多用户 MIMO 系统基于消息块预编码的可信通信技术

朱耀[1,2]，朱义君[1]，张水莲[1]，刘永刚[2]
(1. 国家数字交换系统工程技术研究中心，河南 郑州 450002；2. 61580 部队，北京 100193)

摘 要：针对多用户 MIMO 窃听信道，提出了在未知非法接收者任何信息的前提下，实现可信通信的基于消息块的人为干扰和预编码算法，并且在实现可信通信“可信性”的同时，考虑了“有效性”和“效率”问题。人为干扰仅干扰非法接收者，而不对合法接收者产生任何影响。预编码算法是已有的用于消除多用户干扰的“迫零”方式与基于 SVD 分解的线性预编码方式的结合。与基于单消息符号的预编码方式相比，提高了可信通信的效率。仿真结果表明，其进一步降低了非法接收者的 SINR，并提高了多用户 MIMO 系统的通信容量。

关键词：MIMO；预编码；可信通信；人为干扰
中图分类号：TN918.91 **文献标识码**：B **文章编号**：1000-436X(2012)03-0155-08

Confidential communications technique based on message block precoder in multi-user MIMO systems

ZHU Yao[1,2], ZHU Yi-jun[1], ZHANG Shui-lian[1], LIU Yong-gang[2]
(1. China National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China;
2. Unit 61580, Beijing 100193, China)

Abstract: For confidential communications in a multi-user MIMO wiretap channel, though no information regarding the illegitimate receiver was presumed at the transmitter, an artificial interference and a precoding technique based on message block were proposed. Except for confidentiality, the effectivity and efficiency of confidential communications were also taken into consideration. The artificial interference selectively degraded the passive illegitimate receiver' signal while did not effect every legitimate receiver. The precoding technique combined the existed zero-forcing method that used to eliminate the multi-user interference with singular value decomposition (SVD)-based linear precoder so that enhances the efficiency of confidential communications. Simulation result shows that this precoding method degrades the illegitimate receiver' signal to interference plus noise ratio (SINR) even more and enhances the capacity of multi-user MIMO system compared with the precoding method based on single message symbol.

Key words: MIMO; precoder; confidential communications; artificial interference

1 引言

无线通信的广播特性决定了它的不安全性，在通信信号传播范围内的非法接收者很容易获得通信双方的通信内容。众所周知，为了防止通信的消息被非法接收者获得，一般使用应用在数据链路层或更高层的加密技术来对通信数据进行加密处理，这样即使通信信号被非法接收者截获，但由于破译运算的异常复杂性，非法接收者依然无法获得通信的消息。随着计算机运算速度等性能的不断提升，加密数据被非法接收者破译的风险正在逐渐加大。因此，对通信双方来说，采用了加密技术的传统通

收稿日期：2011-01-19；**修回日期**：2011-06-18
基金项目：国家重大科技专项基金资助项目（2009ZX03003-005, 2009ZX03007-003）
Foundation Item: The National Sci-Tech Major Special Item (2009ZX03003-005, 2009ZX03007-003)

信方式仍然是不可信任的。针对这种情况有必要在更底层的物理层采取某种方式，使得非法接收者根本无法获得通信的信息，即从信息论的角度来说，使得发射者与非法接收者之间的互信息很小甚至为零，从而最终实现可信通信的目标。

1975 年，Wyner 从信息论的基本原理出发，研究了有关单天线系统的传输有效性、可靠性和安全性的关系，给出了经典的窃听信道模型[1]。文献[2~7]在此模型下，引入了多输入多输出（MIMO）系统安全容量的概念，并推导证明了单用户 MIMO 系统的完美安全容量是合法接收者与非法接收者分别与发射者之间的互信息之差。文献[2,8]基于信道广义奇异值分解（GSVD），将发射者和合法接收者之间的信道和发射者与非法接收者之间的信道同时转化为并行子信道，进而简化了单用户 MIMO 安全容量的求解过程。但是，针对多用户 MIMO 广播信道，安全容量仍然是一个开放的问题。多用户 MIMO 系统实现可信通信的文献往往假设发射者已知非法接收者的完美信道信息，包括非法接收者的天线数目，或者至少已知关于非法接收者的信道概率分布，而这些信息在实际中是很难获得的。由此，大量文献致力于研究在发射者未知非法接收者任何信息情况下的可信通信策略。文献[9,10,11,13]采用人为干扰的策略来实现可信通信。发射者的一部分发射功率用来广播消息信号，这部分功率仅能保证各合法接收者刚好达到所需的信干噪声比（SINR）而能够正确恢复原始信号，剩余的功率用来广播人为干扰，从而干扰非法接收者获得消息。设计的人为干扰与各合法接收者接收到的消息信号正交，从而保证了人为干扰只对非法接收者的 SINR 产生影响。文献[9,10]在保证合法接收者服务质量（QoS）的情况下，尽可能地增加人为干扰功率，最大程度地影响非法接收者的接收。这一思想也成为当前研究 MIMO 可信通信的主流方向。另外，文献[12]指出，在发射者能够获得非法接收者信道信息的情况下，增加人为干扰的方法并不是最佳的。

