多径衰落信道下混沌直扩通信的可破解性*

白 鹭 郭静波†

(清华大学电机系,电力系统国家重点实验室,北京 100084)

(2010 年 7 月 15 日收到;2010 年 10 月 8 日收到修改稿)

本文在文献[1]的基础上,研究多径衰落信道条件下采用无先导卡尔曼滤波混沌拟合对混沌直扩通信的可破解性. 由针对混沌直扩信号的无先导卡尔曼滤波混沌拟合的状态空间方程出发,分析了多径衰落信道对于无先导卡尔曼滤波混沌拟合过程中的跟踪误差的影响,得到了信息码状态估计的值域范围,从而提出了多径衰落信道下混沌直扩信号可被破解的充分条件定理. 仿真结果表明,在满足充分条件下,混沌直扩信号无论是通过时不变信道还是时变信道,都可以被成功破解,并且具有良好的误码率性能.

关键词: 混沌通信, 破解, 多径衰落信道, 无先导卡尔曼滤波

PACS: 05.45.–a, 05.45.Vx

1. 引 言

由特定的非线性动力学系统产生的混沌信号,具有对初始条件极为敏感、宽频谱、不同混沌信号间相互正交以及不可复制性等特点,被广泛地应用于混沌通信中[1—20]. 混沌通信的主要方式有混沌掩盖[6,7,15]、混沌参数调制[8,17]、混沌键控[8,9,16,18]以及混沌扩频[19,20].

相对于传统的正弦载波通信,混沌通信在一定意义上讲具有某种与生俱来的安全性或保密性,混沌通信方式的安全性或其对立面——可破解性是混沌通信研究和应用中最引人注目的热点前沿问题.

已有的研究表明混沌掩盖可以通过相空间投影[15]等方法进行破解;混沌参数调制和混沌键控可以通过能量分析[16,17]和广义同步[17,18,21—24]等方法对不同吸引子的判别进行破解. 相比之下,由 Parlitz 等[19]和 Heidari-Bateni 等人[20]于 1994 年同时独立提出的混沌直接序列扩频(混沌直扩),由于具有低截获性[25]和物理层上的保密性[26],被认为是四种混沌通信中安全性最好、同时也是最难破解的通信方式.

到目前为止,仅文献[1]给出了一种全盲条件下混沌直扩通信的破解方法. 该方法提出了无先导卡尔曼滤波混沌拟合的全新思想,实现了对混有加性高斯噪声的混沌直扩信号的全盲解调.

然而,实际的信道环境远比加性高斯信道复杂得多. 实际信道中不仅存在加性高斯噪声,还存在导致信号发生畸变的多径衰落效应. 而多径衰落信道的存在使接收到的信号变为原信号的若干个加权延迟信号的叠加,增大了接收信号的破解难度. 文献[1]中没有对多径衰落信道下的混沌直扩信号的破解进行研究.

与混沌信号通过多径衰落信道有关的研究,现有的文献主要集中在信道参数估计或信道均衡. 如基于集元辨识的广义最小均方(SM-GLMS)信道参数估计方法[27]、利用扩展卡尔曼滤波进行信道均衡的方法[28]、基于最小非线性预测误差(MNPE)的信道估计方法[29]、基于逆滤波准则(IFC)的自适应信道参数估计方法[30]等. 在已知混沌动力学方程的前提下,这些方法都可以达到较好的信道参数估计或信道均衡的效果;另外由 Leung 等提出的利用径向基函数(RBF)神经网络进行信道参数估计的方法[31],无需知道混沌动力学方程,通过使用训练序列实现对混沌动力学方程的辨识和信道参数的估计.

在多径衰落信道条件下对混沌直扩信号的破解,既涉及多径衰落信道的盲均衡或信道参数估

* 国家重点实验室项目(批准号:SKLD09M25)资助的课题.

† 通讯联系人. E-mail: guojb@tsinghua.edu.cn

©2011 中国物理学会 Chinese Physical Society

计,又涉及信号的盲解调. 对接收破解方而言,混沌动力学方程是未知的,信息信号是完全随机的,信息信号与混沌载波之间的关系是乘性的,因此利用已知的混沌动力学方程或使用训练序列都是不现实的. 同时,到目前为止也没有关于多径衰落信道条件破解混沌直扩信号的研究报道.

本文旨在研究多径衰落信道条件下无先导卡尔曼滤波混沌拟合方法对混沌直扩信号的可破解性. 提出了无先导卡尔曼滤波混沌拟合在多径衰落信道下破解混沌直扩信号的充分条件定理,通过典型多径衰落信道条件下的计算机仿真验证了所提出定理的正确性.

2. 接收信号模型

混沌直扩通信是以混沌信号作为扩频载波的混沌扩频通信,图 1 给出了混沌直扩通信系统的示意图. 混沌序列 x_n 由下式的混沌动力学方程产生

$$x_n = f(x_{n-1}), \tag{1}$$

混沌序列 x_n 与信息序列 b_k 的直接相乘即为混沌直扩序列

$$s_n = x_n b_k, n = 1 + (k-1)N, \cdots kN, \quad k = 1,2,\cdots \tag{2}$$

其中 N 为扩频因子, $b_k \in \{-1,1\}$ 为信息码元.

