第 57 卷 第 3 期 2008 年 3 月
1000-3290/2008/57(03)/1477-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.3,March,2008

一种破译混沌直接序列扩频保密通信的方法*

胡进峰 郭静波†

(清华大学电机系,电力系统国家重点实验室,北京 100084)

(2007 年 5 月 9 日收到;2007 年 7 月 2 日收到修改稿)

提出了一种新型的混沌保密通信破译方法,并破译了混沌直接序列扩频保密通信(简称混沌直扩).针对混沌直扩信号中只有一个混沌吸引子的特点,基于混沌系统广义同步的思想,提出了混沌拟合方法;针对混沌直扩中混沌实值序列和数字信号相乘的特点,充分利用混沌直扩的基本原理和信息码是慢变信号的特性,提出了用无先导卡尔曼滤波混沌拟合的方法估计信息码的破译方法;进一步针对无先导卡尔曼滤波的过程噪声和混沌拟合的拟合误差共同导致的跟踪误差,提出了跟踪误差控制因子的方法,从而将跟踪误差转变成有利因素并加以利用,根据跟踪误差的值域范围破译混沌直扩,得到改进的无先导卡尔曼滤波混沌拟合算法;所提算法无需知道混沌直扩发射机的结构、混沌映射的参数等,并具有一定的抗噪声能力,仿真结果证明了其有效性.

关键词:混沌保密通信,破译,混沌拟合,无先导卡尔曼滤波

PACC:0545,0540

1. 引 言

由于混沌动力系统具有复杂的非线性和类噪声特性,并对初始条件极为敏感,近年来,将混沌理论应用于保密通信已经成为非线性动力学和信息科学界的一个研究热点[1—25].在人们提出的众多混沌保密通信方式中,混沌直接序列扩频(简称混沌直扩)是主要的混沌保密通信方式之一[6—12].它是 1994 年美国 C. D. McGillem 和德国 U. Parlitz 的研究组同时独立提出的一种混沌保密通信方式[6—10],正被法国海军实际应用于水下通信[8—10].其原理是信息码与混沌信号相乘实现扩频和加密(图 1).它具有低截获率和物理层上的优良保密性[11,12].

与此同时,破译混沌保密通信(文献中也称为"breaking"[13—15,22—25]或"extracting"[17—20])的研究也受到广泛关注[13—28].研究混沌保密通信的破译方法,是根据这些破译方法设计更安全的混沌保密通信系统的迫切需求[1,2,25];随着混沌保密通信的逐步实际应用[8—10],破译混沌保密通信的研究对于通信监管和电子对抗也具有重要的实际意义.

自 1995 年 Perez 破译混沌掩盖保密通信以来[18],人们提出了大量的混沌保密通信破译方法[13—28],然而,从破译对象上看,已有的破译方法主要集中于破译三类混沌保密通信,即破译混沌键控(或混沌切换)[13,14]、破译混沌掩盖[15—23],以及破译混沌参数调制[24—26].尚未见到破译混沌直扩的研究报道;从破译方法来看,目前已有的破译方法大部分是针对这三类混沌保密通信的两个特点提出来的[7—20],即针对混沌掩盖等保密通信中混沌信号和信息码是加性的特点,人们提出了相空间投影重构等破译方法[15—23],针对混沌键控和混沌参数调制中有两个差别较大的混沌吸引子的特点,人们提出了神经网络和广义同步等破译方法[13,14,24,25].然而,混沌直扩中只有一个混沌吸引子,且混沌信号和信息码是乘性的[6,7],因此已有的破译方法对破译混沌直扩不适用;从实际需要来看,法国海军已研制出了可实际应用于水下通信的混沌直扩通信系统[8—10],因而破译混沌直扩的研究具有重要的实际意义;从研究方法来看,目前国际上破译混沌保密通信的研究,通常都不考虑噪声干扰[13—15,22—26],因为国际上通常认为破译混沌保密通信的研究属于混沌保密通信的安全性分析方面的基础理论研究,并且如果混沌信号中有噪声,可以通过混沌噪声抑制[29]、混沌信号

* 国家专项基金(批准号:2004AAXX5071)资助的课题.

† 通讯作者. E-mail:guojb@tsinghua.edu.cn

盲分离或混沌信号盲抽取等方法去除噪声[30,31]，属于另外的热点研究内容.但是，由于混沌直扩已经有明确的工程背景，因此研究具有一定抗噪声能力的破译方法将更具实际意义.

本文针对混沌直扩信号的特点，提出了具有一定抗噪声能力的改进的无先导卡尔曼滤波混沌拟合破译方法.在3.1节中针对混沌直扩中只有一个吸引子的特点，提出了混沌拟合方法；在3.2节中针对混沌信号与数字信号相乘的特点，提出了用无先导卡尔曼滤波混沌拟合方法估计信息码的破译方法；在3.3节中针对无先导卡尔曼滤波的过程噪声和混沌拟合的拟合误差共同导致的较大的跟踪误差，提出加入跟踪误差控制因子，得到改进的无先导卡尔曼滤波混沌拟合破译算法.本文还进一步研究了对有噪声干扰的混沌直扩的破译，并在3.4节中提出了一种具有一定抗噪声能力的提取二进制信息码的方法.在第4节的仿真实验中，窃密者根据混沌拟合的基本原理，自制一个混沌响应系统来拟合发射端的混沌系统，并通过改进的无先导卡尔曼滤波混沌拟合方法估计并窃取发射的信息码.4.1节的仿真结果表明，所提方法在混沌直扩发射机的结构、混沌映射参数等未知的情况下，可以有效地破译混沌直扩保密通信系统.4.2节的仿真结果表明所述方法具有一定的抗噪声能力，可以有效降低对混沌噪声抑制、混沌信号盲分离或盲抽取的要求，具有一定的工程实际意义.

