

# 基于混沌序列的 Simulink 扩频通信仿真

范一鸣<sup>1</sup> 杨亚涛<sup>2,3</sup> 许永涛<sup>2</sup>

(浙江工业大学浙西分校信息与电子工程系 衢州 324000)<sup>1</sup>

(北京电子科技学院 北京 100070)<sup>2</sup>

(北京邮电大学网络与交换国家重点实验室信息安全中心 北京 100876)<sup>3</sup>

**摘要** 首先研究了混沌序列的特性,设计了产生混沌序列的 Simulink 仿真模型,并且把该模型应用于直扩通信系统,仿真实现了基于混沌序列的直接扩频系统,经过理论研究和仿真实验表明,利用混沌序列作为扩频序列的扩频系统可以有效提高通信系统可靠性和抗干扰能力,具有较强的理论研究意义和实际应用价值。

**关键词** 混沌序列,通信仿真,扩频通信

## Simulink Spread Spectrum Communication Based on Chaos Sequence

FAN Yi-ming<sup>1</sup> YANG Ya-tao<sup>2,3</sup> XU Yong-tao<sup>2</sup>

(Department of Electronics and Information Engineering, West Branch of Zhejiang University of Technology, Quzhou 324000, China)<sup>1</sup>

(Beijing Electronic Science & Technology Institute, Beijing 100070, China)<sup>2</sup>

(Information Security Center, State Key Laboratory of Networking and Switching, Beijing University of Posts and Telecommunications, Beijing 100876, China)<sup>3</sup>

**Abstract** The performance of the Chaos sequence was studied firstly, and the model to generate chaos sequences was designed and also applied to direct sequence spread spectrum (DSSS) communication system; this paper also simulated DS communication system based on chaos sequence by designing simulink modules, some simulation experiments were also implemented. By theories studying and experimental simulation, it is obvious that chaos spread spectrum sequence can improve the communication system reliability and Anti-jamming capability, with a strong theoretical research and practical application value.

**Keywords** Chaos sequence, Communications simulation, Spread spectrum communication

扩频通信是一种传输信号所占据的带宽超过发送信息所需最小带宽的传输方式,带宽的扩展是通过高频码与信息数据调制来完成的,在接收端用相同的码字进行接收,其中包括解扩和信息数据的恢复<sup>[1]</sup>。混沌是由确定性方程产生的,只要方程参数和初值确定就可以重现混沌现象;另一方面,由于它对初值极端敏感,使得其长期行为难以预测,即混沌过程既非周期又不收敛。混沌区的数据具有迭代不重复性和初值敏感性,它是理论意义上的完全随机而不是通常所用的伪随机<sup>[2]</sup>。通过混沌系统产生的混沌序列进行扩频通信可以较明显地提高通信系统的安全性。文献[3]利用 Kent 混沌序列作为扩频码对多用户下的 CDMA 通信系统进行了仿真,但对基于混沌序列的直扩通信系统模型的相关输出结果没有深入分析。本文将 Logistic 混沌序列作为扩频序列进行了扩频通信系统的 Simulink 建模,通过实验结果,对基于混沌序列的扩频通信系统的性能进行了深入分析。

### 1 混沌扩频的基本原理

扩频通信有直接序列扩频、跳频扩频、跳时扩频等几种方

式。直接序列扩频的原理图如图 1 所示。

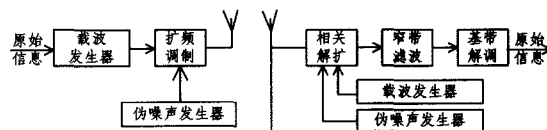


图 1 直接序列扩频的原理图

传统扩频通信中,通常采用 M 序列, GOLD 序列, WALSH 函数正交码等作为伪随机序列码型<sup>[4,5]</sup>,这些扩频算法中的扩频码是伪随机序列,即在扩频和解扩时都要用相同的伪随机序列,当要处理的数据量较大时,编码调制的伪随机序列就很长,由此对扩频序列的产生和存储带来麻烦。另外由于这种序列具有一定的周期性,因此它的码的数量很有限,抗截获性也较差。为了增强扩频调制的鲁棒性和实用性,可以把混沌理论引入到扩频技术中。

用混沌系统产生的混沌序列作为扩频通信的高频扩频序列,会大大提高扩频通信抗截获能力,实现性能良好的保密通信。而且由于混沌序列的高度伪随机性,混沌序列永远不会

到稿日期:2008-06-11 本文受浙江省自然科学基金项目(Y1080023),北京电子科技学院信息安全与保密重点实验室项目资助。

范一鸣(1964—),男,硕士,副教授,主要研究方向为网络通信技术、无线传感器网络技术等,E-mail:fyim@21cn.com;杨亚涛(1978—),男,博士研究生,主要研究方向为通信安全。

