

MIMO 系统发射端多天线选择保障 物理层安全传输研究

蔡晓霞 曾凌清 陈 红 朱文丽

(电子工程学院 402 教研室, 合肥 230037)

摘要 针对 MIMO 系统信号传输策略中单天线选择方案在增大系统保密容量方面存在的局限性, 提出发射端多天线选择方案以保障物理层安全通信。首先在已知全局信道状态信息的理想条件下讨论最优多天线选择方案; 然后考虑较为实际的情况, 即在未知窃听方信道状态信息条件下提出次优多天线选择方案; 最后, 为改进次优方案在低信噪比条件下系统保密容量较小的不足, 提出次优多天线选择发射功率分配方案。通过理论推导保密容量表达式和数值分析, 结果表明, 与现有单天线选择方案相比, 所提的多天线选择方案有效地提高了系统的保密容量。

关键词 物理层安全 保密容量 多天线选择 信道状态信息

中图法分类号 TN918.28; 文献标志码 A

由于无线传输媒介的开放特性, 未授权的窃听方可以采取窃听方法截获合法通联双方的传输信号。因此, 应用物理层安全技术保障通信安全成为了近期研究的热点。Oggier F 完成了 MIMO 信道的保密容量推导^[1], 为 MIMO 系统物理层安全技术的发展和应用提供理论依据。近年来, 几类 MIMO 系统物理层安全技术相继提出。MIMO 信道安全编码技术^[2,3]利用信道状态信息进行编码方法的构造, 在保证接收端正常译码的前提下使窃听方译码错误。然而安全编码设计的研究主要以理论分析为主, 且编码的构造对信道估计误差精度的需求较苛刻, 难以实际应用。人工噪声方法^[4]和波束成型方法^[5]利用主信道和窃听信道之间的差异进行人工辅助噪声和波束成型矩阵的设计, 旨在提高合法接收端的接收性能并干扰窃听方的接收。但与此同时, 人工噪声方法不可避免地增大了发射端功耗, 造成通信资源的浪费; 波束成型则因为信道矩阵的提取和预处理参数的设计带来了较高的算法复杂度。与这些技术不同, 采用物理层安全天线选择分集技术^[6–10]在提高系统保密性能的同时, 降低了射频模块等硬件成本和应用复杂度。Zou Y 讨论了采用分集技术提高物理层安全^[6]具有低复杂度且不降低分集增益等优点, Alves H 和 Yang N 分别在瑞利信道^[7]条件下和 nakagami-m 衰落信道^[8]条件下分析采用发射天线选择方案得到的系统保密性能。Hu Yujia 则提

出了利用交换 - 检验合并^[9]进行天线选择的方案, 实现了合法接收端低信噪比条件下较少估计损耗的保密性能。基于仅选出单根发射天线的已知全局信道状态信息 (CSI) 的最优天线选择方案 (OAS)^[10]和未知窃听信道状态信息的次优天线选择 (SAS)^[11]方案随后提出。

前述研究中, 仅选出单根天线的天线选择方案^[7,8,10,11]在提高系统保密容量方面存在局限性, 主要体现在单天线选择将 MIMO 信道容量的推导转化为 SIMO 信道或 MISO 信道容量的推导, 简化理论推导和方案实现的同时, 也减小了主信道容量。相比发射端单天线选择方案, 本文考虑牺牲一定的计算简洁度, 采用多发射天线选择方案保障物理层安全通信。一方面, 基于信道容量最大化升序排列的多天线选择算法^[12]一定程度上增大了计算复杂度, 但多天线选择算法是在单天线选择算法的基础上进行迭代, 实现难度和计算复杂度较低; 另一方面, 多天线选择方案为联合其他物理层安全技术如空时编码和功率分配等方案的研究提供了可行性。根据上述讨论, 本文余下安排为: 第一节先是讨论已知全局信道状态信息 (CSI) 条件下的最优多天线选择方案 (OMAS), 而后考虑未知窃听方信道状态信息条件下的次优多天线选择方案 (SMAS); 第二节分别推导了 OMAS 和 SMAS 方案的保密容量, 考虑到对窃听信道的未知导致次优方案的保密性能弱于最优方案, 提出次优多天线选择联合功率分配的方案并推导保密容量; 第三节进行数值对比分析和仿真实例验证方案的可行性; 最后总结全文。

