# γ 约束均方误差下的无线信道加密方法

罗文宇,金 梁,黄开枝,钟 州
(信息工程大学信息技术研究所,河南郑州 450002)

**摘 要:** 无线信道的开放性和电磁信号的广播特性对无线通信系统的安全提出了极大挑战.无线信道引入的安全问题还需要从无线信道本身加以根本解决.现有基于无线信道的物理层安全方法大多利用了多天线带来的空间冗余,无法应用于单天线点对点的场景.为此,本文首先提出了 γ 约束均方误差的概念,通过放宽授权用户的最佳线性接收条件在发送端引入预编码权值的冗余.在此基础上将物理层安全问题转变为发送信号随机化问题,并给出了具体分析和相应的理论推导.然后利用无线信道特征的短期可逆性、快速去相关性提出一种全新的物理层加密方法.分析和仿真结果表明,该方法在保证授权用户无条件正常接收的同时大大降低了信号被非法用户截获的概率.

**关键词:** 物理层安全; 无线信道; 低截获概率; γ 约束均方误差
**中图分类号:** TN929.5 **文献标识码:** A **文章编号:** 0372-2112 (2012) 07-1289-09
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.07.001

# A Wireless Channel Encryption Method with γ Mean Square Error

LUO Wen-yu, JIN Liang, HUANG Kai-zhi, ZHONG Zhou
(*Institute of Information Technology, Information Engineering University, Zhengzhou, Henan* 450002, *China*)

**Abstract:** The design of secure wireless communication suffers a great challenge for openness of wireless channel and the broadcast nature of radio signals. The security problem introduced by wireless channel may be solved adequately by wireless channel itself. The space redundancy is often used in existing physical-layer security method to enhance security. So the concept of γ mean square error is proposed in the paper, which is used to introduce redundancy for pre-coding weight. The concrete analysis and corresponding formal derivations are also given in the paper. Based on these, a novel physical-layer encryption method is proposed according to short-term reciprocity, rapid Decorrelation of wireless channel. Simulation results show that the proposed method guarantees wireless transmission in the authorized receiver and reduces the probability of interception.

**Key words:** physical-layer security; wireless channel; low probability of interception; γ mean square error

## 1 引言

随着无线通信技术的迅速发展,其安全问题变得越来越重要[1,2].传统上,无线通信安全主要分两类:一类是直接移植有线通信系统中的方法,该方法回避了无线信号本身易被截获的问题,同时也面临密码设备管理、密钥管理、密钥在无线开放环境下的传输等一系列问题;另一类是采用序列扩频/跳频、超宽带等低截获概率(LPI)传输技术,该类技术仍然没有考虑无线信道传输等因素,属于"治标"而非"治本",一旦信号体制及其关键参数(如扩频码)被破解则失去作用.因此传统无线安全方法没有根本解决信号辐射泄露带来的问题.

无线通信的特点具有两面性,不利的一面集中表现在电磁信号传播具有广播特性,通信信息极易被期望用户以外的非法用户获取;有利的一面是无线信道具有多样性和时变性,通信双方的信道特征具有唯一性和互易性,可以充分利用这些物理层传输特性,在保证期望用户通信质量的同时,实现无线信号的安全传输[3].目前,物理层加密的研究主要集中在多天线系统中空域信息的使用上[4].文献[5]利用通信的发端使用多天线将主瓣对准授权用户,在其他波束中发送人工噪声抑制其他方向的非法用户.文献[6]将其推广到了接收端也使用多天线的情况.要求发送额外的、对授权用户毫无用处的人工噪声使得该方法的功率利用率很低.因此,文献[3]提出一种利用天线阵列冗余进行物理层加密的方法.该方法通过随机选取各阵元的加权系数,使发送信

收稿日期:2011-05-09;修回日期:2012-02-23
基金项目:国家自然科学基金(No.61171108);信息工程大学博士研究生学位论文创新基金(No.BSLWCX201102)

号经过无线信道叠加后在授权用户端能够被直接解调;而对于非法用户来说,阵元权系数的随机化使恒模算法[7](CMA)等基于盲解卷积的信道盲均衡方法失效,从而满足 LPI 的要求[8~10].然而这种随机加权处理会降低接收信号功率,于是文献[11]提出一种随机选择天线的物理层加密方法.然而,这类方法仅适用于 MIMO/MISO 等能够提供空间冗余的多天线系统,针对协作通信中每个延迟节点仅有一个天线的问题,文献[12]提出一种使用分布式差分编码加密无线信道的方法.由以上分析可知,无线信道加密方法的主要思想是通过引入冗余让授权用户的等效信道(无线信道与预编码权值的组合)缓变甚至不变,而窃听者的等效信道快速剧烈随机变化而导致其无法正确接收.对于本文考虑的单天线点对点系统,每个确定的接收信号只能对应一个输入,无法引入与多天线系统或者分布式协作系统类似的冗余.因此必须通过其他途径引入冗余才能达到加密效果.

本文通过松弛授权用户端的最佳线性接收条件达到提高发送端预编码权值自由度的目的,即松弛最佳接收条件带来了预编码权值的冗余.发送端利用这些冗余随机化发送信号,这些被随机化的发送信号经过授权用户信道后仍然满足松弛后的最佳线性接收条件,因此这种随机化对其影响不大,而且可控(发送端可以通过上行信道探测信号获取它与授权用户之间的无线信道).然而,窃听用户信道和授权用户信道的差异放大了这种随机效果.即窃听端受这种随机化的影响很大,且不可控(发送端、授权用户和窃听用户三方均无法得到窃听用户信道信息).由于发送端与窃听端之间的等效信道是快速随机变化的,窃听端接收的信号也是随机快速变化的.这种随机性使得窃听端利用恒模等盲算法进行迭代时无法收敛,从而达到了安全传输的目的.分析和仿真结果表明利用该方法的通信系统,不用引入多天线和多点协作也能达到很好的加密效果.该方法利用了无线信道的短期可逆性、快速去相关性,在一些特殊的场合如自由空间,信道的去相关性不强.在这些场景中可以考虑文献[3,4,11]提出的基于天线阵列的无线信道加密方法,但这需要以增加系统复杂度为代价.

## 2 无线安全传输模型与问题的提出

由文献[3,4]可知,无线安全传输主要涉及三方,Alice 作为基站需要把信息安全传输给授权用户 Bob,而 Eve 作为窃听端只进行被动接收.由于本文只考虑单天线的情况,结合丰富散射环境下的无线信道模型,Alice 与 Bob、Alice 与 Eve 之间均可建模为多径信道.因此,基于多径冗余的无线安全传输模型可由图 1 表示.

