一种基于混沌调制的保密通信方法

李建芬，李 农
(空军工程大学 工程学院，陕西 西安 710038)

摘 要：提出一种适合较大动态范围信息信号的混沌调制通讯方法，由于该方法允许较大幅度的信息信号，从而提高了通信的安全性。在接收端，用一个由自适应线性神经元(Adaline)构成的控制器来维持收发系统的混沌同步，并通过检测 Adaline 权值的变化规律恢复出信息信号。以蔡氏电路为例进行了数值模拟，结果表明该方法是可行的。

关键词：混沌调制；保密通信；自适应线性神经元；蔡氏电路
中图分类号：TP273；TN918　　**文献标识码**：A　　**文章编号**：1009－3516(2002)01－0052－04

近年来，混沌同步及其在保密通信中的应用研究得到了广泛的关注[1-2]。人们相继提出了混沌同步系统传输信息的各种方法，几乎所有方法的基本思想是：想办法将信息信号混在混沌系统或混沌信号中，然后设法在接收端将信息信号从混合信号中检测和恢复出来。但是这些方法对信息信号的动态变化范围有较严格的限制，如混沌掩盖法要求信息信号的幅值比混沌信号至少低 30 dB，否则，将使系统不易达到同步，由此使通信的安全性降低。其一，破译者接收到加密信号后，可通过神经网络或回归方法把混沌信号的系统所遵守的方程近似地重构出来，因而有可能进行非线性噪声减缩加以破译。其二是目前所用的混沌系统一般还是只有一个正指数的弱混沌系统，它们在适当的回归映象上一般表现为曲线或分段的曲线，这时加入小的调制信号只不过在曲线附近出现小的毛刺，容易识别[3]。

1 自适应线性神经元(Adaline)

Adaline[4]是在 1961 年由斯坦福大学教授 Windrow 提出的，它是一个自适应可调的网络，其原理如图 1 所示。如在第 k 时刻，有向量 $\boldsymbol{x}_k$ 输入，权向量为 $\boldsymbol{w}_k$，此时有模拟输出 y_k，$y_k = \boldsymbol{w}_k^{\mathrm{T}}\boldsymbol{x}_K$ 及二进制输出 q_k。y_k 与要求的理想响应的差值，通过 LMS 算法，修改 $\boldsymbol{w}_k$ 为 $\boldsymbol{w}_{k+1}$，从而减小了 y_k 与理想响应的误差。这个单元的输入与输出关系满足

$$y_k = \sum_{i=1}^{n} \boldsymbol{w}_{ik}^{\mathrm{T}} x_{ik} - \theta_k$$

$$q_k = \mathrm{sgn}(y_k)$$

$x_k, \boldsymbol{w}_k \in \boldsymbol{R}^n$，$\theta(t)$ 为阈值。图 1 所示为一个多输入单输出网络，它的输出分为模拟和数字两个部分，本文提出的方法利用其模拟输出，该输出是作为误差调节之用，对单个 Adaline，其误差为模拟输出和要求响应输出之差，也为模拟量。用 LMS 算法能保证这种网络在自适应学习时的收敛性。

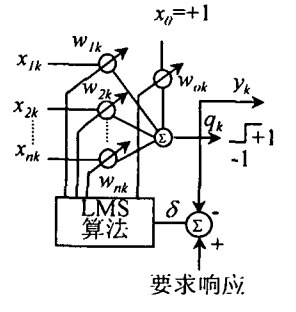


图1 Adaline 原理图

收稿日期：2001－04－04
作者简介：李建芬(1960－)，女，湖南长沙人，讲师，主要从事非线性电路理论、混沌及其应用研究.