2016 年 3 月 21 日收到

第一作者简介: 蔡晓霞(1965), 女, 教授, 硕士生导师。研究方向: 通信信号处主任, 通信网效能评估。

1 系统模型和多天线选择

如图 1,假设 MIMO 系统包含发射端(transmitter)、接收端(receiver)和试图截获信号的窃听方(eavesdropper),天线数分别为 N_T , N_R , N_E ,每根天线编号集合分别属于集合 T , R , E 。并假设主信道和窃听信道为瑞利衰落信道(主信道 $\mathbf{H}_M \in \mathbb{C}^{N_R \times N_T}$,窃听信道 $\mathbf{H}_W \in \mathbb{C}^{N_E \times N_T}$)。且相互独立同分布。假定加性噪声为零均值复高斯随机变量,方差为 N_0 ,信号发射总功率为 P 。

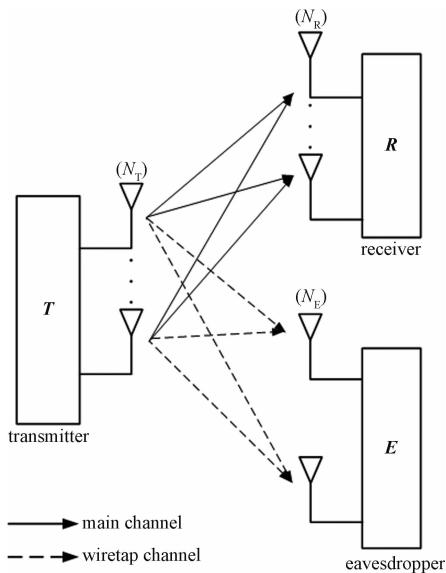


图 1 存在多天线窃听方的 MIMO 信道模型

Fig. 1 MIMO system in the presence of eavesdropper

定理 1:MIMO 系统保密容量表达式为^[1]

$$C_S = \max\{0, C_M - C_W\} \quad (1)$$

式(1)中 C_S 为系统保密容量, C_M 和 C_W 分别为主信道容量和窃听信道容量。

定理 2:MIMO 信道容量的表达式为^[13]

$$C = \lg_2 \left(\mathbf{I}_{N_R} + \frac{P}{N_0} \mathbf{H} \mathbf{R}_{xx} \mathbf{H}^H \right) \quad (2)$$

式(2)中 I 是维数为接收天线数 N_R 的单位矩阵, \mathbf{R}_{xx} 是发射信号 x 的自相关矩阵, \mathbf{H} 为 MIMO 信道的衰落系数矩阵。

1.1 最优多天线选择(OMAS)方案

已知全局信道状态信息(CSI)的最优天线选择(OAS)方案^[10]以保密容量最大化为目的选出单根发射天线。单天线选择时,主信道容量和窃听信道容量表达式分别为

$$C_M = \lg_2 \left(1 + \sum_{j=1}^{N_R} \frac{P |h_{iRj}|^2}{N_0} \right) \quad (3)$$

$$C_W = \lg_2 \left(1 + \sum_{j=1}^{N_E} \frac{P |h_{iEj}|^2}{N_0} \right) \quad (4)$$

结合式(1)、式(3)、式(4),最优天线选择判决式如式(5)。

$$p_1 = \arg \max_{i \in T} (C_M - C_W) = \arg \max_{i \in T} \frac{1 + \sum_{j=1}^{N_R} \frac{P |h_{iRj}|^2}{N_0}}{1 + \sum_{j=1}^{N_E} \frac{P |h_{iEj}|^2}{N_0}} \quad (5)$$

p_1 即为 OAS 方案选出的“最优”天线。式(3)~式(5)中 h_{iRj} 是发射天线 i 到接收天线 j 的主信道衰落系数, h_{iEj} 是发射天线 i 到窃听天线 j 的窃听信道衰落系数, P 为信号发射总功率, N_0 为噪声功率。

