

## DM-UKF 混沌拟合破译混沌直接序列扩频通信\*

甘露<sup>†</sup> 熊波

(电子科技大学电子工程学院, 成都 611731)

(2012年4月17日收到; 2012年5月22日收到修改稿)

针对已有混沌直接序列扩频通信系统的破译算法在低扩频因子和较大多径衰落下无法有效破译信息码的问题, 提出了一种基于双模型无迹卡尔曼滤波混沌拟合的破译算法. 所提算法联合多模型滤波原理, 利用信息符号为有限集的特点, 针对其不同取值分别建立对应的滤波模型. 各模型下滤波器并行工作, 利用广义同步系统同时拟合原混沌系统并估计混沌直扩信号, 通过估计误差确定最佳匹配滤波模型, 从而得到信息符号的估计. 进一步通过引入误差控制因子, 增大了不同模型下估计误差的距离, 不仅有利于信息符号判定, 并且减小了噪声和多径衰落对破译结果的影响. 理论推导和仿真结果均证明提出的算法优于已有破译算法.

**关键词:** 双模型, 无迹卡尔曼滤波, 混沌直扩, 破译

**PACS:** 05.45.-a, 05.45.Vx

## 1 引言

混沌信号特有的对初值敏感、非周期、类随机、宽频谱和长期不可精确预测性, 使得其在军事通信与保密通信中具有一定优势<sup>[1,2]</sup>. 自从美国海军实验室的 Pecora 和 Carroll 于 1990 年利用驱动-响应法实现了两个混沌系统的同步以来<sup>[3]</sup>, 针对混沌通信技术的研究逐步展开. 目前, 混沌通信技术主要包含混沌掩盖、混沌键控、混沌参数调制和混沌扩频等方面<sup>[4-17]</sup>.

自适应滤波技术作为信号处理的基本手段, 近年来被广泛用于解决混沌通信中的问题<sup>[18-22]</sup>. 文献[18]提出基于扩展卡尔曼滤波器 (extended Kalman filter, EKF) 的混沌通信, 文献[19]基于均方误差和克拉美罗界对 EKF 混沌同步性能进行了评估, 证明了其有效性和优越性. 冯久超等<sup>[21]</sup>在文献[20]的基础上, 将无迹卡尔曼滤波器 (unscented Kalman filter, UKF) 应用于混沌通信中的盲信道均衡问题, 得到一种较为实用的均衡器. 徐茂格<sup>[22]</sup>研究了粒子滤波 (particle filter, PF) 在混沌同步、信道

估计与均衡、混沌通信信号检测等方面的应用.

将混沌信号作为直扩通信的扩频序列, 不仅具有良好的抗干扰性、隐蔽性和低截获概率等传统伪随机序列所具备的优点, 而且容易得到大量的永不重复的码序列, 因而混沌直扩通信技术受到了广泛重视<sup>[13-17]</sup>, 其性能在水下通信中得到了验证<sup>[16,17]</sup>. 与混沌通信相对应发展起来的是混沌通信破译技术<sup>[23-30]</sup>, 二者此消彼长的关系不停地推动着混沌保密通信的进一步发展. 近年来, 混沌直扩通信系统的破译取得了进展, 其中胡进锋等<sup>[28,29]</sup>提出了用 UKF 混沌拟合估计混沌直扩通信信息码的破译方法. 该方法利用混沌直扩信号中只有一个混沌吸引子和信息码为慢变信号的特性, 分别建立了基于信息符号和拟合混沌的滤波模型, 两个滤波器交替工作完成混沌破译. 同时, 加入跟踪误差控制因子将混沌拟合误差和过程噪声变成有利因素加以利用, 在原始混沌映射未知条件下实现了破译. 文献[30]进一步讨论了多径衰落信道下混沌直扩通信的可破译性. 然而, 上述方法将信息符号建立为慢变模型, 使得扩频因子较小的情况下该方法破译效果变差; 同时, 当多径衰落较大时, 该

\* 中国工程物理研究院科学基金 (批准号: 2010A040317) 和中央高校基本科研业务费专项资金 (批准号: ZYGX2010J027) 资助的课题.

<sup>†</sup> E-mail: ganlu@uestc.edu.cn

方法也会失效.

针对 UKF 混沌拟合破译算法的缺陷, 联合多模型滤波算法, 本文提出基于双模型 (dual model, DM) UKF (DM-UKF) 混沌拟合破译算法, 进一步加入误差控制因子以改善破译性能, 并通过相应的信息判定表达式推导出误差控制因子的自适应取值. 与 UKF 破译算法直接估计信息符号不同, DM-UKF 混沌拟合破译方法利用信息符号为有限集的特点, 针对其不同取值分别建立对应的滤波模型. 各个滤波器利用一个广义系统拟合原混沌系统并估计混沌直扩信号, 继而通过估计误差判断最佳匹配滤波模型, 得到信息符号的破译结果. 由于各模型滤波器在采样时间内始终同时存在, 故破译算法受扩频因子长度影响较小. 同时, 推导出的自适应误差控制因子增大了不同模型下估计误差的距离, 从而减小了测量值不精确带来的误差, 故所提算法具有一定的抗多径衰落和低信噪比的性能. 理论推导和仿真均证明所提算法优于文献 [28—30] 中使用的方法.