重复,因此众多混沌扩频可以共用同一个信道,这样就使频率资源的利用率得到提高。

本文中我们选用 Logistic 映射动力方程。它具有很好的自相关性和互相关抑制性,而且序列为零均值。混沌是由确定性方程产生的,只要方程参数和初值确定就可以重现混沌现象;由于它对初值极端敏感,使得其长期行为难以预测,即混沌过程既非周期又不收敛。混沌区的数据有两个特性:迭代不重复性和初值敏感性,它是理论意义上的完全随机而不是通常所用的伪随机。其动力方程定义为:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

其中,  $\mu$  称为分枝参数,当  $x_n \in (0, 1)$  且  $3.5699456 < \mu \leq 4$  时, Logistic 映射工作于混沌态。也就是说,由两个不同初始态的  $x_0$ ,在上式映射的作用下所产生的两个序列是非周期的、不收敛的、不相关的,并对初值非常敏感。

对于上式的 Logistic 映射,其生成序列的概率密度函数 PDF(Probability Density Function)为:

$$p(x) = \begin{cases} \frac{1}{\pi \sqrt{x(1-x)}} & 0 < x < 1, \mu = 4 \\ 0 & \text{其他} \end{cases} \quad (2)$$

通过  $p(x)$ ,可以很容易得到 Logistic 映射产生混沌序列的统计特性:

对于任意初值产生的混沌序列,其均值为:

$$\bar{x} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} x_i = \int_{-1}^1 x p(x) dx = 0 \quad (3)$$

独立选取两个初始值  $x_0$  和  $y_0$ ,则产生序列的互相关函数为:

$$\begin{aligned} \text{cov}(x_0, y_0) &= \lim_{N \rightarrow \infty} \left( \sum_{i=0}^{N-1} (x_i - \bar{x})(y_i - \bar{y}) \right) / N \\ &= \int_{-1}^1 \int_{-1}^1 p(x) p(y) (x - \bar{x})(y - \bar{y}) dx dy \\ &= \delta(x_0 - y_0) \end{aligned}$$

由于 Logistic 映射的概率分布密度函数  $\rho(x)$  不依赖于初始值  $x_0$ ,因此由式(1)和式(3)表达的混沌系统具有遍历性。对于保密通信而言,既要求对初值的敏感性又要求信号的随机性,敏感性越强同时随机性越好,则保密性越强。这些特性可由概率统计特性均值、自相关和互相关性来定量描述。利用概率密度函数,可以计算得到所关心的一些统计特性  $\rho(x)$  关于偶对称,所以式(1)和式(3)所产生的混沌序列的均值分别为 0.5 和 0。自相关函数近似为  $\delta$  函数,互相关为零。其概率统计特性与白噪声一致,适合于在保密通信中的应用。

从以上推导可以看出, Logistic 映射遍历统计特性等同于零均值白噪声的统计特性而初值微小的差异将产生截然不同的混沌序列。也就是说,如果初始条件只有有限的精度,则

随时间的推移,其状态的精度会变得越来越差,最终不可接受,即所谓的长期不可预测性。

由以上分析可知,混沌序列具有以下不同于其他序列的独特优点<sup>[6,7]</sup>:

(1)具有确定的、随机的和不可预测的特征,并且具有连续宽频谱特征。混沌序列没有周期,类似于一个随机过程,且任意截取一段序列,均不能预测出整个序列,不同于普通扩频系统中的伪随机序列,因此,具有很好的保密性和抗干扰能力。

(2)混沌序列的自相关性很强而互相关性很弱,因此易于从其它信号或者干扰中分离出来。可以代替传统的线性反馈移位寄存器产生的伪随机序列,用于扩频通信和安全信息传输。

(3)混沌序列容易产生和存储。只要给定混沌映射和初值便可产生出大量的、不同的混沌序列,并且序列长度是任意的,因此有利于计算机设计和硬件实现,设备成本低。

Logistic 序列的上述性质表明,由于混沌动力系统有确定性,其统计特性等同于白噪声,因而可被应用于语音隐秘通信中的扩频调制。

## 2 基于混沌序列的扩频仿真模型设计

本文研究了直接扩频通信系统的仿真,扩频序列采用 Logistic 随机码。设计的仿真模型主要包括混沌序列产生部分、扩频部分、解扩部分、结果显示和比较部分。设计的基于 Logistic 混沌序列直扩系统 Simulink 仿真图如图 2 所示。