针对各合法接收者的消息相互独立的 MIMO 下行广播信道，文献[13]给出了基于单消息符号的预编码方式，预编码矢量为对广义信道进行 SVD 分解后的最小奇异值所对应的特征矢量。这样设计的优点是：预编码矢量不仅使得多用户干扰降到最低，同时使得消息信号沿着一个子信道进行传播，其方向性更强，从可信、安全的角度来说此设计方法无疑是最佳的。该设计的不足之处是：①仍然仅考虑了通信的可信性而没有考虑通信的有效性。由于奇异值的大小反映了子信道的优劣，因此，上述子信道一定是最差的，导致发射者与合法接收者之间的有效性较低。事实上，通信的“可信性”完全可以通过较高发射功率下的人为干扰来保证，其对“方向性”的要求可以降低。这样有必要在可信通信中考虑通信的有效性，尽量提高可信通信的效率。②基于单消息符号的预编码矢量将单消息符号分别映射到每一根发射天线，从空间的角度看，无法再进行其他的变换，因此，其对空间的挖掘程度不够高。基于消息块的预编码矩阵与消息块矩阵相乘实际上包含一个将单消息符号加权累加的作用，可以理解为对消息符号的简单加密，增加了非法接收者破译的难度。另一方面，基于消息块的预编码矩阵相对于基于单消息符号的预编码矢量，其在“空间”范畴上的变换更加灵活，有利于充分利用 MIMO 信道，从而提高可信通信的效率。

综上分析，本文在多用户 MIMO 下行链路和发射者未知非法接收者任何信息的假设下，研究了利用人为干扰实现可信通信的块预编码技术，给出了最佳预编码矩阵，比较了基于单消息符号的预编码方式与基于消息块的预编码方式下的合法接收者与非法接收者的 *SINR*、可信性、发射者和合法接收者之间的信道容量（有效性）以及两者的可信通信效率。研究表明，块预编码方式下可信通信的效率更高。但是，通常需要付出较大的计算代价。

2 多用户 MIMO 系统窃听信道模型

多用户 MIMO 系统窃听信道模型如图 1 所示，该模型假设存在一个发射者、K 个合法接收者和一个非法接收者（可以将此非法接收者理解为众多非法接收者中的任意一个），发射者与非法接收者分别配置 N_A 和 N_E 根天线，合法接收者 i 配置 N_{B_i} 根天线。又设发射者向合法接收者 i 发射的消息块为

$$\boldsymbol{z}_i = \begin{bmatrix} a_{11}^{(i)} & \cdots & a_{1m}^{(i)} \\ \vdots & & \vdots \\ a_{r_i1}^{(i)} & \cdots & a_{r_im}^{(i)} \end{bmatrix}_{r_i \times m} \tag{1}$$

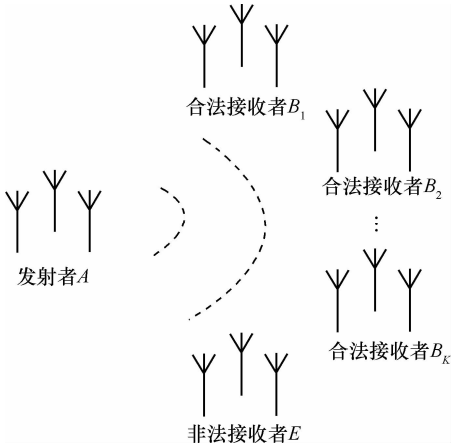


图 1　多用户 MIMO 系统窃听信道模型

其中，$a_{jk}^{(i)}$ $(1\leqslant j\leqslant r_i, 1\leqslant k\leqslant m)$表示发射者向合法接收者 i 发射消息流中的某一消息符号，m 由系统根据信道的时变特性来设定，这里假设 m 已知，且各合法接收者的 m 值相同，r_i 与发射者与各合法接收者之间的信道状况有关，由下文给出，另外，假设非法接收者仅对合法接收者 i 的消息感兴趣。这样，发射者发射给所有 K 个合法接收者的消息记为 $\boldsymbol{Z}=\left[(\boldsymbol{z}_1)^{\mathrm{T}},\cdots,(\boldsymbol{z}_K)^{\mathrm{T}}\right]^{\mathrm{T}}_{(r_1+\cdots+r_K)\times m}$。发射者的预编码矩阵记为 $\boldsymbol{F}=\left[\boldsymbol{F}_{B_1},\cdots,\boldsymbol{F}_{B_K}\right]$，其中，$\boldsymbol{F}_{B_i}$ $(1\leqslant i\leqslant K)$ 是与合法接收者 i 相关的预编码矩阵，且 $\boldsymbol{F}_{B_i}\boldsymbol{F}_{B_i}^{\mathrm{H}}=\boldsymbol{I}$。令 $\boldsymbol{H}=\left[(\boldsymbol{H}_{B_1})^{\mathrm{T}},\cdots,(\boldsymbol{H}_{B_K})^{\mathrm{T}}\right]^{\mathrm{T}}_{\sum_{i=1}^{K}N_{B_i}\times N_A}$，其中，$\boldsymbol{H}_{B_i}$ $(1\leqslant i\leqslant K)$ 为发射者和合法接收者 i 之间的信道增益矩阵，且其各元素独立同分布，服从均值为 0，方差为 1 的循环对称复高斯分布。假设发射者和合法接收者之间的信道为准静态平坦衰落信道，并且发射者能够获得这些信道的完美信道信息。记 $\boldsymbol{Y}=\left[(\boldsymbol{y}_{B_1})^{\mathrm{T}},\cdots,(\boldsymbol{y}_{B_K})^{\mathrm{T}}\right]^{\mathrm{T}}$，其中，$\boldsymbol{y}_{B_i}$ $(1\leqslant i\leqslant K)$ 为合法接收者 i 的接收信号，则