通信过程中,Bob 首先向 Alice 发送未加密的请求信息,该请求信息同时包含用于信道估计的训练序列;Alice 接收请求信息,并估计它们之间的多径信道状态.因为 Alice 并不发送任何用于信道估计的训练序列,Bob 和 Eve 均不知道他们与 Alice 之间的信道信息,因此处于一种全盲状态.根据互易定理[10],在信道慢变的情况下,可以认为 Alice 和 Bob 之间的上下行信道相同.因此 Alice 可以利用估计到的多径信道对即将发送给 Bob 的信息进行加密.这种情况下 Alice 和 Bob 之间的信道即为 Alice 使用的"密钥"*,加密后的信息经过 Alice 和 Bob 之间的信道后自动完成解密,因此 Bob 无需知道他与 Alice 之间的信道即可完成正常通信.而当 Eve-Alice 和 Bob-Alice 之间的距离差超过几个波长,它们与 Alice 之间的信道可以认为是不相关的[13],此时 Alice 和 Eve 之间的信道不再为 Alice 使用的"密钥".Eve 接收到的是一个加密后的信号,在不知道"密钥"的情况下无法解出 Alice 发送的符号.

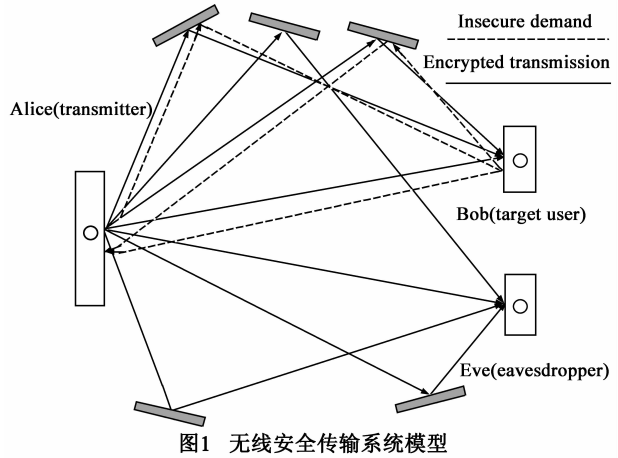


图1 无线安全传输系统模型

因此,要达到加密效果,需要在 Alice 端引入冗余以增加发送信号的自由度.这类方法归根结底是让 Alice 和 Bob 之间的等效信道 $C=[C_1(t),C_2(t),\cdots,C_M(t)]$ 不变或随时间变化不大;同时让 Alcie 和 Eve 之间的等效信道 $E=[E_1(t),E_2(t),\cdots,E_M(t)]$ 随时间变化剧烈而无法正确接收.然而在设计加密系统时,Alice 和 Eve 之间的物理信道通常是未知的.因此如何保证 Bob 正常工作的同时 Eve 无法正确接收是这类方法面临的主要问题.对于多天线系统和分布式协作系统,每一个接收信号均对应着无穷多个可能输入.因此可以通过引入冗余进行加密;而对于本文考虑的单天线点对点系统,每个确定的接收信号只能对应一个输入,无法引入与多天线系统或者分布式协作系统类似的冗余.因此必须通过其他途径引入冗余才能达到加密效果.本文利

* 用来对发送信号进行预处理的参数,非传统意义上的密钥.

用放宽 Bob 的最小均方误差约束条件在 Alice 端引入预编码权值的冗余,从而利用这些冗余对发送信号进行随机化处理以达到加密效果.该方法属于线性处理方法,下面对该方法进行分析和理论推导.

## 3　γ 约束均方误差及无线信道加密新方法

### 3.1　γ 约束均方误差

为了引入冗余以达到加密效果,首先引入均方误差代价函数

$$J = E\{|\boldsymbol{\varepsilon}|^2\} \tag{1}$$

其中,$\boldsymbol{\varepsilon}$ 表示接收信号与发送信号的差,即 $\boldsymbol{\varepsilon} = \boldsymbol{H}_{AB}\boldsymbol{W}\boldsymbol{s} + \boldsymbol{N}_{AB} - \boldsymbol{s}$. $\boldsymbol{H}_{AB}$为 Alice 和 Bob 之间的信道拓展成的 Toeplitz 矩阵, $\boldsymbol{W}$ 为发送端预编码矢量拓展成的 Toeplitz 矩阵, $\boldsymbol{N}_{AB}$为噪声矢量, $\boldsymbol{s}$ 为发送的信息序列.将 $\boldsymbol{\varepsilon}$ 带入式(1)得

$$\begin{aligned} J &= E\{|\boldsymbol{H}_{AB}\boldsymbol{W}\boldsymbol{s} + \boldsymbol{N}_{AB} - \boldsymbol{s}|^2\} \\ &= E\{(\boldsymbol{H}_{AB}\boldsymbol{W}\boldsymbol{s} + \boldsymbol{N}_{AB} - \boldsymbol{s})^{\mathrm{H}}(\boldsymbol{H}_{AB}\boldsymbol{W}\boldsymbol{s} + \boldsymbol{N}_{AB} - \boldsymbol{s})\} \\ &= E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W} - \boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}} - \boldsymbol{H}_{AB}\boldsymbol{W})\boldsymbol{s}\} + \sigma_n^2 + \sigma_s^2 \end{aligned} \tag{2}$$

其中 $\sigma_n$ 和$\sigma_s$ 分别表示噪声和输入信号的方差, $\boldsymbol{R}_{AB} = \boldsymbol{H}_{AB}^{\mathrm{H}}\boldsymbol{H}_{AB}$为 Alice 和 Bob 之间信道的相关矩阵.这个代价函数为凸函数,证明见附录 A.显然 Bob 端利用最佳线性接收条件接收时,发送端 Alice 的预编码权值唯一存在,无法引入用以随机化发送信号的冗余.为了引入预编码权值的冗余必须松弛这一最佳线性接收条件,因此下面提出 γ 约束均方误差的概念.

**定义 1**　对于任意给定 $\forall\ \gamma \in \mathbf{R}$, $\mathbf{R}$ 为实数空间.总有不少于两个矢量 $\boldsymbol{\varepsilon}$ 使得 $E\{|\boldsymbol{\varepsilon}|^2\} < \gamma$ 成立,称之为 γ 约束均方误差.

根据这个定义,放宽对最佳线性接收条件的限制,即对式(2)设定一个门限 γ,得

$$E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W} - \boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}} - \boldsymbol{H}_{AB}\boldsymbol{W})\boldsymbol{s}\} < \underbrace{\gamma - \sigma_n^2 - \sigma_s^2}_{\gamma'} \tag{3}$$

因为 $\boldsymbol{s}$, $\boldsymbol{R}_{AB}$, $\boldsymbol{H}_{AB}$, γ′ 均已知,不失一般性,假定预编码权值矢量为$[\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \cdots, \boldsymbol{\omega}_{M-1}]$,其中 $M$ 为引入的自由度个数,对预编码权值矢量进行 Toeplitz 扩展[14],得到矩阵 $\boldsymbol{W}$ 并带入式(3)可得一个 $M$ 元二次不等式

$$J(\boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \cdots, \boldsymbol{\omega}_M) < \gamma' \tag{4}$$

因此对式(4)求解,可以在 $M$ 维空间中确定一个满足 Bob 要求的最优预编码权值矢量 $\boldsymbol{W}_{opt}$和一个次优加扰空间 $\boldsymbol{W}_{AB}$.这个最优矢量可通过对式(3)求偏导得到

$$\boldsymbol{W}_{opt} = (\boldsymbol{H}_{AB}^{\mathrm{H}}\boldsymbol{H}_{AB})^{-1}\boldsymbol{H}_{AB}^{\mathrm{H}} \tag{5}$$

