



## 信道估计误差对物理层安全加密方案的影响

奚晨婧, 高媛媛, 沙楠

(陆军工程大学 通信工程学院, 南京 210007)

**摘 要:** 为在物理层中进行信息安全传输, 提出一种基于星座模糊的物理层加密方案。将信道系数作为密钥, 采用信道系数与已调符号矢量叠加的方式实现加密。考虑信道估计存在误差的实际情况, 分析信道估计误差对星座模糊加密方案性能的影响, 推导带有相位估计误差的接收端误码率理论公式。仿真结果表明, 该方案能实现保密通信, 且其系统对信道相位误差具有一定的容忍度, 信道相位误差在  $15^\circ$  内时系统具有鲁棒性, 但误差大于  $42^\circ$  时系统误码率为 1。

**关键词:** 物理层安全; 物理层加密; 星座模糊; 信道估计误差; 调制; 星座映射

开放科学(资源服务)标志码(OSID):



**中文引用格式:** 奚晨婧, 高媛媛, 沙楠. 信道估计误差对物理层安全加密方案的影响[J]. 计算机工程, 2020, 46(6): 122-129.

**英文引用格式:** XI Chenjing, GAO Yuanyuan, SHA Nan. Influence of channel estimation error on physical layer security encryption scheme[J]. Computer Engineering, 2020, 46(6): 122-129.

## Influence of Channel Estimation Error on Physical Layer Security Encryption Scheme

XI Chenjing, GAO Yuanyuan, SHA Nan

(School of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China)

**[Abstract]** In order to safely transmit information in the physical layer, this paper proposes a physical layer encryption scheme based on constellation obfuscation. The channel coefficient is used as the key and superimposed with the modulated symbol vector to achieve encryption. Considering the actual situation of channel estimation error, this paper analyzes the influence of channel estimation error on the performance of constellation obfuscation encryption scheme and conducts the theoretical formula of bit error rate of receiver with phase estimation error. Simulation results show that the proposed scheme can achieve secure communication and it has certain tolerance for the channel phase error. The system is robust when the channel phase error is with  $15^\circ$ , but when the error exceeds  $42^\circ$ , the system bit error rate is 1.

**[Key words]** physical layer security; physical layer encryption; constellation obfuscation; channel estimation error; modulation; constellation mapping

**DOI:** 10.19678/j.issn.1000-3428.0054050

### 0 概述

物理层安全技术作为上层加密技术的一种补充, 通过探索物理层传输介质的随机性来实现信息的保密和身份认证。物理层安全领域的技术研究可分为两大类, 即从理论出发推导提高物理层安全容量的方法和从具体技术出发实现物理层安全保密通信的系统策略。

第 1 类方法以提升安全容量为目的, 可以细分为物理层安全多天线技术(包括人工噪声干扰技术)、中

继技术等。物理层安全多天线技术可归纳为 4 个类别, 分别为波束成型<sup>[1-2]</sup>、迫零预编码<sup>[3]</sup>、凸优化预编码<sup>[4-5]</sup>和人工噪声预编码<sup>[6]</sup>。物理层安全中继技术<sup>[7-8]</sup>研究中继合作策略, 如译码转发<sup>[9]</sup>、放大转发<sup>[10]</sup>、噪声转发<sup>[11]</sup>和压缩转发<sup>[12]</sup>。文献[13]提出一种提高 RFID 系统物理层安全性能的方法, 其以安全容量为评价指标, 分析 2 种情景: 当窃听者信息已知时, 通过中继选择的方式保证通信安全, 并使得安全容量最大化; 当窃听者信息未知时, 采用人工干扰的方式降低窃听者能力, 得到最佳的功率分配方案。文

**基金项目:** 国家自然科学基金(61501511)。

**作者简介:** 奚晨婧(1993—), 女, 硕士研究生, 主研方向为物理层安全; 高媛媛, 教授、博士; 沙楠, 讲师。

**收稿日期:** 2019-03-01 **修回日期:** 2019-05-15 **E-mail:** chenjing\_xi@foxmail.com

献[14]针对认知无线电(CR)网络中的安全传输问题,提出基于传输中继和干扰中继联合优化选择的物理层安全方案。

第2类方法可以细分为物理层安全信道编码技术、物理层安全密钥生成技术、物理层安全身份认证技术和物理层加密技术。物理层安全信道编码技术通过采用差错控制编码和扩频编码等物理层编码手段来提高系统对抗干扰和窃听的能力。物理层安全密钥生成技术有4种类型,即基于信道状态信息(Channel State Information, CSI)<sup>[15]</sup>、基于接收信号强度<sup>[16]</sup>、基于相位<sup>[17]</sup>和基于编码<sup>[18]</sup>的窃听信道密钥生成技术。此外,研究者提出3种身份认证技术,分别为基于CSI的身份认证<sup>[19]</sup>、基于射频识别的方法<sup>[20]</sup>和基于编码的窃听信道身份认证<sup>[21]</sup>。

近年来,物理层加密技术的相关安全传输策略逐渐引起关注。文献[22]对相关文章进行总结归纳。物理层加密技术通过相位旋转、调制星座多样性、幅度调节、符号顺序变化和符号模糊等多种加密技术设计信号星座,保护已调符号内容和调制方式等信息,使窃听者无法识别新的星座图样并难以解出正确信息。

