基于间歇耦合和广义混沌同步的数字信号传输方案 [1]

杨 涛 戴晓明 邵惠鹤

(上海交通大学自动化系 上海 200030)

摘 要 该文讨论了一种基于间歇耦合思想和广义混沌同步的保密通信方案. 在这种数字信号传输过程中, 每个信号周期被分为两部分 T_1, T_2 , 分别用于实现同步和信号提取, 分析了 T_1, T_2 与安全性能和信息解调精度的关系. 数值仿真表明效果良好.

关键词 混沌保密通信, 广义混沌同步, 间歇耦合

中图号 TN918

1 引 言

混沌系统因其在保密通信中的广阔应用前景而成为研究热点, 其关键是发送、接收系统的同步, 已经出现了各种实现混沌信号或混沌系统同步控制的机理与方法 [1] . 在混沌保密通信中, 主要问题有两个: 信息调制方式、安全性能。对于前者, 目前主要有混沌演码调制、参数调制、混沌编码调制、脉冲幅值、脉冲相位调制等 [2,3] ; 后者一直是一个热门话题, 众多学者从各个方面对之进行了探讨, 提出了多种解决方案, 但结果都不完美 [3] .

目前的各种混沌保密通信方案都是在发送、接收系统之间的完全精确同步基础上进行, 而这种同步只有在较理想的条件下才能实现, 这就限制了混沌保密通信在工程中的应用. 最近提出了一种称为广义同步的思想引起了广泛的关注 [4] , 但把广义同步用于混沌保密通信的研究较少, 文献 [5] 结合完全同步和广义同步对这个问题进行了探讨; 文献 [6] 在文献 [5] 的基础上提出了一种基于广义同步的通信方案, 但其需要两条信道, 这无疑增加了成本; 并且信道 2 在整个信号周期中都进行信号传输, 提高了拦截的可能性; 文献 [7] 提出一种基于间歇耦合思想的混沌通信方式; 文献 [8] 把间歇耦合思想和信息的参数调制策略和参数辨识技术相结合, 实现一种安全性能高的全双工通信方式. 本文利用间歇耦合思想, 只使用一条信道即可实现一种基于广义同步的数字信号传输方式, 并对安全性能进行了分析.

2 间歇耦合与广义同步结合的数字信号传输

本文给出一种基于广义同步的混沌通信方案. 对于混沌动力学系统 X, Y, 如果在相空间中存在区域: $\Xi = \{(X, Y) : \phi(X) = Y\}$, 且该区域至少具有一个 Milnor 吸引子, 则称 X, Y 为广义同步, 函数 ϕ 为广义同步函数 [4] . 可见广义同步比完全精确同步的要求有所降低。本文的这种基于广义同步的通信原理如图 1 所示. 在该系统中, 发送、接收端各由两个混沌系统构成: 系统 1, 3 ; 系统 2, 4 的结构完全一致. 信息传输的基本思想可以描述为: 在发送端, 根据传输信号类型 $(1, 0)$ 使系统 1, 2 以 ϕ_1, ϕ_2 为广义同步函数实现广义同步; 在接收端, 系统 3, 4 按 ϕ_1 实现广义同步。于是根据系统 2, 4 输出信号的差异即可实现信息恢复。具体地, 传输信号为 1 时, 通过耦合, 系统 1 和 3 之间实现精确同步, 系统 1 和 2, 系统 3 和 4 之间以 ϕ_1 实现广义同步, 于是系统 2,4 输出信号的差值趋于 0 ; 当传输信号为 0 时, 系统 1 和 2 以 ϕ_2, 系统 3 和 4 以 ϕ_1 实现广义同步; 则系统 2,4 输出信号的差值不等于 0 ; 即可实现信号的恢复。可见有如下几种信号需要传输: (1) 在发送、接收端内部, 系统 1, 2 之间和系统 3, 4 之间; (2) 在信道

[1] 2001-03-19 收到, 2001-10-24 定稿
国家 973 重点基础研究发展规划 G1998030415

中，保持系统 1 和 3 精确同步的耦合信号及系统 2 的输出用于比较目的的信号. 本文利用间歇耦合的思想，用一条信道进行分时传输两种信号，以实现数字信息的传输，提高安全性能.