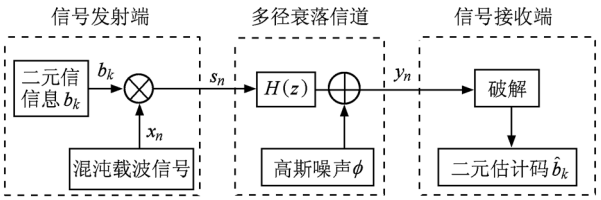

图 1 混沌直扩通信系统示意图

在多径衰落信道的影响下,接收端接收到的信号 y_n 可以用信号及其延时加权和来表示[32],即

$$y_n = H(C_n)[s_n] = c_0 s_n + \sum_{i=1}^{L_n} c_i s_{n-i} + \phi_n, \tag{3}$$

其中 $C_n = \{c_j\}_{j=0,\cdots L_n}$ 为 n 时刻的信道参数, L_n 为信道参数的阶数. 信道参数通常是时变的. s_n 是主径信号, c_0 为主径信号的参数, s_{n-i} 是 s_n 延迟 i 个时刻的信号,又称为旁径信号, $\{c_j\}_{j=1,\cdots L_n}$ 为旁径信号的参数. ϕ_n 为零均值高斯噪声.

图 2 给出了混沌直扩信号的示例图. 其中扩频因子 N 为 127,传递的信息码 b_k 为 $\{-1,1,-1,-1,1,1,-1,1\}$, 每一个信息码扩展为 127 个点,图 2

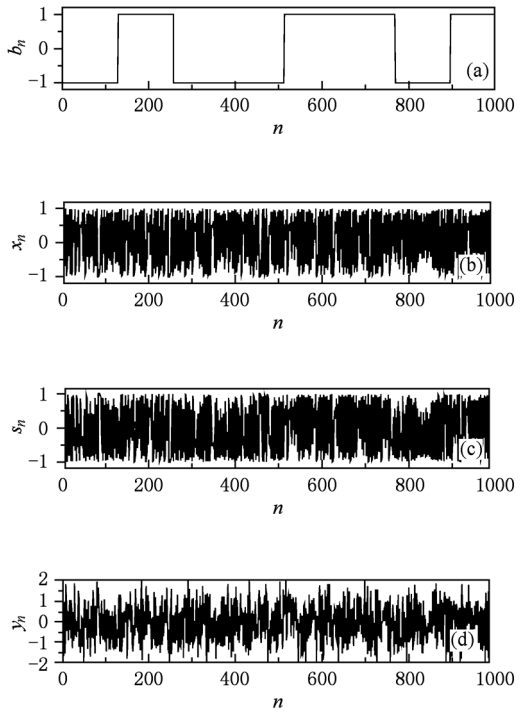

图 2 混沌直扩信号示例图 (a)信息序列 b_n;(b)混沌序列 x_n;(c)混沌直扩序列 s_n;(d)经过多径衰落信道后序列 y_n

(a)为信息序列 b_n;(b)为混沌序列 x_n, 由动力学方程产生;(a)与(b)相乘得到了(c)中的混沌直扩序列 s_n;(d)为经过多径衰落信道后的序列 y_n. 接收破解方在接收端收到的是经过多径衰落信道后的混沌直扩信号.

3. 多径衰落信道下混沌直扩通信的可破解性分析

由(3)式可知,多径衰落信道对接收信号的影响远比高斯噪声信道情形复杂. 这里通过分析多径衰落信道对无先导卡尔曼滤波混沌拟合过程中的跟踪误差的影响,得出多径衰落信道参数需要满足的约束条件并以定理形式给出.

3.1. 无先导卡尔曼滤波混沌拟合

在破解混沌直扩信号过程中,对接收破解方而言,发射端的混沌动力系统结构和参数以及信息码都是未知的. 无先导卡尔曼滤波混沌拟合的思想是在接收端使用另外一个混沌动力系统用无先导卡尔曼滤波的方法对接收到的混沌系统进行拟合. 拟合的结果是对信息码的估计序列,利用混沌直扩信号的估计值与真实值的误差(称为跟踪误差)对信

息码估计序列的值域范围进行分析判决,从而得到信息码的破解结果.

分别以混沌序列和信息序列作为待估计的状态变量. 建立两组状态空间方程如下:

$$\begin{aligned} x'_{n+1} &= g(x'_n) + v_n^{(1)}, \\ z_{n+1} &= \mathrm{sgn}(\hat{b}_{n+1})x'_{n+1} + \phi_n^{(1)}; \\ \hat{b}_{n+1} &= \hat{b}_n + v_n^{(2)}. \end{aligned} \tag{4}$$

$$z_{n+1} = \hat{b}_{n+1}(g(x'_n) + \beta) + \phi_n^{(2)}, \tag{5}$$

其中, $v_n^{(1)}$, $v_n^{(2)}$ 分别为过程噪声, $\phi_n^{(1)}$, $\phi_n^{(2)}$ 分别为观测噪声,这里都假设为高斯噪声.