## 2 已有破译算法描述

在混沌直扩通信中, 系统利用混沌信号的宽频谱特性, 以特定的混沌映射产生扩频序列来实现对低码率信息的频谱扩展. 设系统中采用的混沌序列  $\{X(k)\}$  由混沌映射  $f$  迭代产生, 即

$$X(k+1) = f(X(k)), \quad (1)$$

则扩频后的发送序列为  $s(k) = b_n \times X(k)$ ,  $k = 1 + (n-1)S_f, \dots, nS_f$ , 其中  $b_n$  为信息码序列, 当系统传送信息码为二进制序列时其取值为  $\{-1, 1\}$ ,  $S_f$  为扩频因子. 接收端利用自有的混沌映射系统产生与发射端相同的混沌扩频序列, 从而实现信息码的解扩. 显然在混沌直扩通信系统中要求接收端与发射端采用相同混沌映射及相同的初值并在通信过程中保持收发两端混沌映射的演化同步, 才能实现对接收信号的解扩. 而混沌直扩通信破译就是在未知发射端混沌映射与相关参数时, 破译方仅仅通过截获到通信方发送的信号实现对混沌直扩信号所传输信息码的获取.

文献 [28] 基于两个混沌系统间的广义同步提出了一种不需要知道原始混沌系统, 而利用一个与其广义同步的映射  $X'(k+1) = g(X'(k), H(X(k)))$

拟合原混沌系统获取信息码的方法, 其中  $X \in R^n$ ,  $X' \in R^m$ . 两混沌系统广义同步要求存在广义同步变换  $H: R^n \rightarrow R^m$  和流形  $M = \{(X, X') | X' = H(X)\}$ , 且满足在状态空间  $B \subset R^n \times R^m$ ,  $M \subset B$  内, 以  $B$  中任意初始值开始的两混沌系统轨迹在  $k \rightarrow \infty$  时趋近于  $M$  [24]. 基于以上理论, 文献 [28] 构造如 (2) 式所示的滤波模型:

$$\begin{cases} b(k+1) = b(k) + v^{(2)}(k), \\ Y(k+1) = b(k+1)(g(X'(k)) + \beta) + \varphi^{(2)}(k), \\ X'(k+1) = g(X'(k)) + v^{(1)}(k), \\ Y(k+1) = \text{sgn}(b(k+1)) \cdot X'(k+1) + \varphi^{(1)}(k), \end{cases} \quad (2)$$

其中  $v, \varphi$  分别为过程噪声和观测噪声,  $b(k)$  为  $k$  时刻信息符号取值, 两个滤波器交替工作. UKF 滤波基于上一时刻状态分布按规则取  $2M+1$  个采样点 (即 sigma 点, 其中  $M$  为状态空间维数), 其均值和协方差等于原状态分布的均值和协方差, 用这些 sigma 点代替需要传递的变量进行时间预测和更新, 完成滤波过程, 具有三阶非线性滤波精度 [31].

(2) 式中误差控制因子  $\beta \in (-1, 1)$ , 其取值使估计信息符号在  $b_{n+1}$  取  $+1$  和  $-1$  时错开, 以便于符号判断. 然而 (2) 式中的滤波模型适用于信息符号为慢变信号的情况, 当扩频因子相对较小时, 破译效果变差; 其次, 算法对多径衰落和信噪比要求仍然较高, 当存在较大多径衰落时, 这一算法并不适用. 为解决这些问题, 本文提出基于双模型的 UKF 混沌拟合破译算法.

## 3 DM-UKF 混沌拟合破译混沌直扩通信

### 3.1 DM-UKF 混沌拟合破译算法

与文献 [28, 29] 直接估计信息符号的方式不同, 基于 DM-UKF 混沌拟合的破译算法利用已知信息符号的取值范围, 针对信息符号的不同取值建立不同的滤波模型, 分别用一个广义混沌系统拟合原混沌系统并估计混沌直扩信号, 进而通过估计误差的二范数进行信息判定, 选取当前最佳滤波模型, 以此确定信息符号取值. 由于破译方对于发送方信息几乎一无所知, 故本文所指估计误差 (或跟踪误差) 均为截获信号与滤波估计之间的差值.

