# 基于时空混沌保密通信的研究

石　军[1]，刘联会[2]，石　磊[3]
(1. 北京正有网络通信技术股份有限公司，北京　100083;2. 西安科技大学 通信与信息工程学院，陕西 西安　710054;
3. 西北核技术研究所，陕西 西安　710024)

**摘　要**:提出基于时空混沌序列的保密通信方法,提出了一种用时空混沌模型产生扩频地址码的方法,讨论了驱动序列的选择方法与原则,分析了其耦合同步特性,给出了一种具体的通信系统模型。实验结果表明:此模型具有较高的保密特性和较强的同步能力,并且易于实现。另外,只用很少的几路离散混沌序列作为同步序列就可传输多路信息,有效地提高了系统的信息传输效率。

**关键词**:保密通信;同步;时空混沌;扩频序列
**中图分类号**:TN918　　**文献标识码**:A　　**文章编号**:1009-3516(2004)01-0045-03

混沌通信由于具有几乎不可破译的保密性[1],因而逐渐成为保密通信和混沌应用研究领域的一个重要课题。自1990年美国海军实验室专家提出了混沌同步概念及其驱动——响应方法以来[2],逐渐开始了将混沌序列用于密码的研究工作[3]。结果表明,混沌序列是一种非线性序列,其结构复杂,难于分析和预测,可以提供具有良好随机性、相关性和复杂性的拟随机序列,因而有可能成为一种可实际被选用的流密码体制。但是,混沌序列用于扩频通信的一个关键技术是混沌序列的同步问题,本文选用时空混沌系统产生扩频系列,并研究了通信系统的序列同步问题。

## 1　基于混沌序列的编码通信方法

混沌编码通信是将所需要的信息以二进制的形式对混沌信号进行编码,对于采用数字混沌编码系统来进行的保密通信,由于避免了传输噪声和电路固有参数不匹配所造成不同步的影响,因此,比连续混沌系统更易实现,而且具有更高的保密性。

设每位二进制符号 $b(k)\in\{-1,1\}(k=1,2,3,\cdots)$,用长度为 $N$ 的混沌序列 $c(n)(n=1+(k-1)N,\cdots,kN)$ 来调制,则发送的扩频信号 $s(n)$ 为

$$s(n)=b(k)c(n)$$

由于传输信道中有干扰(设为 $e(n)$,如加性噪声以及其它干扰等)。因此接收到的信号 $r(n)$ 为

$$r(n)=s(n)+\mathrm{coeff}\times e(n)$$

式中:coeff是表征噪声强度的小参数。则译码恢复的输出信号 $\hat{b}(k)$

$$\hat{b}=\begin{cases}1 & r(n)c(n)\geqslant 0\\ -1 & r(n)c(n)<0\end{cases}$$

由于混沌序列的相关函数具有快速衰减特性,因此,一些噪声以及由于多径效应(延迟)而到达接收机的信号与接收机现有的序列是不相关的,因此,此编码方法对噪声和多径效应很不敏感。

## 2　基于单向耦合映射格子 模型[5]的系统及其同步

设发送端OCOML模型为

**收稿日期**:2003-07-07
**作者简介**:石　军(1975-),男,山东曹县人,硕士,主要从事信号处理及混沌在通信系统中的应用;
刘联会(1946-),男,陕西西安人,教授,主要从事信息处理研究.

$$u_{n+1}(i) = (1-\varepsilon_i)f(u_n(i)) + \varepsilon_i f(u_n(i-1)) \tag{1}$$

式(1)中:$n(n=1,2,\cdots,N)$ 为时间坐标,即迭代步骤;$i(i=1,2,\cdots,L)$ 为空间坐标,即混沌序列组中第 $i$ 个振子;$\varepsilon$ 为耦合系数;$u_n(i)$ 为第 $n$ 步迭代中第 $i$ 个振子的状态分量;$f(x)$ 为混沌单元的非线性混沌映射算子,这里选用的是研究得比较成熟的 Logistic 映射:$f(x)=4x(1-x)$ ;边界条件:$u_n(0)=u_n(L)$ 。

设接收端的 OCOML 模型为

$$v_{n+1}(i) = (1-\varepsilon_i)f(v_n(i)) + \varepsilon_i f(v_n(i-1)) \tag{2}$$

式(2)中的参数与式(1)中定义的完全一致。为了使发送端与接收端各对应振子精确同步,可以用发送端的少数(比如第 0 和(或)第$\frac{L}{2}$ 个)振子去驱动(或替代)接收端对应的振子。经研究发现,若取 $\varepsilon_i \in (0.75,1)$,则式(1)和式(2)两系统在任意时间序列(当然要满足驱动序列的选择原则)的驱动下均可以达到同步。

