第19卷 第1期 郑州工业大学学报 Vol.19 No.1
1998年 3 月 Journal of Zhengzhou University of Technology Mar. 1998

混沌在保密通信中的应用研究*

李春生 高金峰 王俊昆鸟

(郑州工业大学计自系)

摘 要 混沌在保密通信中的应用是混沌理论应用方面的一个研究方向。该方向的研究近几年发展较快,本文结合我们的研究成果对该研究方向的现状作一简单综述。

关键词 混沌;保密通信;同步

中图分类号 TN918

混沌是确定性系统产生的不确定信号,它类似噪声,具有不可预测性[1,2]。利用混沌信号类似噪声的宽频谱特性来"包装"信息信号,即将混沌信号作为载波来传输信息信号,这就是所谓的混沌保密通信[3,4]。更具体地讲混沌信号用于保密通信是由于信号所具有的宽频带、类噪声及难以通过时域和常用的频域处理来预测和分离,它自然被用作信息的载体,即作为调制载波以实现加密。混沌用于保密通信是随着对混沌理论的深入研究及同步混沌理论的建立而发展起来的,也是混沌应用研究的一个重要方面。

1 混沌同步理论的发展过程

混沌用于保密通信的关键是:实现发受混沌系统之间的同步。

同步在通信中具有非常重要的意义,它是决定通信系统通信能否实现的一个重要因素。应用于通信的同步可以分为[5]:1.载波同步;2.位同步;3.帧同步;4.网同步等几个大类。通俗地说,"同步"指的是"动态系统中的步调一致的现象"。传统的载波同步是指同步系统接收端产生一个与发送端发送的载波同频、同相的相干载波。

1983年,Tang等人[3]提出混沌电路可以由一个输入信号同步地驱动。这似乎是很奇怪的,因为混沌信号是确定性系统产生的不确定的信号,是类随机的,似乎是不可能同步的。但随之而来的一系列关于混沌同步的报道却揭示出:混沌信号的同步不仅是可以实现的,而且是应用于保密通信的有效工具。1990年,Pecora和Carroll[6]提出自治系统的自同步的混沌同步方案,它能有效地实现自治混沌系统的同步。他们指出:用一个激励信号可以使另外一个信号表现为混沌,但它们却是同步的。这就给混沌实现信息的调制与解调提供了可能。1991年,Endo和Chua[7]报道了锁相环电路的同步现象。同年,Pecora和Carroll[8]报道了用Newcomb等人研究的三阶自治混沌电路实现的同步。1992年,Kocarev等人[9]证实了蔡氏

*河南省自然科学基金资助项目(964060200)
收稿日期:1997—08—29
第一作者 男 1968年生 硕士学位 助工

电路的同步现象。1992 年和 1993 年，Cuomo 和 Oppenheim[10,11,12,]报道了基于 Lorenz 系统的同步混沌系统实现方案。

1992 年以后，当人们掌握了几种混沌同步理论和手段后，便将混沌用于保密通信并提出一些初步的实现方案。

同步方案一：基于系统间连续反馈的控制同步。它包含连续信号误差反馈系统，其中系统间反馈比例因子的值是关键。该比例因子无法从理论上推得，而只有更多地依赖于经验。这种方法很少有报道，仅作为一种思考方案。

同步方案二：1995 年，T·C·Newell[13]等在 Edward Ott 等 OGY 混沌控制论[4]的基础上提出，通过控制非稳定周期轨道，对系统的控制参数进行控制，以使其轨道同步于混沌吸引子的轨道，他们用比例反馈控制法，控制两个混沌振子来实现同步。

以上两种方案均是基于控制理论的。利用控制理论来实现同步，是复杂的。

第三种方案称为 Pecora－Carroll 同步方案[4,6,8,14]。基于该原理可以简单可靠地实现三阶自治混沌系统的同步：如果将系统分为激励部分 D 即“发端”和响应部分 R 即“受端”，当受端子电路所有条件 Lyapunov 指数均负时，受端子电路将同步于发端电路的信号。这是自同步方案。该方案的同步系统包括：(1)第一个混沌电路，称为发端系统、发射机或发射系统(2)第二个混沌电路，称为受端系统、接收机或接收系统。发端系统发射一些状态矢量(激励信号)到受端系统，使两个电路产生的信号同步。Pecora－Carroll 同步方案在电路、信号与系统领域引起了很大的兴趣。