(4)式为混沌序列的状态方程,函数 $g(.)$ 为接收破解方所选取的混沌动力学方程,由于我们研究的是破解算法,因此信号的生成信息未知,所以 $g(.)$ 不同于信号产生过程中使用的动力学方程 $f(\cdot)$. z_{n+1} 表示观测值,根据混沌直扩信号的原理建立,函数 sgn(·) 表示为

$$\mathrm{sgn}(\hat{b}) = \begin{cases} 1, & \hat{b} > 0, \\ -1, & \hat{b} < 0. \end{cases} \tag{6}$$

(5)式为信息序列的状态空间方程,由于信息码相对于混沌信号是慢变信号,因此,在很短的时间内 $\hat{b}_{n+1} = \hat{b}_n$. β 是误差跟踪控制因子, β 的加入使得混沌拟合得以实现[1].

根据建立的状态空间方程(4)式和(5)式,将无先导卡尔曼滤波混沌拟合过程总结如下:

1) $n = 1$, 为(4)式和(5)式中的状态变量 x'_1 和 $\hat{b}_1$ 赋任意初值;

2)以(4)式为状态方程,使用无先导卡尔曼滤波的方法估计混沌序列 x'_{n+1};

3)以(5)式为状态方程,使用无先导卡尔曼滤波的方法[33]估计信息 $\hat{b}_{n+1}$;

4)如果 n 小于信号的长度,则 $n = n + 1$, 从2)开始循环. 如果 n 已经到了信号的结尾,则结束.

3.2. 多径衰落信道下混沌直扩信号的可破解性分析

关于对多径衰落信道影响下的混沌直扩信号的可破解性,本文给出如下定理.

定理 对于多径衰落信道影响下的混沌直接扩频信号,如果对于每一个时刻 n, 信道参数都满足 $|c_0| > \sum_{i=1}^{L_n} \kappa |c_i|$, 且对于任意 n, c_0 正负性保持不变,则无论信道是时变还是非时变信道,都可以用无先导卡尔曼滤波混沌拟合对混沌直扩信号进行破解. 其中 κ 由(22)式给出,是一个由发射端和接收破解端所选取的混沌映射决定的常数,其值不小于1.

证明 在多径衰落信道下接收到的信号 y_n 如(3)式所示. 根据状态空间方程(5)式可以得到它们之间的误差为

$$\begin{aligned} e_{n+1} &= y_{n+1} - z_{n+1} \\ &= c_0 b_{n+1} f(x_n) - \hat{b}_{n+1}(g(x_n) + \beta) \\ &\quad + \sum_{i=1}^{L_n} c_i b_{n+1-i} f(x_{n-i}) + \phi_{n+1}^{(0)} - \phi_{n+1}^{(2)}. \end{aligned} \tag{7}$$

令跟踪误差为 e'_{n+1}, 根据(7)式可以得到

$$e'_{n+1} = e''_{n+1} + \sum_{i=1}^{L_n} c_i b_{n+1-i} f(x_{n-i}), \tag{8}$$

其中

$$e''_{n+1} = \phi_{n+1}^{(0)} - \phi_{n+1}^{(2)} - e_{n+1}, \tag{9}$$

则信息码的估计值为

$$\begin{aligned} \hat{b}_{n+1} &= \frac{b_{n+1} f(x_n) + e'_{n+1}}{g(x'_n) + \beta} \\ &\quad + \frac{\sum_{i=1}^{L_n} c_i b_{n+1-i} f(x_{n-i})}{g(x'_n) + \beta}. \end{aligned} \tag{10}$$

由(8)式可知,跟踪误差分为两部分. 第一部分为 e''_{n+1}, 其方程如(9)式,这一部分误差由高斯噪声和混沌拟合误差引起,与混沌和信息码的状态相互独立,且分布关于0对称,在估计(10)式中的 $\hat{b}_{n+1}$ 的取值范围时, e''_{n+1} 与 $-e''_{n+1}$ 不加区分. 因此,设 $b_{n+1} = 1$ 的估计表示为 $\hat{b}_{n+1}^1$, $b_{n+1} = -1$ 的估计表示为 $\hat{b}_{n+1}^{-1}$, 可以得到估计信息码为

$$\begin{aligned} \hat{b}_{n+1}^1 &= c_0 \frac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta} \\ &\quad + \sum_{i=1}^{L_n} c_i b_{n+1-i} \frac{f(x_{n-i}) + e'''_{n+1}}{g(x'_n) + \beta}, \end{aligned} \tag{11}$$

$$\begin{aligned} \hat{b}_{n+1}^{-1} &= -c_0 \frac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta} \\ &\quad + \sum_{i=1}^{L_n} c_i b_{n+1-i} \frac{f(x_{n-i}) + e'''_{n+1}}{g(x'_n) + \beta}, \end{aligned} \tag{12}$$

其中

$$e''_{n+1} = e'''_{n+1} \sum_{i=0}^{L_n} c_i b_{n+1-i}, \tag{13}$$

e''_{n+1} 与 e'''_{n+1} 仅是幅度上的差别,性质没有发生变化.

设 $\frac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta} \in [d_1, d_2]$. 从(11)式和(12)式可以看出,如果没有多径衰落信道的影响,即如

果对于 $i = 1,\cdots,L_n, c_i = 0$, 那么估计信号 $\hat{b}_{n+1}^{1}$ 的值域范围与 $\hat{b}_{n+1}^{-1}$ 的值域范围关于 $\hat{b} = 0$ 轴对称,分别为 $\hat{b}_{n+1}^{1} \in [d_1, d_2]$, $\hat{b}_{n+1}^{-1} \in [-d_2, -d_1]$, 且文献[1]中已经证明,由于误差跟踪控制因子 β 的加入使得 $d_1 \neq -d_2$, 即 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 的值域范围不完全重叠,因此可以根据值域的范围进行信息码的估计.