传统的预编码方法利用式(5)得到的最优解对发送信号进行预处理,接收端可以获得最小均方误差意义上的最优接收性能,但是无法得到用于发送信号随机化的冗余.我们可以放宽均方误差的约束来获得这种冗余,即针对每一个发送符号序列均从次优加扰空间 $\boldsymbol{W}_{AB}$中选取不同的预编码权值矢量对发送信号进行预处理.由于预处理矢量是从次优加扰解空间中选取的,合法接收端 Bob 获得的是 γ 约束均方误差意义上的次优接收性能.因此该方法提供物理层安全所付出的代价是降低了系统的功率效率.另外,选择随机加扰矢量的前提是尽量让所选的随机加扰矢量满足式(6)

$$E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AE}\boldsymbol{W} - \boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}} - \boldsymbol{H}_{AE}\boldsymbol{W})\boldsymbol{s}\} \geq \gamma' \tag{6}$$

但是 Alice 和 Bob 之间的信道是未知的.因此式(6)并不能被 Alice 所用.即便如此,当 Bob 和 Eve 之间的距离超过几个波长时,它们与 Alice 之间的信道可以认为是相互独立的[3,12,13].通过一定的处理,这种信道差异会放大发送信号的随机化效果,保证式(3)恒成立的条件下,尽可能地让式(6)成立.

### 3.2　基于 γ 约束均方误差的加密方法推导

根据上面的分析,无论是 Bob 还是 Eve,如果要正常接收,他们的 γ 约束均方误差不等式表示为

$$\begin{cases} J_{AB} = E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W} - \boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}} - \boldsymbol{H}_{AB}\boldsymbol{W})\boldsymbol{s}\} < \gamma' \\ J_{AE} = E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AE}\boldsymbol{W} - \boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}} - \boldsymbol{H}_{AE}\boldsymbol{W})\boldsymbol{s}\} < \gamma' \end{cases} \tag{7}$$

这里隐含的一个前提是合法用户 Bob 与 Alice 之间的噪声方差不大于窃听用户 Eve 与 Alice 之间噪声的方差.至于 Eve 端底噪比 Bob 端低的情况,很容易利用文献[5]中的人工噪声法提高 Eve 端的底噪,本文暂不考虑.为了说明放宽约束的程度对 Bob 性能以及系统安全性的影响,我们下面定义约束因子这一概念.

**定义 2**　定义门限 γ 与最优矢量 $\boldsymbol{W}_{opt}$所对应的均方误差值的比为约束因子.

**定理 1**　在 γ′ 足够小的情况下,式(7)的两个解空间不可能出现相互包含的情况,即两个解空间至多有一些交集.

**证明**　见附录 B.

定理 1 表明,Alice-Bob 信道和 Alice-Eve 信道的差异使得它们的可用预编码权值矢量空间不同,当 Alice 利用由 Alice-Bob 信道决定的预编码权值矢量随机化发送信号时候,Eve 无法窃听 Alice-Bob 信道上传送的信号,达到了安全传输的目的.虽然从利用 Alice-Bob 信道得到的预编码权值矢量空间中如何选取预编码权值矢量随机化发送信号对 Bob 的接收性能影响不大,但对阻止 Eve 接收影响很大.选取预编码权值矢量时可利用定理 2 和定理 3 的结论,以保证最大程度地提高安全性.

**定理 2**　若式(7)中 Bob 代价不等式确定的解空间为 $\boldsymbol{W}_{AB}$, $\forall\ i_1, i_2 \in \{1,2,\cdots\}$, $\boldsymbol{W}_{AB}$中的两个解 $\boldsymbol{\omega}_{i_1}$和 $\boldsymbol{\omega}_{i_2}$使得 $\left|J_{AB}(\boldsymbol{\omega}_{i_1}) - J_{AB}(\boldsymbol{\omega}_{i_2})\right|$ 取得最大值,则有 $\left|J_{AE}(\boldsymbol{\omega}_{i_1}) - J_{AE}(\boldsymbol{\omega}_{i_2})\right| = \max\{\left|J_{AE}(\boldsymbol{\omega}_i) - J_{AE}(\boldsymbol{\omega}_j)\right|\}$, $i$,

$j\in\{1,2,\cdots\}$, $i\neq j$ 恒成立.

**证明** 首先令 Bob 端代价函数值域为 $J_{AB}$, Eve 端代价函数值域为 $J_{AE}$. 记 $f_{AB}:\boldsymbol{W}_{AB}\rightarrow J_{AB}$, 而且记 $f_{AE}:\boldsymbol{W}_{AB}\rightarrow J_{AE}$. 由附录 A 可知, 式(7)中两个代价函数均为凸函数. 而代价函数值为实数, 因此代价函数的结果在整个空间中是一条直线. 显然每一个加密矢量在这条直线上的投影均为一个点. 因此这两个映射其实是一种映射, 记为 $f:\boldsymbol{W}_{AB}\rightarrow J$. 因此对于解空间 $\boldsymbol{W}_{AB}$中的任意两个矢量, 保证 $\left|J_{AB}(\boldsymbol{\omega}_{i_1})-J_{AB}(\boldsymbol{\omega}_{i_2})\right|$ 最大的同时也保证了 $\left|J_{AE}(\boldsymbol{\omega}_{i_1})-J_{AE}(\boldsymbol{\omega}_{i_2})\right|$ 取得最大值. 证毕!

**定理 3** 若式(7)中 Bob 代价不等式确定的解空间为 $\boldsymbol{W}_{AB}$, 令 $n$ 表示从解空间中取值的次序 $n\in\{1,2,\cdots\}$ 对 $\forall i\in\{n\}$ 使得 $|\boldsymbol{\omega}_i-\boldsymbol{\omega}_{i+2}|$ 取得最大值, 则有 $\left|J_{AE}(\boldsymbol{\omega}_i)-J_{AE}(\boldsymbol{\omega}_{i+2})\right|=\max\{\left|J_{AE}(\boldsymbol{\omega}_i)-J_{AE}(\boldsymbol{\omega}_j)\right|\}$, $i,j\in\{1,2,\cdots\}$, $i\neq j$ 恒成立.

**证明** 由定理 1 可知在 $\gamma'$ 足够小的情况下, 式(7)的两个解空间不可能出现相互包含的情况, 即两个解空间至多有一些交集. 然而即使有交集, 交集也不会包含解空间中两个代价函数的极值点对应的解, 此时映射 $f_{AE}:\boldsymbol{W}_{AB}\rightarrow J_{AE}$可以等效为 $J_{AE}(\boldsymbol{\omega}_i)$在由门限值确定空间的垂线. 也就是说对于 $\forall i\in\{n\}$, $J_{AE}(\boldsymbol{\omega}_{i+2})-J_{AE}(\boldsymbol{\omega}_i)$在门限值确定空间的投影即为 $|\boldsymbol{\omega}_i-\boldsymbol{\omega}_{i+2}|$. 因此当从解空间中选择的两个解欧式距离最大, 也就对应着 $J_{AE}(\boldsymbol{\omega}_{i+2})-J_{AE}(\boldsymbol{\omega}_i)$取得最大值. 证毕!