$$\boldsymbol{Y}=\boldsymbol{HFZ}+\boldsymbol{N} \tag{2}$$

其中，$\boldsymbol{N}=\left[(\boldsymbol{n}_{B_1})^{\mathrm{T}},\cdots,(\boldsymbol{n}_{B_K})^{\mathrm{T}}\right]^{\mathrm{T}}_{\sum_{i=1}^{K}N_{B_i}\times m}$，$n_{B_i}$ $(1\leqslant i\leqslant K)$ 为各合法接收者收到的加性高斯白噪声，其噪声协方差为 $\mathrm{E}(n_{B_i}n_{B_i}^{\mathrm{H}})=\sigma_{B_i}^2\boldsymbol{I}$。假设发射者发射功率受限，发射者对合法接收者 i 分配的功率为

$$\begin{cases}\mathrm{E}(\boldsymbol{z}_i\boldsymbol{z}_i^{\mathrm{H}})=\boldsymbol{Q}_{B_i}\\ \mathrm{Tr}(\boldsymbol{Q}_{B_i})=\rho_{B_i}P\end{cases} \tag{3}$$

其中，ρ_{B_i} 是用户 i 的功率比例因子。

3　利用人为干扰实现可信通信

从信息论的角度来说，可信通信的目标是使得发射者与非法接收者之间的互信息很小甚至为零。然而，在发射者无法获得非法接收者任何信息的假设下，很难用“互信息”这一指标来评判是否实现了可信通信。因此，使用“信干噪声比”代替“互信息”作为衡量的标准，认为接收者的 SINR 越低，其接收能力就越差，发射者与此接收者之间的互信息也越小。

3.1　人为干扰的思想

发射者不仅要发射消息块 Z，而且还额外发射人为干扰 $\boldsymbol{z}'$，以此干扰非法接收者的窃听。发射者通过利用已知的各合法接收者的信道信息，设计特殊的人为干扰，使得人为干扰正交于各合法接收者的信道，从而不会对各合法接收者的正常接收产生影响，即保证各合法接收者达到能够恢复信号所需的最低 SINR，同时令非法接收者的 SINR 急剧下降，导致其无法恢复信号，从而实现了可信通信[9,10,13]。

本文利用上述思想，首先设计人为干扰矩阵，然后通过预编码技术，在发射总功率受限以及保证各合法接收者所要求的最低 SINR 条件下，尽量增大分配到人为干扰上的发射功率，从而令非法接收者的 SINR 减小，同时在可信通信中考虑通信有效性的问题，尽量使得发射者与合法接收者的通信有效性提高，最终提高可信通信的效率。易知

$$\boldsymbol{Y}=\boldsymbol{HFZ}+\boldsymbol{Hz}'+\boldsymbol{N} \tag{4}$$

其中，用户 i 收到信号可以被表示为

$$\boldsymbol{y}_{B_i}=\boldsymbol{H}_{B_i}\boldsymbol{F}_{B_i}\boldsymbol{z}_i+\boldsymbol{H}_{B_i}\sum_{j=1,j\neq i}^{K}\boldsymbol{F}_{B_j}\boldsymbol{z}_j+\boldsymbol{H}_{B_i}\boldsymbol{z}'+\boldsymbol{n}_{B_j} \tag{5}$$

式(5)中第 1 项与接收者 i 的消息有关；第 2 项为 MIMO 系统的多用户干扰，设计的预编码矩阵的一个作用就是要消除多用户干扰；第 3 项是人为干扰项，人为干扰的设计目标就是要令此项为 0。非法接收者收到的信号表示为

$$\boldsymbol{y}_E=\boldsymbol{H}_E\boldsymbol{F}_{B_i}\boldsymbol{z}_i+\boldsymbol{H}_E\sum_{j=1,j\neq i}^{K}\boldsymbol{F}_{B_j}\boldsymbol{z}_j+\boldsymbol{H}_E\boldsymbol{z}'+\boldsymbol{n}_E \tag{6}$$

其中，$\boldsymbol{H}_E$ 为发射者与非法接收者之间的信道增益矩阵，$\boldsymbol{n}_E$ 为非法接收者收到的加性高斯白噪声，其噪声协方差为 $\mathrm{E}\left(\boldsymbol{n}_E\boldsymbol{n}_E^{\mathrm{H}}\right)=\sigma_E^2\boldsymbol{I}$。式(6)第 1 项为非法接收者期望接收到的合法接收者 i 的消息；第 2 项是其他合法接收者的消息对期望信号的干扰；第 3 项

是人为干扰信号。发射者分配给人为干扰的功率为

$$\mathrm{E}\left(\boldsymbol{z}'\boldsymbol{z}'^{\mathrm{H}}\right)=\boldsymbol{Q}_{z'}$$
$$\mathrm{Tr}\left(\boldsymbol{Q}_{z'}\right)=\left(1-\sum_{i=1}^{K}\rho_{B_i}\right)P \tag{7}$$

3.2 人为干扰的设计

假设 $\sum_{i=1}^{K}N_{B_i}<N_A$，对 $\boldsymbol{H}$ 进行奇异值分解(SVD) $\boldsymbol{H}=\boldsymbol{U}\sum\left[\boldsymbol{V}_1^{(1)}\cdots\boldsymbol{V}_{\mathrm{rank}(\boldsymbol{H})}^{(1)}\boldsymbol{V}_{\mathrm{rank}(\boldsymbol{H})+1}^{(0)}\cdots\boldsymbol{V}_{N_A}^{(0)}\right]^{\mathrm{H}}$，其中，$\boldsymbol{U}$ 为酉矩阵，$\sum$ 为对角阵，$\boldsymbol{V}_1^{(1)},\cdots,\boldsymbol{V}_{\mathrm{rank}(\boldsymbol{H})}^{(1)}$，$\boldsymbol{V}_{\mathrm{rank}(\boldsymbol{H})+1}^{(0)},\cdots,\boldsymbol{V}_{N_A}^{(0)}$ 从左到右分别是从大到小排列的奇异值对应的特征矢量。$\boldsymbol{V}_p^{(0)}(\mathrm{rank}(\boldsymbol{H})+1\leqslant p\leqslant N_A)$ 表示零奇异值对应的特征矢量。$\boldsymbol{V}_p^{(1)}\ \left(1\leqslant p\leqslant\mathrm{rank}(\boldsymbol{H})\right)$ 表示非零奇异值对应的特征矢量。令

$$\boldsymbol{z}''=\sum_{i=\mathrm{rank}(\boldsymbol{H})+1}^{N_A}\boldsymbol{V}_i^{(0)} \tag{8}$$