跟踪误差的第二部分误差是由多径衰落信道引起的,根据上面的分析 $\dfrac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta} \in [d_1, d_2]$ 且 $d_1 \neq -d_2$, 由(11)式和(12)式,可以得到

$$\hat{b}_{n+1}^{1} = \Big(c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i}\Big)\frac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta}, \quad (14)$$

$$\hat{b}_{n+1}^{-1} = \Big(-c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i}\Big)\frac{f(x_n) + e'''_{n+1}}{g(x'_n) + \beta}. \quad (15)$$

记新的值域范围为 $\hat{b}_{n+1}^{1} \in [r_l^1, r_h^1]$, $\hat{b}_{n+1}^{-1} \in [r_l^{-1}, r_h^{-1}]$, 从(14)式和(15)式可以看出,在第二部分误差影响下, $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 的值域范围会发生不同的变化,导致 $\hat{b}_{n+1}^{1}$ 的值域范围最大值有可能大于 $\hat{b}_{n+1}^{-1}$ 的取值范围最大值,如图3(a)所示,也有可能小于 $\hat{b}_{n+1}^{-1}$ 的取值范围最大值,如图3(b)所示,如果对于不同的时刻 n, 图3(a)和(b)的情况都出现,则在解调结果中会出现误码. 下面证明如果 $c_0 > 0$, 在 $d_2 > -d_1$ 的情况下,充分条件可以保证 $\hat{b}_{n+1}^{1}$ 的取值范围最大值大于 $\hat{b}_{n+1}^{-1}$ 取值范围的最大值. 从而实现破解.

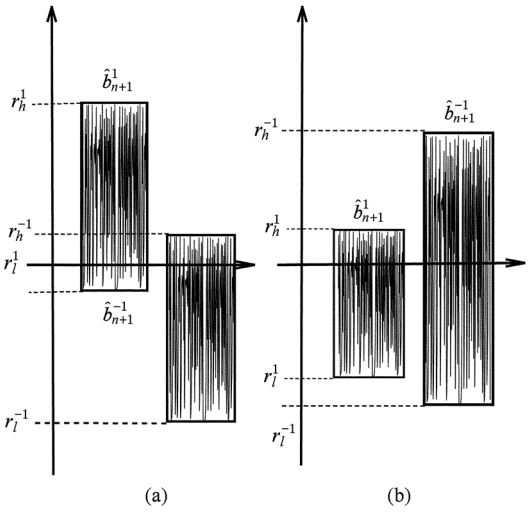

图3 估计值值域变化图 (a) $\hat{b}_{n+1}^{1}$ 最大值大于 $\hat{b}_{n+1}^{-1}$ 最大值; (b) $\hat{b}_{n+1}^{1}$ 最大值小于 $\hat{b}_{n+1}^{-1}$ 最大值

根据充分条件 $|c_0| > \sum_{i=1}^{L_n} \kappa |c_i|$, 并且 $\kappa \geqslant 1$, 可以得到 $c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i} > 0$, 并且 $-c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i} < 0$, 因此根据(14)式和(15)式可以得到 $\hat{b}_{n+1}^{1}$ 和 $\hat{b}_{n+1}^{-1}$ 取值范围的最大值分别为

$$r_h^1 = (c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i}) d_2, \quad (16)$$

$$r_h^{-1} = \Big(-c_0 + \sum_{i=1}^{L_n} c_i b_{n+1-i}\Big) d_1. \quad (17)$$

由 $r_h^1 > r_h^{-1}$ 可以得到

$$c_0 > \frac{d_2 - d_1}{d_2 + d_1} \sum_{i=1}^{L_n} c_i b_{n+1-i}. \quad (18)$$

由于 $b_{n+1-i} \in \{-1, 1\}$, 且 $c_0 > 0$, 则如果

$$|c_0| > \frac{d_2 - d_1}{d_2 + d_1} \sum_{i=1}^{L_n} |c_i| \quad (19)$$

成立,则(18)式成立.

由于在 $d_2 > -d_1$ 的情况下 $d_2 > 0$, 因此在(19)式中,如果 $d_1 < 0$, 则 $\dfrac{d_2 - d_1}{d_2 + d_1} > 1$; 如果 $d_1 \geqslant 0$, $\dfrac{d_2 - d_1}{d_2 + d_1} < 1$, 但是由于在对(16)式和(17)式的推导中要求 $|c_0| > \sum_{i=1}^{L_n} |c_i|$, 因此可以得到充分条件

$$|c_0| > \kappa \sum_{i=1}^{L_n} |c_i|, \quad (20)$$

其中

$$\kappa = \frac{d_2 + |d_1|}{d_2 + d_1}. \quad (21)$$

从(21)式可以看出,当 $d_1 \geqslant 0$ 时, $\kappa = 1$, 而当 $d_1 < 0$ 时, $\kappa > 1$.