2.1 时段 1(T_1)

该时段内传输两种信号：(1) 在发送、接收系统内部，目的是保证实现广义同步；(2) 在信道中，由系统 1 传输到系统 3，目的是为了实现两者的完全精确同步. 前者可以通过辅助系统法来分析 [9]，所以只考虑后者. 设混沌系统 1(X_t) 描述为

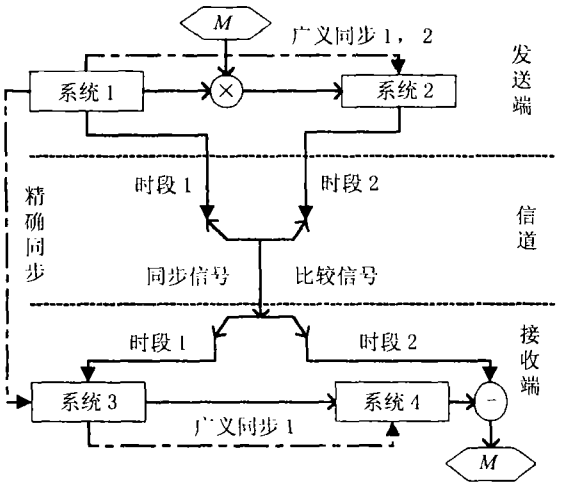


图 1　基于广义同步的混沌通信原理图

$$\dot{X}_t = f(X_t, p), \qquad y_t = c^T X_t \tag{1}$$

$X_t \in R^n$, $p \in R^M$ 为系统参数，y_t 为经信道传输到系统 3 的驱动信号以实现同步. 为了讨论的方便，这里使用误差反馈同步策略，于是系统 3(X_r) 可以表示为

$$\dot{X}_r = f(X_r, p') + s(t)K(\cdot)(y_t - y_r), \qquad y_r = c^T X_r \tag{2}$$

其中 p' 表示接收系统参数，假设 $p = p' \cdot s(t)$ 为切换信号：时段 1, $s(t) = 1$; 时段 2, $s(t) = 0$. 选择反馈增益 $K(\cdot)$, 以保证 X_t, X_r 按指数速度实现同步，即 $\exists M > 0, 0 < \alpha < 1, \forall t_0, w(t_0) \in R^n$, 不等式：

$$\|w(t)\| \le Me^{-\alpha(t-t_0)}\|w(t_0)\|, \qquad t \ge t_0 \tag{3}$$

成立，其中 $w(t)$ 为同步误差 $(X_t - X_r)$. 满足条件的 $K(\cdot)$ 选择方式很多，在已经报道同步策略中，大多能实现指数速度同步的要求 [5] . 这表明 X_t, X_r 之间的同步将在有限时段 T_1 内达到. 为了对这个问题进行说明，把 (1), (2) 式改写为

$$\left.\begin{aligned} \dot{X}_t &= A(p)X_t + \Theta(X_t, p) \\ \dot{X}_r &= A(p)X_r + \Theta(X_r, p) + K(\cdot)(y_t - y_r) \end{aligned}\right\} \tag{4}$$

其中 $s(t) = 1$, $A \in R^{n\times n}$, $\Theta(\cdot) : R^n \to R^n$ 为光滑 Lipschtiz 函数，大多数混沌系统可以描述为这种形式，于是同步误差系统描述为

$$\dot{E} = (A(p) - Kc^T)E + [\Theta(X_t, p) - \Theta(X_r, p)] \tag{5}$$

对于固定的 p, 如果 $(A(p), c)$ 为能观测 (可以通过选择 c 来实现)，则存在增益矩阵 $K \in R^n$, 使矩阵 $A_c = (A(p) - Kc^T)$ 稳定 (特征值为负)，且由于 $\Theta(\cdot)$ 的 Lipschtiz 特性，则在区域 $\Omega \subset R^n \times R^n$ 中存在 $k > 0$, 不等式 $\|\Theta(X_t, p) - \Theta(X_r, p)\| \le k(X_t - X_r)$ 的解有界. 如果 $k > 0$,