则

$$\boldsymbol{z}'=\left[\boldsymbol{z}''\ \cdots\ \boldsymbol{z}''\right]_{N_A\times m} \tag{9}$$

$$\boldsymbol{H}\boldsymbol{z}'=\begin{bmatrix}\boldsymbol{H}_{B_1}\\ \vdots\\ \boldsymbol{H}_{B_K}\end{bmatrix}\boldsymbol{z}'=\begin{bmatrix}\boldsymbol{H}_{B_1}\boldsymbol{z}'\\ \vdots\\ \boldsymbol{H}_{B_K}\boldsymbol{z}'\end{bmatrix}=0 \tag{10}$$

式(10)中 $\boldsymbol{H}_{B_i}\boldsymbol{z}'=\boldsymbol{0}\ (1\leqslant i\leqslant K)$，即发射者的人为干扰没有对合法接收者产生任何影响。另外，式(8)主要考虑到：从可信通信的角度，在无法获得非法接收者信息（包括位置信息）的情况下，将人为干扰分布在尽可能多的空间方向上是最佳的。

做 $\sum_{i=1}^{K}N_{B_i}<N_A$ 的假设主要是考虑到 $\boldsymbol{H}$ 和下文提到 $\bar{\boldsymbol{H}}_i$ 的 SVD 分解一定存在一个或多个零奇异值。从空间的角度考虑，这些零奇异值对应的特征矢量正好处于某些合法接收者信道的零空间。在工程实践中实现这一假设并不困难。

3.3 基于消息块的预编码矩阵的设计

基于消息块的预编码矩阵设计要实现 2 个目标：①通过“迫零”的方法消除多用户干扰，在各合法接收者所要求 SINR 一定的条件下，使得发射者分配到消息信号上的功率减小，从而，在发射总功率受限的条件下，使得人为干扰功率增大，增加对非法接收者的影响。②通过 SVD 分解及功率“注水”技术，在发射者分配到消息数据上的功率一定的情况下，提高发射者与合法接收者之间的有效性。由此，预编码矩阵的作用是提高多用户 MIMO 系统的可信通信的效率。

接收者 i 的预编码矩阵可以通过如下方法设计，令 $\bar{\boldsymbol{H}}_i=\left[\left(\boldsymbol{H}_{B_1}\right)^{\mathrm{T}}\cdots\left(\boldsymbol{H}_{B_{i-1}}\right)^{\mathrm{T}}\left(\boldsymbol{H}_{B_{i+1}}\right)^{\mathrm{T}}\cdots\left(\boldsymbol{H}_{B_K}\right)^{\mathrm{T}}\right]^{\mathrm{T}}$，同样假设 $\sum_{i=1}^{K}N_{B_i}<N_A$，对 $\bar{H}_i$ 进行 SVD 分解[14]

$$\bar{\boldsymbol{H}}_i=\bar{\boldsymbol{U}}_i\bar{\sum}_i\left[\bar{\boldsymbol{V}}_i^{(1)}\ \bar{\boldsymbol{V}}_i^{(0)}\right]^{\mathrm{H}} \tag{11}$$

其中，$\bar{\boldsymbol{V}}_i^{(1)}$ 代表所有非零奇异值对应的特征矢量组成的矩阵，$\bar{\boldsymbol{V}}_i^{(0)}$ 代表所有零奇异值对应的特征矢量组成的矩阵，记 $N_i=N_A-rank\left(\bar{\boldsymbol{H}}_i\right)$，则 $\bar{\boldsymbol{V}}_i^{(0)}$ 的维度为 $N_A\times N_i$。令

$$\boldsymbol{F}_{B_i}'=\bar{\boldsymbol{V}}_i^{(0)} \tag{12}$$

表示发射者为消除多用户干扰而设计的“迫零”预编码矩阵。这样，多用户 MIMO 系统变为多个单用户 MIMO 系统。发射者与合法接收者 i 之间的等效信道变为 $\hat{\boldsymbol{H}}_{B_i}=\boldsymbol{H}_{B_i}\boldsymbol{F}_{B_i}'$。为了进一步减小发射者需要分配到消息数据上的功率以及在可信通信中同时考虑通信的有效性及效率问题，故对 $\hat{\boldsymbol{H}}_{B_i}$ 进行 SVD 分解[14]：

$$\hat{\boldsymbol{H}}_{B_i}=\hat{U}_i\hat{\sum}_i[\hat{\boldsymbol{V}}_1^{(i)}\cdots\hat{\boldsymbol{V}}_{N_i}^{(i)}]^{\mathrm{H}} \tag{13}$$

