doi:10.3969/j.issn.1000-436x.2013.06.024

基于扰动理论无线物理层安全模型及敏度分析

卫红权，罗文宇，兰巨龙，陈鸿昶
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对无线物理层安全多种代表模型在理论描述或者实际应用方面存在一定的局限性这一问题，基于扰动理论研究，提出了一种适用于频率选择性衰落环境的物理层安全模型，该模型能够通过调节扰动阈值来平衡实际系统的可用性和安全性。最后通过敏度分析和应用实例说明了模型的有效性和可靠性。

关键词：安全模型；无线通信；低截获概率；敏度分析
中图分类号：TN929.5 **文献标识码**：A **文章编号**：1000-436X(2013)06-0201-06

Wireless physical-layer security model based on perturbation theory and sensitivity analysis

WEI Hong-quan, LUO Wen-yu, LAN Ju-long, CHEN Hong-chang
（National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China）

Abstract: Many typical models had been proposed for wireless physical-layer security, which have some disadvantages and limitations in theoretical analysis or implementation respectively. Considering these shortages brought about by the existing works, a physical-layer security model used in frequency selective fading channel based on perturbation theory was proposed. The proposed model finds a tradeoff between the availability and the security of the practical system by adjusting the threshold of perturbation. At last, the validity and feasibility are illustrated by the sensitivity analysis and application example.

Key words: security model; wireless communication; low probability of interception; sensitivity analysis

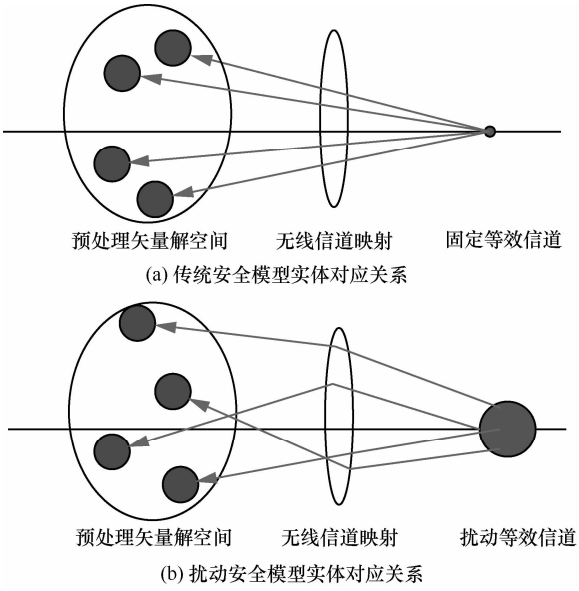
1 引言

在无线物理层安全的发展历史上，出现过多种经典模型，如 Wyner 提出的 wire-tap 模型[1]、Li X H, 提出的阵列冗余模型[2]、Negi R 提出的人工噪声模型[3]等。其中,wire-tap 模型自提出以来得到了广泛的研究[4~6]，尽管如此，该模型仍然无法在大多数无线环境中应用。原因有 2 个：一是在大多数无线环境中，发送端无法获取自己与窃听用户之间的无线信道信息；二是无法保证发送端与合法用户之间的信道质量比与非法用户之间的信道质量好。而这 2 个条件却是 wire-tap 模型建立的前提。为了解决这个问题，阵列冗余模型利用发送天线阵列的冗余来随机化发送信号，以达到使信号具有低截获概率特性的目的。同样，人工噪声模型也是利用发送阵列冗余在发送信号的同时加入人工噪声，人工噪声的产生依赖于发送端和合法用户之间信道零空间的基。这 2 种无线安全模型虽然没有 wire-tap 模型的严格假设条件，但它们要求发送端是多天线，无线信道为平坦衰落。随着各种宽带、超宽带技术的发展，从实际应用来说，针对频率选择性衰落环境的研究越来越受到重视。

由以上文献可知，无线物理层安全的最终目的是让合法用户享受正常通信，同时让非法用户无法实现正常通信。这个思路归根结底是通过发送端预处理，让发送端和合法用户之间的等效信道不变或

收稿日期：2012-09-17；**修回日期**：2012-12-28
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2012CB315901, 2012CB315905）；国家自然科学基金资助项目（61171108）
Foundation Items: The National Basic Research Program of China(973 Program) (2012CB315901, 2012CB315905); The National Natural Science Foundation of China(61171108)