然而,选出单根天线用于信号发射将 MIMO 信道简化为 SIMO 信道,一定程度削弱了主信道容量,导致系统保密容量的提升存在局限性。相比最优单天线选择^[10],本文考虑在相同的全局信道理想已知的条件下,讨论以保密容量最大化为原则的最优多天线选择算法。假设发射端功率平均分配,选出的天线数目为 Q 。

首先,可重写式(3)为

$$p_1 = \arg \max_{p_1 \in T} \frac{\det \left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \mathbf{H}_{N_R, p_1} \mathbf{H}_{N_R, p_1}^H \right)}{\det \left(\mathbf{I}_{N_E} + \frac{P}{QN_0} \mathbf{H}_{N_E, p_1} \mathbf{H}_{N_E, p_1}^H \right)} \quad (6)$$

p_1 为从发射天线中选出的使得系统保密容量最大的天线。其中, \mathbf{H}_{N_R, p_1} 为天线 p_1 到 N_R 根接收天线的信道衰落系数矩阵, \mathbf{H}_{N_E, p_1} 为天线 p_1 到 N_E 根窃听天线的信道衰落系数矩阵。

在选定第一根天线 p_1 的基础上,选出使得保密容量最大的第二根天线。

$$p_2 = \arg \max_{p_2 \neq p_1 \in T} \frac{\det \left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \mathbf{H}_{N_R, [p_1, p_2]} \mathbf{H}_{N_R, [p_1, p_2]}^H \right)}{\det \left(\mathbf{I}_{N_E} + \frac{P}{QN_0} \mathbf{H}_{N_E, [p_1, p_2]} \mathbf{H}_{N_E, [p_1, p_2]}^H \right)} \quad (7)$$

式(7)中 p_2 为选定的第二根天线, $\mathbf{H}_{N_R, [p_1, p_2]}$ 和 $\mathbf{H}_{N_E, [p_1, p_2]}$ 则分别为天线 p_1 、 p_2 到 N_R 根接收天线的信道衰落系数矩阵和天线 p_1 、 p_2 到 N_E 根窃听天线的信道衰落系数矩阵。

经过 n 次迭代选出 n 根天线 $\{p_1, p_2, \dots, p_n\}$,此时额外增选一根天线 k ,系统保密容量为

$$C_S^k = \lg_2 \det \left[\mathbf{I}_{N_R} + \frac{P}{QN_0} (\mathbf{H}_{N_R, [p_1, \dots, p_n]} \mathbf{H}_{N_R, [p_1, \dots, p_n]}^H + \mathbf{H}_{N_R, k} \mathbf{H}_{N_R, k}^H) \right] \times \left\{ \det \left[\mathbf{I}_{N_E} + \frac{P}{QN_0} (\mathbf{H}_{N_E, [p_1, \dots, p_n]} \mathbf{H}_{N_E, [p_1, \dots, p_n]}^H + \mathbf{H}_{N_E, k} \mathbf{H}_{N_E, k}^H) \right] \right\}^{-1} \quad (8)$$

根据行列式的以下性质:

$$\det(\mathbf{A} + \mathbf{BC}^H) = (1 + \mathbf{C}^H \mathbf{A}^{-1} \mathbf{B}) \det(\mathbf{A}) \quad (9)$$

$$\lg_2 \det(\mathbf{A} + \mathbf{BC}^H) = \lg_2 \det(\mathbf{A}) + \lg_2 (1 + \mathbf{C}^H \mathbf{A}^{-1} \mathbf{B}) \quad (10)$$

对式(6)中分子部分进行代换,得

$$\mathbf{A} = \det\left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \mathbf{H}_{N_R, [p_1, \dots, p_n]} \mathbf{H}_{N_R, [p_1, \dots, p_n]}^H\right) \quad (11)$$

$$\mathbf{B} = \mathbf{C} = \sqrt{\frac{P}{QN_0}} \mathbf{H}_{N_R, k} \quad (12)$$