驱动序列的选择方法有多种,如:①用服从 均匀分布的随机序列作为驱动序列;②用一维混沌映射算子直接产生的序列作为驱动序列;③用具有 $L$ 个振子的 OCOML 模型产生的任一格点序列作为驱动序列。但须注意,驱动序列的值域范围应小于模型中算子 $f(x)$ 的取值范围。若用第 2 种方法,则选用的混沌映射算子应与 OCOML 模型中算子 $f(x)$ 不同。否则,将使所有混沌序列都趋于一致。

OCOML 模型产生的是一系列在 区间内分布的连续序列,通过量化和编码,就可以得到一组二值混沌切普(即伪随机地址码)序列。

## 3 基于时空混沌的 CDMA 系统模型

时空混沌系统的同步方法形式上类似于驱动——响应同步法,也具有耦合同步的特性,但其结果却等价于 Dead - Beat 同步法[6](即具有快速性和准确性等)。图 1 给出了一个基于时空混沌系统具体的 CDMA 通信系统模型。

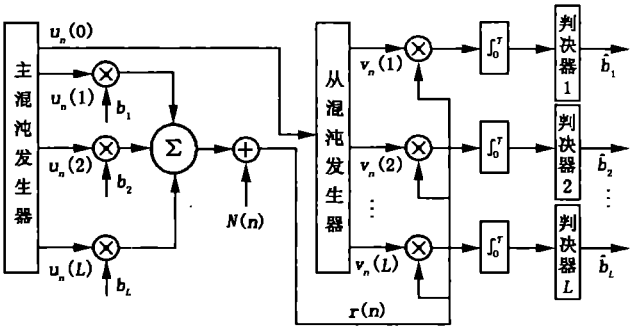


图 1 时空混沌码分多址系统功能框图

## 4 数值实验结果

取参数 $\varepsilon_i=0.98, L=20$ ,第 0 个振子作为传输同步信号,各振子的初值任取服从(0,1) 均匀分布的随机数,序列长度为 $N=100$ ,量化级数为 $2^{10}$。图 2 中 $u(n)$ 为发射端模型产生的混沌序列;$v(u)$ 为接收端模型产生的混沌序列;$e(n)$ 为两者的差值。可以得出,大约经过几十步后,系统(1)和(2)即可完全同步(即差值 $e$ 趋于零,为了增加效果,$e$ 值乘了一个系数)。

设要传输的二进制符号为 $b \in \{1,\cdots,1,\cdots,1\}$ ,选择第 10 个振子来调制信息 $b$ 。图 3 中 $b$ 是要传输的信息;$S$ 是调制后的传输信号 ,可以看出信息被完全遮掩,并且是类似噪声的随机信号;$bb1$ 是同步时译码后输出的信号;$bb2$ 是不同步时译码后输出的信号;$S1$ 是在有噪声的情况下,调制后的传输信号;$bb3$ 是噪声强度为 0.4 时译码后输出的信号。对照 $bb1$ 与 $b$ 可知,信号被准确恢复出来。如果发、收两端的参数不匹配($\varepsilon'_i=0.98002$ ),则不能正确地提取信息 $b$ ,如 $bb2$ 所示;$S1$ 是在噪声强度 coeff = 40% 下译码的结果,这表明,该系统对噪声很不敏感。