2. 混沌直扩保密通信原理

混沌直扩原理如图1[6—9]：设信息码 $b\in\{-1,1\}$，对每一位信息码 b_k，都用混沌信号 $\{x_n\}$ 的 N 个混沌序列值 $x_n(n=(k-1)N+1,\cdots,Nk)$ 扩频，即发射的直扩信号 $\{s_n\}$ 可表示为 $s_n=b_kx_n$，$n=1+(k-1)N,\cdots,kN$，$k=1,2,3,\cdots$，这里的扩频因子 N 是70.图1(a)是信息码 $b_k\in\{-1,1\}$，图1(b)是在发射端用 logistic 混沌映射生成的混沌扩频序列 $\{x_n\}$[6—10,12]，图1(c)是混沌直扩信号，也就是发射端发射的信号.这里的 logistic 映射是 $x_n=f(x_{n-1})=1-2(x_{n-1})^2$，$x_n\in[-1,1]$.该混沌映射是双对称的，即值对称(均值为0)和概率分布对称.在接收端生成同样的混沌序列实现解扩.

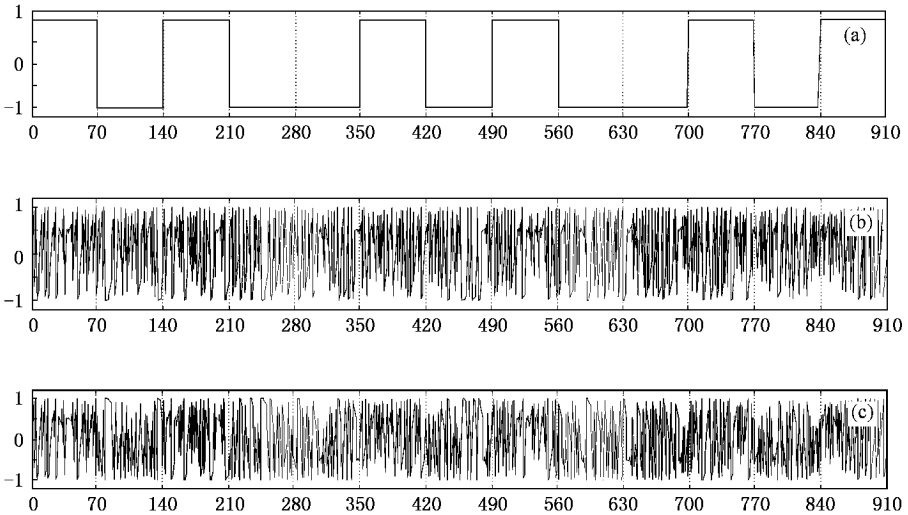

图1 混沌直扩保密通信原理 (a)信息码 b_k；(b)混沌扩频序列 x_n；(c)发射的混沌直扩信号 s_n

3. 破译混沌直扩保密通信的算法

本文将在发射端的混沌系统结构及其参数都是未知的情况下，通过破译图1(c)中的混沌直扩信号 s 来获取信息码 b.破译算法如下.

3.1. 混沌拟合

本文将窃密者用的接收机称为窃密接收机，授权者的接收机称为授权接收机.破译混沌直扩时，由于不知道发射端的混沌系统，我们构造一个混沌系统来拟合对方的混沌系统，在拟合过程中获取信息

码.假设如下两个混沌系统：

$$\begin{aligned} \dot{x} &= f(x), \text{原混沌系统,} \\ \dot{x}' &= g(x', h(x)), \text{拟合混沌系统,} \end{aligned} \tag{1}$$

其中，$x \in R^n$，$x' \in R^m$ 且状态空间有如下对应关系：$h: R^n \to R^m$.

本文中，混沌拟合定义为如果(1)式中第二个混沌系统 $\dot{x}' = g(x', h(x))$ 与第一个混沌系统 $\dot{x} = f(x)$ 广义同步，则称这两个混沌系统是混沌拟合的，或者说第二个混沌系统拟合第一个混沌系统，第一个混沌系统称为原混沌系统，第二个混沌系统称为拟合混沌系统.广义同步的条件是[13,32−34] 存在广义同步变换 $H: R^n \to R^m$，和一个流形 $M = \{(x, x') \mid x' = H(x)\}$，且状态空间 $B \subset R^n \times R^m$，$M \subset B$，使得(1)式在状态空间 B 中以任意初始值开始的轨迹在 $t \to \infty$ 时趋近于 M.

授权接收机情况下，可认为是混沌拟合的特殊情况：$m = n$，$x' = H(x) = x$，此时定义为拟合混沌系统对原混沌系统完全拟合.通常情况下，很难找到变换函数 H 的显式表达式.

根据上述混沌拟合原理，存在一个状态空间映射函数 $H: R^n \to R^m$，使得 $x' = H(x)$，因此，窃密者可以构造一个混沌映射函数 $x' = g(x)$ 来拟合原混沌系统 $\dot{x} = f(x)$，并结合无先导卡尔曼滤波来破译混沌直扩信号从而获得信息码 b_k.