2　蔡氏电路及其同步通信方案

2.1　蔡氏电路

下面以蔡氏电路为例说明本文提出的方法,该电路由一个线性电感 L,一个线性电阻 R,两个线性电容 C_1 和 C_2 以及一个非线性电阻—蔡氏二极管 N_R 组成。其电路如图 2。它的数学描述为

$$\begin{aligned}\frac{du_{C1}}{dt}&=\frac{1}{C_1}[G(u_{C2}-u_{C1})-f(u_{C1})]\\ \frac{du_{C2}}{dt}&=\frac{1}{C_2}[G(u_{C1}-u_{C2})+i_1]\\ \frac{di_1}{dt}&=\frac{1}{L}u_{C2}\end{aligned}\tag{1}$$

其中 $f(\cdot)$ 为非线性电阻 N_R 的伏安特性,曲线见图 3。

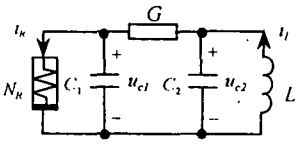


图 2　chua s 电路

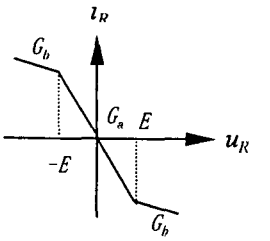


图 3　N_R 的特性曲线

2.2　蔡氏电路的同步通信方案

发射系统的状态方程如式(1),接收系统的状态方程为

$$\left\{\begin{aligned}\frac{du_{C1}}{dt}&=\frac{1}{C_1}[G(u_{C2}-u_{C1})-f(u_{C1})+k(s(t)u_{C1}-w(t)u_{C1})]\\ \frac{du_{C2}}{dt}&=\frac{1}{C_2}[G(u_{C1}-u_{C2})+i_t]\\ \frac{di_1'}{dt}&=-\frac{1}{L}u_{C2}'\end{aligned}\right\}\tag{2}$$

令

$$y=s(t)u_{C1}$$

$$y'=w(t)u_{C1}$$

其中 $s(t)$ 为信息信号,y 为一个单输入单输出 Adaline 神经元的输出;输入为 u_{C1};y 是其要求响应,它是发射系统发出的信号,信息信号 $s(t)$ 通过调制混沌信号 u_{C1} 被隐藏在其中;此处,令阈值 $\theta(t)=0$,权值 $w(t)$ 的变化规律依据梯度下降法满足下面的微分方程

$$\dot{w}(t)=\mu u_{C1}(y-y')\tag{3}$$

式中,μ 为常数,调节步长由

$$y-y'=s(t)u_{C1}-w(t)u_{C1}=s(t)(u_{C1}-u_{C1}')+u_{C1}(s(t)-w(t))\tag{4}$$

设 $e(t)=[e_1,e_2,e_3,e_4]^T=[u_{C1}-u_{C1}',u_{C2}-u_{C2}',i_1-i_1',s(t)-w(t)]^T$

由式(1)~(4)得系统的误差方程为

$$\dot{e}(t)=\begin{bmatrix}-\frac{1}{C_1}(G+KS(t)) & \frac{G}{C_1} & 0 & -\frac{1}{C_1}ku_{C1}\\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} & 0\\ 0 & -\frac{1}{L} & 0 & 0\\ -\mu u_{C1} & 0 & 0 & -\mu(u_{C1}')^2\end{bmatrix}e+\begin{bmatrix}-\frac{1}{C_1}\\0\\0\\0\end{bmatrix}(f(u_{C1})-f(u_{C1}'))+\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\dot{s}(t)=$$

$$A_f e + B(f(u_{C1}) - f(u_{C1})) + C\dot{s}(t)$$

由于$f(*)$为分段线性连续函数,斜率分别为G_a和G_b,且$G_a < G_b < 0$,因此$G_a(u_{C1} - u_{C1}) \leqslant f(u_{C1}) \leqslant G_b(u_{C1} - u_C)$。设$f(u_{C1}) - f(u_{C1}) = \delta(t)(u_{C1} - u_{C1})$,(其中$\delta$为时变参数,且$G_a < \delta < G_b$),则

$$e(t) = \begin{bmatrix} -\frac{1}{C_1}(G + \delta + ks(t)) & \frac{G}{C_1} & 0 & -\frac{1}{C_1}ku_{C1} \\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} & 0 \\ 0 & -\frac{1}{L} & 0 & 0 \\ -\mu u_{C1} & 0 & 0 & -\mu(u'_{C1})^2 \end{bmatrix} e + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \dot{s}(t) = A_f(t)e + C\dot{s}(t) \tag{5}$$