在图 2 中,信号扩频的过程为:

(1)在扩频部分,首先由信号在 Random Integer Generator 产生一个随机的二进制信号,经 BPSK 调制之后被生成的混沌扩频序列调制,产生扩频信号。

(2)信号传输的信道采用高斯信道(信噪比约为 10db),扩频后的信号通过加性高斯白噪声信道时,会出现多径衰落、自由空间信号功率的衰减,从而导致信噪比严重下降。

(3)在解扩部分,扩频信号输入 Product 之后系统利用与扩频部分相同的混沌扩频序列对扩频信号进行解扩,其过程仍然是接收到的信号和原来的伪随机序列进行相乘,把原本的宽带信号恢复到一个很窄的频带内;对解扩后的信号,再用 BPSK 解调,把信号从频带信号转化成基带信号,便能恢复出原始信号。

(4)最后将初始的信号和恢复出的信号同时输入到误码率分析器中对比得到该系统的误码率,计算结果通过显示模块(display)显示。

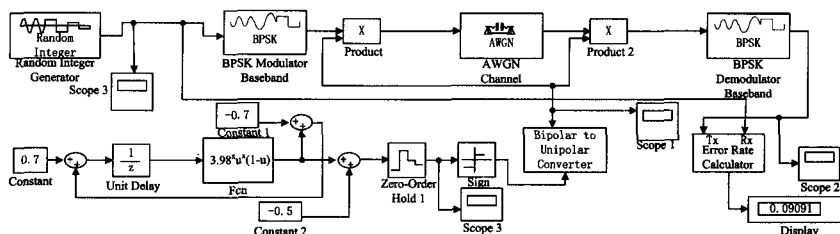


图 2 Logistic 混沌序列扩频通信系统仿真模型图

### 3 Logistic 混沌序列产生器的设计

我们选用 Logistic 映射动力方程。它具有很好的自相关性和互相关抑制性,而且序列为零均值,根据 Logistic 映射动力方程,即式(1)可以设计出如图 3 所示的 Simulink 仿真模型。

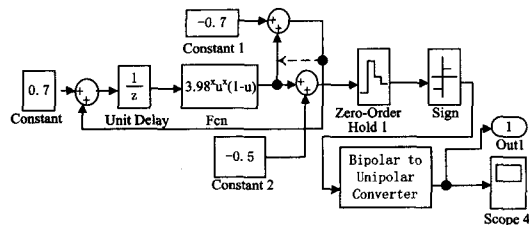


图 3 Logistic 混沌序列产生器

在该仿真模型中,通过输入一个  $x$  的初值得到映射动力方程运算产生的结果(分枝参数  $\mu$  是常数),然后将产生的结果返回到输入端,当作下一次运算的  $x$  值,即将第  $n$  次的计算结果当作第  $n+1$  次的  $x$  值,如此循环迭代计算就可以得到一个随机性很强的序列,然后经过波形变换过程即可得到 0-1 混沌扩频序列。在该模型中设产生混沌扩频序列的初值  $x_0 = 0.7$ ,分枝参数  $\mu = 3.98$  ( $3.5699456 < \mu \leq 4$ ),之后的每次计算都是把第  $n$  次的计算结果当作第  $n+1$  次计算所需  $x$  的值。

Constant 在 Simulink 中是一个可以自定义常数的模块。将 Constant, Constant1, Constant2 的值分别设置为 0.7, -0.7, -0.5,在这里 0.7 为第一次计算的初值,-0.5 与最终结果相加是为了改变输出结果的区间,通过它将 Fcn 输出的结果变换到  $[-1, 1]$ ,以便于通过 Sign 模块将结果变换到  $[0, 1]$  区间。

Fcn 模块是计算混沌扩频序列的关键部分,该模块需要自己定义和设置所需要的计算模型,由于混沌序列产生模块的计算基于 Logistic 映射动力方程,因此需将映射动力方程的数学计算表达式定义到模块中,通过它得到 Logistic 混沌序列。

### 4 结果与分析

本文进行的所有仿真,都是在处理器为 Inter(R) Celeron (R)M 1.6GHZ 的计算机环境下,用 MATLAB6.5 的 Simulink 模块框图模拟实现的。主要对直接扩频通信系统的波形、系统误码率进行了分析。