文献[23-25]旋转相位固定角度,文献[26-27]旋转伪随机角度,收发端需提前共享密钥。关于调制星座多样性的研究分为2种:第1种在多种调制方式内变化;第2种在一种调制中对不同符号进行阶数变换<sup>[28]</sup>或不同的星座映射<sup>[29]</sup>。文献[30-31]探索其他调制方式的多样性加密技术。文献[32]采用非均匀分布的幅度调节方法。文献[33]通过相位旋转矩阵改变每一段符号序列的相位和幅度,将原始符号叠加成多维度符号并进行传输。文献[34]通过酉矩阵进行相位旋转和符号顺序重新排列,实现符号加密。文献[35]提出一种多符号模糊(MIO)方案,其采用密钥与已调符号矢量叠加的符号模糊方法置乱已调符号的星座。此外,文献[36]针对基于OFDM调制的物理层安全算法不能抵抗明文密文对攻击的缺点,提出一种结合OFDM调制并通过密钥控制调制过程以对IFFT变换前的符号进行迭代插值的物理层安全算法。

上述物理层加密技术均假设信道估计无误差,但在实际中,有时无法获得准确的信道状态信息,即存在较大的信道估计误差和时延,信道估计误差又分为信道幅度估计误差和信道相位估计误差。本文以信道系数为密钥,仅考虑信道相位估计误差,提出一种信道系数与已调符号矢量叠加的星座模糊设计方案COD。在信道估计存在误差的情况下,分析合

法接收者和智能攻击型窃听者接收端的信号处理方式,推导出带有信道相位误差的误码率理论公式,在此基础上,结合仿真来研究信道相位对这2类接收者误码率的性能影响。

## 1 系统设计

本文系统模型为三节点的窃听模型,包含一个发送者(Alice)、一个合法接收者(Bob)和一个窃听者(Eve)。如图1所示,假设发送端已知主信道CSI,图中标为 $h_R$ 。非法窃听者在通信范围内可以收到Alice发出的消息,窃听信道为 $h_E$ 。其中,窃听者的攻击方式为智能攻击型,窃听者已知加密方式但未知具体的密钥信息。

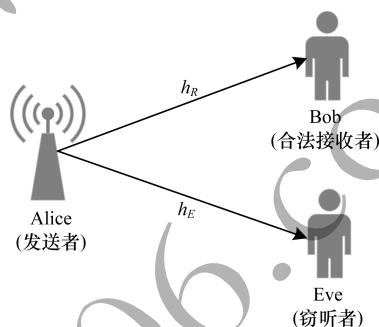


图1 本文系统模型

Fig. 1 System-model proposed herein

在每次传输开始时进行信道估计,信道估计的目的是获取发送端与合法接收端之间的CSI。本文采取一种发送导频的信道探测策略:在同一个时隙内或者相干时间段内,Bob和Alice同时发送导频进行上行和下行信道探测,Alice得到上行信道系数 $h_{RS}$ ,Bob得到下行信道系数 $h_{SR}$ 。由于信道是动态变化的,因此每隔一段时隙重新进行信道估计,2次估计之间认为信道相对稳定且CSI保持不变,仅Alice与Bob知晓估计得到的瞬时信道信息,窃听端无法获得正确的CSI。假设发送端与合法接收端进行上、下行信道探测时无时延,且满足信道互易性准则。发送端与合法接收端估计得到的主信道系数 $h_{RS}$ 与 $h_{SR}$ 一致,合法接收端可以通过此方案避免密钥共享,从而实现与发送端的密钥信息交互。

在一个相干时隙内,发送端发送 $N$ 个数据符号给合法接收端。加密步骤如下:发送端使用某种调制将比特数据映射为星座图上的一个已调符号点 $S_k$  ( $1 \leq k \leq N$ )。在此相干时隙内,发送端与合法接收端同时进行信道估计以得到信道系数 $h_R$ ,将 $h_R$ 作为密钥符号,与数据符号点进行矢量叠加并加密,得到加密的发送符号为:

$$x_k = S_k + h_R \quad (1)$$

如图 2 所示,4 个圆形黑点为 QPSK 星座图上的已调符号点。在星座平面中,将已调符号  $S_k$  与信道系数  $h_R$  进行矢量叠加得到加密符号  $x_k$ 。对每个已调符号进行矢量叠加的加密操作,发送端将加密后的数据符号  $x_k$  通过天线传输给合法接收端。

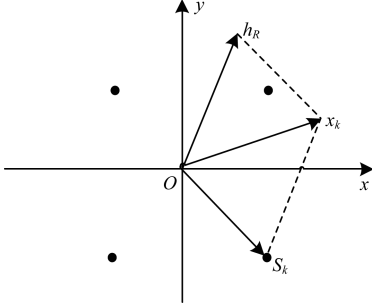


图 2 QPSK 已调符号与信道系数矢量叠加示意图

Fig.2 Schematic diagram of vector superposition of QPSK modulated symbols and channel coefficients

## 2 接收端分析

本节主要在信道相位估计存在误差的情况下对 COD 方案的接收端进行分析。信道系数由幅度  $|h|$  和相位  $\theta$  两部分构成,因此,信道估计误差分为两部分,即幅度误差和相位误差。本文暂不考虑信道幅度误差对系统的影响,估计的信道系数幅度与实际相等,即  $|\hat{h}| = |h|$ 。估计的信道相位用  $\hat{\theta}$  表示,定义实际的信道相位为  $\theta$ ,信道估计的相位误差为:

$$\varepsilon = \hat{\theta} - \theta \quad (2)$$

相位估计误差能够建模为在  $[-\delta, \delta]$  范围内均匀分布的随机变量,其中,  $\delta$  是接收端的最大相位估计误差。下文分别对合法接收端和智能攻击型窃听端进行接收信号处理分析。

