基于对称 α 稳定分布的隐蔽通信系统

王亢¹, 贡毅^{2*}, 周国民¹, 徐志江³, 卢为党³, 华惊宇³

1. 浙江警察学院计算机与信息技术系, 杭州 310053

2. 南方科技大学电子与电气工程系, 深圳 518055

3. 浙江工业大学信息工程学院, 浙江省通信网技术应用研究重点实验室, 杭州 310023

* 通信作者. E-mail: gong.y@sustc.edu.cn

收稿日期: 2016-07-04; 接受日期: 2016-08-31; 网络出版日期: 2017-01-12

国家自然科学基金 – 浙江两化融合联合基金 (批准号: U1509219)、国家自然科学基金 (批准号: 61471322, 61402416, 61531009) 和广东省科技计划项目 (批准号: 2016A010101003) 资助

摘要 提出了一种新的隐蔽通信系统, 利用 α 稳定分布随机序列前后半码元周期的相关性来传输信息对比特. 为了降低调制信号在时域上的相关性, 通过交织器对调制信号进行置乱后传输. 利用改进的循环谱密度来检测信道中信号的隐蔽情况, 验证了所提出系统具有很强的隐蔽性. 最后仿真和分析了系统的误码率性能, 结果表明系统具有很好的性能.

关键词 隐蔽通信, 对称 α 稳定分布, 交织器, 循环谱, 几何功率

1 引言

由于无线信道的广播特性, 窃听方可能会截获合法用户之间的信息交换, 因此, 通过无线信道实现机密信息的安全传输, 仍然是一个具有挑战性的难题^[1,2]. 隐蔽通信是解决保密通信和军事通信安全性的重要通信手段之一^[3], 它既可以保护通信内容, 还可以隐藏通信的存在. 目前关于隐蔽通信的研究也有很多, 主要有混沌调制技术和扩频调制技术. 例如, Narayanan 等^[4]提出了一种噪声调制扩频技术, 噪声调制信号在正交极化下传输来模仿无极性噪声, 使线性极化接收器无法识别解码或提取有用信息.

Salberg 和 Hanssen^[5]提出了一种新的物理层安全的、基于随机过程键控 (SPSK) 的数字通信系统. 比特 “0” 以随机信号 $X_0(t), t \in [0, T_b)$ 的一个样本来表示; 比特 “1” 以随机信号 $X_1(t), t \in [0, T_b)$ 的一个样本来表示, 其中 T_b 为比特持续时间. 由于随机过程样本的随机性, SPSK 调制具有两个突出的优点: 连续两个相同比特, 随机过程的样本是不同的; 不同的比特, 样本的统计特性不同但相似. 这两个特点, 降低了截获的概率; 同时, 窃听方即使截获合法用户的通信信号, 亦难以解调.

引用格式: 王亢, 贡毅, 周国民, 等. 基于对称 α 稳定分布的隐蔽通信系统. 中国科学: 信息科学, 2017, 47: 374–384, doi: 10.1360/N112016-00166
Wang K, Gong Y, Zhou G M, et al. A novel covert communication system based on symmetric α -stable distribution (in Chinese). Sci Sin Inform, 2017, 47: 374–384, doi: 10.1360/N112016-00166

α 稳定分布的概念最早由 Levy 于 1925 年在研究广义中心定理时提出, Shao 等^[6,7]首次将 α 稳定分布的概念和理论引入到信号处理领域, 用于描述那些具有显著的尖峰脉冲状波形和较厚概率密度函数拖尾的噪声. 文献 [8~15] 指出, 在多用户网络中, 多路接入噪声/干扰可用 α 稳定分布来描述. Gulati 等^[8]研究了不同的网络拓扑结构, 空间 Poisson 分布干扰源条件下的共路干扰统计特性, 指出全区域 Poisson 分布, 例如传感网和 Ad hoc 网, 干扰的统计模型为对称 α 稳定 (SaS) 分布. Lee 等^[9]证明了网络节点为 Poisson 点过程 (PPP) 分布的大规模无线传感网络, 其汇聚信号和干扰服从 α 稳定分布. 文献 [10~12] 考察了多个移动运营商, 多种蜂窝技术 (GSM/UMTS/LTE), 不同的应用场景, 指出蜂窝小区中的基站空间分布概率密度函数呈现出强重尾特性, 同样的情况也出现在宽带网络和蜂窝网络中的业务流量中, 因此用 α 稳定分布比 Poisson 分布更符合实际. Lagunna-Sanchez 等以实验数据表明, 用 α 稳定分布能贴切地描述电力线信道 (PLC) 中噪声的统计模型^[13]. 除了无线通信领域, α 稳定分布模型还可用于其他领域, 如医学^[14]、激光陀螺仪^[15]、合成孔径雷达 (SAR)^[16]等.