有些接收端混沌映射的选择会导致 $-d_1 > d_2$, 此时 $-d_1$ 一定大于0, d_2 正负性不确定,则同理充分条件可保证 $\hat{b}_{n+1}^{-1}$ 的取值范围最大值大于 $\hat{b}_{n+1}^{1}$ 取值范围的最大值,因此综合两种情况得到 κ 为

$$\kappa = \frac{|d_2| + |d_1|}{|d_2 + d_1|}. \quad (22)$$

以上的推导都是基于 $c_0 > 0$ 的假设,实际上 $c_0 < 0$ 也可以得到以上结论,只是 $\hat{b}_{n+1}^{1}$ 的值域分布所对应的估计变为 $b_{n+1} = -1$, $\hat{b}_{n+1}^{-1}$ 的值域分布所对应的估计为 $b_{n+1} = 1$. 如果对于任意时刻 n, c_0 恒为负,那么破解得到的信息码与原信息码完全相反,这也属于成功的破解,因为为了防止信道传输中信号反相的问题,在将信息转换为二元码时,大多采用差分的编码方式,即译码时与二元码的绝对正负性无关,只与正负性的相对变化有关. 因此,对于任意时刻 n, 如果 c_0 的正负性保持不变,则破解得到的估计序列与原序列完全相同或完全相反,这样都

可以对信息码进行成功破解. 如果其间 c_0 的正负性发生了变化,解得的信息估计序列某些部分与原序列相同,某些部分与原序列相反,则在对信息估计序列进行译码的过程中会产生误码.

证毕.

在实际应用中,在主路径存在的情况下都可能满足这个充分条件,比如文献[34]中实验得到的水下通信信道,文献[35]中为城市环境和郊区环境所建立的无线通信信道模型等. 因此这个定理的提出具有实际意义.

4. 仿真结果及分析

针对混沌直扩信号通过时不变信道和时变信道,通过仿真验证上述提出的混沌直扩信号可破解的充分条件定理,同时考察在多径衰落信道下无先导卡尔曼滤波混沌拟合破解混沌直扩信号的误码性能.

下列仿真中,发射端都采用对称 logistic 映射作为混沌动力学方程产生信号,其动力学方程为

$$x_{n+1} = f(x_n) = 1 - 2x_n^2. \tag{23}$$

接收端构造 tent 混沌拟合系统进行破解,tent 混沌映射动力学方程为

$$x'_{n+1} = g(x'_n) = 0.5 - 1.99 \mid x'_n \mid . \tag{24}$$

选取扩频因子 $N = 127$, 误差跟踪控制因子 $\beta = 0.9$. 仿真中所提到的信噪比(SNR)为主径信号与高斯噪声的功率比,不包含旁径信号的影响.

4.1. 时不变多径衰落信道下的破解

考虑时不变多径衰落信道,设定信道参数为

$$C = [1, 0.4, 0.3], \tag{25}$$

并且添加信噪比为 10dB 的高斯噪声. 混沌直扩信号通过该信道的破解结果如图 4 所示,可以看出信息序列与破解结果一致. 在此情况下, $1 \leqslant \kappa \leqslant \dfrac{1}{0.7} \approx 1.42$.

图 5 是对三种旁径参数绝对值之和相同但是具有不同信道阶数的信道在不同信噪比下的误码率(BER)进行仿真,三种信道参数分别为

$$\begin{aligned} C_1 &= [1, 0.4, 0.3], \\ C_2 &= [1, 0.4, 0.2, -0.1], \\ C_3 &= [1, 0.35, -0.2, 0.1, 0.1]. \end{aligned} \tag{26}$$

可以看出由于每种信道旁径参数绝对值之和都为 0.7, 因此误码率曲线都相似,在信噪比为 8dB 的情况下均已达到 10^{-4} 以下的误码率,所以不同信道阶数情况下都可以破解.