### 2.1 合法接收端

合法接收端估计得到的信道系数为  $\hat{h}_R$ , 信道相位为  $\hat{\theta}_R$ , 信道相位估计误差为  $\varepsilon_R = \hat{\theta}_R - \theta$ 。相位误差能够建模为在  $[-\delta_R, \delta_R]$  范围内均匀分布的随机变量,其中,  $\delta_R$  是合法接收端的最大相位估计误差。

在信道估计存在误差的情况下,分析合法接收端的接收过程。在矢量信道模型中,合法接收端接收到的信号为:

$$r_R = h_R \cdot S_k + h_R^2 + n_R \quad (3)$$

接收者采用 MAP 准则进行信号接收。在信号等概率的条件下,MAP 检测器转化为最大似然 (ML) 检

测器,此时两者都等价于最小距离检测器。合法接收端进行符号解密:

$$\hat{S}_k = \underset{1 \leq k \leq N}{\operatorname{argmin}} \left\| \frac{r_R}{\hat{h}_R} - \hat{h}_R - S_k \right\| \quad (4)$$

合法接收端通过式 (4) 对接收符号进行判决,最终得到解密后的接收符号。将信道相位估计误差的表达式  $\hat{\theta}_R = \theta + \varepsilon_R$  代入式 (4), 可得合法接收端解密出的信号为:

$$\hat{S}_k = \underset{1 \leq k \leq N}{\operatorname{argmin}} \left\| \frac{r_R}{|h_R|} e^{-j(\theta + \varepsilon_R)} - |h_R| e^{j(\theta + \varepsilon_R)} - S_k \right\| \quad (5)$$

合法接收端通过式 (5) 完成符号解密操作,噪声与信道相位估计误差 2 个量会影响合法接收端的解密并产生符号错误。

### 2.2 智能攻击型窃听端

智能攻击型窃听端已知信道系数与已调符号矢量叠加的加密方式,未知密钥信息信道系数。窃听端通过猜测信道系数并将其作为密钥进行符号解密,其猜测得到的信道系数为  $\hat{h}_{int}$ 。定义智能攻击型窃听端猜测得到的信道相位与实际信道相位的误差为:

$$\varepsilon_{int} = \hat{\theta}_{int} - \theta \quad (6)$$

相位误差  $\varepsilon_{int}$  能够建模为在  $[-\delta_{int}, \delta_{int}]$  范围内均匀分布的随机变量,其中,  $\delta_{int}$  是智能攻击型窃听端的最大相位误差。由于智能攻击型窃听端通过推测得到信道系数,虽然有可能猜对,但从概率角度考虑,窃听端得到的信道系数存在很大误差。因此,本文假设窃听端的最大信道相位误差大于合法接收端的最大信道相位估计误差,即  $\delta_{int} > \delta_R$ 。智能攻击型窃听端估计的信道系数幅度与实际信道系数幅度相等,即  $|\hat{h}_{int}| = |h_{int}|$ 。

在矢量信道模型中,智能攻击型窃听端接收到的信号为:

$$r_{int} = h_{int} \cdot S_k + h_R \cdot h_{int} + n_{int} \quad (7)$$

智能攻击型窃听端已知矢量叠加信道系数的符号加密方式,在信号等概率的条件下,采用最小距离检测器进行信号接收,此时解密得到的数据符号可以表示为:

$$\hat{S}_{int} = \underset{1 \leq k \leq N}{\operatorname{argmin}} \left\| \frac{r_{int}}{\hat{h}_{int}} - \hat{h}_{int} - S_k \right\| \quad (8)$$

其中,  $\hat{S}_{int}$  为智能攻击型窃听端解密得到的信号表达式。将信道相位误差公式  $\hat{\theta}_{int} = \theta + \varepsilon_{int}$  代入式 (8), 得到:

$$\hat{S}_{\text{int}} = \underset{1 \leq k \leq N}{\operatorname{argmin}} \left\| \frac{\mathbf{r}_{\text{int}}}{|h_{\text{int}}|} e^{-j(\theta + \varepsilon_{\text{int}})} - |h_{\text{int}}| e^{j(\theta + \varepsilon_{\text{int}})} - \mathbf{S}_k \right\| \quad (9)$$

智能攻击型窃听端虽然知晓加密方式,但由于其只能猜测合法信道系数,因此无法获取准确的密钥,并且将产生符号错误。信道估计有误差条件下,在智能攻击型窃听端解密得到的信号中,噪声和信道相位误差会影响智能攻击型窃听端的符号错误概率。

### 3 安全性能分析

#### 3.1 判决区域

QPSK调制的符号点 $\{S_1, S_2, S_3, S_4\}$ 分布如图3所示。在信号发送等概率的条件下,采用最小距离检测器进行接收,此时QPSK调制的判决边界是与符号点等距离的点集合。对于符号 $S_1$ 而言,其判决区域为第I象限,其余符号的判决区域以此类推。

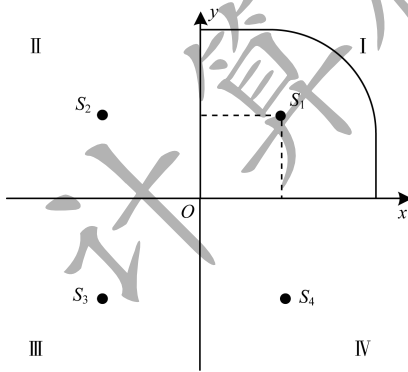


图3 QPSK信号星座图

Fig.3 Constellation graph of QPSK signal

#### 3.2 带有信道相位误差的理论误码率推导

3.1节针对信道估计有误差的情况对合法接收端和智能攻击型窃听端进行信号处理分析。本节在信道相位估计有误差的情况下,对带有相位估计误差的系统的合法接收端理论误码率公式进行推导。