由以上三个定理可知, 在设计单天线点对点加密系统时, 可以放宽对 Bob 接收性能的约束以增加自由度. 即使 Alice 和 Eve 之间的物理信道是未知的, 利用这些自由度也能达到很好的加密效果. 其中约束因子是一个重要的参数, 约束因子越大, 加密效果越好, 然而针对每一次测量的信道状态信息, 最优矢量 $\boldsymbol{W}_{opt}$所对应的均方误差值, 即均方误差凸函数的极值点是确定的. 也就是说, 约束因子越大意味着选择的门限值也越大. 接收机均方误差的门限值越大, 显然接收性能也就越差. 因此约束因子越大, 授权用户的接收性能越差; 约束因子越小, Bob 的接收性能越好, 但是加密效果会变差. 因此需要在系统设计时根据实际情况取得很好的折中. 由于发送端 Alice 无法知道 Alice-Eve 信道状态信息, 不能在保证安全性的条件下联合 Alice-Bob-Eve 三方优化系统的整体性能, 从而得出最优约束因子. 通常可以根据授权用户 Bob 的 Qos 请求, 得出满足 Bob 最低需求的约束因子, 利用此约束因子可以在保证 Bob 最低需求的基础上, 最大化系统的安全性能. 根据以上推导, 可将 $\gamma$ 约束均方误差下的无线信道加密系统结构表示成如图 2 所示.

在安全通信之前, Bob 首先向 Alice 发送请求信息, 该请求信息同时包含用于信道估计的训练序列和 Qos 请求; Alice 根据接收到的训练序列估计出 Alice-Bob 信道状态, 并根据 Qos 请求确定约束因子. 然后 Alice 根据这个约束因子得出预编码权值矢量空间, 并按照一定的算法从中选取编码权值矢量对发送信号进行加扰处理, 最后将预处理后的信号经由发射前端发送出去. 其中 Bob 端的信令发射模块可以控制何时向 Alice 发送请求信息; 同样 Alice 端的信令接收模块是控制 Alice 在 Bob 发送请求信息时顺利接收.

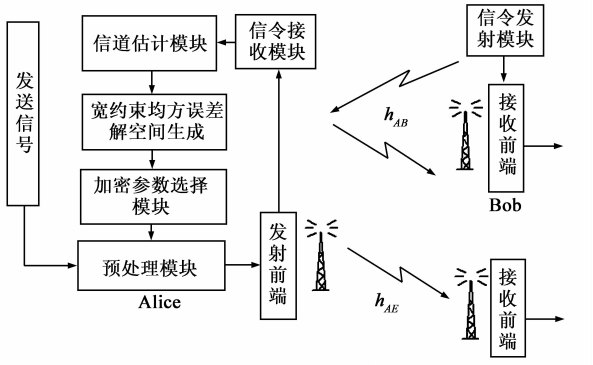


**图2 $\gamma$约束均方误差无线信道安全结构框图**

### 3.3 无线信道加密新方法算法步骤

由 3.2 节, 文中所提方法的核心在于加密参数空间的求解与加密参数的选择. 前者为随机化发送信号提供冗余, 后者是为了保证安全性, 使窃听用户 Eve 无法有效地跟踪等效信道的变化, 从而无法解出 Alice 端发送的符号. 下面分别说明这两部分的算法步骤.

#### 3.3.1 求解解空间

由前面的推导可知, 代价函数

$$J=E\{|\boldsymbol{\varepsilon}|^2\} \tag{8}$$

可以表示为

$$J=E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W}-\boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}-\boldsymbol{H}_{AB}\boldsymbol{W})\boldsymbol{s}\}+\sigma_n^2+\sigma_s^2 \tag{9}$$

因为 $\boldsymbol{R}_{AB}$是对称矩阵, 式(9)的求解是典型的非线性最小二乘问题. 下面对该非线性最优化最小二乘问题求解以便得到其极值和解空间.

**步骤 1** 取初始向量 $\boldsymbol{x}^{(1)}$, 并设置精度 $\xi$, 约束因子 $\alpha$ 和门限 $\gamma_0$, 令计数器 $k=1$ 并令 $r(\boldsymbol{x}^{(1)})=\xi$, 其中 $\boldsymbol{r}=\boldsymbol{H}_{AB}\boldsymbol{W}\boldsymbol{s}+\boldsymbol{N}_{AB}-\boldsymbol{s}$.

**步骤 2** 如果 $\|J(\boldsymbol{x}^{(k)})^{\mathrm{H}}\boldsymbol{r}(\boldsymbol{x}^{(k)})\|\leqslant\xi$, 则记录值 $G_{\min}$并转步骤 4; 否则解线性方程组 $J(\boldsymbol{x}^{(k)})^{\mathrm{H}}\cdot J(\boldsymbol{x}^{(k)})\boldsymbol{d}=-J(\boldsymbol{x}^{(k)})^{\mathrm{H}}\boldsymbol{r}(\boldsymbol{x}^{(k)})$得到 $\boldsymbol{d}^{(k)}$, 转步骤 3.

**步骤 3** 设定 $\boldsymbol{x}^{(k+1)}=\boldsymbol{x}^{(k)}+\boldsymbol{d}^{(k)}$, $k=k+1$, 并转步骤 2.

**步骤 4** 令 $J=\gamma_0 G_{\min}$, 解这个 $M$ 元二次方程得到解空间 $G_{AB}$.

#### 3.3.2 加密参数选择步骤

由定理 2 和定理 3 可知, 加密参数的选择要遵循两

个条件,一是连续选择的每两个解之间必须保证式(7)的代价函数变化最大;二是在保证第一个条件的前提下让间隔一个的解之间的欧氏距离最大,避免选择的解连续落入 Eve 解空间中.

**初始化**:估计信道矩阵 $\boldsymbol{H}_{AB}$,设定 $\gamma$,得出 $G_{AB}$.

**步骤 1**　令 $\bar{G}_{AB}=G_{AB}\setminus\boldsymbol{\omega}_1$ 表示从 $G_{AB}$中删除 $\boldsymbol{\omega}_1$,$\boldsymbol{\omega}_1$ 为从加密解空间 $G_{AB}$中随机选择的一个解.

**步骤 2**　找出集合 $X_2$ 使得它中的每一个元素 $x_2$ 都满足下式在 $\bar{G}_{AB}$空间中最大.

$$|J(x_2)-J(w_1)| \tag{10}$$

**步骤 3**　利用在集合 $X_2$ 中找出的第二个解 $\boldsymbol{\omega}_2$ 进行加密并将该解从解空间中去除,选择时需要保证.

$$\max\left|w_2-w_1\right|,w_2\in X_2 \tag{11}$$

**步骤 4**　找出集合 $X_i$ 使得它中的每一个元素 $x_i$ 都满足下式在 $\bar{G}_{AB}$空间中最大.

$$|J(x_i)-J(w_{i-1})| \tag{12}$$

在集合 $X_i$ 中找出第 $i$ 个解 $\boldsymbol{\omega}_i$ 用于加密并从解空间中去除,并保证.

$$\max\left|w_i-w_{i-2}\right|,w_i\in X_i \tag{13}$$

**步骤 5**　$i=i+1$,返回步骤 4;如果 $i<L$($L$ 为帧长)时,$\bar{G}_{AB}$为空,则将 $G_{AB}$重新赋给 $\bar{G}_{AB}$;否则返回步骤 1.

### 3.4　基于 γ 约束均方误差的发送信号随机化性能分析

为了分析 $\gamma$ 约束均方误差下的物理层安全,首先定义两个重要概念,即快变随机矢量、随机加扰运算.