但足够小，则 E 以指数速度衰减；反之，即使 $k>0$，但不是足够小，在 A, $\Theta(\cdot)$ 的某种特殊形式下，通过选择 $K\in R^n$ 而使 (3) 式成立 [7]。

时段 1 中的另一个任务是实现发送、接收系统内部的广义同步，这是时段 2 中信息恢复的基础，由于实现该任务的信号交换是在发送、接收两端内部进行，故对安全性能不构成影响。设混沌系统 $2(Y_t)$ 、 $4(Y_r)$ 由以下方程来描述

$$\left.\begin{aligned}\dot{Y}_t &= g(X_t,Y_t,h,m(t),q)\\ \dot{Y}_r &= g(X_r,Y_r,h',q')\end{aligned}\right\} \tag{6}$$

$m(t)$ 为要传输的数字信号， h,h' 为 X_t,Y_t 及 X_r,Y_r 之间的耦合以实现广义同步， h,h' 的类型可以不相同，这增加了操作的灵活性，但是以增加设备为代价的，这个问题将在后面阐述。有关 h,h' 的选择可以通过辅助系统法来解决 [4]，这里不再详述。值得注意的是， X_t,Y_t 在 h, $m(t)$ 的作用下实现 ϕ_1,ϕ_2 的广义同步； X_r,Y_r 在 h' 作用下实现 ϕ_1 的广义同步，为了提高安全性能， ϕ_1,ϕ_2 之间的差异不能太大，否则根据时段 2 中信道传输信号的变化情况即可能对传输信息进行拦截。

2.2 时段 $2(T_2)$

X_t 停止向 X_r 传输信号，而改由 Y_t 经信道向 Y_t 传输信号 $\varphi(Y_t)$，以便实现信号恢复：

$$e=\|\varphi(Y_t)-\varphi(Y_r)\|=\begin{cases}0, & m(t)=1\\ \neq 0, & m(t)=0\end{cases} \tag{7}$$

此时信道中的信号只作为参考信号传输到 Y_r，并根据误差信号 e 对传输信息进行提取。由于此时 X_t 和 X_r 之间无直接的信号交换，故两者的完全精确同步将随着时间的推移而恶化，因此 T_2 的长短对误码率的影响很大，下面将作进一步的分析。在实际应用中， X_T,X_R 不可能达到真正的完全精确同步，因此 (5) 式修正为如下更适用的形式：

$$e=\|\varphi(Y_t)-\varphi(Y_r)\|=\begin{cases}\sigma_1, & m(t)=1\\ \sigma_2, & m(t)=0\end{cases} \tag{8}$$

$0<\sigma_1<<\sigma_2$，其大小与 ϕ_1,ϕ_2 的差异有关。同时，可以任意选择 $\varphi(\cdot)$ 以提高安全性能。

2.3 对通信过程的影响

从上述可知， T_1,T_2 的长短对信息的安全性能和信息恢复质量的影响很大。在 T_1 时段内，主要是要实现 X_t,X_r 的快速精确同步，而有关发送、接收系统内部的广义同步，可以通过合理的选择 h,h' 在 T_1 时段内到达 (可以通过辅助系统法来讨论)。从理论上说：当 $T_1\to\infty$ 时， X_t,X_r 的精确同步总可以实现。但随着 T_1 的延长，在信道中暴露的有关 X_t 结构信息就越多，于是拦截者就完全有可能通过信道中的信号，按照相空间重构理论获得有关 X_t 吸引子的信息 (设该时段的最小值为 τ_1，其具体值与混沌系统的结构和维数有关)，则可能进一步获取 Y_t 的信息，实现信息拦截的目的，因此 T_1 要满足这两种要求。对于 T_2 而言，随着 T_2 的延长， X_t,X_r 的同步情况恶化， Y_t,Y_r 信号之间的误差增大，按 (6) 式进行信号提取时的误码率增大，故必须合理选择 T_2 以保证 X_t,X_r 在一定精度上维持同步；同样 T_2 对安全性能也很重要。根据以上讨论，有下面定理。