发送端的已调符号为 $S_1 = (s_1, s_2)$ ,假设已调符号 $S_1$ 的能量为 $\sqrt{E}$ ,则符号矢量为 $\left(\frac{\sqrt{2E}}{2}, \frac{\sqrt{2E}}{2}\right)$ 。假设相干时间内的信道系数为 $h_R$ ,加密后的符号为 $\mathbf{x}_1 = S_1 + h_R$ 。合法接收端的接收信号可表示为:

$$\mathbf{r}_1 = \mathbf{x}_1 \cdot h_R + n = h_R \cdot S_1 + h_R^2 + n_R \quad (10)$$

其中, $n_R$ 为加性高斯白噪声,其均值为0、方差为 $\sigma_n^2$ ,概率密度函数为 $N_0$ ,信道系数 $h_R$ 服从复高斯分布, $h_R \sim \mathcal{CN}(0, \sigma_R^2)$ 。合法接收端解密出的信号为:

$$\hat{S}_1 = \underset{1 \leq k \leq N}{\operatorname{argmin}} \left\| \frac{\mathbf{r}_1}{|h_R|} e^{-j(\theta + \varepsilon_R)} - |h_R| e^{j(\theta + \varepsilon_R)} - \mathbf{S}_k \right\| \quad (11)$$

根据式(11)完成符号解密,求解解密后的差错概率即求解解密后符号点落在判决区域外的概率。求理论误码率可以分成2个步骤:第1步求固定衰落时的差错概率 $P_g$ ;第2步在第1步的基础上求衰落随机变化时的理论误码率 $P_e$ 。

1)第1步在有信道相位估计误差时计算差错概率 $p_g$ 。接收信号为 $\mathbf{r}_1 = S_1 + h_R + n_R$ ,解密后信号点为 $\hat{S}_1 = |h_R| e^{j\theta} - |h_R| e^{j(\theta + \varepsilon_R)} + n_R$ 。其中,实部与虚部分别用 $x, y$ 表示。在噪声和衰落影响下,解密后信号点发生偏移,若加密后点的偏移超过 $\sqrt{2E}/2$ ,则会产生差错。

首先计算解密后点的概率密度函数 $p(\hat{S}_1)$ 。分别求出 $\hat{S}_1$ 中每个系数的概率密度函数: $p(|h_R| e^{j\theta})$ 、 $p(|h_R| e^{j(\theta + \varepsilon_R)})$ 和 $p(n_R)$ 。对 $p(|h_R| e^{j(\theta + \varepsilon_R)})$ 进行拆解得:

$$p(|h_R| e^{j(\theta + \varepsilon_R)}) = p(|h_R| \cos(\theta + \varepsilon_R) + j|h_R| \sin(\theta + \varepsilon_R)) \quad (12)$$

将式(12)表示为矢量点的形式,具体如下:

$$p(|h_R| e^{j(\theta + \varepsilon_R)}) = (|h_R| \cos(\theta + \varepsilon_R), |h_R| \sin(\theta + \varepsilon_R)) \quad (13)$$

分别求出 $p(|h_R| \cos(\theta + \varepsilon_R))$ 与 $p(|h_R| \sin(\theta + \varepsilon_R))$ 的概率密度函数后得到 $p(|h_R| e^{j(\theta + \varepsilon_R)})$ :

$$p(|h_R| e^{j(\theta + \varepsilon_R)}) = p(|h_R| \cos(\theta + \varepsilon_R)) \cdot p(|h_R| \sin(\theta + \varepsilon_R)) = \frac{xy}{\sigma_R^4 \cos^2(\theta + \varepsilon_R) \sin^2(\theta + \varepsilon_R)} e^{-\frac{\sin^2(\theta + \varepsilon_R)x^2 + \cos^2(\theta + \varepsilon_R)y^2}{2\sigma_R^2 \cos^2(\theta + \varepsilon_R) \sin^2(\theta + \varepsilon_R)}} \quad (14)$$

同理可得 $p(|h_R| e^{j\theta})$ 为:

$$p(|h_R| e^{j\theta}) = p(|h_R| \cos \theta) \cdot p(|h_R| \sin \theta) = \frac{xy}{\sigma_R^4 \cos^2 \theta \sin^2 \theta} e^{-\frac{\sin^2 \theta x^2 + \cos^2 \theta y^2}{2\sigma_R^2 \cos^2 \theta \sin^2 \theta}} \quad (15)$$