**定义 3**　在 $\boldsymbol{R}_N$ 空间上,给定参数集 $T$,对于任意的 $t\in T$,若矢量 $\boldsymbol{\omega}$ 的每一个元素对应一个不同的随机变量 $x(t,e)$,$e$ 代表样本空间的元素,则称矢量 $\boldsymbol{\omega}$ 为快变随机矢量*.

**定义 4**　称二元运算⊙为 $\boldsymbol{R}_N$ 空间上的随机加扰运算,若对任意的 $\boldsymbol{b}\in\boldsymbol{R}_N$,$\boldsymbol{b}=(\boldsymbol{b}_0,\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{N-1})$,$\boldsymbol{\omega}=(\boldsymbol{\omega}_0,\boldsymbol{\omega}_1,\cdots,\boldsymbol{\omega}_{N-1})$,则有 $\boldsymbol{\omega}\odot\boldsymbol{b}=(\boldsymbol{\omega}_0+\boldsymbol{b}_0,\boldsymbol{\omega}_1+\boldsymbol{b}_1,\cdots,\boldsymbol{\omega}_{N-1}+\boldsymbol{b}_{N-1})$,其中 $\boldsymbol{b}$ 不变,$\boldsymbol{\omega}$ 为快变随机矢量.

**定理 4**　设 Bob 和 Alice 之间的慢变信道冲激响应可以表示为 $h_{AB}(n)$,矢量 $\boldsymbol{b}=\boldsymbol{W}_{opt}$,快变随机矢量 $\boldsymbol{\omega}$ 满足 $\|\boldsymbol{\omega}\|<\zeta$,若 Alice 利用随机加扰后的矢量 $f(n)=\boldsymbol{\omega}(n)\odot\boldsymbol{b}$ 随机化发送信号 $s(n)$,得发送信号为 $s(n)*f(n)$,Bob 接收信号可以表示为 $y(n)=s(n)*f(n)*h_{AB}(n)+n(n)$.如果 $J_{AB}(\boldsymbol{\omega}_{\max})\leqslant\gamma-\sigma_n^2$,其中 $\boldsymbol{\omega}_{\max}$为满足 $\|\boldsymbol{\omega}_{\max}\|=\zeta$ 的快变随机矢量,Bob 就可以实现 $\gamma$ 约束意义下的次优接收性能,受随机加扰影响很小.

**证明**　因为 Bob 接收信号为 $y(n)=s(n)*f(n)*h_{AB}(n)+n(n)$,根据已知条件,整理可得 $y(n)=s(n)*\boldsymbol{\omega}(n)*h_{AB}(n)+\boldsymbol{s}(n)*\boldsymbol{W}_{opt}(n)*h_{AB}(n)+n(n)$.将 $y(n)$带入式(2),得

$$J_{AB}=E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W}-\boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}-\boldsymbol{H}_{AB}\boldsymbol{W})\boldsymbol{s}\}+\sigma_n^2 \tag{14}$$

因为 $J_{AB}(\boldsymbol{\omega}_{\max})\leqslant\gamma-\sigma_n^2$,可得 $J_{AB}<\gamma$,因此 Bob 能够得到 $\gamma$ 约束意义下的次优接收性能,受随机加扰影响很小.证毕!

由定理 4 可知,$\gamma$ 约束均方误差下的物理层安全方法相当于在最优预编码的基础上加入随机扰动,以达到随机化发送信号的目的.其物理意义是以降低系统功率效率为代价实现物理层安全.

**定理 5**　设 Eve 和 Alice 之间的慢变信道冲激响应可以表示为 $h_{AE}(n)$,矢量 $\boldsymbol{b}=\boldsymbol{W}_{opt}$,快变随机矢量 $\boldsymbol{\omega}$ 满足 $\|\boldsymbol{\omega}\|<\zeta$,若 Alice 利用随机加扰后的矢量 $f(n)=\boldsymbol{\omega}(n)\odot\boldsymbol{b}$ 随机化发送信号 $s(n)$,得发送信号为 $s(n)*f(n)$,Eve 接收信号可以表示为 $y_{Eve}(n)=s(n)*f(n)*h_{AE}(n)+n(n)$.如果 $J_{AB}(\boldsymbol{\omega}_{\max})\leqslant\gamma-\sigma_n^2$,其中 $\boldsymbol{\omega}_{\max}$为满足 $\|\boldsymbol{\omega}_{\max}\|=\zeta$ 的快变随机矢量,Eve 受随机加扰影响无法实现盲接收.

**证明**　因为 Eve 接收信号可以表示为 $y_{Eve}(t)=s(n)*f(n)*h_{AE}(n)+n(n)$,根据已知条件,整理可得 $y_{Eve}(n)=s(n)*\boldsymbol{\omega}(n)*h_{AE}(n)+s(n)*\boldsymbol{W}_{opt}(n)*h_{AE}(n)+n(n)$.将 $y_{Eve}(n)$带入式(2),得

$$\begin{aligned}J_{AE}=&E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AE}\boldsymbol{W}-\boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}}-\boldsymbol{H}_{AE}\boldsymbol{W})\boldsymbol{s}\}+\sigma_n^2\\&+E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}_{opt}^{\mathrm{H}}\boldsymbol{R}_{AE}\boldsymbol{W}_{opt}-\boldsymbol{W}_{opt}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}}-\boldsymbol{H}_{AE}\boldsymbol{W}_{opt})\boldsymbol{s}\}+\sigma_s^2\end{aligned} \tag{15}$$

由定理 1 可知,合法用户 Bob 均方误差代价函数的极值点一定在非法用户均方代价函数包含图形的外部,反之亦然.因此有 $J_{AE}(\boldsymbol{W}_{opt}^{\mathrm{H}})>\min(J_{AE})=\sigma_n^2$,带入式(15)可得

$$J_{AE}>E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{R}_{AE}\boldsymbol{W}-\boldsymbol{W}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}}-\boldsymbol{H}_{AE}\boldsymbol{W})\boldsymbol{s}\}+\sigma_n^2 \tag{16}$$

同样由定理 1 可知,对于合法用户 Bob,$\gamma$ 约束解空间的未包含在非法用户解空间中的部分 $\boldsymbol{W}_{out}$,恒有 $J_{AE}(\boldsymbol{W}_{out})>J_{AB}(\boldsymbol{W}_{out})$成立.因此,式(16)可表示如下

$$J_{AE}>E\{\boldsymbol{s}^{\mathrm{H}}(\boldsymbol{W}_{out}^{\mathrm{H}}\boldsymbol{R}_{AB}\boldsymbol{W}_{out}-\boldsymbol{W}_{out}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}-\boldsymbol{H}_{AB}\boldsymbol{W}_{out})s\}+\sigma_n^2 \tag{17}$$

因为 $J_{AB}(\boldsymbol{\omega}_{\max})\leqslant\gamma-\sigma_n^2$,而且 $\boldsymbol{W}_{\mathrm{out}}$中必定包含有 $\boldsymbol{\omega}_{\max}$中的部分值,因此得 $J_{AB}>\gamma$,即当从次优解空间中选取随机加扰矢量时,包含在非法用户解空间之外的解不满足 $\gamma$ 约束均方误差的条件,非法用户 Eve 无法解调出原始信号.而且由于 Eve 的等效信道 $f(n)*h_{AE}(n)$ 随机快速变化,当 Eve 使用恒模算法等盲均衡算法进行迭代时无法收敛,从而达到低截获概率的目的.证毕!