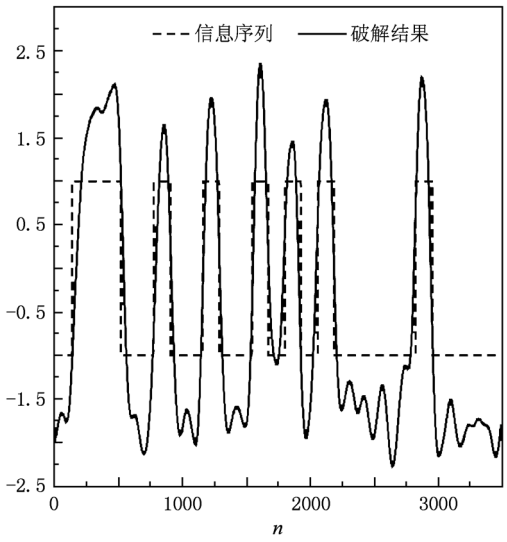

图 4 参数为 $C = [1, 0.4, 0.3]$ 信道下的破解结果

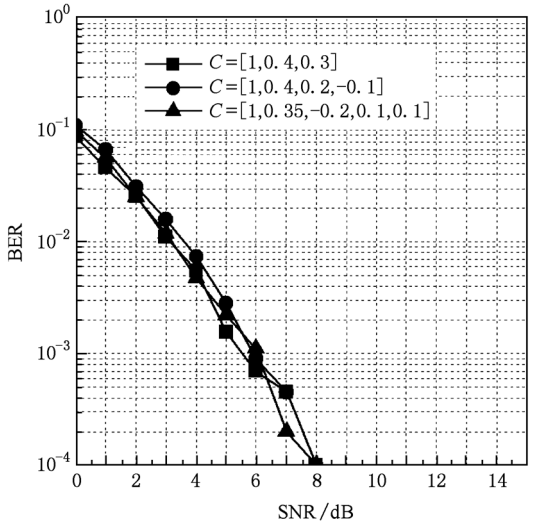

图 5 三种旁径参数绝对值之和相同但信道阶数不同的信道在不同信噪比下的误码率曲线

图 6 是对四种旁径参数绝对值之和不同的信道在不同信噪比下进行仿真的误码率曲线,四种信道参数分别为

$$\begin{aligned} C_1 &= [1, 0.4, 0], \\ C_2 &= [1, 0.4, 0.3], \\ C_3 &= [1, 0, 4, 0.6], \\ C_4 &= [1, 0.4, 0.9], \end{aligned} \tag{27}$$

其中 C_1 和 C_2 旁径参数绝对值之和都小于主径参数绝对值,分别在信噪比为 7 dB 和 8 dB 的情况下误

码率达到 10^{-4} 以下. 信道参数 C_3 的信道旁径参数绝对之和与主径相等(不满足充分性条件),在信噪比大于7dB 的情况下,误码率基本稳定在1% 左右. 而信道参数为 C_4 的信道旁径参数绝对值之和为 1.3 > 1 (严重不满足充分性条件),其误码率基本在 50% 左右,这属于破解中最坏的误码率.

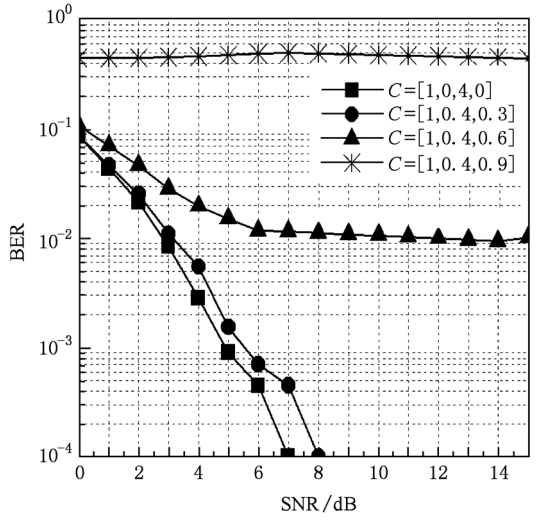

图6 四种旁径参数绝对值之和不同的信道在不同信噪比下的误码率曲线

4.2. 时变多径衰落信道下的破解

信道参数由正余弦函数产生

$$C = \left[1, 0.4\sin\left(\frac{\pi n}{640}\right), -0.3\cos\left(\frac{\pi n}{640}\right)\right]. \quad (28)$$

参数 c_1 和 c_2 的变化曲线如图7 所示,图8 为信道参数为(28)式情况下的破解结果,可以看出破解结果与实际信号一致.

图9 是三种信道阶数不同的信道在不同信噪比下的误码率曲线. 三种信道的信道参数分别为

$$C_1 = A_1\Delta = [1, 0.4, -0.3, 0, 0]\Delta,$$
$$C_2 = A_2\Delta = [1, 0.35, 0.24, -0.22, 0]\Delta,$$
$$C_3 = A_3\Delta = [1, 0.35, 0.24, -0.12, 0.1]\Delta, \quad (29)$$

其中

$$\Delta = \mathrm{diag}\left\{1, \sin\left(\frac{\pi n}{640}\right), \cos\left(\frac{\pi n}{640}\right), \sin\left(\frac{\pi n}{160}\right), \cos\left(\frac{\pi n}{160}\right)\right\}. \quad (30)$$

三种信道都在信噪比为 5dB 的情况下误码率达到 10^{-4} 以下,因此满足充分条件情况下,经过不同信道阶数信道的信号都可以被破解.

图10 是对四种旁径参数绝对值之和不同的信道在不同信噪比下破解的误码率对比曲线,四种信道参数分别为

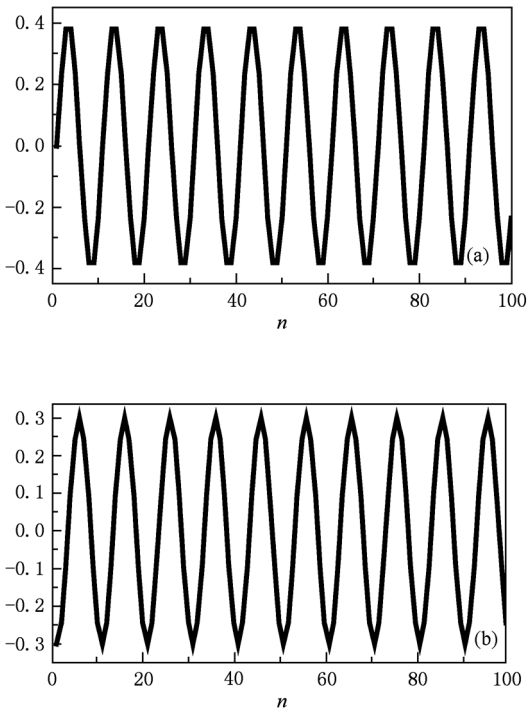

图7 时变信道参数变化图 (a) 信道参数 $c_1 = 0.4\sin(\pi n/640)$; (b) 信道参数 $c_2 = -0.3\cos(\pi n/640)$