$p(n_R)$ 为:

$$p(n_R) = \frac{2}{\pi N_0} e^{-\frac{2x^2 + 2y^2}{N_0}} \quad (16)$$

可求得差错概率为:

$$\begin{aligned}
p_g = & \int_{-\infty}^{-\sqrt{\frac{E}{2}}} \int_{-\infty}^{-\sqrt{\frac{E}{2}}} p(\hat{S}_1) dx dy = \\
& \int_{-\infty}^{-\sqrt{\frac{E}{2}}} \int_{-\infty}^{-\sqrt{\frac{E}{2}}} e^{\frac{-2N_0 x^2 + 8\sigma_R^2 \cos^2 \theta (N_0 - 2)x}{N_0 A}} \cdot \\
& \left\{ \frac{\sqrt{2N_0}}{\sqrt{\pi\sigma_R^2 \cos^2(\theta + \varepsilon_R)A}} + \operatorname{erfc}\left(-\frac{4\sigma_R x \cos \theta}{\sqrt{2N_0 A}}\right) \cdot \right. \\
& \left[ \frac{4x \cos \theta}{\sigma_R \cos^2(\theta + \varepsilon_R)A^{\frac{3}{2}}} + \right. \\
& \left. \left. \frac{1}{\sigma_R^3 \cos^2(\theta + \varepsilon_R) \cos \theta \sqrt{A}} \right] \right\} \cdot \\
& e^{\frac{-2N_0 y^2 + 8\sigma_R^2 \sin^2 \theta (N_0 - 2)y}{N_0 B}} \left\{ \frac{\sqrt{2N_0}}{\sqrt{\pi\sigma_R^2 \sin^2(\theta + \varepsilon_R)B}} + \right. \\
& \operatorname{erfc}\left(-\frac{4\sigma_R y \sin \theta}{\sqrt{2N_0 B}}\right) \left[ \frac{4y \sin \theta}{\sigma_R \sin^2(\theta + \varepsilon_R)B^{\frac{3}{2}}} + \right. \\
& \left. \left. \frac{1}{\sigma_R^3 \sin^2(\theta + \varepsilon_R) \sin \theta \sqrt{B}} \right] \right\} dx dy \quad (17)
\end{aligned}$$

其中,  $A = N_0 + 4\sigma_R^2 \cos^2 \theta$ ,  $B = N_0 + 4\sigma_R^2 \sin^2 \theta$ 。式(17)与信噪比  $\gamma_b = |h_R|^2 E / N_0$  有关, 式(17)求差错概率时的条件为  $|h_R|$  固定不变。

2) 第2步在式(17)的基础上得到  $|h_R|$  随机变化时的理论误码率。 $\gamma_b$  的概率密度函数为:

$$p_b(\gamma_b) = \frac{1}{\bar{\gamma}_b} e^{-\frac{\gamma_b}{\bar{\gamma}_b}}, \quad \gamma_b \geq 0 \quad (18)$$

其中,  $\bar{\gamma}_b$  为平均信噪比。则理论误码率为:

$$\begin{aligned}
P_e = & \int_{-\infty}^{+\infty} p_b(\gamma_b) P_g(\gamma_b) d\gamma_b = \int_0^{+\infty} \frac{1}{\bar{\gamma}_b} e^{-\frac{\gamma_b}{\bar{\gamma}_b}} \cdot \\
& \int_{-\infty}^{-\sqrt{\frac{E}{2}}} \int_{-\infty}^{-\sqrt{\frac{E}{2}}} e^{\frac{-2N_0 x^2 + 8\sigma_R^2 \cos^2 \theta (N_0 - 2)x}{N_0 A}} \cdot \\
& \left\{ \frac{\sqrt{2N_0}}{\sqrt{\pi\sigma_R^2 \cos^2(\theta + \varepsilon_R)A}} + \operatorname{erfc}\left(-\frac{4\sigma_R x \cos \theta}{\sqrt{2N_0 A}}\right) \cdot \right. \\
& \left[ \frac{4x \cos \theta}{\sigma_R \cos^2(\theta + \varepsilon_R)A^{\frac{3}{2}}} + \frac{1}{\sigma_R^3 \cos^2(\theta + \varepsilon_R) \cos \theta \sqrt{A}} \right] \cdot \\
& e^{\frac{-2N_0 y^2 + 8\sigma_R^2 \sin^2 \theta (N_0 - 2)y}{N_0 B}} \left\{ \frac{\sqrt{2N_0}}{\sqrt{\pi\sigma_R^2 \sin^2(\theta + \varepsilon_R)B}} + \right. \\
& \operatorname{erfc}\left(-\frac{4\sigma_R y \sin \theta}{\sqrt{2N_0 B}}\right) \left[ \frac{4y \sin \theta}{\sigma_R \sin^2(\theta + \varepsilon_R)B^{\frac{3}{2}}} + \right. \\
& \left. \left. \frac{1}{\sigma_R^3 \sin^2(\theta + \varepsilon_R) \sin \theta \sqrt{B}} \right] \right\} dx dy d\gamma_b \quad (19)
\end{aligned}$$

#### 4 仿真结果与分析

本节将针对信道相位估计存在误差的情况, 在星座模糊设计方案下, 分别对合法接收端和智能攻击型窃听端进行误码率性能仿真和分析, 利用

Matlab 仿真软件, 在瑞利衰落信道下采用 QPSK 调制。合法接收端进行信道探测获取带有误差的信道系数, 智能攻击型窃听端通过猜测获取信道系数, 由于合法接收端通过信道估计得到的信道相位更准确, 仿真时设置合法接收端的最大信道相位估计误差为  $0^\circ \leq \delta_R \leq 50^\circ$ , 智能攻击型窃听端的最大信道相位误差为  $0^\circ \leq \delta_{in} \leq 360^\circ$  (仿真时设置的相位均为角度制)。

##### 4.1 合法接收端

不同 SNR 和  $\delta_R$  下合法接收端误码率的变化情况如图 4 所示。仿真设置信道系数服从均值为 0、方差  $\sigma_R^2$  为 1 的复高斯分布, 信道相位在  $[0, 2\pi]$  之间呈均匀分布。从  $0^\circ$  开始以  $10^\circ$  为间隔增加信道相位误差至  $50^\circ$ 。从图 4 可以看出:

1) 蒙特卡洛仿真值与理论值基本能够互相对应, 即验证了本文公式推导的正确性。

2) 当  $\delta_R$  为  $10^\circ$ 、 $20^\circ$  时, 合法接收端的误码率曲线逐渐提升, 但与信道估计无误差时的误码率性能相差较小; 当  $\delta_R$  变为  $30^\circ$ 、 $40^\circ$  时, 合法接收端的误码率性能迅速变差, 说明合法接收端的误码率对较小的  $\delta_R$  值不敏感, 当  $\delta_R$  较大时性能才会变差, 即 COD 方案的合法接收端对信道相位估计误差具有一定的鲁棒性。

3) 当  $\delta_R$  变为  $50^\circ$  时, 合法接收端的误码率约为 1, 说明当信道相位估计误差积累到一定程度时, 合法接收端的正常通信将受到影响。

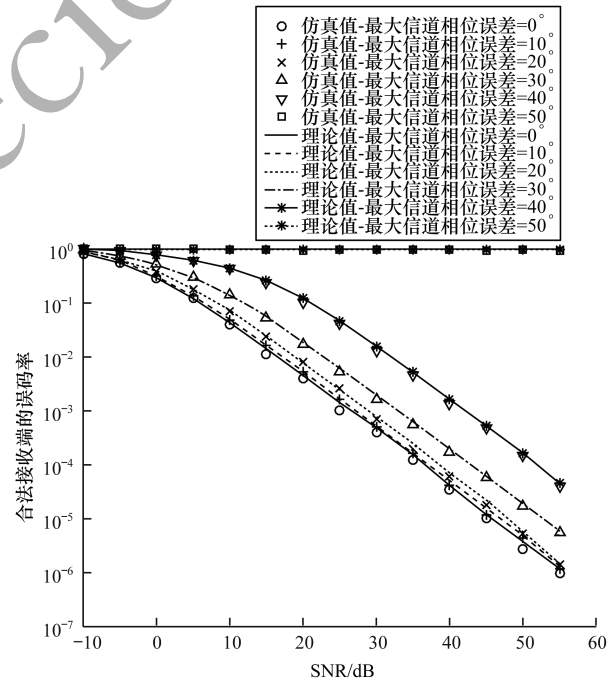


图 4 不同  $\delta_R$  下合法接收端的误码率随 SNR 的变化曲线  
Fig. 4 Curve of bit error rate of legitimate receivers changing with SNR under different  $\delta_R$

综上,信道相位估计误差对合法接收端的性能具有影响。系统对信道相位估计误差有一定的容忍度,在信道相位误差较小的情况下具有鲁棒性。过高的信道相位估计误差会使系统性能急速变差。当信道相位估计误差大到一定程度时,合法接收端的误码率保持为1,符号判决完全错误。

由于带有幅度估计误差的理论分析较复杂,因此本文仅针对信道幅度估计误差对合法接收端性能的影响进行仿真分析。仿真设置信道系数服从均值为0、方差 $\sigma_R^2$ 为1的复高斯分布,信道相位在 $[0, 2\pi]$ 之间呈均匀分布。信道幅度估计误差用比值系数 $\alpha = |\hat{h}|/|h|$ 表示,设置比值系数为1.0、1.2、1.5、2.0和3.0。

信道幅度估计误差对合法接收端误码率的影响如图5所示,可以看出:1)在同等信噪比的条件下,信道幅度估计误差越大,合法接收端的误码率越大;2)在同等幅度估计误差的条件下,当信噪比增大到一定程度时,合法接收端的误码率保持不变。

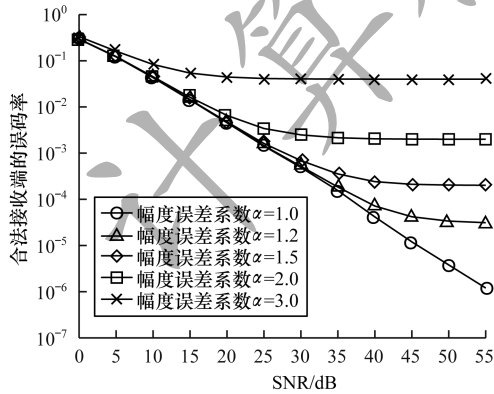


图5 不同幅度估计误差下合法接收端误码率随SNR的变化曲线

Fig. 5 Curve of bit error rate of legitimate receivers changing with SNR under different amplitude estimation errors

#### 4.2 智能攻击型窃听端

在蒙特卡洛仿真时,设置SNR的值为0 dB、10 dB、20 dB和30 dB。在不同信噪比条件下,仿真智能攻击型窃听端的误码率随SNR的变化情况,结果如图6所示。由图6可以看出:1) $\varepsilon_{\text{int}}$ 约为 $42^\circ \sim 319^\circ$ 时误码率为1,此时符号完全跳出判决区域,符号错误概率为100%,可知信道相位估计误差不能大于 $42^\circ$ ;2)当信道相位估计误差在 $15^\circ$ 以内时,误码率曲线相对平坦。这是由于在 $\varepsilon_{\text{int}}$ 较小时, $\varepsilon_{\text{int}}$ 对智能攻击型窃听端的误码率影响很小,智能攻击型窃听

端的误码率对 $\varepsilon_{\text{int}}$ 不敏感;3)当信道相位估计误差在 $15^\circ \sim 42^\circ$ 时,智能攻击型窃听端的误码率随 $\varepsilon_{\text{int}}$ 的增大而增大。这是因为信道相位误差较大时,接收符号发生跳转与偏移,符号落在非判决区域内产生符号错误。