2 混沌同步系统在保密通信中的应用情况

同步混沌系统能够实现混沌保密通信。

1992 年，Oppenheim 等[12]报道了“混沌开关”和“混沌加密、调制”的实际应用。特别地，他们以实例说明了怎样把混沌同步的概念应用于信息加密，怎样把信息加到混沌载波上而被传输。所采用的混沌电路是 Lorenz 吸引子。并得出了混沌同步在一定的摄动条件下具有较强的鲁棒性的结论。也就是说，当发受电路间满足一定的条件时，即使有干扰存在也会发生同步。在实现保密通信时，将信息信号作为干扰加入混沌信号中，利用混沌信号频谱的宽带性对信息信号进行“包装”以实现加密，而后利用混沌同步的鲁棒性，通过实现混沌同步来进行解调。1992 年，Kocarev 等人[9]基于蔡氏电路，用 Pecora－Carroll 同步方案设计，也完成了保密通信。应当注意：他们都是将信息信号作为干扰加在混沌信号上，信息信号的功率应大大低于混沌信号的功率，为的是利用混沌同步的鲁棒性，在不破坏同步的基础上实现保密通信。

混沌保密通信系统可以表示为图 1，其中信息信号为 m(t)，解调出的信息信号为 m′(t)．这是一个混沌载波同步系统。

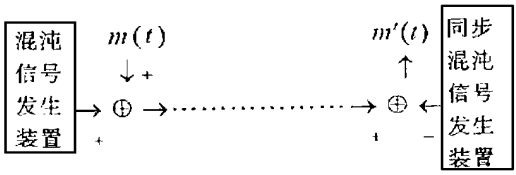

图 1

综合已有报道，将混沌保密通信分为模拟通信和数字通信。Cuomo 和 Oppenheim[10,11,12,]实现的基于 Lorenz 吸引子的混

沌保密通信，属于模拟通信的范畴；混沌移相键控(CSK)方式[15,16]和 D·R·Frey 等[3]混沌数字编码方式则属于数字通信的范畴。混沌保密通信，从混沌电路是自治电路还是非自治电路，可分为自治的混沌保密通信和非自治的混沌保密通信，如 Oppenheim 等[10,11,12,]和 Kocarev 等[9]分别利用自治电路构成了通信系统，属于自治的保密通信；而 Carroll 等[19,20]采用非自治电路，用滤波器处理，属于非自治的保密通信。

纵观目前用于保密通信的“同步混沌系统”的实现方案，无论采用哪种混沌电路和方式，其重点在于“同步”问题。从传统的同步理论来看，为了将接收端的信息解调出来，必须在接收端产生与发射端同频、同相用于解调出信息信号的同步信号。对“同步混沌系统”而言，即在接收端产生与发射端形状完全相同的用于解调的信号。因此，从实用的角度考虑，讨论通信系统的同步性能尤为重要。

我们采用 Pacora-Carroll 同步方案，研究三阶自治同步混沌系统。受到 Oppenheim 和 Cuomo 等人[10,11,12,]工作的启示，引入地磁场反向方程(REMF 方程)[17]，研究基于 REMF 吸引子的保密通信方案，并和基于 Lorenz 吸引子、基于 Rossler 吸引子的情况作以对比。考虑到 H·Dedieu 文章[15]中，“0”状态和“1”状态过渡时间是毫秒数量级的，发射端只有等到接收端同步或失谐确实发生才能发出下一个数字信息。这使研究“0”混沌吸引子和“1”混沌吸引子中间的过渡时间很必要。类比于传统的同步系统的同步性能，我们在文章[18]提出同步混沌系统的同步性能的概念。主要研究同步建立时间、同步保持时间和同步稳态误差等，这对考察三阶自治同步混沌系统的同步质量好坏和同步混沌系统的设计是很必要的，因为这会直接决定保密通信系统的质量。在分析同步性能的基础上，我们设计出基于 REMF 吸引子的同步混沌系统并进行了模拟保密通信的研究。同步混沌系统可以有多种混沌电路构成，并且同种混沌电路构成的同步系统它们的参数也可以不同，这都对同步系统的同步性能有很大影响。