由定理 4 和定理 5 可知,只要能有有效的方法引入冗余,就可以对系统进行加密.这在多天线系统中很容易实现,因为有可扩展的空域冗余可以利用(天线阵列

---

* 注:与标准数学意义上的随机矢量定义不完全一致

冗余).而对于本文考虑的单天线点对点系统,每个确定的接收信号最多只能对应一个输入,无法引入与多天线系统或者分布式协作系统类似的冗余,因此必须通过其他途径引入冗余才能实现加密功能.本文通过放宽对 Bob 端最小均方误差的约束,同样能引入冗余以保障无线物理层安全.

## 4 仿真结果及分析

本节给出数值和仿真结果.采用的信道模型与第 2 节描述的相同,即为单天线多径信道模型.仿真中采用的信道状态矢量均为利用 cait 软件针对 cdma 信号实测得到.Cait 软件是一个能够对空口和手机信息进行测试和分析的工具.通过使用 cait 软件,可以观察、收集和分析手机状态、网络参数和消息等.此软件可以运行在个人 PC 上,并通过串口、双串口卡或者 USB 口与 CDMA 手机相连.分析 cait 软件下载下来的信道状态信息,能够提取出当前无线信道的多径幅度和时延信息.当前利用的 cait 软件版本能下载保存 4 条多径信息,为了分析方便只取最强的两条径进行分析.主要针对约束因子与 $\gamma$ 约束解空间的关系;约束因子对误码性能的影响;约束因子对功率效率的影响;加密参数选择算法仿真;Bob、Eve 与 Alice 之间信道关系对 Eve 误比特率影响.在算法仿真之前,首先给出以下说明:为了分析方便,文中仅给出 2 阶信道状态的仿真,与之对应的随机加扰矢量维数也设定为 2;噪声均设为加性高斯白噪声,均值为 0,方差 $\sigma^2$;输入的信号矢量为 0 – 1 随机序列.

### 4.1 约束因子与 γ 约束解空间的关系

根据第 2 节给出的信道模型,从前面提取的多径信息中随机选择二个二阶信道作为 Alice 与 Bob 以及 Alice 与 Eve 之间的信道,信噪比为 8dB,约束因子 $\alpha$ 分别取值为 1.05,1.1,2,16 时的解空间对比,如图 3 所示.可见随着约束因子 $\alpha$ 越来越小,两个代价函数的解空间逐渐分离,最终完全相互隔离,即当 $\alpha$ 足够小的时候两个解空间不可能出现相互包含的情况.这也从数值的角度证明了定理 1 的正确性.

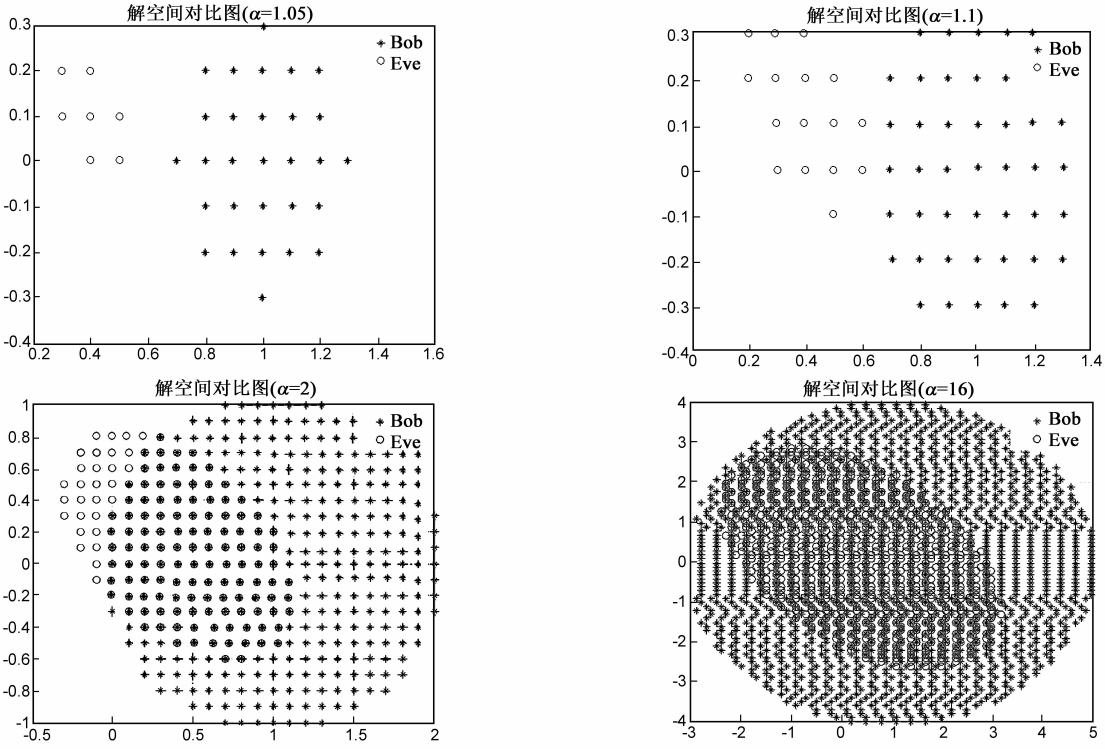


图3 约束因子对解空间关系的影响

### 4.2 约束因子对误码性能的影响

下面考察约束因子对授权用户 Bob 以及非法用户 Eve 的影响,对于每一个约束因子,用 10000 个符号仿真以统计授权用户 Bob 以及非法用户 Eve 的误码率性能.每次采用的加密参数根据 4.1 节得出的 Bob 解空间去掉 Eve 解空间重叠部分、从 Bob 解空间中直接随机选取,仿真 10000 次取平均值,得到与约束因子对应的误码率,信噪比为 8dB.如图 4 和图 5 所示,Bob 的误码率性能随约束因子的增大越来越差.图 4 是 Bob 和 Eve 的误比特率随小约束因子的变化;而图 5 是两个用户对大约束因子的误比特率变化.可见,小约束因子使得授权用户 Bob 的接收性能大大改善,而对非法用户 Eve 的加