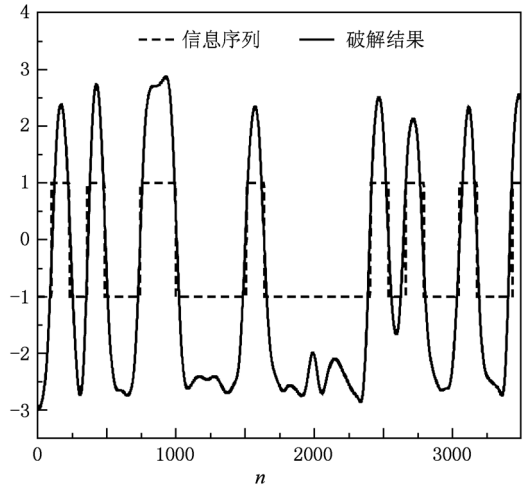

图8 参数为二阶时变信道下的破解结果

$$C_1 = A_1\Delta_2 = [1, 0.4, 0]\Delta_2,$$
$$C_2 = A_2\Delta_2 = [1, 0.4, -0.3]\Delta_2,$$
$$C_3 = A_3\Delta_2 = [1, 0.4, -0.6]\Delta_2,$$
$$C_4 = A_4\Delta_2 = [1, 0.8, -0.9]\Delta_2, \quad (31)$$

其中

$$\Delta_2 = \mathrm{diag}\left\{1, \sin\left(\frac{\pi n}{640}\right), \cos\left(\frac{\pi n}{640}\right)\right\}. \quad (32)$$

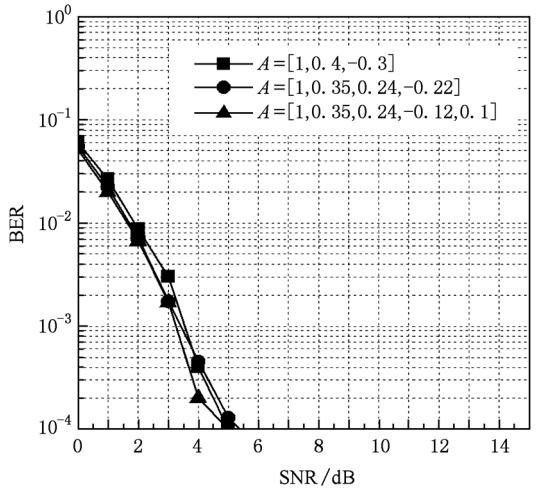

图9 三种旁径参数绝对值之和基本相同而信道阶数不同的信道在不同信噪比下的误码率曲线

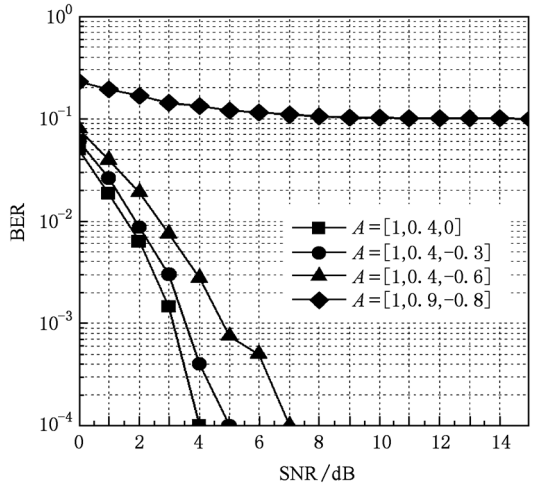

图10 四种旁径参数绝对值之和不同的信道在不同信噪比下的误码率对比

可以看出,前三种信道情况都满足充分条件,分别在信噪比为4 dB,5 dB 和7 dB 情况下,误码率达到 10^{-4} 以下. 第四种信道每一时刻旁径参数绝对值之和的分布,有20% 在[0,1]范围内,有40% 在[1,1.05]范围内,有40% 在[1.15,1.2],其误码率在10 dB 以后基本上稳定在10% 左右.

以上仿真结果说明,混沌直扩信号无论通过时变还是时不变信道,只要信道满足定理中的条件,不管信道阶数如何,混沌直扩信号都可以被成功破解,且其误码性能优良,可满足工程实际要求. 在不满足定理中条件的情况下,信息码状态估计值域完全重合的概率明显增大,破解效果严重变坏,这与第3节中的分析完全符合.

5. 结 论

目前没有全盲的消除多径衰落信道对混沌直扩信号影响的均衡方法,也没有直接的破解方法. 本文基于无先导卡尔曼滤波混沌拟合对多径衰落信道下的混沌直扩信号的可破解性进行了理论研究和仿真分析,提出了多径衰落信道需要满足的充分条件定理,即只要信道参数中主径参数的绝对值大于旁径的参数绝对值之和的某个倍数,并且主径参数的正负性保持不变,则混沌直扩信号无论是通过时不变信道还是时变信道,都可以被成功破解. 仿真结果验证了所提出的充分条件定理的正确性,同时也显示出在多径衰落信道下无先导卡尔曼滤波混沌拟合破解混沌直扩信号具有良好的误码性能.