正因为无线通信信道中的干扰/噪声服从 α 稳定分布, Cek 等^[17]提出了一种调制 SaS 随机过程特征指数的隐蔽通信系统: 用两个不同特征指数的 SaS 随机过程序列分别对应二进制比特 “0” 和比特 “1”, 即当传输比特 “0” 时发送 $S_{\alpha_0}S$ 序列; 当传输 “1” 时发送 $S_{\alpha_1}S$ 序列. 但是, 这种方法存在一些缺点: 它需要很多个样本来估计 SaS 分布的特征指数, 计算量比较大; 同时, 不同特征指数的 SaS 随机序列, 例如 Cauchy 分布和 Gauss 分布, 在时域上具有明显不同的脉冲特性, 降低了通信的隐蔽性. 本文在此基础上提出了一种新的隐蔽通信系统: 将两个 SaS 分布信号源精简为一个, 比特周期 T_b 分成前半周期和后半周期, 传输的二进制比特来调制前后两个半周期随机序列之间的相关性. 在接收端, 通过相关器计算前后半周期序列之间的相关系数来解调. 再者, 在调制器中引入了交织器, 在降低传输信号时域相关性的同时, 增加了窃听方正确解调的难度. 为了验证通信的隐蔽性, 利用循环谱来检测信道中是否存在信号.

本文的组织如下: 第 2 节介绍了 SaS 分布, 几何功率和循环谱密度等理论背景知识. 第 3 节介绍了所提出的通信系统结构, 分别对发送端的调制系统和接收端的解调系统进行了阐述. 然后, 分析了系统的隐蔽性并用循环谱的方法来验证. 第 4 节是仿真与分析, 通过设置不同的仿真参数, 获得了系统的误码率性能. 最后, 在 5 节做了总结.

2 理论背景

本节简单介绍了 SaS 分布, 几何功率和循环谱密度的理论基础.

2.1 对称 α 稳定分布

除了几个例外, 服从 SaS 分布的随机过程 $X(t)$, 其闭合解析式的概率密度函数 (PDF) 是不存在的, 通常用特征函数 (CF) 来进行描述^[7],

$$\Phi(t) = e^{-\gamma|t|^\alpha}, \quad (1)$$

其中参数 $\alpha \in (0, 2]$ 称为特征指数 (characteristic exponent), 它决定了该随机过程脉冲特性的程度. 特征指数 α 越小, 脉冲特性越明显, PDF 曲线的尾部越厚重, 并以 $-(\alpha + 1)$ 次幂的代数速率衰减; 反之, 则脉冲特性减弱. 参数 $\gamma = \sigma^\alpha$ 称为尺度系数 (scale), σ 称为散度系数 (dispersion), 它们均表示相对于均值 (或中值) 的分散程度, 类似于 Gauss 分布中的方差.

表 1 几种常见分布的几何功率与相应的二阶功率
Table 1 Geometric and second-order powers of several common distributions

Name	PDF	Geometric power	2nd-order power
Uniform	$f(x) = \frac{1}{\sigma}, x < \sigma/2$	$\frac{\sigma}{2e}$	$\frac{\sigma^2}{12}$
Gaussian	$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}, x \in \mathbb{R}$	$\frac{\sigma}{\sqrt{2C_g}}$	σ^2
Cauchy	$f(x) = \frac{1}{\pi} \frac{\sigma}{x^2 + \sigma^2}, x \in \mathbb{R}$	σ	∞
S α S	$\mathbb{F}^{-1}[e^{- \sigma\omega ^\alpha}]$	$\sigma C_g^{\frac{1}{\alpha}-1}$	∞

S α S 分布随机过程的概率密度函数是其特征函数的 Fourier 反变换, 也即

$$f_\alpha(x) = \mathbb{F}^{-1}[\Phi(t)] = \int_{-\infty}^{+\infty} e^{-\gamma|t|^\alpha - jxt} dt = 2 \int_0^{+\infty} e^{-\gamma t^\alpha} \cos(xt) dt, \quad (2)$$

式中 $\mathbb{F}^{-1}$ 表示 Fourier 反变换. 存在闭合解析式的概率密度函数的 S α S 分布为 $\alpha = 1$ 时的 Cauchy 分布和 $\alpha = 2$ 时的 Gauss 分布.