近似不变，而非法用户与发送端之间的等效信道剧烈变化。无线物理层安全的设计主要包含 3 个实体：无线信道特征、预处理参数和通信双方之间的等效信道。由这 3 个实体可以构建一个不适定方程，因此可以将发送信号的随机化问题转化为反向求解这个不适定方程的问题。整个物理层安全模型分为 2 个部分：首先求解这个不适定方程，得出预处理参数集；然后对每一个发送符号，利用预处理参数对待发送数据进行预处理后发送。因此合法用户的接收性能不会受到影响；而由于等效信道随机变化，非法用户接收到的信号也随机变化。 由于各种冗余的存在，wire-tap 模型、阵列冗余模型和人工噪声模型的发送端均能得到无穷多个预处理参数来保证与合法用户端的等效信道恒定，其实体对应关系如图 1(a)所示。对于频率选择性衰落环境下的 SISO 系统，发送端失去了多天线冗余，以上建立的方程解具有唯一性，因此这 3 种安全模型均不适用。



(a) 传统安全模型实体对应关系

(b) 扰动安全模型实体对应关系

图 1 扰动安全模型与传统安全模型实体关系对比

然而，频率选择性衰落环境中，无线信道特征、预处理参数和通信双方之间的等效信道这 3 个实体可以建模为一个卷积方程，求解这个方程的过程是一种反卷积的过程。这种反问题是一种典型的病态问题[7,8]。因此本文利用反问题的扰动现象提出了一种新的无线物理层安全模型。在新模型中，首先对等效信道加随机微小扰动，逐个求出预处理参数得到一个预处理参数集，由于不适定现象的存在，求出的预处理参数之间发生剧烈的变化；然后对每一个发送时隙，利用预处理参数对待发送数据进行预处理后发送。合法用户接收到的信号只受到微小扰动，而非法用户接收的信号随机变化，它的实体对应关系如图 1(b)所示。本文在建立扰动安全模型的基础上，对其安全性进行分析，最后通过一个设计实例验证本文所提模型的有效性。

2 无线物理层扰动安全模型

2.1 模型描述

由文献[1~5]可知，无线安全传输主要涉及三方，Alice 作为基站端需要把信息安全传输给合法用户 Bob，而 Eve 作为窃听用户只进行被动接收而不做任何主动发射。Alice、Bob 和 Eve 均可采用单天线或多天线，由于本文考虑的是频率选择性衰落下 SISO 系统的信道加密，不涉及空域分集，因此只考虑单天线的情况。Alice 与 Bob、Alice 与 Eve 之间建模为多径信道。

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 接收经过多径的请求信息，并根据接收到的信号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[9]，在信道慢变的情况下，可以认为 Alice 和 Bob 之间的收发信道相同。因此 Alice 可以根据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 Alice 是如何加密即可直接完成正常通信。而 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 发射的符号。

假定 Alice 和 Bob 之间以及 Alice 和 Eve 之间多径信道分别为 $\boldsymbol{h}_{\mathrm{AB}}=[h_{\mathrm{AB},1},\cdots,h_{\mathrm{AB},L}]^{\mathrm{T}}$，$\boldsymbol{h}_{\mathrm{AE}}=[h_{\mathrm{AE},1},\cdots,h_{\mathrm{AE},Q}]^{\mathrm{T}}$，预处理参数矢量为 $\boldsymbol{w}=[w_1,\cdots,w_M]^{\mathrm{T}}$，其中，$L$、$Q$、$M$ 为多径和加扰矢量维数。利用预处理参数对发送数据进行处理后，Alice 和 Bob 之间的等效信道 $\boldsymbol{C}_{\mathrm{AB}}$ 可以表示为 $\boldsymbol{C}_{\mathrm{AB}}=\boldsymbol{h}_{\mathrm{AB}}*\boldsymbol{w}$，其中，“$*$”为卷积运算。为了方便以下的讨论，这里以矩阵形式表示如下。

$$\boldsymbol{C}_{\mathrm{AB}}=\boldsymbol{H}_{\mathrm{AB}}\tilde{\boldsymbol{w}} \tag{1}$$

其中，$\boldsymbol{H}_{\mathrm{AB}}$ 为由信道矢量 $\boldsymbol{h}_{\mathrm{AB}}$ 拓展成的 Toeplitz 矩