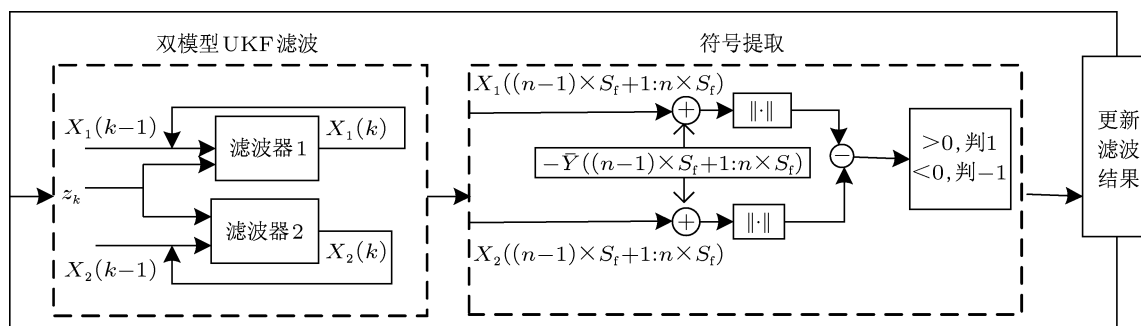


图1 DM-UKF混沌拟合破译框图

针对二进制混沌直扩信号, 图1给出了基于DM-UKF混沌拟合的破译算法框图. 其中滤波器1, 2分别是在信息码 $\{-1, 1\}$ 时建立的UKF滤波器;  $X_1(k-1)$ 和 $X_2(k-1)$ 分别为两个滤波模型下, 混沌拟合系统在 $k-1$ 时刻得到的滤波结果;  $X_i((n-1) \times S_f + 1:n \times S_f)$ ,  $i=1, 2$ 为滤波器 $i$ 在第 $n$ 个符号间隔内的输出序列;  $\bar{Y}((n-1) \times S_f + 1:n \times S_f)$ 为对应截获序列. 在DM-UKF混沌拟合破译算法中, 两个滤波器并行工作. 通过两个滤波器跟踪误差的关系在给定时间提取信息符号, 并将其中的最佳滤波结果保留下来作为下一个符号初始时刻两个滤波器的输入. 即在每个符号时间内, 混沌信号的初始值相同. (3)式为滤波模型的统一表达式:

$$\begin{cases} X_i(k+1) = g_i(X_i(k)) + \beta + W(k), \\ Y_i(k+1) = h_i(X_i(k+1)) + V(k), \end{cases} \quad (3)$$

其中 $X_i$ 为 $M$ 维混沌信号变量, 下标 $i$ 为模型标号,  $W(k)$ ,  $V(k)$ 分别为 $k$ 时刻状态噪声和观测噪声,  $g_i(\cdot)$ ,  $h_i(\cdot)$ 分别为模型 $i$ 对应的混沌动力学方程和观测方程,  $\beta$ 为误差控制因子, 其作用将在3.2节具体介绍. DM-UKF混沌拟合破译二进制混沌直扩时 $i=1, 2$ ,  $g_1(\cdot) = g_2(\cdot)$ 且

$$\begin{cases} h_1(X_1(k+1)) = 1 \times X_1(k+1) + V_k, \\ h_2(X_2(k+1)) = -1 \times X_2(k+1) + V'_k. \end{cases} \quad (4)$$

结合多模型算法和UKF滤波算法<sup>[31-34]</sup>, 写出DM-UKF滤波步骤为如下.

1) 确定模型下混沌直扩信号的UKF滤波, 得到两个滤波器输出结果

(a) 预测

若已知 $k$ 时刻滤波模型 $j$ 下混沌信号均值 $X_j(k/k)$ 及其方差 $P_j^X(k/k)$ , 则其对应

的sigma点为

$$\begin{aligned} \chi^{(0)}(k/k) &= X_j(k/k), \\ \chi_j^{(d)}(k/k) &= X_j(k/k) + \left( \sqrt{(M+\lambda)P_j^X(k/k)} \right)_d, \\ & \quad d=1, 2, \dots, M, \\ \chi_j^{(d)}(k/k) &= X_j(k/k) - \left( \sqrt{(M+\lambda)P_j^X(k/k)} \right)_d, \\ & \quad d=M+1, M+2, \dots, 2M; \\ w_0^{(m)} &= \lambda/(M+\lambda), \\ w_r^{(m)} &= 1/(M+\lambda) \quad r=1, \dots, 2M, \\ w_0^{(c)} &= \lambda/(M+\lambda) + (1-\alpha^2 + \eta), \\ w_r^{(c)} &= 1/(M+\lambda), \quad r=1, \dots, 2M; \end{aligned}$$

其中 $\left( \sqrt{(M+\lambda)P_j^X(k/k)} \right)_d$   $d=1, 2, \dots, 2M$ 为根号内矩阵平方根的第 $d$ 列;  $w_r^{(m)}$ 为sigma点均值的权值 $r=0, \dots, 2M$ , 相应地,  $w_r^{(c)}$ 为方差权值; 参数 $\lambda = \alpha^2(M+\kappa) - M$ ;  $\kappa$ 的取值应确保矩阵 $(M+\lambda)P_j^X$ 为半正定矩阵, 通常取为0, 调节 $\alpha$ 确定围绕均值的sigma点的散步程度, 其通常取较小的正数;  $\eta$ 为状态向量 $X$ 分布的先验知识, 对高斯分布一般取2.

则混沌信号预测均值和协方差可由sigma点计算得:

$$\begin{aligned} \chi_j^{(d)}(k+1/k) &= g_j(\chi_j^{(d)}(k/k), k) + \beta, \\ X_j(k+1/k) &= \sum_{d=0}^{2M} w_d^{(m)} \chi_j^{(d)}(k+1/k), \\ P_j^{(X)}(k+1/k) &= \sum_{d=0}^{2M} w_d^{(c)} (\chi_j^{(d)}(k+1/k) \\ & \quad - X_j(k+1/k)) (\chi_j^{(d)}(k+1/k) \\ & \quad - X_j(k+1/k))^T, \end{aligned}$$

其中  $P_j^X$  表示模型  $j$  下变量  $X$  的方差.

(b) 更新

更新状态  $\sigma$  点由观测方程计算得到:

$$\gamma_j^{(d)}(k+1) = h_j(\chi_j^{(d)}(k+1/k), k+1),$$

$$d = 0, \dots, 2M,$$

$$Y_j(k+1/k) = \sum_{d=0}^{2M} w_d^{(m)} \gamma_j^{(d)}(k+1),$$

$$P_j^Y(k+1/k) = \sum_{d=0}^{2M} w_d^{(c)} (\gamma_j^{(d)}(k+1) - Y_j(k+1/k)) (\gamma_j^{(d)}(k+1) - Y_j(k+1/k))^T,$$

$$P_j^{XY}(k+1/k) = \sum_{d=0}^{2M} w_d^{(c)} (\chi_j^{(d)}(k+1) - X_j(k+1/k)) (\gamma_j^{(d)}(k+1) - Y_j(k+1/k))^T,$$

其中  $P_j^Y P_j^{XY}$  分别表示对应模型下  $Y$  的方差和  $X, Y$  的协方差.