在无线通信中, 干扰/噪声服从 S α S 分布的假设是合理的. 虽然 Gauss 分布 ($\alpha = 2$) 是 S α S 分布的一个特例, 为了明确起见, 本文假定 $\alpha < 2$. 对服从 S α S 分布的随机过程 $X(t)$, 记为 $X(t) \sim \mathcal{S}(\alpha, \sigma)$.

2.2 几何功率

对 S α S 分布的随机过程 $X(t)$, $p \geq \alpha$ 阶以上的统计量为无穷大^[7], 因此, 基于二阶统计量的方差(功率)就失去了意义. Gonzalez 等在随机过程对数矩的基础上, 提出了几何功率的概念^[18]. 随机过程 $X(t)$ 的几何功率定义为

$$S_0 = S_0(X(t)) = e^{\mathbb{E}[\log |X(t)|]}, \quad (3)$$

式中 $\mathbb{E}[\cdot]$ 表示期望运算. 对服从 $\mathcal{S}(\alpha, \sigma)$ 分布的随机过程 $X(t)$, 其几何功率 $S_{0,\alpha}$ 为^[18]

$$S_{0,\alpha} = \sigma C_g^{\frac{1}{\alpha}-1}, \quad (4)$$

式中 $C_g \approx 1.78$, 称为 Euler 常数. 表 1 列出了几种常见随机过程的几何功率与相应的二阶功率. 假设信号 $X(t) \sim \mathcal{S}(\alpha_c, \sigma_c)$ 分布, 噪声 $N(t) \sim \mathcal{S}(\alpha_n, \sigma_n)$ 分布, 定义几何信噪比 (GSNR) ρ (dB) 为

$$\rho = 10 \lg \frac{S_{0c}^2}{S_{0n}^2} = 10 \lg \frac{S_0^2(X(t))}{S_0^2(N(t))} = 20 \lg \left(C_g^{\frac{1}{\alpha_c} - \frac{1}{\alpha_n}} \frac{\sigma_c}{\sigma_n} \right). \quad (5)$$

2.3 循环谱密度函数

循环谱理论可用来检测周期平稳信号. 由于 S α S 分布的随机过程不具有 $p \geq \alpha$ 阶以上的统计量, 因此二阶及以上的统计量在处理 S α S 分布信号时会出现性能退化. 为了解决这个问题, 文献 [19] 提出了基于分数低阶矩的循环谱密度, 但需要预先知道 S α S 分布的特征指数, 且计算复杂. 文献 [20] 在对 $X(t) \sim \mathcal{S}(\alpha, \sigma)$ 的随机过程做幅度变换的基础上, 提出了广义二阶循环自相关函数的定义. 变换函数为

$$g(X(t)) = \frac{\arctan(|X(t) + j\mathbb{H}[X(t)]|)}{|X(t) + j\mathbb{H}[X(t)]|} X(t), \quad (6)$$

图 1 变换后的 $S_{\alpha}S$ 序列的自相关性和互相关性

Figure 1 Auto correlation function (ACF) and cross correlation function (CCF) of the transformed $S_{\alpha}S$ stochastic sequence. (a) ACF; (b) CCF

其中 $\mathbb{H}[\cdot]$ 为 Hilbert 变换. 对于任一时刻的信号 $X(t)$, 可以表示为 $X(t) = R(t) \cos \theta(t)$, 其中 $R(t)$ 为幅值, $\theta(t)$ 为相位. 对于窄带通信信号, $R(t) \cos \theta(t) + \mathbb{H}[R(t) \cos \theta(t)] = R(t)e^{j\theta(t)}$, 则式 (6) 可简化为

$$g(X(t)) = \frac{\arctan(|R(t)e^{j\theta(t)}|)}{|R(t)e^{j\theta(t)}|} R(t) \cos \theta(t) = \arctan(R(t)) \cdot \cos \theta(t). \quad (7)$$

因此 $g(X(t))$ 变换, 将随机过程 $X(t)$ 的幅值映射到了一个有限区间, 这就保证了其二阶循环统计量是有意义的, 并且式 (6) 的变换前后, 它们的相位是相同的, 也即变换不对相位做任何改变.