同理代换式(6)中的分母。

由于天线选择的原则是第 $n+1$ 根天线仍应使保密容量最大,因此对式(6)进行最大化判决并化简,选出第 $n+1$ 根天线的判决式如式(13)。

$$\begin{aligned} p_{n+1} = \arg \max_{k \neq p_1, \dots, p_n \in T} & \left[1 + \mathbf{H}_{N_R, k} \left(\frac{QN_0}{P} \mathbf{I}_{N_R} + \right. \right. \\ & \left. \left. \mathbf{H}_{N_R, [p_1, \dots, p_n]}^H \mathbf{H}_{N_R, [p_1, \dots, p_n]} \right)^{-1} \mathbf{H}_{N_R, k}^H \right] \\ & \left[1 + \mathbf{H}_{N_E, k} \left(\frac{QN_0}{P} \mathbf{I}_{N_E} + \mathbf{H}_{N_E, [p_1, \dots, p_n]} \mathbf{H}_{N_E, [p_1, \dots, p_n]}^H \right)^{-1} \mathbf{H}_{N_E, k}^H \right]^{-1} \end{aligned} \quad (13)$$

反复迭代直至 $n+1 = Q$, 最优多天线选择完毕。

1.2 次优多天线选择(SMAS)方案

实际通信场景中,发射端可以通过接收端信道条件反馈或根据信道互易性^[14]推导得知主信道的信道状态信息,但无法准确获知窃听信道的信道状态信息。因此,上述最优多天线选择方案对全局信道条件已知的假设条件过于理想。本节考虑较为实际的情况,在未知窃听方信道状态信息条件下进行次优多天线选择。文献[12]中次优单天线选择的判决式如式(14)。

$$s = \arg \max_{i \in T} \sum_{j=1}^{N_R} |h_{ij}|^2 \quad (14)$$

式(14)中 s 即选出的“次优”天线, h_{ij} 是发射天线 i 到接收天线 j 的主信道衰落系数。

同上节推导,此节提出的次优多天线选择方案按照主信道容量升序排列,从 N_T 根发射天线中选出 Q 根天线。选择过程如下。

首先对 SAS 方案天线选取判决式(14)进行重写,选出最大化主信道容量的天线。

$$s_1 = \arg \max_{s_1 \in T} \det\left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \mathbf{H}_{N_R, s_1} \mathbf{H}_{N_R, s_1}^H\right) \quad (15)$$

给定第一根选择的天线后,选择第二根天线使得信道容量最大。

$$s_2 = \arg \max_{s_2 \neq s_1 \in T} \det\left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \mathbf{H}_{N_R, [s_1, s_2]} \mathbf{H}_{N_R, [s_1, s_2]}^H\right) \quad (16)$$

同上节, n 次迭代后选出 n 根天线,额外增加一根天线(如天线 k),增加的 $n+1$ 根天线应使信道容量最大。由此选出第 $n+1$ 根天线。

$$s_{n+1} = \arg \max_{k \neq s_1, \dots, s_n \in T} \mathbf{H}_k \left(\frac{QN_0}{P} \mathbf{I}_{N_R} + \mathbf{H}_{N_R, [s_1, \dots, s_n]} \mathbf{H}_{N_R, [s_1, \dots, s_n]}^H \right)^{-1} \mathbf{H}_k^H \quad (17)$$

当 $n+1 = Q$ 时,次优多天线选择完毕。

综上推导可知,当 $Q=1$ 时,本文所提的两种多天线选择方案分别等效于选出单根发射天线的最优天线选择(OAS)和次优天线选择(SAS)方案。

2 保密容量分析

2.1 OMAS 和 SMAS 方案的保密容量

首先推导采用 OMAS 方案后,MIMO 系统的保密容量表达式。过程如下。

采用 OMAS 方案选出了 Q 根天线,取主信道矩阵 $\mathbf{H}_M \in \mathbb{C}^{N_R \times N_T}$ 的 Q 列表示等效主信道,可以用 $N_R \times Q$ 矩阵建模相应的等效主信道,记为 $\mathbf{H}_M^{\text{OMAS}} = \mathbf{H}_{N_R, [P_1, \dots, P_Q]} \in \mathbb{C}^{N_R \times Q}$,同理,等效窃听信道记为: $\mathbf{H}_W^{\text{OMAS}} \in \mathbb{C}^{N_E \times Q}$ 。

