概率的数值计算与仿真结果相吻合, 这表明理论推导的准确性。在相同 $f_d\tau$ 下, TASP/OSTBC 与 TASP/OSTBC 无线通信系统的安全中断概率均随接收天线数 N_B 的增加而减小, 这是由于增加了合法接收分集增益, 从而提高了系统的安全性能。在相同 N_B 和 $f_d\tau$ 下, TASP/OSTBC 无线通信系统具有更低的安全中断概率, 即具有更好的物理层安全性能。如当安全中断概率在 10^{-6} , $f_d\tau = 0.3$, $N_B = 2$ 时, TASP/OSTBC 较 TASP/OSTBC 无线通信系统有约 2.6 dB 的 SNR 增益。

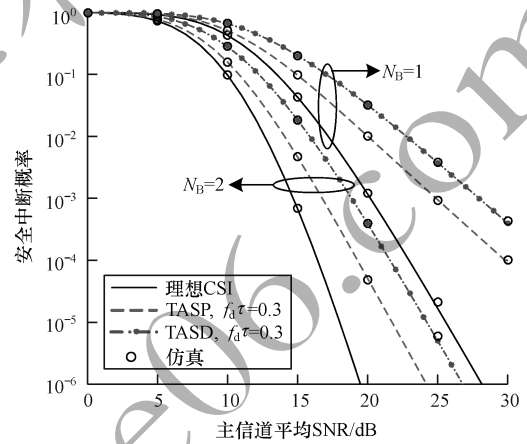


图 5 不同 N_B 和 $f_d\tau$ 下 TASP/OSTBC 的安全中断概率
Fig. 5 Secrecy outage probabilities of TASP/OSTBC under different N_B and $f_d\tau$

当 $f_d\tau = 0.5$, $N_B = N_E = 2$ 时, TASP/MRC 与 TASP/OSTBC 无线通信系统的安全中断概率曲线如图 6 所示。

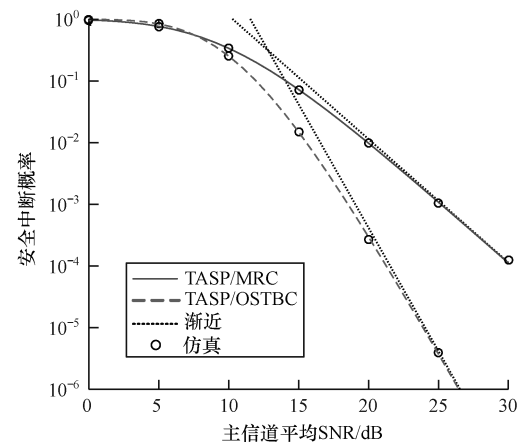


图 6 TASP/MRC 与 TASP/OSTBC 的安全中断概率
Fig. 6 Secrecy outage probabilities of TASP/MRC and TASP/OSTBC

由图6可知,渐近线在主信道 SNR 较高的情况下能够较好地接近精确值,这证明了渐近推导的准确性。随着 $\bar{\gamma}_B$ 的逐渐增大,TASP/OSTBC无线通信系统的物理层安全性能逐渐优于 TASP/MRC 无线通信系统。这是由于在反馈延时下,TASP/MRC 无线通信系统的安全分集增益为 N_B ,而TASP/OSTBC无线通信系统的安全分集增益为 $N_T N_B$,因此 TASP/OSTBC无线通信系统具有更大的安全性能优势。如当安全中断概率为 10^{-3} 时,TASP/OSTBC较 TASP/MRC 无线通信系统有约 6.7 dB 的 SNR 增益。

4 结束语

本文采用 MMSE 信道预测器提高 TASP/OSTBC 无线通信系统的物理层安全性能,通过理论推导非零安全容量概率、安全中断概率以及渐近安全中断概率的精确解析表达式,分析得到系统的安全分集增益和安全阵列增益。数值计算和仿真结果表明,该方案可以通过增大系统的安全阵列增益来改善反馈延时对其物理层安全性能的影响,即增大接收端天线数、减小窃听者天线数等措施都将提高TASP/OSTBC无线通信系统的物理层安全性能,并且在反馈延时下采用 OSTBC 可以获得部分发射分集增益。下一步将考虑节点距离对系统物理层安全性能的影响,此外,将该方案运用到大规模 MIMO 协作中继网络等更加复杂的通信系统中也是未来研究方向。