$S_{\alpha}S$ 随机过程经过式 (6) 变换之后具有自相关最大, 互相关为 0 的性质. 如图 1 所示, 长度为 100 的两个参数相同的 $S(\alpha, \sigma)$ 随机序列样本, 可看到自相关类似于 $\delta(n)$ 函数, 而互相关近似为 0.

广义二阶循环自相关函数的定义为

$$\text{GR}_{X(t)}^{\epsilon}(\tau) = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} g(X(t + \tau/2)) g^*(X(t - \tau/2)) \exp(-j2\pi\epsilon t) dt, \quad (8)$$

其中 T_0 为时间平均的周期; ϵ 为循环频率; $(\cdot)^*$ 为共轭运算. 广义二阶循环自相关函数经过 Fourier 变换, 得到广义二阶循环谱密度函数, 其表达式为^[20]

$$\text{GS}_{X(t)}^{\epsilon}(f) = \int_{-\infty}^{+\infty} \text{GR}_{X(t)}^{\epsilon}(\tau) \exp(-j2\pi f \tau) d\tau. \quad (9)$$

取不同的特征指数值, 利用式 (9) 计算 $S_{\alpha}S$ 分布噪声的广义二阶循环谱密度, 得到如图 2 所示. 图中 $\alpha = 2$ 的 Gauss 噪声, 与文献 [21] 中 Gauss 噪声的循环谱密度图相一致.

3 系统结构及隐蔽性分析

本节详细阐述所提出的通信系统结构, 包括为了降低传输波形在时域上的相关性而引入的交织器, 以及用 Matlab 仿真和循环谱检测, 验证了所提出的通信系统具有很好的隐蔽性.

3.1 通信系统结构

本文提出的通信系统发送端结构如图 3 所示. 信源产生二进制比特序列, T_b 为比特周期. 用 $S_{\alpha}S$ 分布序列的前后 $T_b/2$ 之间的相关性来进行调制, 也即, 如果传输的是比特 “0”, 则后半周期与前半周

图 2 (网络版彩图) 不同特征指数 $S_{\alpha}S$ 随机过程的循环谱密度

Figure 2 (Color online) Cyclic power spectral density (CPSD) of $S_{\alpha}S$ stochastic process with various characteristic exponents. (a) $\alpha = 2.0$; (b) $\alpha = 1.5$

图 3 系统结构框图

Figure 3 Schematic for the proposed communication system

期序列相同; 如果传输的是比特“1”, 则后半周期与前半周期序列的极性相反. 记 $c(t)$ 为长度为 T_b 的 $S_{\alpha}S$ 分布信号, 传输比特 $m \in \{0, 1\}$ 时, 发送的信号为

$$s(t) = \begin{cases} c(t), & 0 \leq t < T_b/2, \\ (-1)^m c(t - T_b/2), & T_b/2 \leq t < T_b. \end{cases} \quad (10)$$

因为前半周期信号与后半周期信号的相关性 $r = \pm 1$, 调制后的随机过程在时域上具有明显的相关性. 为了增加通信的隐蔽性, 通过交织器置乱以降低传输信号在时域上的相关性. 同时, 窃听方对合法方所采用的交织器的结构是未知的. 因此, 交织器的引入, 增加了窃听者破解的难度.

如图 3 所示的系统框图中包含了接收端的结构. 接收机先对接收到的信号进行解交织, 利用信号的前后半周期的相关性, 可以解调出发送端的比特序列. 对比特 m , 发送端发送调制信号 $s(t)$; 假定系

图 4 交织前后信号在时域上的对比图

Figure 4 Modulated signal in time domain comparison before and after the interleaver. (a) Message bit sequence; (b) modulated signal before the interleaver; (c) modulated signal after the interleaver

统已经同步, 不考虑噪声, 则接收机端收到后, 经过解交织和变换后为 $g(s(t))$; 进入相关器, 做前后半周期的相关运算, 相关器的输出值为 z ; 最后与判决门限 0 相比较, 得到发送比特 m 的估计 $\hat{m}$. 解调过程数学表达式为

$$\begin{aligned} z &= \int_{T_b/2}^{T_b} g(s(t))g(s(t - T_b/2))dt = \int_{T_b/2}^{T_b} g((-1)^m c(t - T_b/2))g(c(t - T_b/2))dt \\ &= (-1)^m \int_0^{T_b/2} g^2(c(t))dt \stackrel{\hat{m}=0}{\geq} 0. \end{aligned} \quad (11)$$

在解调器中引入了 $g(\cdot)$ 变换, 可以抑制异常且幅值很大的脉冲信号对整个相关器的错误影响. 也即, 在整个相关运算过程中, 如果出现一个异常的强脉冲性信号, 那么经过 $g(\cdot)$ 变换, 降低了如式 (12) 所示的判决错误影响.