为使接收端和窃听方获得最好的接收性能,本文考虑在接收方和窃听方分别采用最大比合并技术(MRC)^[8]接收信号,则等效主信道为 $\tilde{\mathbf{H}}_M^{\text{OMAS}} = (\mathbf{H}_M^{\text{OMAS}})^H \mathbf{H}_M^{\text{OMAS}}$,等效窃听信道为 $\tilde{\mathbf{H}}_W^{\text{OMAS}} = (\mathbf{H}_W^{\text{OMAS}})^H \mathbf{H}_W^{\text{OMAS}}$ 。

此时,上述参量代入式(1)和(2),可得采用 OMAS 方案的系统保密容量为

$$\begin{aligned} C_S^{\text{OMAS}} = \lg_2 & \left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \tilde{\mathbf{H}}_M^{\text{OMAS}} (\tilde{\mathbf{H}}_M^{\text{OMAS}})^H \right) - \\ & \lg_2 \left(\mathbf{I}_{N_E} + \frac{P}{QN_0} \tilde{\mathbf{H}}_W^{\text{OMAS}} (\tilde{\mathbf{H}}_W^{\text{OMAS}})^H \right) \end{aligned} \quad (18)$$

同理,采用 SMAS 方案后系统保密容量为

$$\begin{aligned} C_S^{\text{SMAS}} = \lg_2 & \left(\mathbf{I}_{N_R} + \frac{P}{QN_0} \tilde{\mathbf{H}}_M^{\text{SMAS}} (\tilde{\mathbf{H}}_M^{\text{SMAS}})^H \right) - \\ & \lg_2 \left(\mathbf{I}_{N_E} + \frac{P}{QN_0} \tilde{\mathbf{H}}_W^{\text{SMAS}} (\tilde{\mathbf{H}}_W^{\text{SMAS}})^H \right) \end{aligned} \quad (19)$$

2.2 SMAS-PA 方案的保密容量

次优多天线选择方案对窃听信道的未知,导致了采用次优方案后获得的系统保密性能弱于最优方案。本文考虑在采用次优多天线选择方案选出多根天线后,根据已知的主信道状态信息对选出的天线进行发射功率分配。由于主信道和窃听信道之间存在的特征差异,发射天线功率分配在提高主信道容量的同时能够在一定程度上恶化窃听信道。

由前述已知,采用 SMAS 方案选出了 Q 根天线

后,等效主信道记为 $\mathbf{H}_M^{\text{SMAS}} \in \mathbb{C}^{N_R \times Q}$ 、等效窃听信道记为: $\mathbf{H}_W^{\text{SMAS}} \in \mathbb{C}^{N_E \times Q}$ 。可依照矩阵的奇异值分解特性 $\mathbf{H} = \mathbf{U} \sum \mathbf{V}^H$ (\mathbf{U} 、 \mathbf{V} 均为酉矩阵), 在发射端和接收端分别进行预处理和后处理(预乘 $\mathbf{V}_M \in \mathbb{C}^{Q \times Q}$ 、后乘 $\mathbf{U}_M^H \in \mathbb{C}^{N_R \times N_R}$), 此时主信道等效为特征值矩阵 $\sum_M \in \mathbb{C}^{N_R \times Q}$ 。在接收方采用最大比合并技术接收信号, 则主信道等效为 $\mathbf{H}_M^{\text{SMAS-PA}} = \sum_M^H \sum_M$ 。此时信道可等效为 r 个虚拟的单入单出(SISO)信道, 主信道容量可表示为

$$C_M^{\text{SMAS-PA}} = \sum_{i=1}^r \lg_2 \left(1 + \frac{P\gamma_i}{QN_0} \lambda_i \right) \quad (20)$$

式(20)中 $r = \min(Q, N_R)$, $\gamma_i = E\{|x_i|^2\}$ 为第 i 根发射天线的发射功率。 λ 为 $\mathbf{H}_M^{\text{SMAS-PA}}$ 的特征值矩阵, λ_i 为第 i 个特征值。