阵，维数为 $(L+M-1)\times(L+M-1)$，$\tilde{\boldsymbol{w}}$ 为预处理矢量，它是 $\boldsymbol{w}$ 的补零延拓，维数为 $(L+M-1)\times 1$。设定等效信道矢量 $\boldsymbol{C}_{\mathrm{AB}}=[C_{\mathrm{AB},1},\cdots,C_{\mathrm{AB},L+m-1}]^{\mathrm{T}}$，则由式(1)求解 $\tilde{\boldsymbol{w}}$ 是一种反卷积过程。在观测向量受到扰动的情况下，针对这种反问题病态性的研究主要是找出各种正则化方法，以便得到的解更接近真实解[8]。

需要注意的是，在这里影响合法用户接收性能的是等效信道矢量 $\boldsymbol{C}_{\mathrm{AB}}$，而不是加扰矢量 $\boldsymbol{w}$。而且非法用户的等效信道 $\boldsymbol{C}_{\mathrm{AE}}$ 可以表示如下。

$$\boldsymbol{C}_{\mathrm{AE}}=\boldsymbol{H}_{\mathrm{AE}}\tilde{\boldsymbol{w}} \tag{2}$$

其中，$\boldsymbol{H}_{\mathrm{AE}}$ 为由信道矢量 $\boldsymbol{h}_{\mathrm{AE}}$ 拓展成的 Toeplitz 矩阵，维数为 $(Q+M-1)\times M$，$\boldsymbol{C}_{\mathrm{AE}}$ 为 $(Q+M-1)\times 1$ 矢量，$\tilde{\boldsymbol{w}}$ 为 $\boldsymbol{w}$ 的补零延拓，维数为 $(Q+M-1)\times 1$。显然在对 $\boldsymbol{C}_{\mathrm{AB}}$ 加微小扰动的条件下，$\tilde{\boldsymbol{w}}$ 变化得越剧烈对加密性能越有利。

因此整个加密过程如图 2 所示，首先 Alice 根据接收的上行导频信号估计出与 Bob 之间信道状态；然后设定扰动矢量 $\boldsymbol{\varepsilon}(n)$，$n=1,2,\cdots$ 表示扰动次数；求解式(3)得到 $\tilde{\boldsymbol{w}}$ 的解空间 $\tilde{\boldsymbol{W}}$

$$\boldsymbol{H}_{\mathrm{AB}}\tilde{\boldsymbol{w}}=\boldsymbol{C}_{\mathrm{AB}}+\boldsymbol{\varepsilon}(n) \tag{3}$$

根据划分好的时隙，每一个时隙 i 从解空间 $\tilde{\boldsymbol{W}}$ 中随机选出一个矢量 $\tilde{\boldsymbol{w}}(i)$ 对待发送信号进行预处理。合法用户接收的信号可以表示为

$$\boldsymbol{y}_{\mathrm{B}}(i)=\boldsymbol{s}(i)*\tilde{\boldsymbol{w}}(i)*\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{n}_{\mathrm{B}}(i) \tag{4}$$

将式(3)代入式(4)可得

$$\boldsymbol{y}_{\mathrm{B}}(i)=\boldsymbol{Toep}(\boldsymbol{C}_{\mathrm{AB}}+\boldsymbol{\varepsilon}(i))\boldsymbol{s}(i)+\boldsymbol{n}_{\mathrm{B}}(i) \tag{5}$$

其中，$\boldsymbol{s}(i)$ 和 $\boldsymbol{y}_{\mathrm{B}}(i)$ 分别为第 i 个时隙发送和接收信号矢量，$\boldsymbol{Toep}(\cdot)$为矢量的 Toeplitz 拓展矩阵。$\boldsymbol{n}_{\mathrm{B}}(i)$ 为第 i 个时隙均值为零，方差为 σ_{B}^2 的加性高斯白噪声矢量。同样 Eve 接收信号为

$$\boldsymbol{y}_{\mathrm{E}}(i)=\boldsymbol{s}(i)*\tilde{\boldsymbol{w}}(i)*\boldsymbol{h}_{\mathrm{AE}}+\boldsymbol{n}_{\mathrm{E}}(i) \tag{6}$$