定理 对于本文的通信过程，在一定条件下，存在 T_1,T_2 使安全性和信息解调的精度都能得到保证。

证明　首先为了安全性能，必须有

$$0 < T_1 \le \tau_1,\ 0 < T_2 \le \tau_2 \tag{9}$$

$\tau_{1,2}$ 的估算方法在文献 [7] 中有描述。对于混沌系统 X_t, X_r, 设 $f(\cdot)$ 具有 Lipschitz 特性，其初始条件为 $\|w(0)\| \le r$, $r \ge 0$ 。设第 j 位信息传输过程为 T_1^j, T_2^j, 即

$$T_1^j = (j-1)(T_1+T_2),\quad T_2^j = jT_1 + (j-1)T_2,\qquad j = 1,2,\cdots \tag{10}$$

由 (3) 式有

$$\|w(t)\| \le Me^{-\alpha(t-T_1^j)} \cdot \|e(T_1^j)\|,\qquad T_1^j < t < T_2^j \tag{11}$$

于是

$$w(t) = w(T_1^j) + \int_{T_1^j}^{t} [f(X_t(\tau),p) - f(X_r(\tau),p)]\mathrm{d}\tau,\qquad T_2^j \le t \le T_1^{j+1} \tag{12}$$

根据 Lipschitz 假设和 Bellman-Gronwall 定理，有

$$\|w(t)\| = e^{k_u(t-T)}\|w(T_1^j)\| \tag{13}$$

式中 k_u 为 Lipschitz 常数。由 (9), (11) 式有

$$\|w(t)\| = Me^{(k_uT_2-\alpha T_1)}\|w(T_1^j)\| \le (Me^{(k_uT_2-\alpha T_1)})^j\|w(0)\|,\qquad T_2^j \le t < T_1^{j+1} \tag{14}$$

根据上述讨论，为了降低误码率，T_2 时段内必须保证 X_t, X_r 在一定精度 ε 上的同步：$\|w(t)\| \le \varepsilon$ 。于是有

$$\ln M + k_uT_2 - \alpha T_1 \le \frac{1}{j}\ln\frac{\varepsilon}{r},\qquad j = 1,2,\cdots \tag{15}$$

在满足 (9) 式，(15) 式时，安全性能和精度均能得到保证，一种方便的选择方法为

$$0 > T_1 \le \tau_1,\qquad 0 < T_2 \le \tau_2,\qquad \left.\begin{array}{l} \ln\frac{\varepsilon}{r} < 0,\ \ln M + k_uT_2 - \alpha T_1 \le \ln\frac{\varepsilon}{r} \\ \ln\frac{\varepsilon}{r} \ge 0,\ \ln M + k_uT_2 - \alpha T_1 \le 0 \end{array}\right\} \tag{16}$$

一般是在选择较小的 T_2 后，再在满足 (16) 的条件下选择 T_1 即可。

讨论　从上面的分析可知，这种通信方案的保密性能体现在以下几方面：(1) 以间歇耦合思想为基础，通过合理选择 T_1, T_2 满足 (16) 式，选择 X_t, X_r 之间的耦合形式，使得 T_1 时段内信道中的信号成分复杂，故很难从传输信号中重构出 X_t, Y_t 吸引子结构；(2) 以广义同步为基础：由于信息的恢复是根据误差信号幅值的相对大小进行的，而不像传统的从误差信号幅值中提取有用信号，故 T_2 可以很短，因此拦截者最有可能是在 T_1 时段内重构出 X_t 的吸引子结构，如果对 ϕ_1, ϕ_2 无如何先验知识，则很难从 X_t 吸引子结构信息中获得 Y_t 的任何信息；(3) 选择 $\varphi(\cdot)$ 的形式使之是 Y_t 各个分量的函数，这样即使 T_2 较长也很难从信号中提取 Y_t 的吸引子信息；(4) 合理选择 h, h' 参数使 ϕ_1, ϕ_2 相差不大，则在每个信号周期内信道中的信号相似，因此很难从信号的变化中提取有用信息。