假定发射功率满足约束条件 $\sum_{i=1}^r \gamma_i^{\text{opt}} = Q$, 采用注水算法进行功率分配。

$$\gamma_i^{\text{opt}} = \left(\mu - \frac{QN_0}{P\lambda_i} \right)^+; i = 1, \dots, r \quad (21)$$

式(21)中 γ_i^{opt} 为各天线功率分配的系数, μ 为常数, $(x)^+$ 定义为取 x 的正值部分。因此 SMAS-PA 方案下的主信道容量为

$$C_M^{\text{SMAS-PA}} = \sum_{i=1}^r \lg_2 \left(1 + \frac{P\gamma_i^{\text{opt}}}{QN_0} \lambda_i \right) \quad (22)$$

窃听信道特征矩阵经预处理、并在窃听方采用 MRC 后, 窃听信道等效为

$$\mathbf{H}_W^{\text{SMAS-PA}} = (\mathbf{H}_W^{\text{SMAS}} \mathbf{V}_M \boldsymbol{\gamma})^H \mathbf{H}_W^{\text{SMAS}} \mathbf{V}_M \boldsymbol{\gamma}.$$

将等效窃听信道代入式(2)中得窃听信道容量:

$$C_W^{\text{SMAS-PA}} = \lg_2 \left\{ \det \left(\mathbf{I} + \frac{P}{QN_0} \mathbf{H}_W^{\text{SMAS-PA}} (\mathbf{H}_W^{\text{SMAS-PA}})^H \right) \right\} \quad (23)$$

因此 SMAS-PA 方案的保密容量 $C_S^{\text{SMAS-PA}}$ 由式(15)、式(16)代入式(1)得出。

3 数值结果和仿真分析

3.1 保密容量

按照图 1 所示模型, 采用不同天线选择方案进行对比分析。设定 MIMO 系统的天线数为总发射天线数 $N_T = 8$, 接收天线数 $N_R = 5$, 窃听天线数 $N_E = 5$, 进行 1 500 次蒙塔卡罗仿真。如图 2, 在分别采用最优多天线选择方案(OMAS)、次优多天线选择方案(SMAS)和次优多天线选择-功率分配(SMAS-PA)方案选出不同天线数 Q 的情况下, 系统保密容

量随着信噪比的增大而增大。值得注意的是, 当选出的天线数 $Q = 1$ 时, 所提的 SMAS 和 OMAS 方案等效为 SAS^[11] 和 OAS^[12] 方案, 且 SMAS-PA 方案(单天线不进行功率分配)与 SMAS 方案等效。可以看出, 采用三种方案后, 随着选择天线数 Q 增多, 系统保密容量增大, 从数值上体现了文中所提的三种多天线选择方案在保密容量的提升上优于单天线选择方案。

图 2 中还可观察到, 当选择天线数 Q 相等, 如 $Q = 2$ 时, 采用最优多天线选择 OMAS 方案得到的系统的保密容量最大, SMAS-PA 方案次之, SMAS 方案最小; 然而, 对全局信道状态信息已知的最优多天线选择方案较难实现, 而未知窃听信道状态信息的次优多天线选择方案在低信噪比条件下的保密容量较小, 因此文中提出的次优多天线选择功率分配方案在改善低信噪比条件系统保密容量方面有一定的优势。理论上, 选择更多发射天线进行功率分配, 进一步增大主信道容量的同时在一定程度上对窃听信道容量有恶化效果, 如图 2 中 $Q = 3$ 时, 采用 SMAS-PA 方案相比 SMAS 方案的优势比 $Q = 2$ 时更加明显。

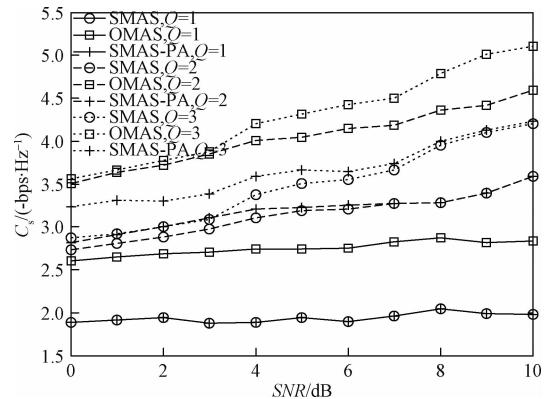


图 2 三种方案在不同天线数目情况下系统的保密容量

Fig. 2 Secrecy capacity versus SNR with different number of antennas using three proposed scheme