3.2. 无先导卡尔曼滤波混沌拟合算法

根据 3.1 所述，假设窃密者构造一个离散的混沌系统 $x'_{n+1} = g(x'_n)$，该混沌系统拟合授权接收机的离散混沌系统 $x_{n+1} = f(x_n)$.由于信息码 b_k 相对于混沌扩频信号 $\{x_n\}$ 是慢变信号，因此在很短时间内估计的信息码 $\hat{b}_{n+1} = \hat{b}_n$.根据混沌直扩的原理，估计的混沌直扩信号为 $z_{n+1} = \mathrm{sgn}(\hat{b}_{n+1}) \cdot x'_{n+1}$，于是，可以写成如下形式：

$$\begin{aligned} \hat{b}_{n+1} &= \hat{b}_n + v_n^{(2)}, \\ z_{n+1} &= \hat{b}_{n+1} g(x'_n) + \varphi_n^{(2)}; \end{aligned} \tag{2}$$

$$\begin{aligned} x'_{n+1} &= g(x'_n) + v_n^{(1)}, \\ z_{n+1} &= \mathrm{sgn}(\hat{b}_{n+1}) \cdot x'_{n+1} + \varphi_n^{(1)}. \end{aligned} \tag{3}$$

(2)式和(3)式是无先导卡尔曼滤波的状态方程的形式，因此可以用无先导卡尔曼滤波估计上述两式的状态向量，从而估计出信息码：首先用(2)式估计 $\hat{b}_{n+1}$，然后用(3)式估计出 x'_{n+1}；再根据(2)式估计 $\hat{b}_{n+2}$，接着根据(3)式估计 x'_{n+2}，如此循环估计，实现破译.其中，$v_n^{(1)}$，$v_n^{(2)}$ 是过程噪声，$\varphi_n^{(1)}$，$\varphi_n^{(2)}$ 是观测噪声，过程噪声和观测噪声都是白噪声.

3.3. 改进的无先导卡尔曼滤波混沌拟合算法

上述算法中，过程噪声的作用是通过非线性状态转移函数驱动(2)式和(3)式的动态系统[35,36].

通常，无先导卡尔曼滤波的跟踪误差(即估计误差)来自过程噪声[35,36]，而本文所述的无先导卡尔曼滤波混沌拟合算法中，跟踪误差来自两个方面，即过程噪声引起的跟踪误差；由于两个不同的混沌系统拟合时必然存在的拟合误差导致的跟踪误差.两方面的跟踪误差相叠加将产生较大的跟踪误差，使得难以破译混沌直扩信号.

既然跟踪误差不可避免，最好的办法就是利用它.为此，本文通过加入跟踪误差控制因子的方法将混沌拟合误差和过程噪声共同带来的较大的跟踪误差变成有利因素并加以利用，根据跟踪误差的值域范围不同来破译混沌直扩信号.在(2)式中加入误差控制因子

$$\begin{aligned} \hat{b}_{n+1} &= \hat{b}_n + v_{n+1}^{(2)}, \\ z_{n+1} &= \hat{b}_{n+1}(g(x'_n) + \beta) + \varphi_{n+1}^{(2)}, \end{aligned} \tag{4}$$

其中，β 是本文所提的跟踪误差控制因子，它可以控制估计的信号 $\hat{b}$ 中对应于不同信息码的跟踪误差的值域范围，根据该误差值域范围就可以破译出信息码，证明如下：

设在 $n+1$ 时刻窃密接收机接收的混沌直扩信号为 $s_{n+1} = b_{n+1} \cdot f(x_n) + \varphi_{n+1}^{(0)}$，其中，$\varphi_{n+1}^{(0)}$ 是观测噪声.无先导卡尔曼滤波混沌拟合估计的混沌直扩信号是

$$z_{n+1} = \hat{b}_{n+1}(g(x'_n) + \beta) + \varphi_{n+1}^{(2)}, \beta \in (-1, 1).$$

则它们之间的误差是

$$\begin{aligned} e_{n+1} &= s_{n+1} - z_{n+1} = b_{n+1} \cdot f(x_n) \\ &\quad + \varphi_{n+1}^{(0)} - \hat{b}_{n+1}(g(x'_n) + \beta) - \varphi_{n+1}^{(1)}. \end{aligned} \tag{5}$$

假设由混沌拟合误差和过程噪声引起的跟踪误差为 e''_{n+1}，则根据(5)式有

$$\begin{aligned} e''_{n+1} &= \hat{b}_{n+1} g(x'_n) - b_{n+1} \cdot f(x_n) \\ &= \varphi_{n+1}^{(0)} - \varphi_{n+1}^{(1)} - e_{n+1} - \hat{b}_{n+1}\beta \\ &= e'_{n+1} - \hat{b}_{n+1}\beta, \end{aligned} \tag{6}$$

其中，e'_{n+1} 是没有加误差控制因子(即 $\beta = 0$)的跟踪误差 $e'_{n+1} = \varphi_{n+1}^{(0)} - \varphi_{n+1}^{(1)} - e_{n+1}$.