(c) 滤波结果

$$X_j(k+1/k+1) = X_j(k+1/k) + \frac{P_j^{XY}(k+1)}{P_j^Y(k+1)} \times (\bar{Y}(k+1) - Y_j(k+1/k)),$$

$$P_j^X(k+1/k+1) = P_j^X(k+1/k) - P_j^{XY}(k+1) \times [P_j^{XY}(k+1)/P_j^Y(k+1)]^T,$$

其中  $\bar{Y}(k+1)$  为  $k+1$  时刻观测值, 定义滤波残差和增益分别为

$$\varepsilon_j(k+1) = \bar{Y}(k+1) - Y_j(k+1/k),$$

$$G_j(k+1) = \frac{P_j^{XY}(k+1)}{P_j^Y(k+1)}.$$

2) 信息码提取

通过两个滤波器的跟踪误差的关系可以得到扩频因子与信息码起始点的估计, 则在每个符号间隔对应时刻点就能完成信息码提取, 涉及到的判定

准则如下:

$$norm1 = \left\| X_1((n-1) \times S_f + 1:n \times S_f) - \bar{Y}((n-1) \times S_f + 1:n \times S_f) \right\|,$$

$$norm2 = \left\| X_2((n-1) \times S_f + 1:n \times S_f) - \bar{Y}((n-1) \times S_f + 1:n \times S_f) \right\|,$$

if( $norm1 > norm2$ )

$$\bar{b}_n = -1; X_1(n \times S_f) = X_2(n \times S_f);$$

$$P_1^X(n \times S_f) = P_2^X(n \times S_f),$$

else

$$\bar{b}_n = 1; X_2(n \times S_f) = X_1(n \times S_f);$$

$$P_2^X(n \times S_f) = P_1^X(n \times S_f),$$

其中  $norm1$  与  $norm2$  分别为第  $n$  个符号时间内, 两个滤波器得到的跟踪误差序列的二范数,  $\bar{b}_n$  为第  $n$  个信息码估计值, 提取信息以后, 重新设置两个滤波器输入.

### 3.2 DM-UKF 破译中误差控制因子确定

与文献 [28—30] 不同, DM-UKF 破译算法中的误差控制因子的提出, 旨在令基于跟踪误差二范数的判定更容易进行, 即尽量增大两个模型的跟踪误差二范数之间的差异. 考虑到无迹卡尔曼滤波的实现步骤, 每一时刻状态值为预测值的修正, 如 (5) 式所示, 其中  $X_1(k+1/k)$  和  $X_2(k+1/k)$  分别为两个滤波器的状态预测值,  $G_1$  和  $G_2$  分别为其滤波增益,  $\beta$  为误差控制因子. 则:

$$\begin{cases} X_1(k+1) = X_1(k+1/k) + G_1 \left[ \bar{Y}(k+1) - g(X_1(k/k)) - \beta \right], \\ X_2(k+1) = X_2(k+1/k) + G_2 \left[ \bar{Y}(k+1) + g(X_2(k/k)) + \beta \right]. \end{cases} \quad (5)$$

由滤波过程可得:  $X_1(k+1/k) = g(X_1(k/k)) + \beta$ ;  $X_2(k+1/k) = g(X_2(k/k)) + \beta$ , 则 (5) 式可写为

$$\begin{cases} X_1(k+1) = g(X_1(k/k)) + \beta + G_1 \left[ \bar{Y}(k+1) - g(X_1(k/k)) - \beta \right], \\ X_2(k+1) = g(X_2(k/k)) + \beta + G_2 \left[ \bar{Y}(k+1) + g(X_2(k/k)) + \beta \right]. \end{cases} \quad (6)$$

在第  $k + 1$  个采样点时刻, 两个模型下跟踪误差的二范数  $norm'_1(k + 1)$  与  $norm'_2(k + 1)$  分别为

$$\begin{cases} norm'_1(k + 1) = |\bar{Y}(k + 1) - 1 \times X_1(k + 1/k + 1)| \\ \quad = |\bar{Y}(k + 1) - g(X_1(k/k)) - \beta - G_1 [\bar{Y}(k + 1) - g(X_1(k/k)) - \beta]|, \\ norm'_2(k + 1) = |\bar{Y}(k + 1) - (-1) \times X_2(k + 1/k + 1)| \\ \quad = |\bar{Y}(k + 1) + g(X_2(k/k)) + \beta + G_2 [\bar{Y}(k + 1) + g(X_2(k/k)) + \beta]|. \end{cases} \quad (7)$$

(7) 式可化简为

$$\begin{cases} norm'_1(k + 1) = |(1 - G_1)(\bar{Y}(k + 1) - g(X_1(k/k)) - \beta)|, \\ norm'_2(k + 1) = |(1 + G_2)(\bar{Y}(k + 1) + g(X_2(k/k)) + \beta)|. \end{cases} \quad (8)$$