参考文献

- [1] CHEN X, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security [J]. IEEE Communications Surveys and Tutorials, 2017, 19(2): 1027-1053.
- [2] ALVES H, SOUZA R D, DEBBAB M, et al. Performance of transmit antenna selection physical layer security schemes [J]. IEEE Signal Processing Letters, 2012, 19(6): 372-375.
- [3] YANG N, YEOH P L, ELKASHLAN M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels [J]. IEEE Transactions on Communications, 2013, 61(1): 144-154.
- [4] FERDINAND N S, COSTA D B D, LATVA-AHO M. Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation [J]. IEEE Wireless Communications Letters, 2013, 2(5): 467-470.
- [5] ZHANG Yajun, LIANG Tao, LIU Yongxiang, et al. Hybrid transmit antenna selection and full-duplex artificial-noise-added receiver scheme for physical layer security enhancement [J]. Journal of Electronics and Information Technology, 2015, 37(9): 2183-2190. (in Chinese)
- 张亚军, 梁涛, 柳永祥, 等. 联合发端天线选择和收端人工噪声的物理层安全传输方法 [J]. 电子与信息学报, 2015, 37(9): 2183-2190.
- [6] CAI Xiaoxia, ZENG Lingqing, CHEN Hong, et al. Guaranteeing physical layer security using multi-antennas selection at the transmitter in MIMO system [J]. Science Technology and Engineering, 2016, 16(21): 261-265. (in Chinese)
- 蔡晓霞, 曾凌清, 陈红, 等. MIMO 系统发射端多天线选择保障物理层安全传输研究 [J]. 科学技术与工程, 2016, 16(21): 261-265.
- [7] YAN S, YANG N, MALANEY R, et al. Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels [J]. IEEE Transactions on Wireless Communications, 2014, 13(3): 1656-1667.
- [8] YANG Maoqiang, ZHANG Bangning, HUANG Yuzhen, et al. Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise [J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 11394-11398.
- [9] XIONG Jun, TANG Yanqun, MA Dongtang, et al. Secrecy performance analysis for TAS-MRC system with imperfect feedback [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(8): 1617-1629.
- [10] HUANG Y, AL-QAHTANI F S, DUONG T Q, et al. Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI [J]. IEEE Transactions on Communications, 2015, 63(8): 2959-2971.
- [11] HU Jianwei, CAI Yueming, YANG Nan, et al. A new secure transmission scheme with outdated antenna selection [J]. IEEE Transactions on Information Forensics and Security, 2017, 10(11): 2435-2446.
- [12] ZHAO Rui, LIN Hongxin, HE Yucheng, et al. Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI [J]. IEEE Transactions on Communications, 2018, 66(2): 546-559.
- [13] LIN Hongxin, ZHAO Rui, HE Yucheng, et al. Secrecy performance analysis of opportunistic relay selection systems with outdated CSI [J]. Journal of Signal Processing, 2016, 32(7): 810-818. (in Chinese)
- 林鸿鑫, 赵睿, 贺玉成, 等. 过时信道状态信息下的机会式中继选择系统的安全性能分析 [J]. 信号处理, 2016, 32(7): 810-818.
- [14] PRAKASH S, MCLOUGHLIN I. Effects of channel prediction for transmit antenna selection with maximal-ratio combining in Rayleigh fading [J]. IEEE Transactions on Vehicular Technology, 2011, 60(6): 2555-2568.
- [15] LI Debing, LI Guangqiu, JIN Xufeng. Symbol error rate performance analysis of RQAM with channel prediction and joint transceiver diversity [J]. Computer Engineering, 2018, 44(1): 121-127. (in Chinese)
- 李得兵, 李光球, 金徐凤. 信道预测和联合收发分集的 RQAM 误符号率性能分析 [J]. 计算机工程, 2018, 44(1): 121-127.

(上接第 147 页)

- [16] WANG Zhanwan, LI Guangqiu, QIAN Hui. Physical layer security performance analysis of TASP/MRC system in multi-eavesdropper scene [J]. Computer Engineering, 2019, 45(10):160-165, 170. (in Chinese)
王占湾, 李光球, 钱辉, 多窃听者场景下 TASP/MRC 系统的物理层安全性能分析[J]. 计算机工程, 2019, 45(10):160-165, 170.
- [17] TAROKH V, JAFARKHANI H, CALDERBANK A R. Space-time block coding for wireless communications; performance results[J]. IEEE Journal on Selected Areas in Communications, 1999, 17(3):451-460.
- [18] YU X, XIA X, LEUNG S. Performance analysis of MIMO systems with arbitrary number transmit antenna selection and OSTBC in the presence of imperfect CSI[J]. Science China Information Sciences, 2016, 59(8):1-16.
- [19] AHN K S, HEATH R W J, BAIK H K. Shannon capacity and symbol error rate of space-time block codes in MIMO Rayleigh channels with channel estimation error[J]. IEEE Transactions on Wireless Communications, 2008, 7(1):324-333.
- [20] GRADSHTEYN I S, RYZHIK I M. Table of integrals, series and products [M]. Pittsburgh, USA: Academic Press, 2007.
- [21] CHAUHAN S S, VERMA P, MATHUR M, et al. Physical layer security of MIMO STBC over Rayleigh fading channels in the presence of channel estimation error [J]. Optik-International Journal for Light and Electron Optics, 2016, 127(19):7625-7630.
- [22] YILMAZ A, KUCUR O. Performances of transmit antenna selection, receive antenna selection, and maximal-ratio-combining-based hybrid techniques in the presence of feedback errors [J]. IEEE Transactions on Vehicular Technology, 2014, 63(4):1976-1982.

编辑 刘盛龄