整理得

$$\boldsymbol{y}_{\mathrm{E}}(i)=\boldsymbol{Toep}(\boldsymbol{H}_{\mathrm{AE}}\tilde{\boldsymbol{w}}(i))\boldsymbol{s}(i)+\boldsymbol{n}_{\mathrm{E}}(i) \tag{7}$$

其中，$\boldsymbol{y}_{\mathrm{E}}(i)$为 Eve 在第 i 个时隙接收信号矢量，$\boldsymbol{n}_{\mathrm{E}}(i)$ 为第 i 个时隙均值为 0，方差为 σ_{E}^2 的加性高斯白噪声矢量。

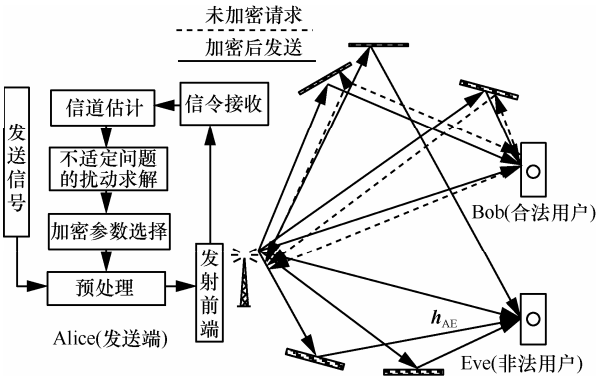


图 2　扰动安全模型

2.2　安全特性分析

由于 Alice 不发送导频信号，Eve 必须通过盲均衡的方法对接收信号进行估计。盲均衡技术能够不借助训练序列，仅利用接收信号本身的统计信息，便可以均衡信道特性，使均衡器的输出尽量接近发送序列[10,11]。恒模算法是盲均衡算法中最常用的一种，具有复杂度低、易于实时实现等特点[12]。本文主要针对这种算法进行安全特性分析，其他盲处理算法的分析可以类比得出。

盲均衡器的抽头系数矢量为 $\boldsymbol{\omega}=[\omega_1,\cdots,\omega_K]^{\mathrm{T}}$，其中，$K$ 是均衡器抽头数目。则恒模代价函数为[12]

$$J(\boldsymbol{\omega})=\min\left\{\left(\left\|\boldsymbol{\omega}(n)\boldsymbol{y}_{\mathrm{B},i}(n)\right\|^2-R_2\right)^2\right\} \tag{8}$$

其中，R_2 表示均衡器输出端期望信号的能量，它是一个实常数而且依赖于信源序列的高阶统计量，表示为 $R_2=\mathrm{E}\{|s(n)|^4\}/\mathrm{E}\{|s(n)|^2\}$，$\boldsymbol{y}_{\mathrm{B},i}(n)$ 为第 i 个时隙接收信号的第 n 段数据，表示为 $\boldsymbol{y}_{\mathrm{B},i}(n)=[\boldsymbol{y}_{\mathrm{B}}(i,n),\boldsymbol{y}_{\mathrm{B}}(i,n-1),\cdots,\boldsymbol{y}_{\mathrm{B}}(i,n-K+1)]^{\mathrm{T}}$。通常采用最陡下降法求解 $\boldsymbol{\omega}$，可得

$$\boldsymbol{\omega}(n+1)=\boldsymbol{\omega}(n)-\mu\nabla J(\boldsymbol{\omega}(n)) \tag{9}$$

在式(8)中相对于 $\boldsymbol{\omega}$ 求导，得到代价函数在 n 时刻的梯度 $\nabla J(\boldsymbol{\omega}(n))$，最终可得迭代求解公式为

$$\boldsymbol{\omega}(n+1)=\boldsymbol{\omega}(n)-\mu\boldsymbol{y}_{\mathrm{B},i}(n)e_i^*(n) \tag{10a}$$

$$e_i(n)=\left(\left\|r_i(n)\right\|^2-R_2\right)r_i(n) \tag{10b}$$

其中，上标“*”表示共轭运算。$\boldsymbol{r}_i$ 为第 i 个时隙均衡器输出，表示如下

$$\begin{aligned}\boldsymbol{r}_i&=\boldsymbol{\omega}*\boldsymbol{y}_{\mathrm{E}}(i)\\&=\boldsymbol{\omega}*\boldsymbol{s}(i)*\tilde{\boldsymbol{w}}(i)*\boldsymbol{h}_{\mathrm{AE}}+\boldsymbol{\omega}*n_{\mathrm{E}}(i)\end{aligned} \tag{11}$$