进一步定义中间变量  $b, c$  为

$$\begin{cases} b = \bar{Y}(k + 1) - g(X_1(k/k)) - \beta, \\ c = \bar{Y}(k + 1) + g(X_2(k/k)) + \beta, \end{cases} \quad (9)$$

则 (7) 式可写为

$$\begin{cases} norm'_1(k + 1) = |b \times (1 - G_1)|, \\ norm'_2(k + 1) = |c \times (1 + G_2)|. \end{cases} \quad (10)$$

由 (10) 式可知, 增大  $b, c$  之间的差异能有效区分  $norm'_1(k + 1)$  和  $norm'_2(k + 1)$ . 同时  $norm1$  和  $norm2$  可写为

$$\begin{aligned} norm1 &= \left( \sum_{k=(n-1) \times S_f + 1}^{n \times S_f} (norm'_1(k + 1))^2 \right)^{1/2}; \\ norm2 &= \left( \sum_{k=(n-1) \times S_f + 1}^{n \times S_f} (norm'_2(k + 1))^2 \right)^{1/2}. \end{aligned} \quad (11)$$

由于  $norm'_1(k + 1)$  与  $norm'_2(k + 1)$  均大于零, 可知  $norm'_1(k + 1)$  与  $norm'_2(k + 1)$  之间的差异

将决定用于信息符号判定的  $norm1$  与  $norm2$  之间的差异. 结合混沌拟合条件, 控制  $\bar{Y}(k + 1) - \beta$  和  $\bar{Y}(k + 1) + \beta$  的取值, 以便较好地分离两种模型下的滤波结果. 分析 (9) 式可知如果将  $\beta$  取值为观测序列二范数与序列长度的比值, 即  $\beta = \|\bar{Y}(1:N_{ob})\|/N_{ob}$ , 其中  $N_{ob}$  为观测序列长度, 此时  $\bar{Y}(k + 1) - \beta$  和  $\bar{Y}(k + 1) + \beta$  之间具有较大区分距离. 同时, 误差控制因子取为  $\beta = \|\bar{Y}(1:N_{ob})\|/N_{ob}$  将观测值  $\bar{Y}$  对信息符号判定式的影响大大降低, 减小了由于观测值不精确引起的误差. 并且由于  $\beta$  随着观测值变化而进行自适应调整, 整个破译算法具有较强的抗多径衰落和低信噪比的能力.

为了说明误差控制因子  $\beta$  对符号判断的影响, 定义区分距离  $d$  表示两个模型下跟踪误差二范数差的绝对值,  $d$  越大说明区分程度越高. 设加入  $\beta$  后区分距离为  $d_1$ , 未加  $\beta$  时区分距离为  $d_2$ . 图 2 给出了扩频因子  $S_f$  分别为 127 和 63, SNR = 8 dB 时 154 个符号范围内 ( $d_1 - d_2$ ) 取值.

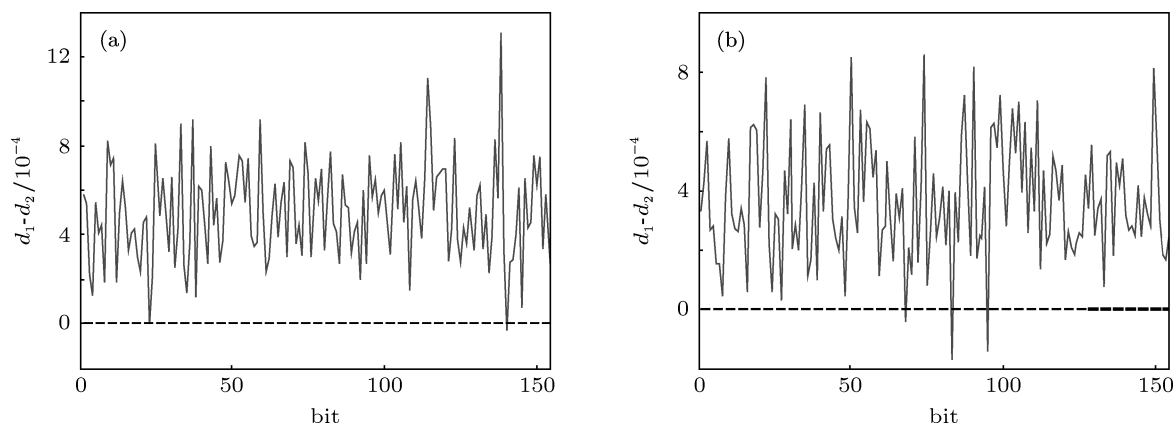


图 2 误差控制因子加入前后的区分距离差 (a) SNR = 8 dB,  $S_f = 127$  条件下; (b) SNR = 8 dB,  $S_f = 63$  条件下

由图 2 可以看出, 在大部分符号点  $d_1 > d_2$ , 即误差控制因子的加入增大了两种模型下原混沌信号的跟踪误差区分度, 有利于符号判定.

### 3.3 多径衰落模型

多径衰落情况下的 DM-UKF 混沌拟合破译算法, 其模型建立与 3.1 相同, 此时接收序列为信号及其延迟的加权和 [29]:  $Y(k+1) = c_0 b(k) f(X(k)) + \sum_{i=1}^{L_n} c_i b(k+1-i) f(X(k-i))$ , 其中  $L_n$  为多径信道数,  $c$  为信道系数向量. 固定信道衰落系数情况下  $c = [c_0 \ c_1 \ \cdots \ c_{L_n}]$ , 其中  $c_0$  为主径系数. 时变信

道衰落系数情况下,  $c = [c_0 \ c_1(n) \ \cdots \ c_{L_n}(n)]$ .