3.2 交织器

式 (10) 所示的调制信号, 其前半周期与后半周期的符号相同或者相反, 在时域上具有很强的相关性, 降低了通信的隐蔽性. 因此, 引入了交织器, 利用交织器的置乱, 减小了调制后随机序列在时域上的相关性; 同时, 接收机必须知道交织器的结构才能正确解调, 增加了窃听者破解合法双方通信的难度. 交织器的种类有很多: 规则交织器, 不规则交织器, 随机交织器. 本文采用的是规则交织器, 也称分组交织器^[22]. 分组交织器是一种最简单的交织器. 它以 $M \times N$ 的矩阵形式, 按行写入列读出.

分组交织器虽然不能做到完全无序, 但其实际置乱效果还是较好的, 而且简单易于实现. 令 $T_b = 100$, 随机产生 SaS 分布序列对传输信息序列进行调制. 如图 4 所示, 交织前码元的前半周期与后半周期相关性很大, 经过交织器置乱后, 其相关性大大减小.

3.3 隐蔽性分析

基于 SaS 分布的隐蔽通信系统, 是将要发送的隐蔽信号, 经过图 3 所示的调制后, 与原系统业务信号 (例如 BPSK 调制) 进行重叠, 重叠的原则是不明显影响原来业务信号的通信质量, 而且保证发送的隐蔽信号能够通信. 因此, 本文所述的隐蔽性是以原业务信号在隐蔽通信信号的干扰下误码率变化为衡量指标. 为了方便分析又不失一般性, 下面以离散基带信号进行分析.

假设原业务信号的比特周期为 T_b , 隐蔽通信信号的比特周期也为 T_b , 并设扩频因子 $2\beta = T_b$, 也即在 T_b 时间内产生 2β 个式 (10) 所示的 s_k 个采样值, $k = 1, \dots, 2\beta$; 原业务信号采用 BPSK 调制,

$b \in \{-1, +1\}$ 表示发送的比特信号, 信号功率为 P_B , 信号可以表示为 $u_k = \sqrt{P_B}b$; 记加性噪声 $w(t)$ 的离散采样为 w_k . 系统的接收信号可以表示为

$$r_k = u_k + s_k + w_k. \quad (12)$$

原业务信号的 BPSK 解调, 是对比特周期内的采样值累加, 并通过门限检测器 (阈值为 0) 判决得到的, 也即比特估计值 $\hat{b}$ 为

$$\hat{b} = \text{sgn} \left(\sum_{k=1}^{2\beta} r_k \right) = \text{sgn} \left(\sum_{k=1}^{2\beta} \left(\sqrt{P_B}b + w_k \right) + \underbrace{\sum_{k=1}^{\beta} (1 + (-1)^m) c_k}_{\text{干扰项}} \right), \quad (13)$$

其中 $\text{sgn}(\cdot)$ 是符号函数, c_k 是 S α S 随机过程 $c(t)$ 的离散采样值.

从式 (13) 可看出, 当隐蔽信号比特 $m = 1$ 时干扰项为 0, 对原业务信号不产生影响; 而当 $m = 0$ 时, 由于干扰项的存在, 造成原业务通信误比特率的增大, 降低了通信质量. 设 $c(t), w(t)$ 为相互独立的 S α S 随机过程, S α S 随机过程不存在闭合的解析式, 因此不易得到相应的误比特率表达式. 然而, 从第 4 节的仿真图 7(a) 可以看出, 当 $T_b = 2\beta = 200$, 几何信噪比 $\rho \approx -3$ dB (也即 $c(t)$ 的几何功率比 $w(t)$ 的几何功率小 3 dB) 时, 隐蔽通信系统的误比特率为 10^{-3} . 因此, 隐蔽通信信号嵌入在原业务信号之中, 如果进一步降低隐蔽通信系统对误码率的要求, 那么式 (13) 中的干扰项几何功率可以远小于噪声的几何功率, 从而降低对原业务通信质量的影响, 提高了隐蔽性.