每个时隙中采用的预处理矢量都是从解空间 $\tilde{\boldsymbol{W}}$ 中随机选取的，因此各个时隙之间的数据完全被

预处理操作随机化，即式(10)的迭代过程必须在一个时隙内稳定收敛，而且下一个时隙还需要重新迭代。因此通过适当地设计，可以控制每个时隙发送的符号数使非法用户无法解调出原始信号，达到了低截获概率的目的。

同时由式(5)可知，预处理过程对合法用户的影响只与微小扰动矢量 $\boldsymbol{\varepsilon}(n)$ 有关。下面进一步分析这种扰动和信道估计误差对整个无线物理层安全模型及其安全性带来的影响。

3 扰动安全模型的敏度分析

假设 Alice 与 Bob 之间信道矢量 $\boldsymbol{h}_{\mathrm{AB}}$ 的估计误差矢量为 $\Delta\boldsymbol{h}_{\mathrm{AB}}$，且满足 $\|\Delta\boldsymbol{h}_{\mathrm{AB}}\|_2 \leqslant \zeta$，其中，参数 ζ 假设已知[13,14]。同样式(3)中的扰动矢量 $\boldsymbol{\varepsilon}$ 满足 $\|\boldsymbol{\varepsilon}\|_2 \leqslant \xi$。

3.1 扰动矢量的敏度分析

首先考虑没有信道估计误差的情况，设由扰动矢量 $\boldsymbol{\varepsilon}$ 引起的解的变化为 $\Delta\tilde{\boldsymbol{w}}$，即

$$\boldsymbol{H}_{\mathrm{AB}}(\tilde{\boldsymbol{w}}+\Delta\tilde{\boldsymbol{w}}) = \boldsymbol{C}_{\mathrm{AB}} + \boldsymbol{\varepsilon} \tag{12}$$

结合式(3)可得

$$\boldsymbol{H}_{\mathrm{AB}}\Delta\tilde{\boldsymbol{w}} = \boldsymbol{\varepsilon} \tag{13}$$

由矩阵范数的性质，得

$$\begin{cases} \|\Delta\tilde{\boldsymbol{w}}\| \leqslant \|\boldsymbol{H}_{\mathrm{AB}}^{-1}\|\|\boldsymbol{\varepsilon}\| \\ \|\boldsymbol{C}_{\mathrm{AB}}\| \leqslant \|\boldsymbol{H}_{\mathrm{AB}}\|\|\tilde{\boldsymbol{w}}\| \end{cases} \tag{14}$$

由式(14)可得

$$\frac{\|\Delta\tilde{\boldsymbol{w}}\|}{\|\tilde{\boldsymbol{w}}\|} \leqslant (\|\boldsymbol{H}_{\mathrm{AB}}\|\|\boldsymbol{H}_{\mathrm{AB}}^{-1}\|)\frac{\xi}{\|\boldsymbol{C}_{\mathrm{AB}}\|} \tag{15}$$

由此可知，扰动对解的影响与 $\boldsymbol{H}_{\mathrm{AB}}$ 的条件数有很大关系。根据式(5)，对于合法用户 Bob，可得

$$\boldsymbol{y}_{\mathrm{B}}(i) = \boldsymbol{Toep}(\boldsymbol{C}_{\mathrm{AB}})\boldsymbol{s}(i) + \boldsymbol{Toep}(\boldsymbol{\varepsilon}(i))\boldsymbol{s}(i) + \boldsymbol{n}_{\mathrm{B}}(i) \tag{16}$$

因为 $\boldsymbol{C}_{\mathrm{AB}}$ 为预设的等效信道矢量（由迫零算法得到的近似脉冲矢量），Bob 可以很容易估计出发送符号，只是受到了由微小扰动 $\boldsymbol{\varepsilon}$ 引入的干扰。而对于非法用户 Eve，由式(7)、式(15)可知，每个时隙接收的信号均受到不同加扰矢量的影响，影响的大小与微小扰动 $\boldsymbol{\varepsilon}$ 和 $\boldsymbol{H}_{\mathrm{AB}}$ 的条件数密切相关。因为这种反卷积问题通常都是病态的[15]，因此微小扰动会被大的条件数放大成解的剧烈变化。