根据(6)式有

$$\hat{b}_{n+1} = \frac{b_{n+1} \cdot f(x_n) + e'_{n+1}}{g(x'_n) + \beta}. \tag{7}$$

若 $b_{n+1}=1$,将 b_{n+1} 的估计信号 $\hat{b}_{n+1}$ 标记为 $\hat{b}_{n+1}^{1}$,则根据(7)式有

$$\hat{b}_{n+1}^{1}=\frac{f(x_n)+e'_{n+1}}{g(x'_n)+\beta}. \tag{8}$$

若 $b_{n+1}=-1$,将 b_{n+1} 的估计信号 $\hat{b}_{n+1}$ 标记为 $\hat{b}_{n+1}^{-1}$,根据(7)式有

$$\hat{b}_{n+1}^{-1}=-\frac{f(x_n)-e'_{n+1}}{g(x'_n)+\beta}. \tag{9}$$

由于 e'_{n+1} 是混沌拟合误差和白噪声引起的随机误差,因此在考虑值域范围时,e'_{n+1} 和 $-e'_{n+1}$ 可以不加区分,则(9)式可改写成

$$\hat{b}_{n+1}^{-1}=-\frac{f(x_n)+e'_{n+1}}{g(x'_n)+\beta}. \tag{10}$$

设 $\dfrac{f(x_n)+e_{n+1}}{g(x'_n)+\beta}\in[c,d]$,则根据(8)式和(10)式,估计的信号的值域范围为 $\hat{b}_{n+1}^{1}\in[c,d]$,$\hat{b}_{n+1}^{-1}\in[-d,-c]$.

当没有加入跟踪误差控制因子时(即 $\beta=0$),由于 $\dfrac{f(x_n)\pm e_{n+1}}{g(x'_n)}$ 的值域 $[c,d]$ 是近似轴对称的(即 $c\approx -d$)[35,36],因此 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 在相同的值域范围内随机波动,难以区分,如图 2(a).

如果加入幅度控制因子(即 $\beta\neq 0$),$\dfrac{f(x_n)\pm e_{n+1}}{g(x'_n)+\beta}$ 的值域将不再轴对称(即 $c\neq -d$),因此 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 将在不同的值域范围内随机波动,可以被准确区分,如图 2(b).

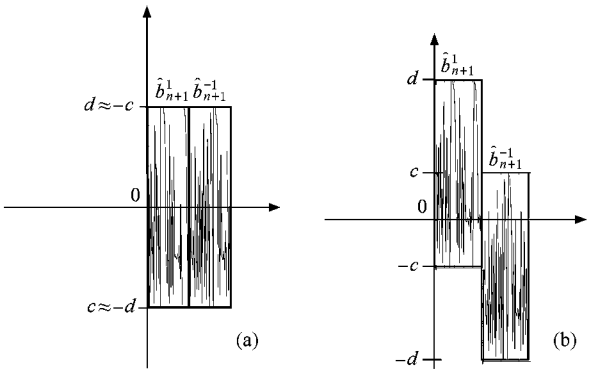

图 2 (a)$\beta=0$ 时 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 的随机波动范围;(b)$\beta\neq 0$ 时 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 的随机波动范围

证毕.后面的仿真实验将演示上述结论.

根据(3)式和(4)式,用无先导卡尔曼滤波算法估计信息码 $\hat{b}$ 的方法是对 x'_n 和 $\hat{b}_n$ 赋予任意初始值,从 $n=1$ 开始循环运算,其中的一个循环为两步:

第一步 对于(4)式用无先导卡尔曼滤波混沌拟合算法估计估计信息码 $\hat{b}_{n+1}$,即利用 x'_n 估计状态向量 $\hat{b}_{n+1}$;

第二步 对(3)式用无先导卡尔曼滤波混沌拟合算法估计混沌信号 x'_{n+1},即利用 $\hat{b}_{n+1}$ 估计 x'_{n+1}.

上述算法中,第一步和第二步中的无先导卡尔曼滤波算法相同.这里以第二步中估计 x'_{n+1} 的无先导卡尔曼滤波算法为例,来说明本文中所用的无先导卡尔曼滤波混沌拟合算法.

设 $h(x'_{n+1})=\hat{b}_{n+1}g(x'_n)+\beta$,则 $z_{n+1}=h(x'_{n+1})+n=\hat{b}_{n+1}g(x'_n)+\beta$.设 m 维的状态向量 $\hat{x}'_{n-1}$ 的均值为 $\hat{x}'_{n-1|n-1}$,协方差 $P_{n-1|n-1}$ 可以用 $2m+1$ 个加权采样点(sigma 点)近似表示,则一个循环步骤为三步[35,36]:

1)计算 sigma 点:计算 $2m+1$ 个点,如下:

$$\chi^{0}_{n-1|n-1}=\hat{x}'_{n-1|n-1},W_0=n/(m+n), \tag{11}$$

$$\chi^{i}_{n-1|n-1}=\hat{x}'_{n-1|n-1}+(\sqrt{(m+n)P_{n-1|n-1}})_i, \tag{12}$$

$$W_i=1/2(n+m),i=1,\cdots,m, \tag{13}$$

$$\chi^{i+m}_{n-1|n-1}=\hat{x}'_{n-1|n-1}-(\sqrt{(m+n)P_{n-1|n-1}})_i, \tag{14}$$

$$W_{i+m}=1/2(n+m),i=1,\cdots,m. \tag{15}$$

这里,$n\in\Re$ 是比例因子,$(\sqrt{(m+n)P_{n-1|n-1}})_i$ 是矩阵 $(m+n)P_{n-1|n-1}$ 的平方根的第 i 行或列(取决于矩阵平方根的形式,如果 $P=A^{\mathrm{T}}A$,则 sigma 点就是矩阵 A 的行,如果矩阵平方根形式为 $P=AA^{\mathrm{T}}$,则 sigma 点是矩阵 A 的列).在本文中矩阵 $(m+n)P_{n-1|n-1}$ 是 1×1 维的矩阵,是一个实数.W_i 是第 i 个点的归一化加权.