从  $\beta$  的选取可以看出, 在减小观测值对滤波结果影响的同时, 也减小了多径信道和噪声对信息符号判断的影响. 因此, 相对文献 [28, 29] 所提出破译算法, 信道衰落对基于 DM-UKF 的破译算法没有那么敏感.

图 3 分别给出了在非时变多径和时变多径衰落下, 扩频因子为 127, 信噪比为 8 dB 时, 误差控制因子的加入对用于符号判决的区分距离的影响, 这里非时变多径存在时  $c = [1, 0.4, 0.3]$ , 多径衰落时变情况下  $c = [1, 0.4 \sin(\frac{\pi k}{640}), -0.3 \cos(\frac{\pi k}{640})]$ .

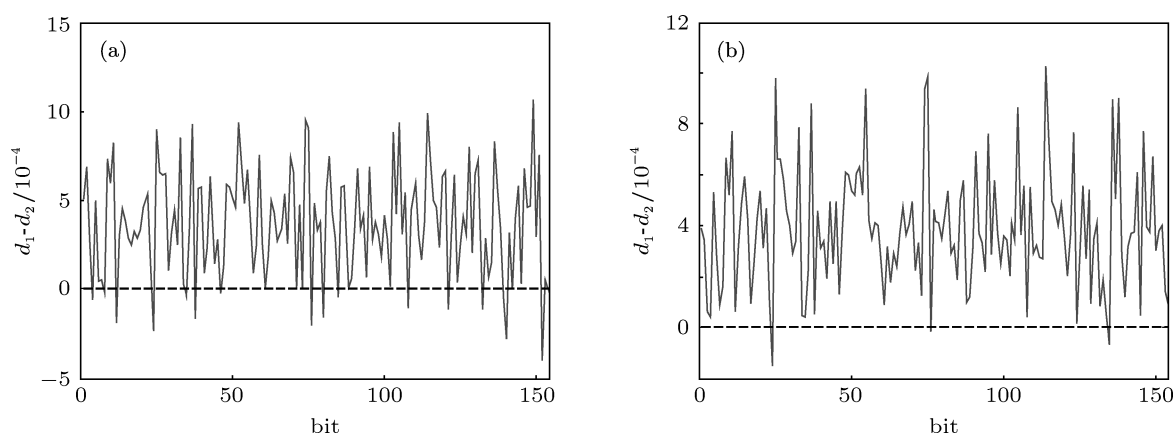


图 3 误差控制因子加入前后的区分距离差 (a)  $S_f = 127$ , SNR = 8 dB, 非时变多径条件下; (b)  $S_f = 127$ , SNR = 8 dB, 时变多径条件下

可以看出, 在大部分符号点上, 误差控制因子的加入, 仍然加大了两种模型下跟踪误差的距离, 有利于符号判定.

## 4 仿真

### 1) 无多径衰落下的仿真结果

仿真条件: 发射端采用 Ulam 映射  $X(k+1) = 1 - \lambda(X(k))^2$ , 其为 Logistic 映射的特例, 当  $1.40115 \leq \lambda \leq 2$  时, Ulam 映射处于混沌状态, 这里取为 2; 破译端采用 tent 混沌系统  $X'(k+1) = 0.5 - 1.99|X'(k)|$  进行拟合. 仿真中取 1540 bit 符号蒙特卡罗 10 次. 这里信噪比采用文献 [13] 中的定义  $SNR = 10 \log_{10} \frac{\sum_{n=1}^M (s^n - \bar{s})^2}{\sum_{n=1}^M (e^n - \bar{e})^2}$ , 其中  $s^n$  为  $n$  时刻信号强度,  $\bar{s}$  为其均值, 分母部分为噪声及其均值. UKF 算法中  $M = 1$ , sigma 点权值对应参数中,  $\alpha$  取 0.005, 由于仿真假设所涉及噪声均服从高斯

分布, 故令  $\eta = 2, \kappa = 0$ . 为了便于与文献 [28, 29] 中结果进行比较, 过程噪声协方差取为  $10^{-2}$ .

图 4(a) 为 UKF 混沌拟合破译算法 [28] 中误差控制因子  $\beta = 0.9$ , 扩频因子 127 时的破译误码率与相同条件下 DM-UKF 混沌拟合破译算法误码率对比曲线. 图 4(b) 为降低扩频因子为 63 时的误码率对比曲线. 可以看出, 当扩频因子  $S_f = 63$  时, 所提方法破译精度虽有所降低, 但仍然可以满足实际需求并且明显优于文献 [28] 所提算法.

### 2) 多径衰落下的仿真结果

仿真条件与 1) 同. 图 5 为多径系数向量取值不满足文献 [29] 可破译条件, 且旁径系数绝对值和大于主径系数, 扩频因子取 127 时两种方法的误码率曲线对比结果. 图 5(a) 为非时变衰落系数下  $c = [1, 0.4, 0.9]$  破译结果, 图 5(b) 比较了时变多径系数向量取值下,

$$c = \left[ 1, 0.4 \sin\left(\frac{\pi n}{640}\right) \quad -0.7 \cos\left(\frac{\pi n}{640}\right) \right] \text{ 两种方法}$$

破译的误码率. 可见, 与文献 [29] 相比, DM-UKF 混沌拟合破译算法在多径衰落较大或信噪比较低情

况下, 仍然可以获得较低误码率, 具有较好的抗低信噪比和多径衰落性能, 这与理论推导相符.