3.2 信道估计误差下的扰动矢量敏度分析

考虑信道估计误差的影响，线性方程组可以表示为

$$(\boldsymbol{H}_{\mathrm{AB}} + \Delta\boldsymbol{H}_{\mathrm{AB}})(\tilde{\boldsymbol{w}} + \Delta\tilde{\boldsymbol{w}}) = \boldsymbol{C}_{\mathrm{AB}} + \boldsymbol{\varepsilon} \tag{17}$$

根据线性方程组的扰动理论可得，当 $\|\boldsymbol{H}_{\mathrm{AB}}^{-1}\| \cdot \zeta < 1$ 时，

$$\frac{\|\Delta\tilde{\boldsymbol{w}}\|}{\|\tilde{\boldsymbol{w}}\|} \leqslant \frac{\|\boldsymbol{H}_{\mathrm{AB}}\|\|\boldsymbol{H}_{\mathrm{AB}}^{-1}\|}{1-(\|\boldsymbol{H}_{\mathrm{AB}}\|\|\boldsymbol{H}_{\mathrm{AB}}^{-1}\|)\dfrac{\zeta}{\|\boldsymbol{H}_{\mathrm{AB}}\|}}\left(\frac{\xi}{\|\boldsymbol{C}_{\mathrm{AB}}\|} + \frac{\zeta}{\|\boldsymbol{H}_{\mathrm{AB}}\|}\right) \tag{18}$$

由式(18)可知，信道估计误差同样会被大的条件数放大为解的剧烈变化，这一点对扰乱发送信号有利，但是这种变化同样会影响 Bob 的接收性能。需要注意的是，Bob 接收时随机预处理对信号的影响会被小的估计误差弱化。即便如此，实际应用时仍然要尽量降低信道估计的误差。

4 设计实例

下面举一个例子来说明模型的应用。发送 1 000 组数据，每组数据由 1 000 个随机生成的 QPSK 调制信号组成。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．噪声服从均值为零，方差为 σ^2 的高斯分布。这里采用 IMT-2000 中的多径信道模型，Alice 和 Bob 之间信道 $\boldsymbol{h}_{\mathrm{AB}}$ 的多径个数 6，多径分布如表 1 所示。

表 1 Alice 与 Bob 之间多径信道

参数	多径条数					
	1	2	3	4	5	6
衰减/dB	−2.5	0	−12.8	−10.0	−25.2	−16.0
时延/ns	0	300	8 900	12 900	17 100	20 000

为了分析方便，假设 Alice 和 Eve 之间信道 $\boldsymbol{h}_{\mathrm{AE}}$ 的多径个数为 6，多径分布如表 2 所示。采样周期均为 100 ns，因此 $\boldsymbol{h}_{\mathrm{AB}}$ 和 $\boldsymbol{h}_{\mathrm{AE}}$ 均为稀疏矢量，长度 L,Q 分别为 201 和 38。由 $\boldsymbol{h}_{\mathrm{AB}}$ 拓展成的 Toeplitz 矩阵 $\boldsymbol{H}_{\mathrm{AB}}$ 的条件数为 $1.724\,9\times10^{17}$，因此 $\boldsymbol{H}_{\mathrm{AB}}$ 是一个病态矩阵。仿真中要求时隙长短可变，用每个时隙发送的符号个数 T 表示。下面主要从 2 个方面进行仿真验证：扰动阈值 ξ 和信道估计误差阈值 ζ 对合法用户性能以及模型安全性能的影响；T 的大小对模型安全性能的影响。

表 2 Alice 与 Eve 之间多径信道

参数	多径条数					
	1	2	3	4	5	6
衰减/dB	−2.5	−0.9	−4.9	−8.0	7.8	−23.9
时延/ns	0	200	800	1 200	2 300	3 700

图 3 为扰动阈值ξ对合法用户性能以及模型安全性能的影响，T取值为 64，信道估计误差阈值ζ为 0.000 1。ξ的取值分别为 0.4、0.01、0.001、0.000 1。由图可见，ξ的取值越大，因为受到的扰动越大，Bob 的接收性能越差。ξ的取值在小于 0.001 以后，对 Bob 接收性能的影响可以忽略。然而，ξ的取值越小，对预处理矢量的影响也越小，Eve 利用盲解卷积进行监听的误码率也会降低，因此会影响整个系统的安全性。