这里，$\hat{\boldsymbol{V}}_1^{(i)},\cdots,\hat{\boldsymbol{V}}_{N_i}^{(i)}$ 是从大到小排列的奇异值对应的特征矢量。由此，可以将等效信道 $\hat{\boldsymbol{H}}_{B_i}$ 看作并行的子信道，特别地，这些子信道的信道状况与 $\hat{\boldsymbol{H}}_{B_i}$ 的奇异值大小有关，奇异值越大，表示该子信道受加性高斯白噪声的影响越小，越有利于传输消息。在此基础上，对这些并行子信道进行功率的“注水”分配，舍弃受噪声影响较大的子信道。记剩余的较好子信道数为 L_i。且令 $\boldsymbol{F}_{B_i}''=[\hat{\boldsymbol{V}}_1^{(i)}\cdots\hat{\boldsymbol{V}}_{L_i}^{(i)}]$ 表示由大到小排列的前 L_i 个奇异值对应的特征矢量组成的矩阵，其维度为 $N_i\times L_i$。则

$$\boldsymbol{F}_{B_i}=\boldsymbol{F}_{B_i}'\boldsymbol{F}_{B_i}'' \tag{14}$$

即合法接收者 i 的预编码矩阵的一部分用来消除多用户干扰；另一部分用来将信道转变成并行的子信道，而这些并行子信道是通过功率“注水”技术得

到的优质信道。通信消息仅在这些子信道上传输，从而提高了发射者的功率效率，这样在各合法接收者所需的 SINR 一定的条件下，增大了人为干扰的功率，即增大了对非法接收者的影响，在发射者分配给消息信号功率一定的条件下，提高了可信通信的容量。上述本质上反映了可信通信效率的提高。特别地，

$$r_i = L_i \tag{15}$$

也就是：发射者向合法接收者 i 发射的消息块矩阵的行数为 $\hat{\boldsymbol{H}}_{B_i}$ 奇异值分解形成的子信道经功率“注水”后剩余较好的子信道数。

若合法接收者 i 使用 $\boldsymbol{w}_{B_i}$ 来预处理信号，则其信干噪声比为

$$SINR_{B_i} = \frac{\mathrm{Tr}(\boldsymbol{w}_{B_i}^{\mathrm{H}}\boldsymbol{H}_{B_i}\boldsymbol{F}_{B_i}\boldsymbol{Q}_{B_i}\boldsymbol{F}_{B_i}^{\mathrm{H}}\boldsymbol{H}_{B_i}^{\mathrm{H}}\boldsymbol{w}_{B_i})}{\mathrm{Tr}(\sigma_{B_i}^2\boldsymbol{w}_{B_i}^{\mathrm{H}}\boldsymbol{w}_{B_i})} \tag{16}$$

其中，$\boldsymbol{Q}_{B_i}$ 为发射者经功率“注水”后发射信号协方差，其主对角线之和为 $\rho_{B_i}P$，因此，若合法接收者 i 能够恢复信号所需的最低信干噪声比为 $SINR'_{B_i}$，则一定可以通过计算或者搜索的方法得到用户 i 的功率比例因子 ρ_{B_i}，使得 $SINR_{B_i} = SINR'_{B_i}$。

假定非法接收者仅对接收者 i 的消息 $\boldsymbol{z}_i$ 感兴趣，且其接收预处理矩阵为 $\boldsymbol{w}_E$，则存在多用户干扰和人为干扰的非法接收者的信干噪声比为

$$SINR_E = \frac{\mathrm{Tr}(\boldsymbol{w}_E^{\mathrm{H}}\boldsymbol{H}_E\boldsymbol{F}_{B_i}\boldsymbol{Q}_{B_i}\boldsymbol{F}_{B_i}^{\mathrm{H}}\boldsymbol{H}_E^{\mathrm{H}}\boldsymbol{w}_E)}{\mathrm{Tr}(\boldsymbol{s}_p + \boldsymbol{z}'_p + \boldsymbol{n}_p)} \tag{17}$$

其中，

$$n_p = \sigma_E^2\boldsymbol{w}_E^{\mathrm{H}}\boldsymbol{w}_E \tag{18}$$

$$\boldsymbol{z}'_p = \left(1 - \sum_{i=1}^{K}\rho_{B_i}\right)P\boldsymbol{w}_E^{\mathrm{H}}\boldsymbol{H}_E\boldsymbol{H}_E^{\mathrm{H}}\boldsymbol{w}_E \tag{19}$$

$$s_p = \boldsymbol{w}_E^{\mathrm{H}}\boldsymbol{H}_E\left(\sum_{j=1,\,j\neq i}^{K}\boldsymbol{F}_{B_j}\left(\rho_{B_j}P\right)\boldsymbol{F}_{B_j}^{\mathrm{H}}\right)\boldsymbol{H}_E^{\mathrm{H}}\boldsymbol{w}_E \tag{20}$$

其中，n_p 为信道噪声的成分，$\boldsymbol{z}'_p$ 为人为干扰成分，s_p 是多用户干扰的成分。在上述 3 种成分的作用下，非法接收者的信干噪声比急剧下降，最终导致其无法获得通信的消息，达到了可信通信的目标。

人为干扰和预编码矩阵的设计主要依赖于发射者假设能够获得各合法接收者完美精确的信道信息。在工程实践中，若发射者获得的各合法接收者的信道信息存在误差，则人为干扰和多用户干扰对各合法接收者将产生一定程度的影响，导致各合法接收者的 SINR 降低，而且，将对发射者与合法接收者之间优异子信道的选择和功率“注水”产生影响，致使通信有效性的降低，最终降低了可信通信的效率，因此，发射者有必要通过各种方法获得各合法接收者完美的信道信息。