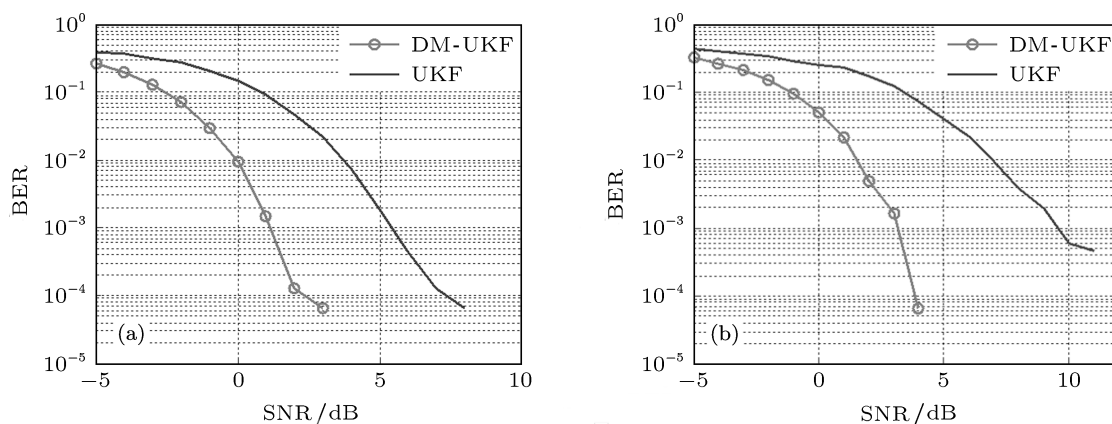


图4 不同扩频因子条件下两种算法破译误码率对比 (a)  $S_f = 127$ ; (b)  $S_f = 63$

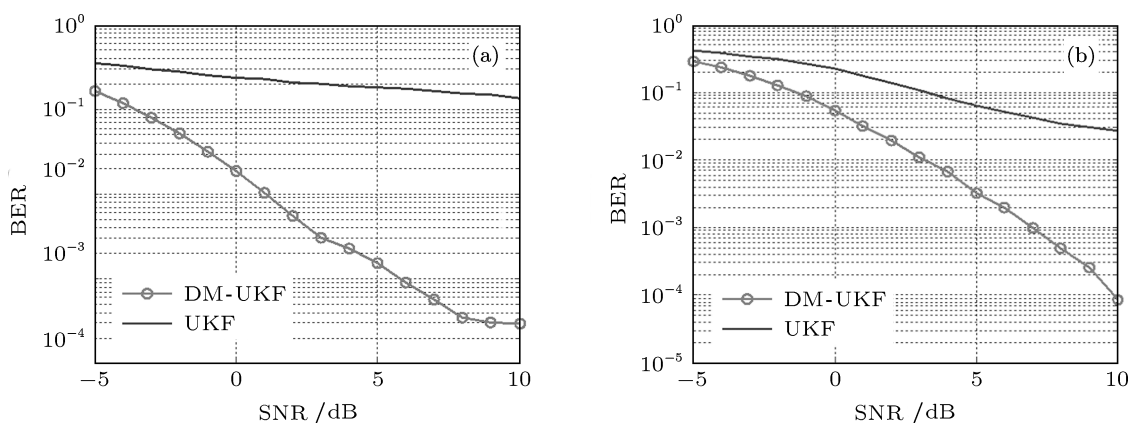


图5 多径环境下两种算法破译误码率对比 (a) 非时变多径; (b) 时变多径

## 5 结论

目前已经存在直接估计信息符号的混沌直扩信号破译方法, 在小扩频因子、低信噪比及多径衰落较大的情况下, 其破译效果不理想. 本文充分利用信息符号取值范围已知, 并将其作为一组并行滤波器的模型取值, 通过拟合混沌系统在各个滤波器

下分别恢复原始混沌直扩信号, 选取最佳匹配模型的对应值作为信息符号. 同时, 推导出了这种模型判定表达式中误差控制因子的自适应取值. 仿真证明了得到的误差控制因子不仅有利于符号判定, 还在一定程度上减小了观测值包含的不确定因素对破译结果的影响, 使得提出的 DM-UKF 破译算法具有较强的抗多径衰落和低信噪比的性能.

- [1] Kocarev L 2001 *IEEE Circuits Syst. Mag.* **1** 6
- [2] Yang T 2004 *Int. J. Comput. Cogn.* **2** 81
- [3] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
- [4] Wang F P, Wang Z J, Guo J B 2002 *J. China Inst. Commun.* **23** 71 (in Chinese) [汪芙平, 王赞基, 郭静波 2002 通信学报 **23** 71]

- [5] Zhao B S, Zhu Y S 2007 *J. Electron. Inform. Tech.* **29** 699 (in Chinese) [赵柏山, 朱义胜 2007 电子与信息学报 **29** 699]
- [6] Zhang J S, Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese) [张家树, 肖先赐 2001 物理学报 **50** 2121]
- [7] Sun L, Jiang D P 2006 *Acta Phys. Sin.* **55** 3283 (in Chinese) [孙