式(5)是一个时变的非齐次线性方程组,因此它的解具有下面形式

$$e(t) = \phi(t)e(0) + \phi(t)\int_0^t \phi^{-1}(\tau)C(\tau)\dot{s}(\tau)\mathrm{d}\tau \tag{6}$$

式中$\phi(t)$是$A_f(t)$的基本矩阵。由式(6)看出,只要求出$\phi(t)$,$e(t)$总是可以计算出来的。但是,只有在少数情况下,$\phi(t)$可以由$A_f(t)$算出,故一般只能用数值解法来求解。通过数值计算,若k和μ选择适当,可以使$A_f(t)$在零点一致渐进稳定,这时同步误差$e(t)$为式(5)的第二项,减小$\dot{s}(t)$,即可减小$e(t)$,当$e(t)$小到允许的误差范围内时,就可以认为系统同步,$\dot{s}(t)$越小,同步误差就越小。Adaline 神经元可采用如图 4 所示电路实现。

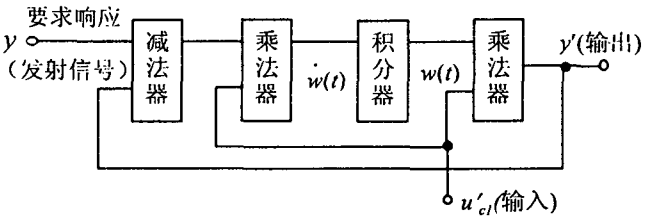
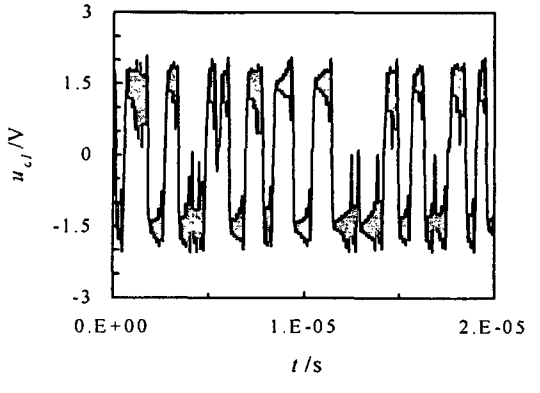


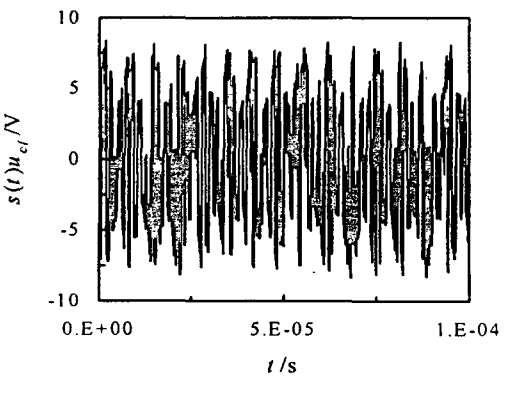
图 4 Adaline 电原理图

2.3 数值模拟结果

参数选$C_1 = 5.56$ pF, $C_2 = 50$ pF, $G = 0.70028$ ms, $L = 7.14$ μH, $G_a = -0.8$ ms, $G_b = -0.5$ ms 时,电路处于混沌状态,见图 5(a)。图 5(b)为经$s(t)$调制后的混沌信号。当$k > 1$,且$k/\mu \in [0.02, 1] \times 10^{-7}$,$A_f$一致渐进稳定,此时同步误差为零状态响应分量。由式(5)可知若要减小同步误差,须尽量减小$\dot{s}(t)$,即信息信号$s(t)$的变化速率。模拟结果见图 6,其中$\mu = 10$, $k = 10^{-9}$, $s(t) = 3 - \sin 2\pi ft$。图 6(a)和图 6(b)分别是f为 150 kHz;50 kHz 时,恢复的信息信号$s(t)$($s(t) = w(t)$)及其与原信号$s(t)$的误差。可见,$s(t)$的频率越小,误差也就越小,其幅值可与混沌信号相当,模拟结果与分析是相吻合的。