3.4　可信通信的效率

在人为干扰机制下，发射者与合法接收者 i 之间的通信容量可表示为[15,16]

$$C_i = \max_{tr(\boldsymbol{Q}_{B_i})\leqslant\rho_{B_i}P}\log\det\left[I + \frac{\boldsymbol{w}_{B_i}\boldsymbol{H}_{B_i}\boldsymbol{F}_{B_i}\boldsymbol{Q}_{B_i}\boldsymbol{F}_{B_i}^{\mathrm{H}}\boldsymbol{H}_{B_i}^{\mathrm{H}}\boldsymbol{w}_{B_i}^{\mathrm{H}}}{\sigma_{B_i}^2}\right] \tag{21}$$

从式(12)和(14)可知，预编码矩阵 $\boldsymbol{F}_{B_i}\ (1\leqslant i\leqslant K)$ 消除了多用户干扰，因此，人为干扰机制下的多用户 MIMO 系统的可信通信容量为

$$C = \sum_{i=1}^{K}C_i \tag{22}$$

令

$$\rho = \sum_{i=1}^{K}\rho_{B_i} \tag{23}$$

假设不考虑各合法接收者的预处理方式，由式(21)~式(23)可知，在合法接收者的信道和预编码矩阵 $\boldsymbol{F}$ 一定条件下，C 与 ρP 有关，即发射者分配给消息信号的功率越大，可信通信的容量越高。从这个角度来说，人为干扰的引入势必减小了可信通信的容量，造成了发射功率的浪费。另外，在信道和总功率 P 和 ρ 一定条件下，C 与 $\boldsymbol{F}$ 有关。这里，由于 $\boldsymbol{F}$ 的不同而导致 C 的高低恰好反映了可信通信效率的高低。

可信通信的效率包含两层含义：①在发射总功率和分配到各合法接收者消息信号上的功率相同的条件下，发射者与合法接收者的有效性（通信容量）越大，根据香农公式，在一定的条件下，表明合法接收者的 SINR 越高（注：下文直接认为通信容量大等同于各合法接收者的 SINR 高），可信通信的效率就越高；②在发射总功率和各合法接收者所要求的最低 SINR 相同的条件下，非法接收者的 SINR 越低，可信通信的效率就越高。因此，可信

通信的效率可以表示为

$$\eta=\frac{\frac{1}{K}\sum_{i=1}^{K}SINR_{B_i}}{\frac{1}{K}\sum_{i=1}^{K}SINR_{B_i}+SINR_E} \tag{24}$$

式(24)的分子项和分母第 1 项间接地反映了发射者与合法接收者之间的通信的“有效性”，分母第 2 项反映了通信的“可信性”。若发射总功率受限，“可信性”要求发射者尽可能地将功率分配给人为干扰，而“有效性”则要求尽可能地将其分配给消息信号，因此，两者需要折中考虑。从式(24)知，在“有效性”一定时，“可信性”越高，即 $SINR_E$ 越小，可信通信的效率越高。在“可信性”一定时，“有效性”越大，可信通信的效率越高。事实上，可信通信的效率越高，表明在相同的消息信号功率下，发射者与合法接收者之间的容量有效性越高，在一定的条件下，反映出合法接收者的接收 SINR 越高。反过来，在合法接收者所需的 SINR 相同的情况下，可信通信的效率越高，则发射者分配到消息信号上的功率就越少，这样在相同的发射总功率下，人为干扰的功率就越大，导致对非法接收者的影响也越大，即通信的可信性越高。

4　数值仿真和比较

图 2 显示在发射者采用人为干扰的方式下，各合法接收者与非法接收者 SINR 的对比，反映了各合法接收者与非法接收者的相对接收能力。仿真假设发射者天线数为 8，各合法接收者和非法接收者的天线数都为 2，用户数为 3，各信道增益矩阵的元素服从循环复高斯随机分布，合法接收者与非法接收者都使用相同的最佳线性预处理技术，并且假定各合法接收者要求的 SINR 分别为 18dB、15dB、12dB，非法接收者对合法接收者 1 的数据感兴趣。由图 2 可见，在发射功率较小时，非法接收者与各合法接收者的 SINR 的变化趋势相同，这是由于在各合法接收者未达到所要求的 SINR 时，没有多余的功率用来发射人为干扰。但是，在合法接收者达到要求的 SINR 后，非法接收者的 SINR 随着发射功率的增加急剧地下降，这是由于发射者将多余的功率全部分配给了人为干扰。图 2 充分反映了利用人为干扰恶化非法接收者接收能力的实际效能。