2)传播:传播 sigma 点,并获得状态向量的均值和协方差

$$\chi^{i}_{n|n-1}=g_i(\chi^{i}_{n-1|n-1}), \tag{16}$$

$$\hat{x}'_{n|n-1}=\sum_{i=0}^{2m}W_i\chi^{i}_{n|n-1}, \tag{17}$$

$$P_{n|n-1}=Q_{n-1}+\sum_{i=0}^{2m}W_i[\chi^{i}_{n|n-1}-\hat{x}'_{n|n-1}]\times[\chi^{i}_{n|n-1}-\hat{x}'_{n|n-1}]^{\mathrm{T}}. \tag{18}$$

3)更新:用 $h(\cdot)$ 计算测量的 sigma 点 $\zeta^{i}_{n|n-1}=h(\chi^{i}_{n|n-1})$

$$\hat{z}_{n|n-1} = \sum_{i=0}^{2m} W_i \zeta^i_{n|n-1}, \tag{19}$$

$$\tilde{e}_n = z_n - \hat{z}_{n|n-1}, \tag{20}$$

$$\hat{x}'_n = \hat{x}'_{n|n-1} + K_n \tilde{e}_n, \tag{21}$$

$$P_{n|n} = P_{n|n-1} - K_n P_{zz} K_n^{\mathrm{T}}, \tag{22}$$

$$P_{zz} = R_n + \sum_{i=0}^{2m} W_i [\zeta^i_{n|n-1} - \hat{z}_{n|n-1}] \times [\zeta^i_{n|n-1} - \hat{z}_{n|n-1}]^{\mathrm{T}}, \tag{23}$$

$$P_{xz} = \sum_{i=0}^{2m} W_i [\chi^i_{n|n-1} - \hat{x}'_{n|n-1}] \times [\zeta^i_{n|n-1} - \hat{z}'_{n|n-1}]^{\mathrm{T}}, \tag{24}$$

$$K_n = P_{xz} P_{zz}^{-1}. \tag{25}$$

3.4. 二进制信息码提取

通常对估计的 $\hat{b}$ 加阈值就可以准确的从估计的信息码 $\hat{b}$ 中提取二进制的信息码 $\hat{b}'_k$. 然而，如果有噪声干扰，通过简单的阈值的方法将难以准确破译并提取二进制信息码，因此这里提出一种具有一定抗噪声能力的方法，实现从估计的信息码中进一步较准确地提取二进制信息码.

设 N_k 是窃密接收机接收的混沌直扩信号中第 k 比特信息码的长度；$\hat{b}_{k,n}$ 表示估计的信息码 $\hat{b}$ 的第 k 比特的第 n 个扩频点，$n = 1,2,\cdots,N_k$ 则提取二进制信息码 $\hat{b}'_k$ 的算法如下：

$$c_k = \sum_{n=1}^{N_k} \hat{b}_{k,n}, \tag{26}$$

$$\hat{b}'_k = \begin{cases} 1, & c_k > 0 \\ -1, & c_k < 0. \end{cases} \tag{27}$$

通常，估计的信息码 $\hat{b}'_k$ 可能与原始发射的信息码反相，这不影响信息的提取. 设窃密接收机接收的混沌直扩信号长度为 l，第一个信息码长度为 q，该混沌直扩信号中有 K 比特的信息码，N 是扩频因子，则 $l \leqslant K \times N$. 其中 N 和 q 可以通过阈值等方法较容易地获得. 于是(26)式中的 N_k 为

$$N_k = \begin{cases} q, & k = 1; \\ N, & k = 2,3,\cdots,K-1; \\ l - 1 - (K-1)N, & k = K. \end{cases} \tag{28}$$

4. 仿真及分析

在 4.1 中通过实验验证了所述算法的有效性，即如果窃密者构造的混沌系统可以与发射端的混沌系统广义同步，则窃密者的混沌系统拟合原混沌系统，此时，所述方法可以准确破译混沌直扩信号. 实际上，由于所述的无先导卡尔曼滤波混沌拟合方法中，窃密者的混沌系统与混沌直扩信号发射端的混沌系统是直接耦合，属于强耦合，因此窃密者能比较容易地构造出广义同步的拟合混沌系统.

在 4.2 中进一步考虑了噪声的影响，仿真结果表明，所述方法具有较强的抗噪声干扰能力，因此所述方法不但具有理论研究意义，还具有一定的工程意义.

以下实验中，扩频因子为 127[6−10]. 用 logistic 混沌序列对某任意信息码序列扩频[6−10]；窃密者构造的拟合混沌系统是 tent 混沌系统.

4.1. 无噪声情况下的破译

文献 [32] 中证明并演示了 tent 混沌系统和 logisit 系统可以在较弱的耦合下实现广义同步，而在本文中的无先导卡尔曼滤波混沌拟合是直接耦合，属于强耦合，因此用 tent 混沌系统可以有效拟合 logistic 混沌系统.