2.4 仿真结果

为了验证上述通信思想，以 Rössler 和 Lorenz 系统为例进行仿真，效果良好。

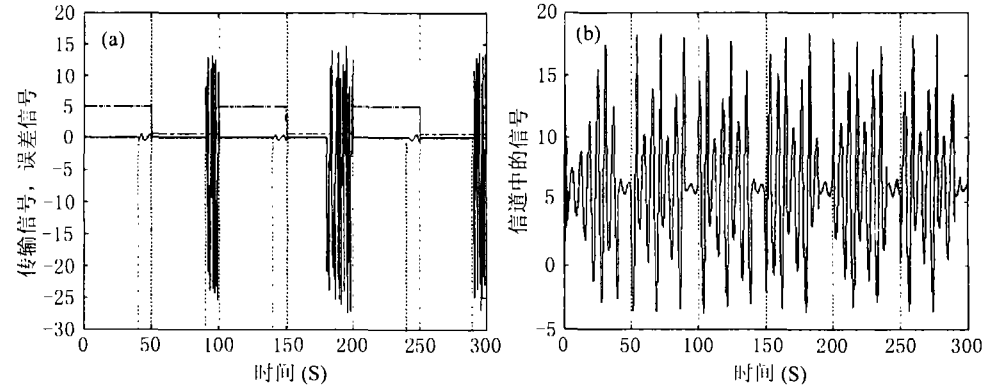
发送端 系统 $1(X_t)$ 、 $2(Y_t)$ 描述为

$$\left.\begin{aligned}&\dot{x}_{t1}=-(x_{t2}-x_{t3}),\quad \dot{x}_{t2}=x_{t1}+\alpha x_{t2},\quad \dot{x}_{t3}=\beta+x_{t3}(x_{t1}-\mu)\\&\dot{y}_{t1}=s(y_{t2}-y_{t1})-h(y_{t1}-m(t)x_{t1}),\quad \dot{y}_{t2}=-y_{t1}y_{t3}+ry_{t1}-y_{t2},\quad \dot{y}_{t3}=y_{t1}y_{t2}-by_{t3}\end{aligned}\right\}\tag{17}$$

接收端 系统 $1(X_r)$ 、 $2(Y_r)$ 描述为:

$$\left.\begin{aligned}&\dot{x}_{r1}=-(x_{r2}-x_{r3})+k(x_{t1}-x_{r1}),\quad \dot{x}_{r2}=x_{r1}+\alpha x_{r2},\quad \dot{x}_{r3}=\beta+x_{r3}(x_{r1}-\mu)\\&\dot{y}_{r1}=s(y_{r2}-y_{r1})-h'(y_{r1}-x_{r1})),\quad \dot{y}_{r2}=-y_{r1}y_{r3}+ry_{r1}-y_{r2},\quad \dot{y}_{r3}=y_{r1}y_{r2}-by_{r3}\end{aligned}\right\}\tag{18}$$

参数取为: $\alpha=0,2$, $\beta=0.2$, $\mu=5.7$; $s=10$, $r=54$, $b=8/3$ 。误差反馈系数 k 是为了实现指数同步, h, h' 是为了实现广义同步, 它们可以相同, 也可以不同, 当传输信号为 1 时, $m(t)=1$; 传输信号为 0 时, $m(t)=0.95$, 仿真结果如图 2 所示。



(a) 传输信息 (点线) 与误差信号 (实线) (b) 信道中的信号

图 2 仿真结果

从仿真结果看出, 由误差信号按 (6) 式进行判定, 能准确提取有用信号; (b) 表示了信道中的传输信号, 由于传输 1, 0 时 $m(t)$ 差别不大, 故信道中的各个传输周期间的信号相似, 提高了安全性能。

3 另一种通信结构

上述的通信方案由 4 个混沌系统构成, 其目的在于提高操作的灵活性, 即 X_t, Y_t 和 X_r, Y_r 之间信息交换的结构可以不同, 只要保证实现预定种类的广义同步即可, 这是以 X_t, X_r 在足够精度范围内的同步为基础的。因此在整个系统中, X_r 是可以去除, 而直接由 X_t 向 Y_r 传输信号以保证预定广义同步的实现 (如图 1 所示), 但 X_t 向 Y_t, Y_r 传输信号的结构应当相同, 以保证信息解调的准确性 (此时 Y_t, Y_r 完全等价于辅助系统法中的两个系统) 。同样以 (2.4) 节中的系统为例进行仿真, 结果与图 2 相似。