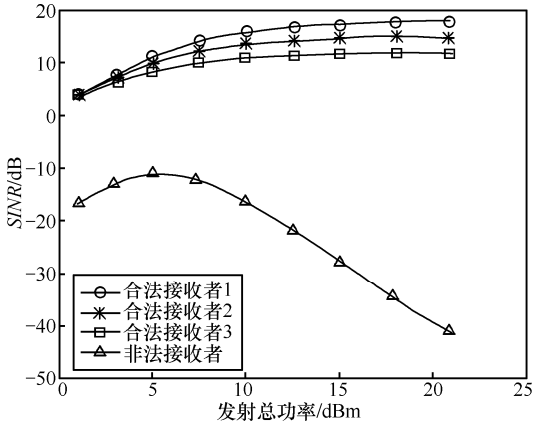


图 2　人为干扰对各合法接收者与非法接收者的影响

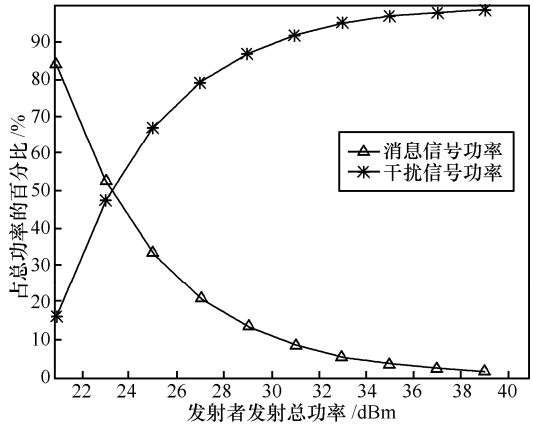


图 3　人为干扰机制下各信号功率占总功率的百分比

图 3 显示了发射者分别分配到消息数据和人为干扰的功率占总功率的百分比。仿真假设存在 4 个合法接收者，其要求的 SINR 相同且为 14dB。由图 3 可见，随着发射功率的提高，所有合法接收者的总消息信号功率所占的比重逐渐降低，同时干扰信号功率所占的比重则不断提高。

图 4 显示了在发射者与合法接收者的天线对分别是（8，2）和（11，3）时，是否采用人为干扰对通信容量的影响对比。仿真假设存在 3 个合法接收者，其要求的 SINR 相同且为 5dB。由图 4 可见：①在发射功率小于 10dBm 时，存在或不存在人为干扰时的通信容量是相同的，且都随发射功率的提高而增大。在发射功率大于 10dBm 时，不存在人为干扰时通信容量仍随发射功率的提高而增大，但存在人为干扰时的通信容量保持不变，这是由各合法接收者所要求的最低 SINR 决定的；②发射功率越大，存在人为干扰与不存在人为干扰时的通信容量的差异越大，其本质反映的是通信效率的降低。图 4 间接表明发射者分配到消息信号上的功率越大，则通信的有效性就越高。

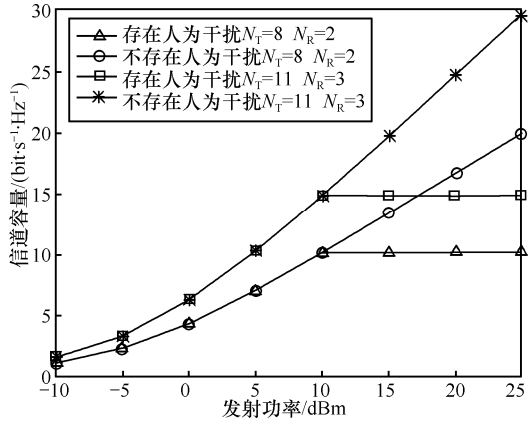


图 4　是否采用人为干扰对发射者与合法接收者通信容量的影响对比

图 5 给出了在发射者分配给消息信号的功率相同的条件下，发射者分别采用单符号和块预编码方式下的任意一个合法接收者与发射者之间通信容量的对比。仿真假设发射者、合法接收者的天线数分别为（8，2）和（17，5），各信道增益矩阵的元素服从循环复高斯随机分布。由图 5 可见，块预编码方式下的信道容量要高于单符号预编码方式下的信道容量。表明与单符号预编码方式相比，块预编码方式有更高的通信有效性。

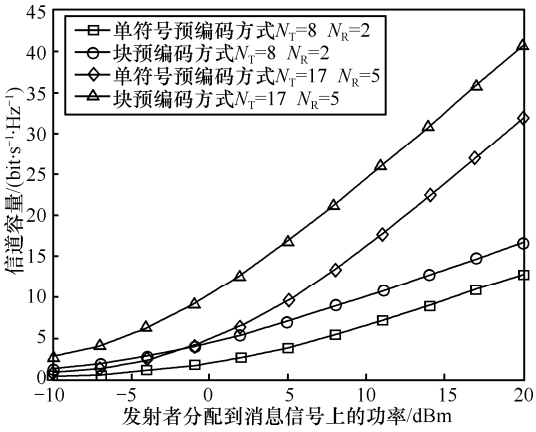


图 5　2 种预编码方式下发射者与合法接收者之间的信道容量对比

图 6 比较了单符号预编码与块预编码 2 种方式下实现可信通信的性能对比。仿真假设发射者、各合法接收者和非法接收者的天线数分别为 16、4 和 8，各信道增益矩阵的元素服从循环复高斯随机分布，合法接收者与非法接收者都使用相同的最佳线性预处理技术，假定非法接收者对合法接收者 1 的数据感兴趣，而且，合法接收者 1 要求的 SINR 为 25dB。由图 6 可见，在相同的发射功率下，合法接收者在块预编码方式下的 SINR 比单符号预编码方式下的 SINR 更高，而非法接收者采用块预编码方式的 SINR 却比单符号预编码方式下的 SINR 更低。从功率的角度考虑，由于基于消息块和单消息符号的人为干扰的设计在本质上没有区别，因此，图 6 实际上反映了块预编码方式比单符号预编码方式有更高的可信通信效率。

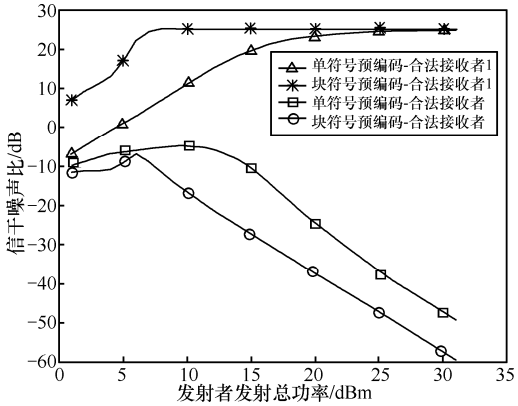


图 6　单符号与块预编码方式下的信干噪声比对比

图 7 直接比较了单符号预编码与块预编码方式下的可信通信效率。仿真条件同上。由图 7 可知，与单符号预编码方式相比，块预编码方式下的可信通信效率更高，且随着总功率的不断增加，单符号方式和块预编码方式下的可信通信效率都将趋于 1。这是由于随着总功率的增加，发射者分配给人为干扰的功率急剧增加，导致非法接收者的 SINR 趋于零。