发射端用对称的 logistic 映射 $x_{n+1} = f(x_n) = 1 - 2(x_n)^2$ 生成的混沌信号对任意信息码扩频[6−10]，窃密者构造 tent 混沌拟合系统来破译该混沌直扩信号. 窃密接收机的 tent 混沌映射为

$$y_k = g(y_{k-1}) = 0.5 - 1.99 \mid y_{k-1} \mid. \tag{29}$$

图 3 是用文献 [6,7] 中所述方法生成的混沌直扩信号，该混沌直扩信号类似白噪声，因此具有较强的保密性. 图 4 是不加跟踪误差控制因子(即 $\beta = 0$)时，用 3.3 节所述方法破译图 2 的混沌直扩信号得到的信息码 $\hat{b}$. 图中，由于拟合误差和过程噪声导致了较大的跟踪误差，因此 $\hat{b}$ 比较杂乱，$\hat{b}^{1}_{n+1}$ 和 $\hat{b}^{-1}_{n+1}$ 在相同的值域范围内随机波动，无法区分，与图 2(a)的结论相符合. 此时无法破译信息码 b.

图 5 是 $\beta = 0.9$ 时破译图 3 中混沌直扩信号获得的信息码 $\hat{b}$. 图中，$\hat{b}^{1}_{n+1}$ 和 $\hat{b}^{-1}_{n+1}$ 波动的值域范围明显相差很大，可以准确提取信息码. 这一点与图 2(b)的结论相符合. 对图 5 设阈值就可以较容易地实现破译. 这说明，跟踪误差控制因子 β 有利于破译混沌直扩信号. 为了便于比较，以下全部的仿真图中，都同时用虚线绘出了实际发射的信息码 b. 过程噪声协方差可取 10^{-1}—10^{-4}，这里取 10^{-2}. 图 6 是用 3.4 节所述方法对图 5 中估计的信息码 $\hat{b}$ 进一步提

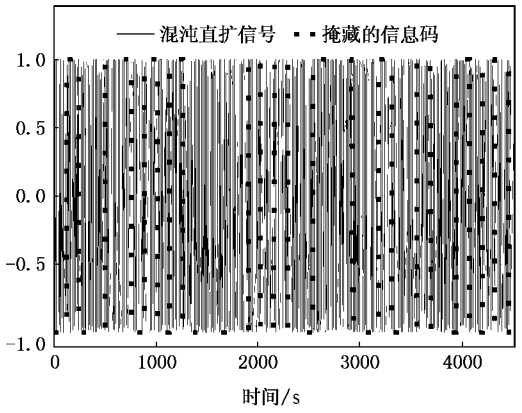

图 3 混沌直扩信号[6,7]

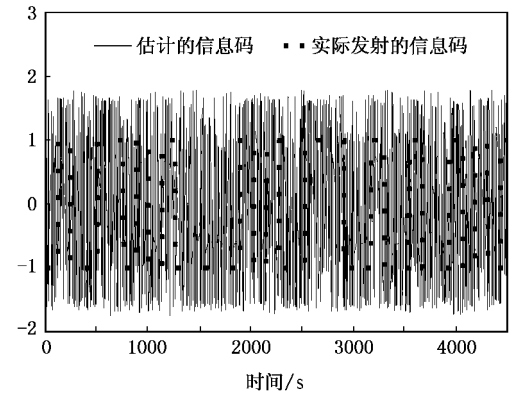

图 4 $\beta = 0$ **估计的信息码** $\hat{b}$

取二进制信息码的结果,为便于与原信息码比较,图中用虚线画出了破译的信息码 $-\hat{b}'_k$.

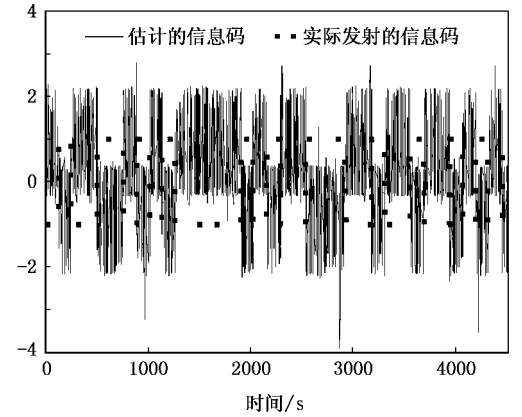

图 5 $\beta = 0.9$ **估计的信息码** $\hat{b}$

4.2. 有噪声情况下的破译

在信噪比 SNR = 15 dB **时,对** 1540 bit **的数据用蒙特卡罗方法进行** 1000 **次仿真实验,扩频因子为** 127**,实验中没有出现误码,表明所述方法具有一定的抗噪声能力.估计的信息码** $\hat{b}$ **结果如图** 7.**根据** 3.4 **所述方法计算的** C_k **和提取的二进制信息码** $-\hat{b}'_k$ **如图** 8.