密效果稍差；大约束因子由于放宽了 Bob 的最佳接收门限使得其误比特率性能大大降低，但是加密效果要比小约束因子好．在对 Bob 的接收性能和对 Eve 的加密效果方面，小约束因子下从 Bob 解空间中随机选择加密矢量与从 Bob 解空间中直接随机选取相差不大；而在大约束因子下却有明显的差异．这一现象可以由定理 1 的结论给予解释：小约束因子下两个用户的解空间很大概率上没有交集．因此以上两种从解空间中选取加密矢量的方法在小约束条件下退化成同一种方法．

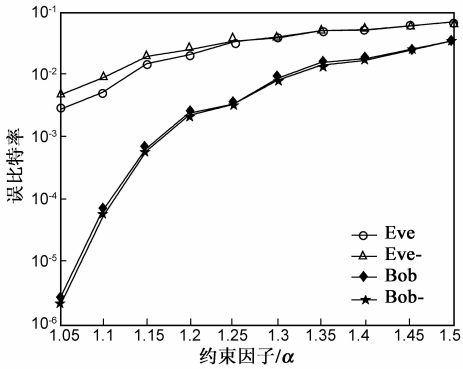


**图4　小约束因子条件下的误码率性能对比**

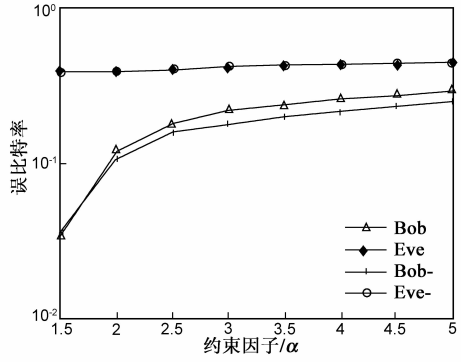


**图5　大约束因子条件下的误码率性能对比**

## 4.3　约束因子对功率效率的影响以及与 Bob 最低信噪比需求的关系

图 6 给出了不同发射功率、不同约束因子的条件下，授权用户 Bob 端的信噪比情况．其中，约束因子为 1 表示发送端 Alice 采用最优预编码矢量对发送信号进行预处理．可以看出约束因子为 1 时，能获得比其他几种约束因子更高的功率效率．结果与 3.1 节的理论分析相同，但是约束因子为 1 时，发送端 Alice 采用的预编码矢量只有一种可能．没有冗余可以利用，Alice 无法在授权用户 Bob 正常工作的情况下，保障无线系统的物理层安全．另外，随着约束因子的增大，该方法的功率效率也越来越低．同时，图 6 还给出了 Bob 提出最低信噪比请求时，Alice 应该选取的约束因子．可见，随着授权用户 Bob 的最低信噪比要求越来越高，约束因子也逐渐接近于 1．即，当 Bob 端具有很高的接收信噪比要求时，它的最佳线性接收条件不能被放宽，否则无法满足其 QoS．对比第 3 节的分析可知，仿真结果与理论分析结果基本吻合．

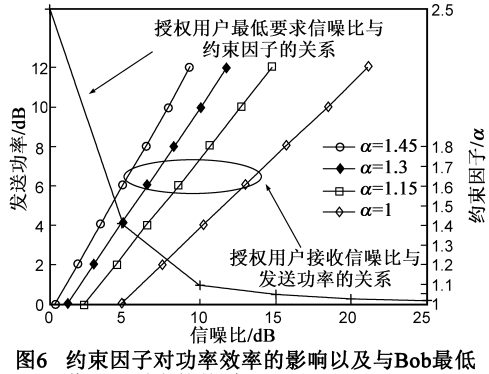


**图6　约束因子对功率效率的影响以及与Bob最低信噪比需求的关系**

## 4.4　加密参数选择算法仿真

下面分析 3.3.2 节所提的加密参数选择方法对误比特率性能的影响，仿真条件与 4.2 节相同．由图 7 可见，按照 3.3.2 节所提算法选择加密矢量比直接随机选择加密矢量加密性能更好，而对 Bob 的接收性能影响不大．因为整个解空间的加密矢量均能使 Bob 具有比较好的接收性能，因此从平均的角度来说，随机选择加密矢量和按照 4.2 节方法选择矢量对误比特率性能影响不大．但是对于加密性能来说，满足 4.2 节方法能够从平均意义上取得最佳的加密性能．

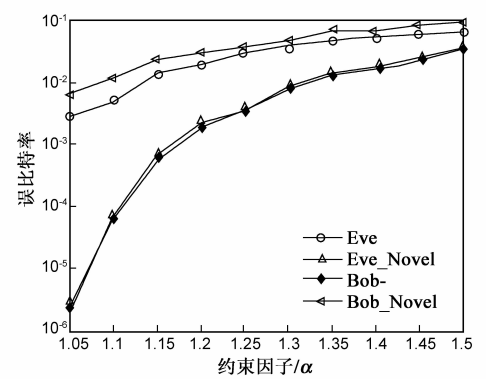


**图7　加密参数选取算法对误比特性能的影响**

## 4.5　信道关系对 Eve 误比特率影响

最后根据第 2 节考虑的信道模型，利用实际测量的信道状态信息，考察了信道关系对 Eve 误比特率的影响．由图 8 可见，当固定 Alice 和 Bob 之间的信道，从测量的 Alice 和 Eve 之间的信道中选择不同信道时，其误码率性能发生很大地变化．两个信道状态相关性越大，Eve 接收性能越好，即加密效果越差；反之越好．因为本文提出的加密方法利用了无线信道的短期可逆性、快速去相关性，比较适合存在丰富散射环境下使用．在一些特殊的场合如自由空间，信道的去相关性不强，可以采用传统的加密方式或文献[3,12]中的天线阵列冗余

的方式.

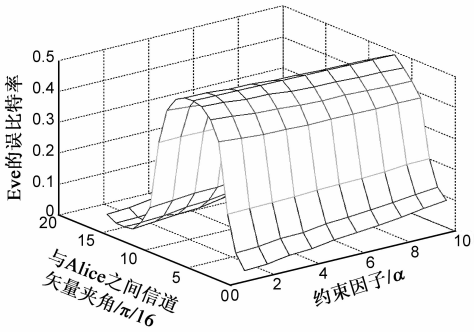


**图8 Bob、Eve与Alice之间信道关系对Eve误比特率影响**

## 5 结论

本文首先提出了 $\gamma$ 约束均方误差的概念,在此基础上提出一种物理层加密方法.该方法首先利用估计出来的信道状态信息和预处理未知信息构造授权用户端的均方误差不等式,并求出该不等式的解空间.然后按照提出的算法从解空间中选择加密参数来随机化发送信号.文中给出了详细的理论分析和推导,并利用实测的信道状态信息进行仿真分析.仿真结果表明该方法能够很好地抑制非法用户 Eve 的接收,同时对授权用户 Bob 正常接收影响不大.需要说明的是本方法有其适用的信道环境,即多散射环境.脱离这种具有丰富多径的环境会降低该方法的加密性能,需要和其他加密方法进行配合以达到既定的安全要求.