3.2 误码率分析

理论推导与数值分析结果表明所提的物理层安全次优多天线选择功率分配方案提升了系统的保密容量, 现设计实例仿真来验证方案的有效性。发送 1 000 组数据, 每组数据由 100 帧随机生成的 QAM 调制信号组成, 每帧数据里包含 $Q \times 2$ 个符号(调制阶数与选择天线数相乘)。发送符号速率 $R_s = 1$ 。设定 MIMO 信道环境服从瑞利衰落, 主信道和窃听信道相互独立同分布, 瑞利随机变量可以由复高斯随机变量 $W_1 + jW_2$ 表示, 其中 W_1 和 W_2 分别为均值为 0、方差为 1 的高斯随机变量(利用 MATLAB 内置

randn 函数产生服从高斯分布的维数分别为 $N_R \times N_T$ 和 $N_E \times N_T$ 的随机变量)。不失一般性,假设信道在每组数据持续时间内保持不变,而在不同数据组之间独立变化。

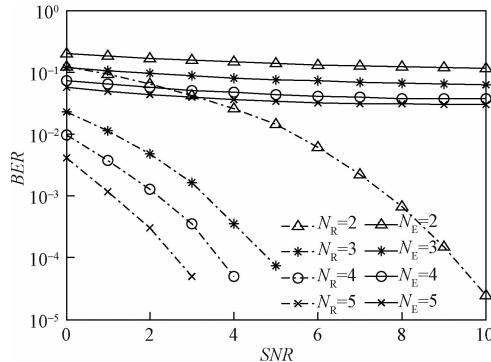


图3 不同接收、窃听天线数目条件下,接收端和窃听端接收误码率随信噪比变化情况

Fig.3 Received BER at the receiver and eavesdropper versus SNR with $N_T = 6$, $Q = 2$, N_R and N_E increase from 2 to 5, respectively

设定发射天线数 $N_T = 8$,选择天线数 $Q = 2$,接收端和窃听端分别采用最大比合并技术接收信号。图3为接收方和窃听方的误码率随着信噪比改变而改变的情况。由图3可以看出,在接收方,随着接收天线数和信噪比变大,接收误码率急剧减小,相反,在窃听方,随着窃听天线数和信噪比增大,窃听误码率仍维持较高。当接收天线数较多时($N_R > 2$),接收方误码率在信噪比较低时误码率较小,即系统可以在低信噪比条件下实现保密传输。因此,采用次优多天线选择功率分配(SMAS-PA)方案后,系统保密性能得到了提升。

4 结论

为保障 MIMO 系统物理层安全,进一步提高系统的保密容量,本文提出发射端多天线选择功率分配方案。文中分别考虑已知全局信道状态信息条件下的最优多天线选择和未知窃听信道状态信息的次优多天线选择,推导判决式、形成选择算法,选出多根天线用于发射信号。由于最优方案对全局信道已知的条件在实际中较难达到,为加强实用性,本文考虑牺牲一定的保密容量性能,采用次优方案。此外,为解决低信噪比条件下系统保密容量较小的问题,本文在次优方案选出多发射天线的基础上采用注水算法进行发射功率分配,进一步增大系统的保密容量。经过数值结果对比分析和接收误码率的仿真实

例验证,可以看出,相比单天线选择方案,本文所提出的多天线方案能达到更大的保密容量,有效地保障低信噪比条件下的保密传输。针对次优多天线选择中对主信道估计存在估计误差的情况可以作为进一步研究内容。