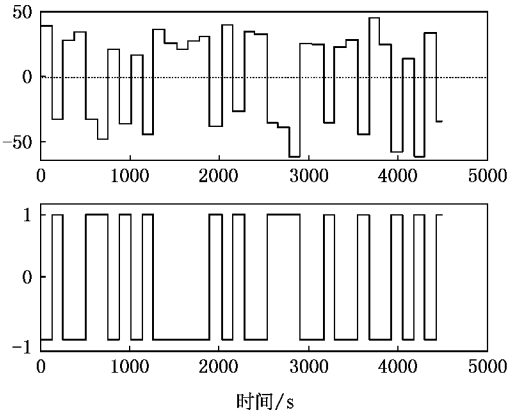

图 6 c_k **和破译的信息码** $-\hat{b}'_k$

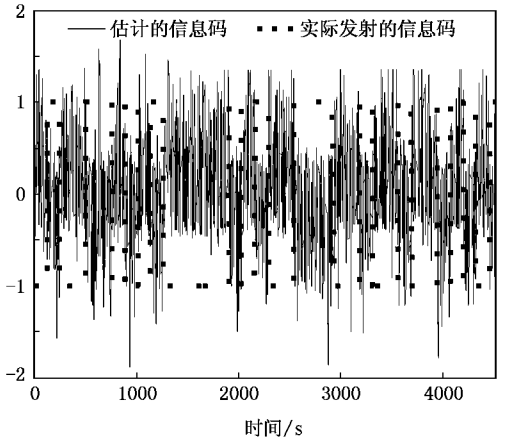

图 7 $\beta = 0.9$ **时估计的信息码** $\hat{b}$ (SNR = 15 dB)

文献[10]**中,在友方通信情况下并且** SNR = 7—8 dB **时,接收** 200 bit **数据没有出现误码,文献**[12]**在友方通信条件下,信噪比为** 10 dB **时误码率为** 10^{-3}—10^{-4}.**而本文所述方法破译混沌直扩信号时,在** SNR = 8 dB **的情况下,对** 1540 bit **的数据用蒙特卡罗方法进行** 1000 **次仿真实验,扩频因子为** 127**,实验中也没有出现误码,表明本文所述破译方法已经接近文献**[10]**和文献**[12]**中的友方通信的水平.本文所述方法在信噪比为** 8 dB **时估计的信息码如图** 9**,这里如果直接对图** 9 **中估计的信息码** $\hat{b}$ **设阈值将难以准确破译,而根据** 3.4 **所述方法则可较准确的破译混沌直扩.图** 10 **是根据** 3.4 **节所述方法计算的**

c_k 和提取的二进制信息码 $-\hat{b}'_k$.

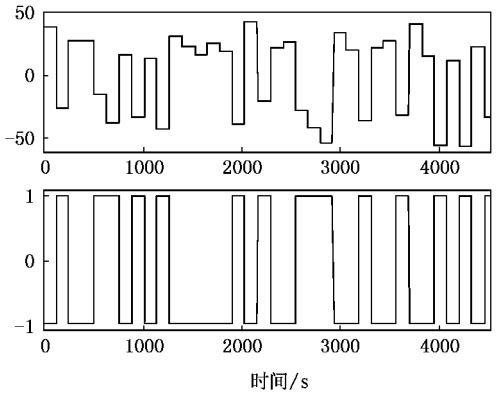

图 8　计算的 c_k 和破译的信息码 $-\hat{b}'_k$ (SNR = 15 dB)

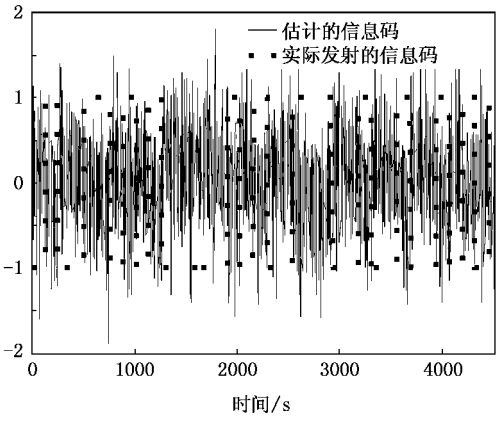

图 9　$\beta = 0.9$ 时估计的信息码 $\hat{b}$ (SNR = 8 dB)

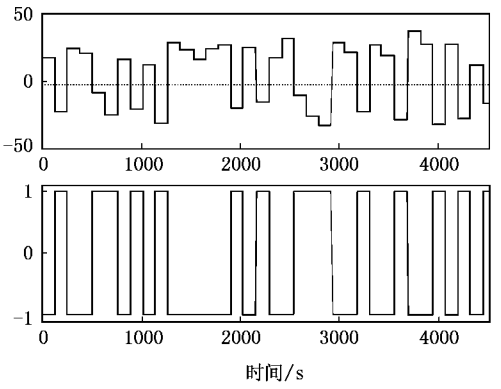

图 10　计算的 c_k 和破译的信息码 $-\hat{b}'_k$ (SNR = 8 dB)

5. 结　论

目前尚未见到破译混沌直扩的研究报道，并且由于混沌直扩具有不同于其他保密通信的两个特点：只有一个混沌吸引子以及混沌信号与信息码是相乘的，因此已有的混沌保密通信的破译方法对混沌直扩不适用.

本文针对混沌直扩保密通信的两个特点，提出了改进的无先导卡尔曼滤波混沌拟合的破译算法.所提算法无需知道混沌直扩发射机的结构、混沌映射参数等，可以准确的从混沌直扩信号中盲提取信息.

国际上破译混沌保密通信的研究中通常不考虑噪声干扰，而本文则考虑了噪声干扰，研究结果表明所述破译算法具有一定的抗噪声能力，可以有效降低对混沌噪声抑制、混沌信号盲分离或盲抽取的要求，具有一定的工程实际意义.