## 附录 A

下面对式(2)的凸函数性质进行证明.首先设代价不等式为:

$$J = E\{|\varepsilon|^2\} \leqslant \gamma \tag{A1}$$

其中,$\varepsilon$ 为接收信号与发送信号的差,$\gamma$ 为误差最大限.将式(4)写成一般形式为

$$J = a_1^2x_1^2 + a_2^2x_2^2 + \cdots + a_M^2x_M^2 + 2a_1a_2x_1x_2 + \cdots + 2a_{M-1}a_Mx_Mx_{M-1} + \cdots \tag{A2}$$

因此 $J$ 的黑塞矩阵 $\boldsymbol{\Delta}^2 J$ 可以表示如下

$$\boldsymbol{\Delta}^2 J = \begin{pmatrix} 2a_1^2 & 2a_1a_2 & \cdots & 2a_1a_M \\ 2a_1a_2 & 2a_2^2 & \cdots & 2a_2a_M \\ \vdots & \vdots & \ddots & \vdots \\ 2a_1a_M & 2a_2a_M & \cdots & 2a_M^2 \end{pmatrix} \tag{A3}$$

因为 $\boldsymbol{\Delta}^2 J$ 在定义域内满足半正定条件[15],因此 $J$ 为凸函数,证毕!

## 附录 B

下面对定理1进行证明,首先将问题分为两种情况讨论:

(1)Bob 代价函数的极值点在 Eve 代价函数构成图形的外部,结论显然!

(2)假设 Bob 代价函数的极值点在 Eve 代价函数构成图形的内部,设 Bob 的极值点为 $E_B$,所对应解空间中的解为 $\boldsymbol{W}_{opt}$.即有下式成立

$$J_B(\boldsymbol{W}_{opt}) = E_B \tag{B1}$$

因为 Bob 代价函数的极值点在 Eve 代价函数构成图形的内部,则有

$$J_B(\boldsymbol{W}_{opt}) = E_B > J_E(\boldsymbol{W}_{opt}) \tag{B2}$$

Bob 代价不等式为

$$J_B = E\{\| \boldsymbol{H}_{ab}\boldsymbol{W}\boldsymbol{s} + \boldsymbol{N}_{ab} - \boldsymbol{s} \|^2\} \tag{B3}$$

$J_B$ 达到极值点时,$\boldsymbol{W}_{opt} = (\boldsymbol{H}_{ab}^{\mathrm{H}}\boldsymbol{H}_{ab})^{-1}\boldsymbol{H}_{ab}^{\mathrm{H}}$带入式(B3)得

$$J_B(\boldsymbol{W}_{opt}) = E\{\| \boldsymbol{N}_{ab} \|^2\} \tag{B4}$$

将式(B4)与式(B2)联立得

$$E\{\| \boldsymbol{N}_{ab} \|^2\} > J_E(\boldsymbol{W}_{opt}) = E\{\| \boldsymbol{H}_{ae}\boldsymbol{W}_{opt}\boldsymbol{s} + \boldsymbol{N}_{ae} - \boldsymbol{s} \|^2\} \tag{B5}$$

然而由于下式恒成立

$$J_E(\boldsymbol{W}_{opt}) = E\{\| \boldsymbol{H}_{ae}\boldsymbol{W}_{opt}\boldsymbol{s} + \boldsymbol{N}_{ae} - \boldsymbol{s} \|^2\} \geq E\{\| \boldsymbol{N}_{ae} \|^2\} \tag{B6}$$

因此式(B5)与式(B6)矛盾,假设的第二种情况不成立,即不存在 Bob 代价函数的极值点在 Eve 代价函数构成图形的内部.同理也不存在 Eve 代价函数的极值点在 Bob 代价函数构成图形的内部的情况.证毕!

## 参考文献


[1] M Shin, J Ma, A Mishra, W A Arbaugh. Wireless network secutity and interworking [J]. Proceedings of IEEE, 2006, 94(2): 455 – 466.

[2] A S K Pathan, H W Lee, CS Hong. Security in wireless sensor networks: Issues and challenges [J]. Proceedings of International Conference Advanced Communications Technology, 2006, 2(2): 1043 – 1048.

[3] X Li, J Hwu, E P Ratazzi. Using antenna array redundancy and channel diversity for secure wireless transmissions [J]. Journal of Communications, 2007, 2(5): 24 – 32.

[4] J M Carey, D Grunwald. Enhancing WLAN security with smart antennas: a physical layer response for information assurance [J]. Vehicular Technology Conference, 2004, 1(9): 318 – 320, 973.

[5] R Negi, S Goel. Secret communication using artificial noise [J]. IEEE Vehicular Technology Conference (VTC-2005-Fall), 2005, 3(9): 01906 – 1910.

[6] S Goel, R Negi. Secret communication in presence of colluding eavesdroppers [J]. IEEE Military Communications Conference (MILCOM), 2005, 3(5): 1501 – 1506.

[7] 唐洪,邱天爽. Alpha 稳定分布噪声下广义恒模算法收敛

性能的研究[J].电子学报,2009,37(1):118 – 121.
Tang Hong, Qiu Tianshuang. Convergence properties of the GCMA in alpha stable noise environment [J]. Acta Electronica Sinica,2009,37(1):118 – 121.(in Chinese)
[8] 张炜,戴旭初,许小东.基于非均匀子带分解得宽带线性盲均衡器[J].电子学报,2010,38(4):758 – 765.
ZhangWei, Dai xuchu, Xu Xiaodong. A wideband blind linear equalizer based on non-uniform sub band decomposition [J]. Acta Electronica Sinica,2010,38(4):758 – 765.(in Chinese)
[9] 徐先锋,冯大政.一种充分利用变量结构的解卷积混合盲源分离新方法[J].电子学报,2009,37(1):112 – 117.
Xu Xianfeng, Feng dazheng. A new method based on the full utilizations of concerning variables structures for blind source separation of convolutive mixtures [J]. Acta Electronica Sinica,2009,37(1):112 – 117.(in Chinese)
[10] Xiaohua Li. Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors [J]. IEEE Transactions on Signal Processing,2005,53(4):1511 – 1519.
[11] Mu Pengcheng, Yin Qinye, Wang Wenjie. A physical layer encryption method of using antenna arrays for wireless communication security [J]. Academic Journal of Xi'an Jiaotong University,2010,44(6):62 – 66.
[12] Zheng Li, Xiang-Gen Xia. A distributed differentially encoded OFDM scheme for asynchronous cooperative systems with low probability of interception [J]. IEEE Transactions on Wireless Communications,2009,8(7):3372 – 3379.
[13] J Proakis. Digital Communications,4th ed [M]. New York: McGraw-Hill,2000.
[14] 张贤达等.矩阵分析与应用[M].北京:清华大学出版社,2004.
[15] 何坚勇.最优化方法[M].北京:清华大学出版社,2006.

## 作者简介

**罗文宇**　男.1982 年 9 月出生,河南正阳人.解放军信息工程大学博士生,从事物理层安全、软件无线电、超宽带等方向的研究.
E-mail:lwy_xd@163.com

**金　梁**　男.1969 年 4 月出生,北京人.解放军信息工程大学教授、博士生导师.1999 年毕业于西安交通大学,获博士学位.从事数字通信、通信中的数字信号处理等方面的研究.