参 考 文 献

- Oggier F, Hassibi B. The secrecy capacity of the MIMO wiretap channel. IEEE International Symposium on Information Theory, 2008;524—528
- Fakoorian S A A, Swindlehurst A L. MIMO interference channel with confidential messages: achievable secrecy rates and precoder design. IEEE Trans Inf Forensics Security, 2011;6(3): 640—649
- Tsai S H, Poor H V. Power allocation for artificial-noise secure MIMO precoding systems. Signal Processing IEEE Transactions on, 2014;62(13):3479—3493
- 侯晓赟,黄庭金,朱艳,等.增强物理层安全的联合发射天线选择和人工噪声技术.信号处理,2014;30(11): 1263—1266
- Hou X Y, Huang T J, Zhu Y, et al. Enhanced physical-layer security through joint transmit antenna selection and artificial noise. Journal of Singal Processing, 2014;30(11): 1263—1266
- Mukherjee A, Swindlehurst A L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. IEEE Trans Signal Process, 2011;59(1):351—361
- Zou Y, Zhu J, Wang X, et al. Improving physical-layer security in wireless communications using diversity techniques. Network IEEE, 2015;29(1):42—48
- Alves H, Souza R D, Debbah M, et al. Performance of transmit antenna selection physical layer security schemes. IEEE Signal Process Letter, 2012;19(6):372—375
- Yang N, Yeoh P L, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans Communications, 2013;61(1):144—154
- Hu Y, Tao X, Xu J, et al. Secrecy outage analysis of transmit antenna selection with switch-and-examine combining over rayleigh fading. Vehicular Technology Conference (VTC Fall), 2014;1—5
- Zou Y, Zhu J, Zheng B. Defending against eavesdropping attack leveraging multiple antennas in wireless networks. Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on, 2013:699—703
- Zhu J, Zou Y, Wang G, et al. On secrecy performance of antenna selection aided MIMO systems against eavesdropping. IEEE Transactions on Vehicular Technology, 2015;1—11
- Gharavi-Alkhansari M, Gershman A B. Fast antenna subset selection in MIMO systems. Signal Processing IEEE Transactions on, 2004;52(2):339—347
- Telatar E. Capacity of multi-antenna Gaussian channels. European Transactions on Telecommunications, 1999;10(6):585—595
- Haykin S. Unsupervised adaptive filtering v. II: blind deconvolution. New York: Wiley, 2000

(下转第 271 页)

Design of Fast Matrix Transposition Algorithm for SAR Image Systems

ZHANG Lan, QIN Si-qi, TANG Rui

(School of Electronics and Information, Wuhan University, Wuhan 430072, P. R. China)

[Abstract] Matrix transpose plays a critical role in the real-time signal processing of SAR, and the efficiency of matrix transpose greatly influences the performance of the signal processing system. Some popular methods are utilized to achieve matrix transpose nowadays. A new matrix transpose method called matrix divide-joint is proposed based on some existing methods and the flexible transfer method of EDMA3. The performance of the proposed method is tested on TMS320C6678. The result demonstrates that this new method performs more efficiently in signal processing of SAR than traditional methods and handles the matrix transpose problem better. The method is 255 times faster than traditional methods when the data size is 512 MB.

[Key words] matrix transpose synthetic aperture radar imaging EDMA3

(上接第 265 页)

Guarantying Physical Layer Security Using Multi-antennas Selection at the Transmitter in MIMO System

CAI Xiao-xia, ZENG Ling-qing, CHEN Hong, ZHU Wen-li

(Department of 402, school of Electronic Engineering, Hefei 230037, P. R. China)

[Abstract] Because the secrecy capacity of MIMO system is limited when utilizing single antenna selection scheme, the multi-antennas selection schemes at the transmitter are proposed to guarantee physical layer security. First, it assumes that the global channel state information of both main channel and wiretap channel is known to the transmitter, and the optimal multi-antennas selection (OMAS) scheme is proposed. Then it consider a more practical condition that the wiretap channel state information is unknown to the transmitter, and the suboptimal multi-antennas selection (SMAS) scheme is come up. Finally, a suboptimal multi-antennas selection and power allocation (SMAS-PA) scheme is considered to improve the secrecy capacity of SMAS scheme in lower signal to noise ratio condition. The secrecy performance of SMAS-PA scheme is discussed then. The expression of secrecy capacity and numerical results demonstrate that the proposed scheme can improve the secrecy capacity of MIMO system effectively with compare to the existing works about antenna selection scheme which selects only one antenna at the transmitter.

[Key words] physical layer security secrecy capacity multi-antennas selection channel state information