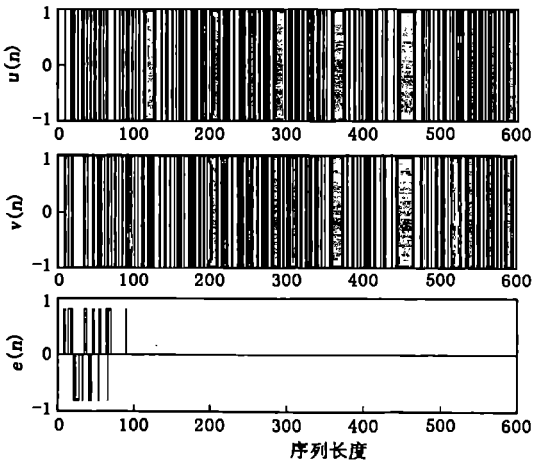


图 2 发射、接收端模型产生的混沌序列及其差值

## 5　结论

基于单向耦合映射格子模型的混沌系统,由于每个(甚至某一个)振子的初始条件不同,就可以产生不同的混沌序列,因此,当振子较多时,别人无法根据截获的单路或多路传输信息来预测或分离出有用信息。既使获得了所有的在信道中传输的信息,也无法搜索出每个振子的初始值和耦合系数 $\varepsilon_i$,从而很难在根本上破坏系统的安全性。另外,在混沌序列的产生中加入了舍入误差,混沌序列已不完全满足非线性系统方程,并且编码方法有很多种,因此较难重构。最后,混沌序列具有快速衰减的相关特性,多个用户可以在同一时间占用同一频段实现码分多址,具有较广泛的应用前景。

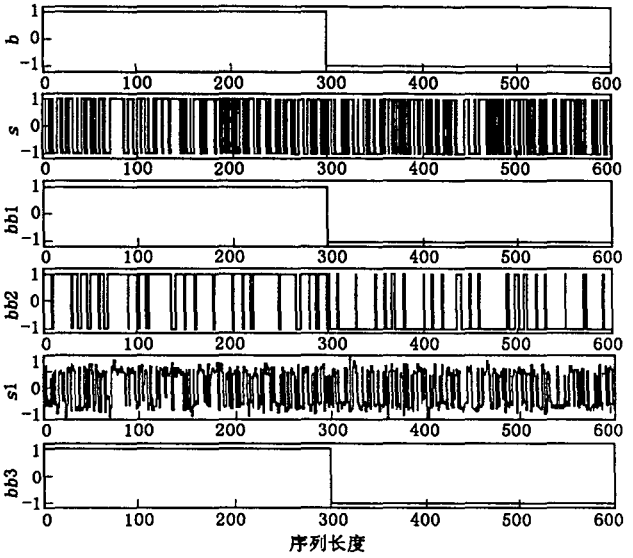


图3　信息在加密、同步、非同步、噪声下的解密过程

**参考文献:**

[1] Ling Cong, Sun Songgeng. Optimal Demodulation for Binary Chaos Shift Keying Signals[J]. Journal of China Institute of Communications, 1998, 19(7): 72 - 75.

[2] Pecora L M, Carroll T L. Driving Systems with Chaotic Signals[J]. Phys RevA, 1991, 44(4): 374 - 378.

[3] Mazzini G, Setti G, Rovatti R. Chatioc Complex Spreading Sequences for Asynchronous DS - CDMA—Part I: System Modeling and Results[J]. IEEE Trans, CAS I, 1997, 44(10): 937 - 947.

[4] Ling Cong, Sun Songgeng. A Chaotic Spreading Sequences Generator[J]. Journal of Electronics, 1998, 20(2): 235 - 240.

[5] Cheng Shichen, Zhu Bing, Kuang Jinyu. Enhancement of Transmission Efficiency in Synchronized Chaotic Communication Systems[J]. ACTA Electronica SINICA, 2001, 29(7): 873 - 876.

[6] Angeli A D, Genesic R, Tesi A. Dead - Beat Chaos Synchronization in Discrete - Time System[J]. IEEE Trans CAS, 1995, 42(1): 54 - 56.

(编辑:门向生)

# Research on Secure Communication Based on Spatiotemporal Chaos

SHI Jun[1], LIU Lian - hui[2], SHI Lei[3]

(1. Beijing Zhengyou Network & Communication Technology Co., Ltd, Beijing 100083, China; 2. School of Communication and Information Engineering Xi'an University of Science & Technology, Xi'an, Shaanxi 710054, China; 3. Northwest Institute of Nuclear Technology, Xi'an, Shaanxi 710024, China)

**Abstract**: The method of secure communication based on Spatiotemporal chaotic sequence is proposed, a method using spatiotemporal chaotic model to create spread - spectrum sequence is presented, and the problem of choosing a driving system synchronous sequence is discussed. Based on the above, a model of CDMA communication system is given. The result illustrates that the system possesses high security and stronger synchronizing ability and is easy to realize. In addition, by using only one or two discrete - line synchronizing chaotic sequences the system can be driven to work in multi - channel communications, thus the communication efficiency is enhanced significantly.

**Key words**: secure communication; synchronous; spatiotemporal chaos; spread - spectrum sequence