[1] Hu J F, Guo J B 2008 *Acta Phys. Sin.* **57** 1477 (in Chinese) [胡进峰、郭静波 2008 物理学报 **57** 1477]

[2] Wang Y C, Zhao Q C, Wang A B 2008 *Chin. Phys.* B **17** 2373

[3] Mou J, Tao C, Du G H 2003 *Chin. Phys.* **12** 381

[4] Li N, Li J F 2008 *Acta Phys. Sin.* **57** 6093 (in Chinese) [李农、李建芬 2008 物理学报 **57** 6093]

[5] 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]

[6] Cuomo K M, Oppenheim A V, Strogatz S H 1993 *IEEE Trans. Circuits Syst.* II **40** 626

[7] Li J F, Li N 2002 *Chin. Phys.* **11** 1124

[8] Dedieu H, Ckennedy M P, Hasler M 1993 *IEEE Trans. Circuits Syst.* II **40** 634

[9] 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]

[10] Wang M J, Wang X Y, 2009 *Acta Phys. Sin.* **58** 1467 (in Chinese) [王明军、王兴元 2009 物理学报 **58** 1467]

[11] Zhou W J, Yu S M, 2009 *Acta Phys. Sin.* **58** 113 (in Chinese) [周武杰、禹思敏 2009 物理学报 **58** 113]

[12] Yan S L 2005 *Acta Phys. Sin.* **54** 2000 (in Chinese) [颜森林 2005 物理学报 **54** 2000]

[13] Hu M F, Xu Z Y 2007 *Chin. Phys.* **16** 3231

[14] Li C Y, Li X H, Deng F G, Zhou H Y 2008 *Chin. Phys.* B **17** 2352

[15] 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]

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

[17] Alvarez G, Montoya F, Romera M, Pastor G 2004 *Chaos, Solitons and Fractal* **21** 783
[18] Yang T, Yang B L, Yang C M 1998 *IEEE Trans. Circuits Syst.* I **45** 1062
[19] Parlitz U, Lakshmanan S 1994 *Phys Lett.* A **188** 146
[20] Heidari-Bateni G, McGillem C D 1994 *IEEE Trans. Communications* **42** 1524
[21] Zhou P 2007 *Chin. Phys.* **16** 1263
[22] Xiao Y Z, Xu W 2007 *Chin. Phys.* **16** 1597
[23] Li Z, Han C Z 2002 *Chin. Phys.* **11** 666
[24] Li G H, Zhou S P, Xu D M 2004 *Chin. Phys.* **13** 168
[25] Tsatsanis M K, Proakis G B 1997 *IEEE Trans. Signal Processing* **45** 1241
[26] Hwang Y, Papadopoulos H C 2004 *IEEE Trans. Signal Processing* **52** 2637
[27] Zhang J S 2006 *Chin. Phys. Lett.* **23** 3187
[28] Zhu Z W, Leung H 2001 *IEEE Trans. Circuits Syst.* I **48** 979
[29] Zhu Z W, Leung H 2002 *IEEE Trans. Circuits Syst.* I **49** 170
[30] Vural C, Cetinel G 2010 *Digital Signal Processing* **20** 201
[31] Xie N, Leung H 2005 *IEEE Trans. Neural Networks* **16** 709
[32] Fang Y, Chow T W S 1999 *IEEE Trans. Neural Networks* **10** 918
[33] Kandepu R, Foss B, Imsland L 2008 *J. Process Control* **18** 753
[34] King P, Venkatesan R, Li C 2008 *Proc IEEE Globecom* 2008 Nov 30- Dec 4, 2008 p1
[35] Amitay N 1992 *IEEE Trans. Vehicular Technology* **41** 337

Breakability of chaotic direct sequence spreading spectrum secure system under multi-path fading channel*

Bai Lu Guo Jing-Bo†

(*State Key Lab, Department of Electrical Engineering, Tsinghua University, Beijing* 100084, *China*)

(Received 15 July 2010; revised manuscript received 8 October 2010)

Abstract

Blind demodulation (breaking) of chaotic direct sequence spread spectrum (CD3S) signals is a challenging and leading issue under multipath fading channel in the field of chaotic communication. Until now, there are neither equalization methods to remove the impact of the channel, nor the immediate breaking methods. Based on the existing study, the breakability of CD3S signals is analyzed under multipath fading channel by using unscented Kalman filter (UKF) chaotic fitting in this paper. Beginning with the state space equation for the CD3S signals in UKF chaotic fitting, the channel influence on the tracking error is analyzed in the process of UKF chaotic fitting, then the range of the message state estimation is derived, and finally a sufficient condition theorem is proposed for the CD3S signals to be broken. Simulation results show that CD3S signals can be broken successfully under the proposed condition with excellent performance of bit error rate (BER), no matter whether the channel characteristic is either time-invariant or time-variant.

Keywords: chaotic direct sequence spread spectrum secure communication, breaking, multi-path fading channel, unscented Kalman filter

PACS: 05.45.-a, 05.45.Vx

* Project supported by the State Key Lab of Power Systems, Tsinghua University (Grant No. SKLD09M25).

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