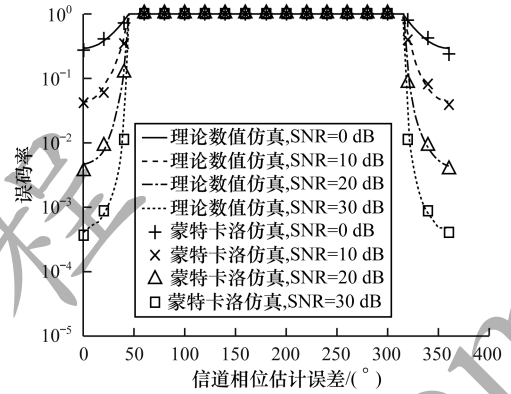


图6 不同SNR下智能攻击型窃听端的误码率变化曲线  
Fig. 6 Curve of bit error changes of intelligent attacking eavesdroppers under different SNR

综上,系统的信道相位误差会导致符号错判,当信道相位估计误差大于 $15^\circ$ 小于 $42^\circ$ 时,接收端误码率随相位误差的增大而增大;当信道相位估计误差大于 $42^\circ$ 时,符号完全错判;当信道相位估计误差小于 $15^\circ$ 时,相位误差对接收端误码率的影响较小。

#### 5 结束语

本文在信道估计存在误差的情况下,研究信道相位对星座模糊设计方案的影响,分析系统合法接收端和智能攻击型窃听端信号接收方式,推导出带有信道相位误差的合法接收端理论误码率公式。结合理论公式仿真分析信道相位估计误差对合法接收端和智能攻击型窃听端误码率的影响。仿真结果表明,接收端对 $15^\circ$ 以内的信道相位误差有一定的容忍度,信道相位误差在 $15^\circ \sim 42^\circ$ 之间时,接收端的误码率随相位误差的增大而提高,过高的信道相位估计误差会使系统性能快速下降。基于星座模糊的物理层加密技术能从实际信号的角度来解决窃听问题,具有现实意义与实用价值,下一步将结合信道幅度估计误差对系统性能进行研究。此外,本文主要采用信道系数与已调符号矢量叠加的星座模糊设计方案,信号星座还有其他多种设计方法,研究不同的加密方法以提高本文系统的安全性能也是今后的研究方向。

## 参考文献

- [1] SHAFIEE S, ULUKUS S. Achievable rates in Gaussian MISO channels with secrecy constraints [C]//Proceedings of 2007 IEEE International Symposium on Information Theory. Washington D. C., USA: IEEE Press, 2007: 2466-2470.
- [2] KHISTI A, WORNELL G, WIESEL A, et al. On the Gaussian MIMO wiretap channel [C]//Proceedings of 2007 IEEE International Symposium on Information Theory. Washington D. C., USA: IEEE Press, 2007: 2471-2475.
- [3] WANG Kun, WANG Xiyuan, ZHANG Xianda. SLNR-based transmit beamforming for MIMO wiretap channel [J]. Wireless Personal Communications, 2013, 71(1): 109-121.
- [4] LI Q, MA W K. Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming [J]. IEEE Transactions on Signal Processing, 2011, 59(8): 3799-3812.
- [5] BAGHERIKARAM G, MOTAHARI A S, KHANDANI A K. The secrecy capacity region of the Gaussian MIMO broadcast channel [J]. IEEE Transactions on Theory, 2013, 59(5): 2673-2682.
- [6] NEGI R, GOEL S. Secret communication using artificial noise [C]//Proceedings of Vehicular Technology Conference. Washington D. C., USA: IEEE Press, 2005: 1906-1910.
- [7] LI Xiangyu, JIN Liang, HUANG Kaizhi, et al. A physical layer security transmission mechanism of relay system based on joint channel characteristics [J]. Chinese Journal of Computers, 2012, 35(7): 1399-1406. (in Chinese)  
李翔宇, 金梁, 黄开枝, 等. 基于联合信道特征的中继物理层安全传输机制 [J]. 计算机学报, 2012, 35(7): 1399-1406.
- [8] GAO Ruifeng, NI Danyan, BAO Zhihua, et al. Time-bandwidth allocation scheme for physical layer security in cooperative cognitive radio networks [J]. Computer Science, 2016, 43(4): 163-166, 187. (in Chinese)  
高锐锋, 倪丹艳, 包志华, 等. 基于时频资源分配的认知无线中继网络物理层安全研究 [J]. 计算机科学, 2016, 43(4): 163-166, 187.
- [9] LAI L, EL GAMAL H. The relay-eavesdropper channel: cooperation for secrecy [J]. IEEE Transactions on Information Theory, 2008, 54(9): 4005-4019.
- [10] LUO S, LI J, PETROPULU A. Physical layer security with uncoordinated helpers implementing cooperative jamming [C]//Proceedings of 2012 IEEE Sensor Array and Multichannel Signal Processing Workshop. Washington D. C., USA: IEEE Press, 2012: 97-100.
- [11] DONG L, HAN Z, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888.
- [12] EKREM E, ULUKUS S. Secrecy in cooperative relay broadcast channels [J]. IEEE Transactions on Information Theory, 2011, 57(1): 137-155.
- [13] SONG Huiying, GAO Yuanyuan, SHA Nan. An effective method of improving security performance of RFID system physical layer [J]. Computer Engineering, 2018, 44(5): 119-123. (in Chinese)  
宋慧颖, 高媛媛, 沙楠. 一种有效提高 RFID 系统物理层安全性能的方法 [J]. 计算机工程, 2018, 44(5): 119-123.
- [14] WANG Shaodi, GAO Baojian, ZHANG Yucheng, et al. Physical layer security scheme based on jointly optimal relay selection [J]. Computer Engineering, 2019, 45(2): 148-153. (in Chinese)  
王少迪, 高宝建, 张育铨, 等. 基于中继联合优化选择的物理层安全方案 [J]. 计算机工程, 2019, 45(2): 148-153.
- [15] LIU Y, DRAPER S C, SAYEED A M. Exploiting channel diversity in secret key generation from multipath fading randomness [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(5): 1484-1497.
- [16] AONO T, HIGUCHI K, OHIRA T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels [J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784.
- [17] REN Kui, SU Hai, WANG Qian. Secret key generation exploiting channel characteristics in wireless communications [J]. IEEE Wireless Communications, 2011, 18(4): 6-12.
- [18] BLOCH M, BARROS J, RODRIGUES M R D, et al. Wireless information-theoretic security [J]. IEEE Transactions on Information Theory, 2008, 54(6): 2515-2534.
- [19] GOERGEN N, LIN W S, LIU K J R, et al. Extrinsic channel-like fingerprint embedding for authenticating MIMO systems [J]. IEEE Transactions on Wireless Communications, 2011, 10(12): 4270-4281.
- [20] WILLIAM E C. Intrinsic physical-layer authentication of integrated circuits [J]. IEEE Transactions on Information Forensics and Security, 2011, 7(1): 14-24.
- [21] CHEN B, MARTINIAN E, WORNELL G W. Authentication with distortion criteria [J]. IEEE Transactions on Information Theory, 2005, 51(7): 2523-2542.
- [22] XI Chenjing, GAO Yuanyuan, SHA Nan, et al. Introduction of signal constellation design approach for physical layer security [J]. Journal of Chinese Computer Systems, 2018, 39(12): 2675-2680. (in Chinese)  
奚晨婧, 高媛媛, 沙楠, 等. 物理层安全信号星座的设计方法研究 [J]. 小型微型计算机系统, 2018, 39(12): 2675-2680.