(a)



(b)

图 5 混沌信号u_{C1}时域波形和调制后的时域波形

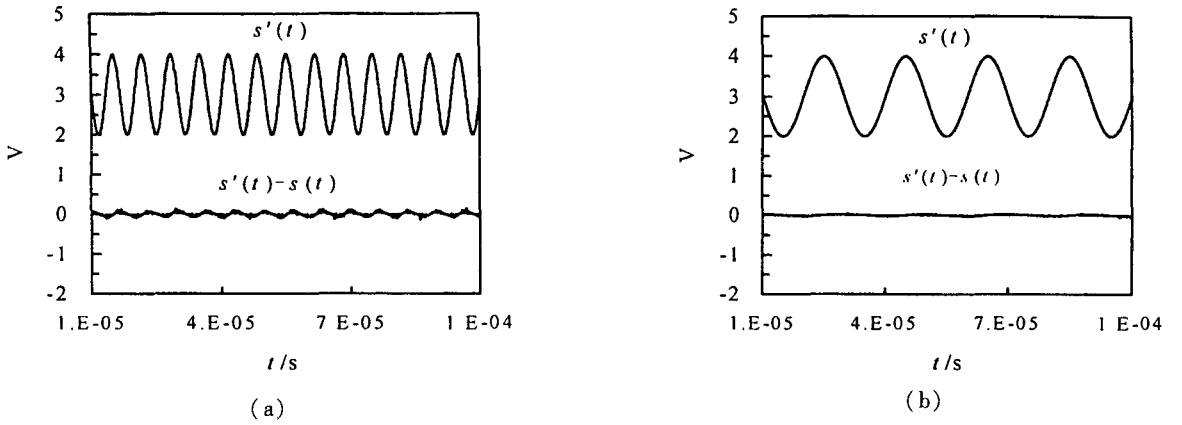


图 6　频率分别为 150 KHz 和 50 KHz 时恢复出的信号 $s'(t)$ 及其与原信号的误差 $s'(t)-s(t)$

3　结论

本文提出的混沌信号调制保密通信方法,由于采用了一个自适应线性神经元,使信息信号的动态变化范围可以较大甚至可与混沌信号相当,从而可提高保密通信的防破译能力。

参考文献:

[1] PECORA L M, CARROLL L T L. Synchronization in chaotic circuits[J]. Phys Rev Lett, 1990, 64(8): 821 - 824.
[2] PECORA L M, CARROLL L T L. Driving Systems with Chaotic Signals[J]. Phys Rev A, 1991, 44(4): 2374 - 2378.
[3] 倪皖荪,华一满,邓　浩,等. 混沌通讯[J]. 物理学进展,1996,16(3):645 - 656.
[4] 张立明. 人工神经网络的模型及其应用[M]. 上海:复旦大学出版社, 1993.

(编辑:姚树峰)

Secure Communications Method Based on Chaos Modulation

LI Jian - fen,　LI Nong
(The Engineering Institute, Air Force Engineering University, Xi'an 710038, China)

Abstract: Secure communications method for higher level of information signal based on chaotic modulation is proposed. In this method, because the level of information signal can be equivalent to the level of chaotic signal, the degree of security is high. At the receiving end, an Adaline maintains the chaotic synchronization of transmitting and receiving systems and simultaneously recovers information signal. Chua's circuits is considered as illustrative example to demonstrate the effectiveness of the proposed method.

Key words: chaotic modulation; secure communications; adaline; Chua's circuits