4 结 论

本文讨论了一种基于间歇耦合和广义混沌同步的保密通信方案。在这种数字信号传输过程中, 每个信号周期被分为两部分, 分别实现同步和信号提取。通过变换 $\varphi(\cdot)$ 的形式, 使信道中

的信号形式复杂，并且 $\varphi(\cdot)$ 可以不直接包括有用信号的信息，合理选择 T_1, T_2, 使得很难从信道中的信号获得传输信号 $r(t)$ 的信息，安全性能很高；信号恢复是基于误差信号幅值的相对大小进行的，而不像 CM(Chaotic Masking)[3] 等常用的混沌通信方案那样直接从误差信号幅值中提取传输信息，误码率降低；易于实现：广义同步的要求比精确同步宽松。本文的要求是 X_t, X_r 及 Y_t, Y_r 的结构和参数必须一致，在实际工程中很难满足这个要求，这可以通过参数的自适应调整技术来补偿 [8]，对于噪声的影响，文献 [9] 提供了一种利用可测同步误差进行补偿的算法。不过广义同步在通信中的应用还有待进一步的研究。

参 考 文 献

[1] G. Chen, Control and synchronization of chaotic systems(abibilography).(ECE Department, University of Houston, Houston. K. M. Cuomo, A. V. Oppenheim, Phys. Rev. Lett., 1993, 65(1), 71–74.

[2] N. F. Rul'kov, A. R. Volkovskii, In Chaos in Communication, ed. L. M. Pecora, (SPIE-the International Society for Optical Engineering, Bellingham, Washington, 98227-0010, USA, 1993, 132.

[3] G. Perez, H. A. Cerdeira, Extracting message masked by chaos, Phys. Rev. Lett., 1995, 74(11), 1970–1793.

[4] H. D. I. Abarbanel, N. F. Rulkov, *et al.*, Generalized synchronization of chaos: the auxiliary system approach, Phys Rev E., 1996, 53(5), 4528–4535.

[5] Lee Chungyong Lee, B. Douglas, *et al.*, A secure communication system using chaotic switching, Int. J. of Bifurcation and Chaos in Applied Sci. and Eng., 1997, 7(6), 1383–1394.

[6] J. R. Terry, D. Gegory, *et al.*, Chaotic communication using generalized synchronization, Chaos, Solition and Fractals, 2001, 12(1), 145–152.

[7] ÖMer Morgiil, Synchronization and chaotic masking scheme based on occasional coupling, Phys Rev E., 2000, 62(3), 3543–3551.

[8] 杨涛，邵惠鹤，基于间歇耦合思想的全双工混沌保密通信方案，高技术通讯，2002, 2(2), 26–29.

[9] Naresh Sharma, Edward OTT, Exploting synchronization to combat channel distortions in communication with chaotic systems, Int. J. of Bifurcation and Chaos in Applied Sci. and Eng., 2000, 10(4), 777–785.

DIGITAL COMMUNICATION BASED ON OCCASIONAL COUPLING AND GENERALIZED CHAOTIC SYNCHRONIZATION

Yang Tao　　Dai Xiaoming　　Shao Huihe

(*Department of Automation, Shanghai Jiaotong University, Shanghai* 200030, *China*)

Abstract　In this paper, a way of secure digital communication based on occasional coupling and generalized chaotic synchronization is proposed. The period of every signal bit is divided into two parts: T_1 and T_2. During T_1, generalized chaotic synchronization is fulfilled, and in T_2, the transmitted signal is extracted by a special way. The relation between T_1, T_2 and the security as well as the performance of signal extraction are also analyzed. Numerical simulations are performed to show the effectiveness of this communication scheme.

Key words　Chaotic secure communication, Generalized chaotic synchronization, Occasional coupling

杨　涛：　男，1972 年生，博士生，目前研究领域为智能控制、混沌控制、混沌同步及其在保密通讯中的应用.

戴晓明：　男，1973 年生，博士生，目前研究领域为智能控制，优化控制等.

邵惠鹤：　男，1963 年生，教授，博士生导师，研究方向为智能控制，工业过程控制等.