另一方面, 也可利用式 (9) 定义的循环谱来对调制后的信号进行通信系统隐蔽性的检测. 设信息传输速率为 200 比特/秒, 采样频率为 20 kHz, 也即传输一个比特需要长度 $T_b = 100$ 的随机过程样本序列. 假设背景噪声为浅海水声噪声, 文献 [23] 指出, 浅海水声噪声具有非 Gauss 特性和显著的脉冲性, 可用 S α S 稳定分布来描述, 其特征指数 α 集中在 (1.6, 2.0), 平均值为 1.79, 方差为 0.0226. 仿真中, 假设载波与噪声分布均为 S α S 分布. 设噪声特征指数 $\alpha_n = 1.79$; 载波特征指数 $\alpha_c = 1.79$, 散度 $\sigma_c = 1$; 几何信噪比 $\rho = 0$ dB. 以 $10 \times T_b$ 的分组交织器来实现交织, 接收端分别对解交织前后的信号进行检测.

从图 5 所示的循环谱图可看出, 谱线与图 2 一样, 只在循环频率为 0 处存在谱值. 从接收到的信号中, 无法检测出是否隐藏了传输信号. 改变噪声的特征指数再做仿真, 接收到的信号循环谱如图 6 所示, 与背景噪声循环谱仍然相似, 不能有效地区分. 因此, 所提出的通信系统具有很强的隐蔽性.

4 误码率仿真与分析

采用 Matlab 软件对系统的误码率性能进行仿真. 在仿真中, 设载波信号 $X(t) \sim \mathcal{S}(\alpha_c, \sigma_c)$ 分布的随机过程, 其中 $\sigma_c = 1$; 加性噪声信号 $N(t) \sim \mathcal{S}(\alpha_n, \sigma_n)$ 分布; 比特长度为 T_b ; 几何信噪比为 ρ (dB); 除了明确说明外, 假定 $\alpha_c = 1.79$, $T_b = 100$. 仿真时, 分别改变比特长度 T_b , 载波特征指数 α_c 和噪声特征指数 α_n , 在不同几何信噪比 ρ 条件下的系统误比特率. 仿真的系统框图如图 3 所示, 得到结果如图 7 所示.

从图 7 可看出, 随着几何信噪比 ρ 的增大, 误码率逐渐减小. 比特周期 T_b 越大, 在一个周期内, 积累的能量越大, 越不容易出错, 因此误码率越低. 固定噪声的特征指数 $\alpha_n = 1.79$, 改变 α_c 值. 随着

图 5 (网络版彩图) $\alpha_n = 1.79$ 时, 接收信号的循环谱密度图

Figure 5 (Color online) CPSD of the received signal corrupted by additive S α S noise with the characteristic exponent $\alpha_n = 1.79$. (a) Before the deinterleaver; (b) after the deinterleaver

图 6 (网络版彩图) 不同特征指数的噪声下, 接收信号的循环谱密度图

Figure 6 (Color online) CPSD of the received signal corrupted by additive S α S noise with various characteristic exponent α_n . (a) $\alpha_n = 2.0$; (b) $\alpha_n = 1.5$

α_c 的减小, 载波与背景噪声的特征指数相差越大, 这两种随机过程的区别就越明显, 导致误码率降低. 类似地, 固定载波的特征指数 $\alpha_c = 1.79$, 改变噪声的特征指数 α_n , 也可获得相同的结论.

Xu 等^[24] 在 Cek 等^[17] 的基础上, 接收端采用了对数矩的方法来估计接收到信号的特征指数值, 以提高通信系统的误比特率性能; 分析和推导了在无噪声/平坦/频率选择性衰落信道下的理论误比特率 P_b 与参数比特周期 T_b , 特征指数 α_0, α_1 之间的关系. 从文献 [24] 中的图 6 可以看出, 在无噪声无衰落的理想信道条件下, 当 $\alpha_0 = 1, \alpha_1 = 2, T_b = 200$ 时的误比特率大于 0.01. 从图 7(a) 可看出, 本文提出的方法, 在几何信噪比 $\rho = -5$ dB 时, 误比特率小于 0.01, 而且, 误比特率随几何信噪比的增大而快速降低. 因此, 从误比特率性能的角度来比较, 本文提出的方法远远优于文献 [17].