- [23] MA Ruifeng, DAI Linglong, WANG Zhaocheng, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion[J]. IEEE Transactions on Consumer Electronics, 2010, 56(3): 1328-1332.
- [24] HAN C, HASHIMOTO T, SUEHIRO N. Constellation-rotated vector OFDM and its performance analysis over rayleigh fading channels [J]. IEEE Transactions on Communications, 2010, 58(3): 828-838.
- [25] PÖPPER C, TIPPENHAUER N O, DANEV B, et al. Investigation of signal and message manipulations on the wireless channel [C]//Proceedings of European Conference on Research in Computer Security. Berlin, Germany: Springer, 2011: 40-59.
- [26] CHEN Bin, ZHU Chunsheng, LI Wei, et al. Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper[J]. IEEE Access, 2016, 4: 3016-3025.
- [27] XU Zhijiang, YUAN Teng, GONG Yi, et al. Achieving secure communication through random phase rotation technique[C]//Proceedings of Wireless Communications and Mobile Computing Conference. Washington D. C., USA: IEEE Press, 2017: 23-36.
- [28] ALTHUNIBAT S, SUCASAS V, RODRIGUEZ J. A physical-layer security scheme by phase-based adaptive modulation[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 9931-9942.
- [29] HUSAIN M I, MAHANT S, SRIDHAR R. CD-PHY: physical layer security in wireless networks through constellation diversity [C]//Proceedings of 2012 IEEE Military Communications Conference. Washington D. C., USA: IEEE Press, 2012: 1-9.
- [30] MA R, WANG Z, YANG Z. Improving physical layer security using APSK constellations with finite-alphabet inputs[C]//Proceedings of 2013 International Wireless Communications and Mobile Computing Conference. Washington D. C., USA: IEEE Press, 2013: 149-152.
- [31] ZANG Guozhen, HUANG Baohua, CHEN Lihua, et al. One transmission scheme based on variable MSK modulator for wireless physical layer security [C]//Proceedings of 2015 International Conference on Wireless Communications and Signal Processing. Washington D. C., USA: IEEE Press, 2015: 1-5.
- [32] MAO Xiangning, LIN Kaijia, LIU Hao. A physical layer security algorithm based on constellation [C]//Proceedings of IEEE International Conference on Communication Technology. Washington D. C., USA: IEEE Press, 2018: 52-69.
- [33] HUANG Y, EL-HAJJAR M. Multi-dimensional encryption scheme based on physical layer for fading channel[J]. IET Communications, 2018, 12(19): 25-36.
- [34] LEI Beibei. Research on modulation concealment algorithm based on physical layer encryption [D]. Xi'an: Northwest University, 2012. (in Chinese)  
雷蓓蓓. 基于物理层加密的调制方式隐蔽算法研究[D]. 西安: 西北大学, 2012.
- [35] XIONG Tao, LOU Wei, ZHANG Jin, et al. MIO: enhancing wireless communications security through physical layer multiple inter-symbol obfuscation [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(8): 1678-1691.
- [36] LIU Sijing, GAO Baojian, WU Qian, et al. Algorithm for OFDM physical layer security based on iterative encryption[J]. Computer Engineering and Applications, 2014, 50(22): 88-91. (in Chinese)  
柳斯婧, 高宝建, 吴谦, 等. 基于迭代加密的 OFDM 系统物理层安全算法[J]. 计算机工程与应用, 2014, 50(22): 88-91.

编辑 吴云芳