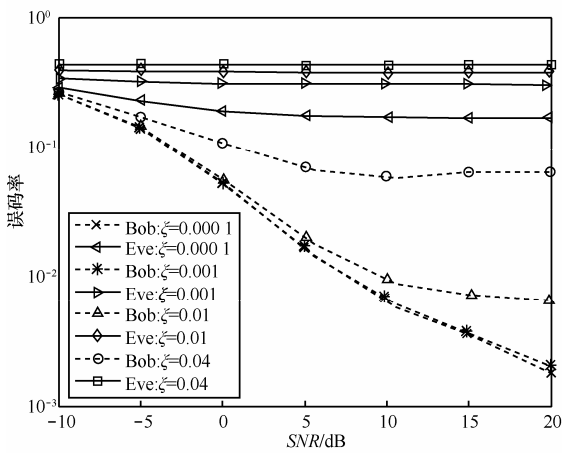


图 3　扰动阈值对合法用户性能以及模型安全性能的影响

图 4 为信道估计误差阈值ζ对合法用户性能以及模型安全性能的影响，T取值为 64，扰动阈值ξ为 0.000 1。ζ的取值也分别为 0.4、0.01、0.001、0.000 1。对比图 2 可见，信道估计误差对 Bob 接收性能的影响要弱于扰动带来的影响，这是因为信道估计误差对病态方程解的影响被小的信道估计误差值弱化的缘故，同样对 Eve 来说，利用盲解卷积进行监听的误码率也会降低，因此会影响整个系统的安全性。

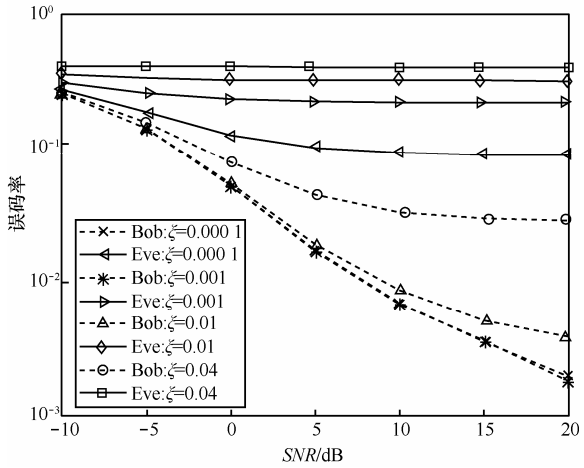


图 4　信道估计误差阈值ζ对合法用户性能以及模型安全性能的影响

图 5 为时隙长度T的大小对模型安全性能的影响。这里同时考虑 2 种扰动：扰动阈值ξ和信道估计误差阈值ζ均为 0.01。由图可见，随着时隙长度T的增加，Bob 的接收性能几乎没有什么改善，但 Eve 的误码率越来越低。因为随着T的增加，Eve 可以在一个时隙内通过迭代盲处理的方式估计出发送符号。当T大于 512 时，Eve 接收性能就取得了明显的改善。

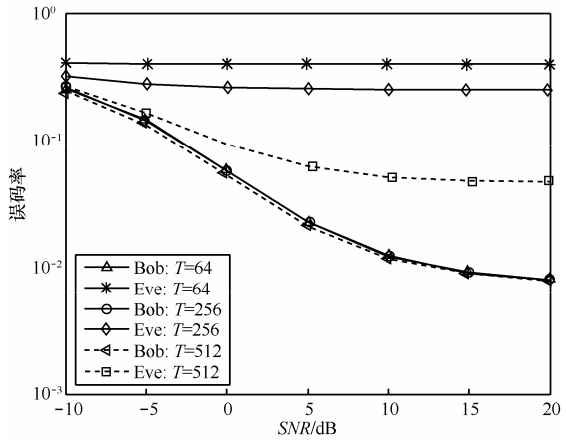


图 5　时隙长度T的大小对模型的安全性能影响

5　结束语

本文考虑了丰富散射环境下的频率选择性衰落环境，提出了无线物理层扰动安全模型，用户可以根据实际系统的具体需求，设置不同的扰动阈值来调节系统的可用性和安全性。与 wire-tap 模型相比，该模型不需要假定合法用户的信道质量优于非法用户的信道质量，也不需要提前知道非法用户信道状态。与阵列冗余模型和人工噪声模型相比，该模型考虑的是频率选择性信道，可用性更强，对于该文章提出模型与频率选择性信道之间的关系是下一步需要研究的内容。而且，和现有模型相同，该模型的有效性建立在非法用户的信道和合法用户的信道统计无关这一假设条件成立的基础之上。