通过仿真实现了直接扩频通信系统中各主要环节的波形,包括:初始的二值序列波形、Logistic 二值混沌序列波形扩频后的信号波形以及相应的解调后的波形,图 4 至图 8 是 Simulink 仿真波形图。

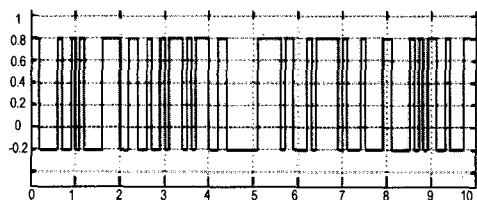


图 4 发送初始的二值序列波形

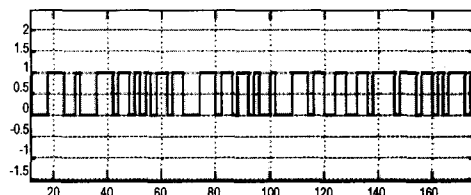


图 5 Logistic 混沌序列的单极性波形

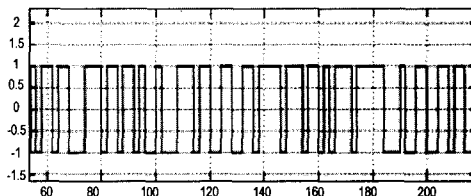


图 6 Logistic 混沌序列的双极性波形

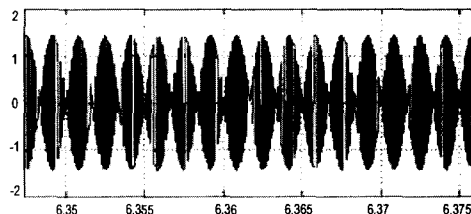


图 7 扩频后的信号波形

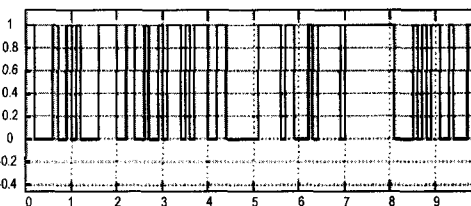


图 8 解调后的信号波形

从仿真框图组成可以看出,信号在加性高斯白噪声无线信道中传输时,会受到严重的衰减和失真,如果用普通的调制方式,在接收端很难准确地恢复原始信息。通过仿真分析,系统的误码率达到 0.9%,即在平均传输 1000 个码字,出现错误码字为 9 个,在这种误码率的条件下,无论从理论上还是从实践上都能较理想地传输信号和恢复信号。

对波形 4 和 8 进行对比分析,原始信号的波形和在接收端解扩、解调后的信号波形较为一致,不同的是接收端的信号和原始信号相比有一定的时间延迟且有一定的误码。因此从误码率和信号波形两个方面都可以验证利用扩频技术是一种较为优良、快速、可靠的通信传输手段。

本文所设计的仿真框图,具有良好的性能和可视化的优点,可以直观分析出基于混沌序列的扩频通信系统的工作机理。下一步可以研究具有自适应特性的、对调制方式、载波数、扩频码的参数可以适时更改的、更加智能化和实用化的混沌序列扩频通信系统。

### 参考文献

- [1] 孟宪艳. 无线扩频通信技术[J]. 有线电视技术, 2007, 14(11): 66-68

(下转第 111 页)

器的广播域范围;另一部分就是在三层交换机上进行安全策略的配置,这样可以大大提升交换机的抗攻击能力,从而提高 IP SAN 整体的抗攻击能力。

### 3 性能测试和分析

三层交换机都可以很好地支持 IP SAN 抗攻击部署模型采用的安全策略,在实际的使用环境中,可以证明那些安全策略对于提高交换机的抗攻击能力是很有效的。下面的测试,主要是验证采用路由技术进行数据转发的性能,从而验证这种模型的在实际应用中的可行性。

测试主要对带宽进行分析。带宽主要是反映存储系统的最大传输率,这是这次测试的重点。实验中通过对两种模型的带宽进行测试,考察 IP SAN 抗攻击模型的数据转发性能。

#### 3.1 实验环境

实验拓扑结构如图 3 所示。若对 IP SAN 实际部署模型的数据转发性能进行测试,则直接用交换机将 IP SAN 存储设备和应用服务器相连,直接用二层交换技术对数据进行转发。若对 IP SAN 抗攻击模型的数据转发性能进行测试,则实验中将 IP SAN 存储器划分至 Vlan2,分别将服务器划分至 Vlan3,Vlan4,Vlan5 中。这样将各个应用服务器和 IP SAN 存储器划分在不同的 Vlan 之中,在三层交换机上通过路由协议对数据进行转发。