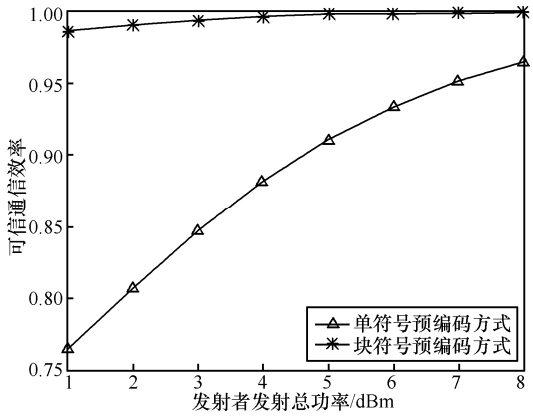


图 7　单符号与块预编码方式下的可信通信效率对比

5　结束语

本文研究了多用户 MIMO 系统实现可信通信的人为干扰技术，在基于单消息符号的预编码方式的基础上引入了基于消息块的预编码方式，使得一方面能够消除多用户干扰，另一方面，通过 SVD 分解，将信道转化成并行子信道并采用功率的“注

水”技术，将全部消息集中到优质子信道上传输，进一步提高了功率效率，在满足各合法接收者所要求的最低 SINR 前提下，增大了人为干扰对非法接收者的影响，同时在可信通信中考虑了通信的有效性，最终提高了可信通信的效率。

本文的研究均基于发射者能够获得合法接收者的完美信道信息以及信道为平坦慢衰落信道的假设。针对非完美的信道信息、快衰落以及频率选择性信道等情况，如何实现可信通信以及在人为干扰的机制下，如何进一步提高可信通信的效率，还需要继续研究。

参考文献：

[1] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[2] KHISTI A, WORNELL G. W. Secure transmission with multiple antennas II: the MIMOME wiretap channel[J]. IEEE Trans Inform, Theory, 2010, 56(11):5515-5532.

[3] OGGIER F, HASSIBI B. The secrecy capacity of the MIMO wiretap channel[J].IEEE Trans Inform Theory, 2001, 57(8): 4961-4972.

[4] LI J, PETROPULU. A. Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels[A]. Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP`10)[C]. Dallas, 2010. 3362-3365.

[5] LIU R, LIU T, POOR H V, *et al*. The capacity-equivocation region of the MIMO Gaussian wiretap channel[A]. Proceedings of IEEE International Conference on International Symposium on Information Theory(ISIT'10)[C]. Austin, Texas, 2010. 2568-2572

[6] EKREM E, ULUKUS S. Capacity-Equivocation Region of the Gaussian MIMO Wiretap Channel[EB/OL]. http://arxiv.org/abs/1005.0419.

[7] EKREM E, ULUKUS S. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel[EBOL]. http://arxiv.org/PScache/ arxiv/pdf/0903/0903.3096v1.pdf.

[8] FAKOORIAN S, SWINDLEHURST A L. Optimal power allocation for GSVD-based beamforming in the MIMO wiretap channel[EB/OL]. http://arxiv:1006.1890. 2010.

[9] SWINDLEHURST A L. Fixed SINR solutions for the MIMO wiretap channel[A]. Proceedings of IEEE Conference on Acoustics Speech and Signal Processing (ICASSP`09)[C]. Taipei, 2009.2437-2440.

[10] MUKHERJEE A, SWINDLEHURST A L. Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels[A]. Proceedings of IEEE Conference on Signal Processing Advances in Wireless Communication (SPAWC `09)[C]. Perugia, 2009. 343-348.

[11] ZHOU X, MCKAY M R. Physical layer security with artificial noise: Secrecy capacity and optimal power allocation[A]. Proceedings of 2009 Conference on Signal Processing and Communication Systems[C]. Omaha, 2009.

[12] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

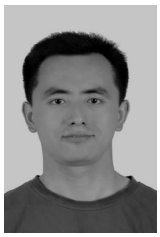
[13] MUKHERJEE A, SWINDLEHURST A L. Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels[A]. Proceedings of 47th Conference on Communications, Control and Computing[C]. Monticello, 2009. 1134-1141.

[14] SPENCER Q H, SWINDLEHURST A L, HAARDT M. Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels[J]. IEEE Transactions on Signal Processing, 2004, 52(2): 461-471.

[15] TELATAR E. Capacity of multi-antenna Gaussian channels[J]. Eur Trans Telecommun, 1999,(6):585-595.

[16] FOSCHINI G J. Layererd space-time architecture for wireless communication in a fading environment when using multiple antennas[J]. Bell Laboratories Technical Journal, 1996.1(2):41-59.

作者简介：



朱耀（1985-），男，山西五台人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为无线通信技术。

朱义君（1976-），男，湖北黄冈人，博士，国家数字交换系统工程技术研究中心副教授，主要研究方向为通信信号处理。

张水莲（1954-），女，江西新余人，国家数字交换系统工程技术研究中心教授、硕士生导师，主要研究方向为无线通信技术。

刘永刚（1964-），男，江西萍乡人，主要研究方向为语言文学。