参考文献：

[1] WYNER A. The wire-tap channel[J]. Bell Syst Tech J, 1975,54: 1355-1387.

[2] LI X, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. J Commun, 2007, 2:24-32.

[3] ZHOU X, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation [J].

IEEE Transactions on Vehicular Technology, 2010, 59 (8):3831-3842.

[4] LIANG Y, POOR H V, SHAMAI S. Secure communication over fading channels[J]. IEEE Trans Inform Theory, 2008,54(6):2470-2492.

[5] GOPALA P K, LAI L, GAMAL H E. On the secrecy capacity of fading channels[J]. IEEE Trans Inform Theory, 2008,54(10):4687-4698.

[6] BARACCA P, LAURENTI N, TOMASIN S. Physical layer authentication over MIMO fading wiretap channels[J]. IEEE Trans On Wireless Communication, 2012,11(7):2564-2573.

[7] KIRSCH A. An Introduction to the Mathematical Theory of Inverse Problems[M]. Berlin: Springer-Verlag, 1996.

[8] LANCASTER P, TISMENTESKY M. The Theory of Matrix (2nd ed.)[M]. Orlando: Academic Press,1985.

[9] HAYKIN S. Unsupervised Adaptive Filtering v.II: Blind Deconvolution[M]. New York: Wiley, 2000.

[10] 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.
ZHANG W, DAI X C, XU X D. A wideband blind linear equalizer based on non-uniform subband decomposition[J]. Acta Electronica Sinica, 2010,38(4):758-765.

[11] 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 X F, FENG D Z. A new method basedon the full utilizations of concerning variables structures for blind source separation of convolutive mixtures[J]. Acta Electronica Sinica, 2009, 37(1):112-117.

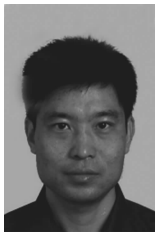
[12] 唐洪, 邱天爽. Alpha 稳定分布噪声下广义恒模算法收敛性能的研究[J]. 电子学报, 2009, 37(1):118-121.
TANG H, QIU T S. Convergence properties of the GCMA in alpha stable noise environment[J]. Acta Electronica Sinica, 2009, 37(1):118-121.

[13] CHEN R, HEATH R, ANDREWS J. Transmit selection diversity for unitary precoding multiuser spatial multiplexing systems with linear receivers[J]. IEEE Trans On Signal Processing, 2007, 55(3):1159-1170.

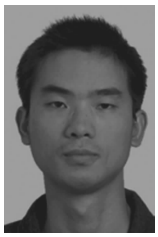
[14] WANG R, LAU V K N. Cross layer design of downlink multiantenna OFDMA systems with imperfect CSIT for slow fading channels[J]. IEEE Transactions on Wireless Communications, 2007, 7(6):2417-2421.

[15] 邹谋炎. 反卷积和信号复原[M]. 北京:国防工业出版社, 2001. 75-88.
ZOU M Y. Deconvolution and Signal Recovery[M]. Beijing: National Defense Industry Press, 2001.75-88.

作者简介：



卫红权（1971-），男，河南唐河人，硕士，国家数字交换系统工程技术研究中心副研究员，主要研究方向为融合网络安全、可重构网络理论与技术。



罗文宇（1982-），男，河南正阳人，博士，国家数字交换系统工程技术研究中心工程师，主要研究方向为通信信号处理、无线物理层安全。

兰巨龙（1962-），男，河北张家口人，博士，国家数字交换系统工程技术研究教授、博士生导师，主要研究方向为可重构网络理论与技术。

陈鸿昶（1964-），男，河南新密人，硕士，国家数字交换系统工程技术研究教授、博士生导师，主要研究方向为通信与信息系统、融合网络安全。