考察调制载波为其他分布随机过程时的系统误码率, 设比特周期 $T_b = 50$, 载波几何功率 $S_{0c}^2 = 1$, 噪声特征指数 $\alpha_n = 1.79$, 其中不同分布的几何功率定义如表 1 所示. 从图 8 可知, 本文提出的调制方式也适用于均匀分布, Cauchy 分布和 Gauss 分布. 不同的载波调制下系统具有不同的误码率性能, 从图 8 中可以看到 Cauchy 分布的误码率性能最好, 均匀分布的误码率性能最差.

图 7 系统误码率

Figure 7 BER performances. (a) Various bit period T_b ; (b) various carrier with α_c ; (c) various noise with α_n

图 8 不同随机过程作载波时的系统误码率

Figure 8 BER Performances for various stochastic processes

5 结论

采用与背景噪声统计特性相似的 SaS 分布随机过程做载波, 以前后半周期序列之间的相关性来

传输信息比特,通过简单的交织器降低了传输波形时域上的相关性.本文提出的通信系统结构简单,仿真表明,循环谱理论不能把传输信号从背景噪声中检测出来,系统具有很好的隐蔽性;同时,在信噪比较低的情况下,系统误码率性能很好,具有很高的可靠性.

参考文献

- 1 Wei H, Zheng B, Hou X. Compressive channel sensing based on random pilot for physical layer communication security. In: Proceedings of IEEE 22nd Wireless and Optical Communication Conference, Chongqing, 2013. 693–698
- 2 Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey. *IEEE Commun Surv Tut*, 2014, 16: 1550–1573
- 3 Zhao D F, Zhu T L, Xue R. Parallel decoding of Turbo codes in covert communications. *J Appl Sci*, 2012, 30: 461–465 [赵旦峰, 朱铁林, 薛睿. 隐蔽通信中的 Turbo 码并行译码. *应用科学学报*, 2012, 30: 461–465]
- 4 Narayanan R M, Chuang J. Covert communications using heterodyne correlation random noise signals. *Electron Lett*, 2007, 43: 1211–1212
- 5 Salberg A B, Hanssen A. Secure digital communications by means of stochastic process shift keying: principles and properties. In: Proceedings of Conference Record of the 33rd Asilomar Conference on Signals, Systems, and Computers, Asker, 1999. 48–53
- 6 Shao M, Nikias C L. Signal processing with fractional lower order moments: stable processes and their applications. *Proc IEEE*, 1993, 81: 986–1010
- 7 Nikias C L, Shao M. *Signal Processing With Alpha-Stable Distributions and Applications*. Hoboken: John Wiley & Sons, 1995
- 8 Gulati K, Evans B L, Andrews J G, et al. Statistics of co-channel interference in a field of Poisson and Poisson-Poisson clustered interferers. *IEEE Trans Signal Process*, 2010, 58: 6207–6222
- 9 Lee J, Tepedelenlioglu C. Distributed detection in coexisting large-scale sensor networks. *IEEE Sens J*, 2014, 14: 1028–1034
- 10 Zhou Y F, Li R P, Zhao Z F, et al. On the α -stable distribution of base stations in cellular networks. *IEEE Commun Lett*, 2015, 19: 1750–1753
- 11 Li R P, Zhao Y F, Qi C, et al. Understanding the traffic nature of mobile instantaneous messaging in cellular networks: a revisiting to α -stable models. *IEEE J Mag*, 2015, 3: 1416–1422
- 12 Chiaraviglio L, Cuomo F, Maisto M, et al. What is the best spatial distribution to model base station density? A deep dive into two European mobile networks. *IEEE Access*, 2016, 4: 1434–1443
- 13 Laguna-Sanchez G, Lopez-Guerrero M. On the use of alpha-stable distributions in noise modeling for PLC. *IEEE Trans Power Delivery*, 2015, 30: 1863–1870
- 14 Achim A, Basarab A, Tzagkarakis G, et al. Reconstruction of ultrasound RF echoes modeled as stable random variables. *IEEE Trans Comput Imag*, 2015, 1: 86–95
- 15 Shen X, Zhang H, Xu Y, et al. Observation of alpha-stable noise in the laser gyroscope data. *IEEE Sens J*, 2016, 16: 1998–2003
- 16 Chen J, Nunez-Yanez J L, Achim A. Bayesian video super-resolution with heavy-tailed prior models. *IEEE Trans Circ Syst Video Tech*, 2014, 24: 905–914
- 17 Cek M E, Savaci F A. Stable non-Gaussian noise parameter modulation in digital communication. *Electron Lett*, 2009, 45: 1256–1257
- 18 Gonzalez J G, Paredes J L, Arce G R. Zero-order statistics: a mathematical framework for the processing and characterization of very impulsive signals. *IEEE Trans Signal Process*, 2006, 54: 3839–3851
- 19 He J A, Pei C Q, Pu Y Y. Cyclic spectrum analysis of BPSK under a non-Gaussian model. *J Lanzhou Univ (Nat Sci)*, 2012, 48: 133–138 [何继爱, 裴承全, 蒲阳阳. 非 Gauss 模型下 BPSK 的循环谱分析. *兰州大学学报 (自然科学版)*, 2012, 48: 133–138]
- 20 Zhao C H, Yang W C, Ma S. Research on communication signal modulation recognition based on the generalized second-order cyclic statistics. *J Commun*, 2011, 32: 144–150 [赵春晖, 杨伟超, 马爽. 基于广义二阶循环统计量的通信信号调制识别研究. *通信学报*, 2011, 32: 144–150]
- 21 Zhang X L, Xu J T, Chen Y S. Detection of BPSK DS signal based on cyclic spectrum correlation technology. *Inf Tech*,