[1] 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]

[2] Chen B, Liu G H, Zhang Y, Zhou Z O 2005 *Acta Phys. Sin.* **54** 5039 (in Chinese) [陈　滨、刘光祜、张　勇、周正欧 2005 物理学报 **54** 5039]

[3] Yu L H, Fang J C 2005 *Acta Phys. Sin.* **54** 4012 (in Chinese) [于灵慧、房建成 2005 物理学报 **54** 4012]

[4] 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]

[5] 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]

[6] Parlitz U, Ergezinger S 1994 *Phys. Lett.* A **188** 146

[7] Ghobad H B, Clare D M 1994 *IEEE Trans. on Communications* **42** 1524

[8] Azou S, Pistre C, Duff L L, Burel G 2003 *IEEE-OCEANS San Diego* **3** 1539

[9] Luca M B, Azou S, Hodina E, Serbanescu A, Burel G 2006 *IEEE Communications Conf. Bucharest Romania* **1** 1

[10] Azou S, Burel G, Duff L L, Pistre C 2003 *IEEE-OCEANS '03 San Diego* **3** 1539

[11] Yu J, Yao Y D 2005 *IEEE Trans. on Wireless Communications* **4** 390

[12] Hwang Y S, Papadopoulos H C 2004 *IEEE Trans. on Signal Processing* **52** 2637

[13] Yang T, Yang L B, Yang C M 1998 *IEEE Trans. on CAS*-I **45** 1062

[14] Yang T, Yang L B, Yang C M 1998 *Phys. Lett.* A **247** 105

[15] Alvarez G, Li S J, Montoya F, Pastor G, Romera M 2004 *Chaos, Solitons and Fractals* **24** 775
[16] Wang F P, Wang Z J, Guo J B 2002 *Acta Phys. Sin.* **51** 474 (in Chinese) [汪芙平、王赞基、郭静波 2002 物理学报 **51** 474]
[17] Wang F P, Wang Z J, Guo J B 2002 *Circuits Systems and Signal Processing* **21** 427
[18] Perez G, Cerdeira H A 1995 *Phys. Rev. Lett.* **74** 1970
[19] Zhou C S, Lai C H 1999 *Phys. Rev.* E **60** 320
[20] Ponomarenko V I, Prokhorov M D 2002 *Physical Review* E **66** 026215
[21] Short K M, Parker A T 1998 *Phys. Rev.* E **58** 1159
[22] Alvarez G, Li S J 2004 *Computer Communications* **27** 1679
[23] Alvarez G, Montoya F, Romera M, Pastor G 2004 *IEEE Trans. on CAS*-II **51** 505
[24] Alvarez G, Montoya F, Romera M, Pastor G 2004 *Chaos, Solitons and Fractal* **21** 783
[25] Li S J, Alvarez G, Chen G R 2005 *Chaos, Solitons and Fractals* **25** 109
[26] Hu G J, Feng Z J, Meng R L 2003 *IEEE Trans. on CSA*-I **50** 275
[27] Li S J, Alvarez G, Chen G R, Mou X Q 2005 *Chaos* **15** 013703
[28] Tomsovic S, Ullmo D, Nagano T 2003 *Phys. Rev.* E **67** 067201
[29] Wang Y Q, Song A G, Huang W Y, Duan J H 2005 *Chinese J. of Scientific Instrument* **26** 403 (in Chinese) [王一清、宋爱国、黄惟一、段江海 2005 仪器仪表学报 **26** 403]
[30] Li X X, Feng J C 2007 *Acta Phys. Sin.* **56** 701 (in Chinese) [李雪霞、冯久超 2007 物理学报 **56** 701]
[31] Wang B Y, Zheng W X 2006 *IEEE Trans. on CAS*-II **53** 143
[32] Afraimovich V, Cordonet A, Rulkov N F 2002 *Phys. Rev.* E **66** 016208
[33] Alexander E, Koronovskii H A A 2005 *Phys. Rev.* E **71** 067201
[34] Zhang P W, Tang G N, Luo X S 2005 *Acta Phys. Sin.* **54** 3497 (in Chinese) [张平伟、唐国宁、罗晓曙 2005 物理学报 **54** 3497]
[35] Michail N P, Alivizatos E G, Uzunoglu N K 2007 *Signal Processing* **87** 665
[36] Merwe R U V D, Wan E A, Julier S I 2004 *AIAA Guidance, Navigation, and Control Conference*, Providence, RI 5120

Breaking a chaotic direct sequence spreading spectrum secure communication system*

Hu Jin-Feng Guo Jing-Bo†

(*Power System State Key Laboratory, Department of Electrical Engineering, Tsinghua University, Beijing* 100084, *China*)

(Received 9 May 2007; revised manuscript received 2 July 2007)

Abstract

In this paper, a novel method is proposed for the breaking of chaotic direct sequence spread spectrum (CD3S) secure communication system. Chaotic fitting is defined based on the concept of generalized synchronization, then the method based on unscented Kalman filter and chaotic fitting is presented based on the principle of CD3S and the characteristic that the information symbol varies slowly. Furthermore, addressing to the tracking error induced by the processing noise and chaotic fitting error, a modified unscented Kalman filter based on tracking-error-controlled factor is suggested. The CD3S is unmasked according to the error-amplitude of the tracking-error. We can extract the binary message signal from the CD3S signal without knowing either the structure or the parameters of the chaotic transmitter. Simulation results verify the method.

Keywords: chaotic secure communication system, breaking, chaos fitting, unscented Kalman filter

PACC: 0545, 0540

* Project supported by the National Special Project (Grant No. 2004AAXX5071).

† Correspondence author. E-mail: guojb@tsinghua.edu.cn