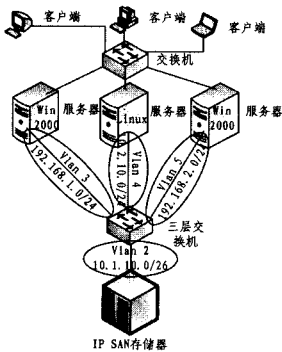


图 3 实验拓扑结构图

在实验中用到 3 台服务器,要求配置千兆网卡;锐捷 5750 以太网交换机 1 台;6 类网线 4 根;锐捷 RG-iS2000 存储 1 台。3 台服务器、锐捷 RG-iS2000 和锐捷 5750 以太网交换机都是以千兆链路相连。在 2 台服务器上运行 windows server2003 操作系统,并在服务器上安装 iSCSI 协议软件。在服务器上用 IOMeter2003 软件对存储空间进行连续读写,连续测试 1 小时以上。

### 3.2 实验结论和分析

图 4 是两种模型中数据块大小与带宽的关系曲线图。在数据块小的时候,IP SAN 抗攻击部署模型的数据转发能力比 IP SAN 实际部署模型的数据转发能力要弱,但是随着数据块的增大,这两种模型的数据转发能力逐渐接近。在实验中,选择具有良好转发性能的交换机将在很大程度上提高 IP SAN 抗攻击部署模型的数据转发性能。

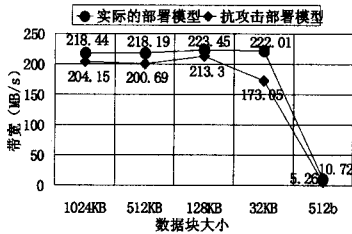


图 4 两种模型带宽比较

通过这个实验可以证明,IP SAN 抗攻击部署模型的最大带宽和 IP SAN 实际部署模型的最大带宽相差不大,IP SAN 抗攻击模型在实际部署中是具有可行性的。

**结束语** 综上所述,本文针对目前 IP SAN 实际部署中二层交换机抗攻击能力差的缺点,提出了 IP SAN 抗攻击部署模型。IP SAN 抗攻击部署模型的设计思想是采用路由技术将应用服务器所在的广播域隔离,缩小其广播域的范围,之后通过配置相应的安全策略,提高交换机的抗攻击能力,从而提高 IP SAN 整体的抗攻击能力。最后经过实际测试,证明了 IP SAN 抗攻击部署模型的性能,指出可以将这种模型应用于实际的 IP SAN 构架之中。

### 参考文献

[1] 白广思. FC SAN 和 IP SAN 构架比较新论. 情报科学, 2007, 25 (9): 1369-1372, 1377

[2] 叶宾, 须文波. IP2SAN 环境下 RA ID 远程管理系统设计与实现. 微型计算机应用, 2007, 28(7): 747-750

[3] 高增荣. 存储区域网络 IP SAN 与 FC SAN 技术. 甘肃科技纵横, 2007, 35(6): 16, 145

[4] 谢长生, 罗益辉. IP-SAN 的研究与设计. 小型微型计算机系统, 2005(06): 912-915

[5] 王佳, 李志蜀. 基于 ARP 协议的攻击原理分析. 微电子学与计算机, 2004, 21(4): 10-12

[6] Forouzan, Behrouz A. TCP / IP Protocol Suite. 2nd. United States; McGraw-Hill, 2003

(上接第 108 页)

[2] 赵耿, 方锦清. 现代信息安全与混沌保密通信应用研究的进展[J]. 物理学进展, 2003, 23(2): 212-230

[3] 杜月林, 陆婷. 混沌扩频序列在 CDMA 通信系统中的应用[J]. 国外电子测量技术, 2006, 25(7): 69-72

[4] 易雄书, 崔华, 余少波, 等. 扩频通信系统中基本扩频序列性能分析与设计[J]. 计算机仿真, 2008, 25(6): 134-137

[5] 戴志诚, 汪秉文. 基于混沌同步的保密通信[J]. 系统工程与电子技术, 2007, 29(5): 699-702

[6] Fang Jin-qing, Ali M K. Control and Synchronization of Spatio-temporal chaos//Chen G R. Controlling chaos and bifurcation in engineering system. USA; CRC Press, 1999: 104-127

[7] 刘嘉辉, 颜景斌, 宋大华. 基于混沌的网络通信数据加密方法[J]. 哈尔滨理工大学学报, 2007, 12(1): 32-35