- 2004, 28: 30–32 [张晓林, 徐建太, 陈源胜. 基于循环谱理论的 BPSK 直扩信号检测. 信息技术, 2004, 28: 30–32]
- 22 Zhao G L, Wu Y N. An analysis of the interleavers for Turbo codes. J Appl Sci, 2002, 20: 38–41 [赵光玲, 吴乐南. 几种用于 Turbo 码的交织器分析. 应用科学学报, 2002, 20: 38–41]
- 23 Zha D F, Shu T, Chen D, et al. Robust blind shallow water channel equalizer based on fractional lowes order impulsivenoise model. J Commun, 2008, 29: 133–138 [查代奉, 舒彤, 陈丁, 等. 基于分数低阶脉冲噪声模型的浅海水声信道盲均衡方法. 通信学报, 2008, 29: 133–138]
- 24 Xu Z J, Wang K, Gong Y, et al. Structure and performance analysis of an SoS-based digital modulation system. IET Commun, 2016, 10: 1329–1339

A novel covert communication system based on symmetric α -stable distribution

Kang WANG¹, Yi GONG^{2*}, Guomin ZHOU¹, Zhijiang XU³, Weidang LU³ & Jingyu HUA³

1. Department of Computer and Information Technology, Zhejiang Police College, Hangzhou 310053, China;

2. Department of Electrical and Electronic Engineering, South University of Science and Technology of China, Shenzhen 518055, China;

3. College of Information Engineering, Zhejiang University of Technology, Zhejiang Provincial Key Laboratory of Communication Networks and Applications, Hangzhou 310023, China

* Corresponding author. E-mail: gong.y@sustc.edu.cn

Abstract A novel structure for covert communication is proposed in this study. The correlation coefficient of two adjacent symmetric α -stable (SoS) noise sequences is modulated by the binary message sequence to achieve a covert communication system. In order to reduce the correlation of the modulated signal in the time domain, the modulated signal is scrambled by an interleaver. To verify the covertness of the proposed communication system, an improved circulation spectral density function is employed to detect whether the transmitted signal exists. The simulation results show that the proposed system has strong concealment. Moreover, the bit error rate (BER) performance is simulated and analyzed. The results show that the system has a good performance.

Keywords covert communication, symmetric α -stable distribution, interleaver, cyclic power spectral density, geometric power

Kang WANG was born in 1978. She received her B.S. and M.S. degrees in information and communication engineering from the Xi'an JiaoTong University, Xi'an, in 2001 and 2004, respectively. She is an associate professor in the Department of Computer and Information Technology at the Zhejiang Police College, Hangzhou, since 2006. Her main research interests include wireless communications theory, signal detection, and physical layer security for wireless systems.

Yi GONG received his Ph.D. degree in electrical engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2002. Currently, he is a professor at the Southern University of Science and Technology, Shenzhen, China. His research interests include cognitive radio, full-duplex communications, wireless energy harvesting, and physical layer security for wireless systems.