- 琳, 姜德平 2006 物理学报 **55** 3283]
- [8] Sathyan T, Kirubarajan T 2006 *IEEE Trans. Circuits Syst. I* **53** 1597
- [9] Li G H, Xu D M, Zhou S P 2004 *Acta Phys. Sin.* **53** 706 (in Chinese) [李国辉, 徐得名, 周世平 2004 物理学报 **53** 706]
- [10] Li J F, Li N, Lin H 2004 *Acta Phys. Sin.* **53** 1694 (in Chinese) [李建芬, 李农, 林辉 2004 物理学报 **53** 1694]
- [11] Zhang Y, Chen T Q, Chen B 2007 *Acta Phys. Sin.* **56** 56 (in Chinese) [张勇, 陈天麒, 陈滨 2007 物理学报 **56** 56]
- [12] Yu Z B, Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese) [余振标, 冯久超 2008 物理学报 **57** 1409]
- [13] Parlitz U, Ergezingler S 1994 *Phys. Lett. A* **188** 146
- [14] Luca M B, Azou S, Burel G, Serbanescu A 2005 *IEEE-ISCAS 2005* Kobe, Japan, 23–26 May 2005 p3813
- [15] Azou S, Luca M B, Burel G, Serbanescu A 2005 *Oceans 2005-Europe* Brest, France, June 20–23, 2005 p616
- [16] Azou S, Burel G, Pistre C 2002 *Oceans Conf. Rec. IEEE Biloxi*, Mississippi, USA 29–31 October, 2002 p2409
- [17] Azou S, Burel G, Duff L L, Pistre C 2003 *Oceans Conf. Rec. IEEE San Diego*, USA 22–26 September, 2003 p1539
- [18] Tsai J S H, Yu J M, Canelon J I, Shieh L S 2005 *Ima. J. Math. Control I* **22** 58
- [19] Leung H, Zhu Z 2001 *IEEE Trans. Circuits Syst. I* **48** 1118
- [20] Zhu Z, Leung H 2001 *IEEE Trans. Circuits Syst. I* **48** 979
- [21] Hu Z H, Feng J C 2012 *Trans. Tianjin Univ.* **18** 033
- [22] Xu M G 2008 *Ph. D. Dissertation* (Nanjing: Nanjing University of Science and Technology) (in Chinese) [徐茂格 2008 博士学位论文 (南京: 南京理工大学)]
- [23] Alvarez G, Montoya F, Romera M, Pastor G 2004 *IEEE Trans. Circuits Syst. II* **51** 505
- [24] Yang T, Yang L B, Yang C M 1998 *IEEE Trans. Circuits Syst. I* **45** 1062
- [25] Li S J, Alvarez G, Chen G R 2005 *Chaos, Solitons and Fractals* **25** 109
- [26] Alvarez G, Montoya F, Romera M, Pastor G 2004 *Chaos* **14** 274
- [27] Ren H P, Han C Z, Liu D 2008 *Chin. Phys. B* **17** 1202
- [28] Hu J F, Guo J B 2008 *Acta Phys. Sin.* (in Chinese) **57** 1477 [胡进峰, 郭静波 2008 物理学报 **57** 1477]
- [29] Hu J F, Guo J B 2008 *Chaos* **18** 013121
- [30] Bai L, Guo J B 2011 *Acta Phys. Sin.* (in Chinese) **60** 070504 [白鹭, 郭静波 2011 物理学报 **60** 070504]
- [31] Julier S, Uhlmann J, Durrant-Whyte H F 2000 *IEEE Trans. Automat. Contr.* **45** 477
- [32] Wan E A, van der Merwe R 2000 *AS-SPCC Symposium 2000* Lake Louise, Alberta, Canada 1–4 Oct., 2000 p153
- [33] Blom H A P, Bar-Shalom Y 1988 *IEEE Trans. Automat. Contr.* **33** 780
- [34] Bar-Shalom Y 2000 *Multitarget-Multisensor Tracking: Applications and Advances* (Vol. 3) (Boston, London: Artech House) p161



# Breaking chaotic direct sequence spreading spectrum communication systems using DM-UKF chaotic fitting method\*

Gan Lu<sup>†</sup> Xiong Bo

(University of Electronic Science and Technology of China, Chengdu 611731, China)

(Received 17 April 2012; revised manuscript received 22 May 2012)

## Abstract

In this paper, a dual model unscented Kalman filter chaotic fitting breaking method is proposed to break chaotic direct sequence spread spectrum communication systems in the cases of low spreading factor, low signal-to-noise ratio or severe multipath fading. Based on the characteristic that the range of information symbol is a finite set, the proposed algorithm fits the original chaotic signal through different filters which work in parallel. The fitting errors are used to choose the optimum matching filter, thus to estimate the information symbols. Furthermore, an error-controlling-factor is introduced to increase the distance of model based tracking errors, which can not only facilitate the information extracting process, but also reduce the influence of noise and multipath fading. Theoretical analysis and simulation results prove that the proposed algorithm is superior to the existing breaking method.

**Keywords:** dual model, unscented Kalman filter, chaotic direct sequence spreading spectrum communication, breaking

**PACS:** 05.45.-a, 05.45.Vx

---

\* Project supported by the Science Foundation of China Academy of Engineering Physics, China (Grant No. 2010A0403017) and the Fundamental Research Funds for the Central Universities of Ministry of Education of China (Grant No. ZYGX2010J027).

<sup>†</sup> E-mail: ganlu@uestc.edu.cn