实际上，关于同步混沌系统的最新报道，基本上都是在同步系统同步性能的某一方面发展。

1996 年，Tao Yang 和 L·O·Chua[19]提出混沌的参数调制方法，目的是为了解决 CSK 通信和模拟混沌保密通信中的通信速率问题，其实质是如何解决同步建立时间问题。1996 年，L·O·Chua 等[20]又针对蔡氏电路构成的同步系统，对时变信道和时变混沌参数的同步系统进行研究，其实质是如何解决同步稳态误差问题。

3　混沌保密通信中的信道问题

由于混沌信号的特点及同步混沌系统的同步机理，要实现较高质理的通信，除对同步系统有一定的要求外，信道的好坏也是重要决定因素。理论上要求用于保密通信的信道频带很宽。光纤是一种较好的选择。光纤具有：近似无穷的带宽、较低的衰减、无线路噪声等。1995 年，P·Celka[16]成功地利用光调制、CSK 技术和光纤技术，解决了混沌保密通信中的信道问题和数字信号的传输问题；1996 年，P·Celka[21]又成功地通过 700 米光纤实现光学动态系统的混沌同步。与光纤信道研究相对比的是，1995 年，钟国群[22]基于蔡氏电路实现混沌保密通信的无线通信，其效果不理想。究其原因是：无线通信的信道不理想所致。如何使无线通信尽可能好地用于混沌保密通信，仍是进一步研究的课题。

4 混沌保密通信中的信号频率

目前文献报道的混沌电路所产生的混沌信号的频率较低，多在音频范围内[23]。以Pecora-Carroll同步方案构成的同步混沌系统是以混沌信号作载波信号来实现保密通信的，即混沌信号是“包装”信号。信息信号的频率应与混沌信号的频率在同一个数量级内。Cuomo等[11]的保密通信模拟中，信息信号在音频内。钟国群[22]的研究，信息信号也在音频内。我们的研究[24]也表明：当信息信号的频率低于混沌信号的主频带时，保密通信的效果较好；当信息信号频率高于混沌信号的主频带时，保密通信效果差，甚至不能进行。研究如何利用典型的混沌电路实现高速信息保密通信，是混沌保密通信走向实用化所必需考虑的。

5 结语

混沌的应用研究，虽然发展很快，但仍处于初始阶段。混沌保密通信是混沌应用研究的一个分支，它在混沌应用性研究中是比较有成果的，但需要做的工作还很多，离实际使用还有一定距离。其中值得一提的是混沌同步理论，它对保密通信起了关键作用。全面考察同步混沌系统的同步性能，以便设计出性能良好的同步系统；拓展保密通信信道的种类，以使混沌保密能应用于各种通信；提高混沌信号的频率，改善同步系统，使系统能对高频信号进行保密，这些都是本方向走向实际应用所应解决的问题。

参考文献

1 陈式刚.映象与混沌：国防工业出版社.1992

2 葛真等.非线性电路及混沌：重庆大学出版社.1989

3 D·R·Frey “Chaotic digital encoding: an approach to secure communication”IEEE Trans·Circuits Syst· vol·40, No·10, Oct·1993

4 L·M·Pecora and T·L·Carroll “Driving systems with chaotic signals”Physical Rev· A,vol·44, NO·4, Aug·1991

5 樊昌信等.通信原理：国防工业出版社.1988

6 L·M·Pecora and T·L·Carroll“Synchronization in chaotic systems”Physical Rev· Lett·, vol· 64 No·8, pp·821824, Feb·1990

7 T·Endo and L·O·Chua·Synchronization of chaos phase-locked loops·IEEE Trans · Circuits Syst, vol·38·Dec·1991

8 T·L·Carroll and L·M·Pecora “Synchronizing chaotic circuits ”IEEE Trans · Circuts Syst· vol·38, No·4, pp,453456, Apr·1991

9 L·Kocarev et al“ Experimental demonstration of secure communications via chaotic synchronization”Int·J·Birfurcation and Chaos, vol·2, No·3, Sep·1992

10 K·M·Cuomo et al“ Circuit implementation of synchronizde chaos with application to communications”, Phys, Rew·Lett·, vol·71, Jul·1993

11 K·M·Cuomo et al“Synchronization of Lorenz-based chaotic circuits with application to communication” IEEE Trans· Circuits Syst·, vol· 40, No·10, Oct·1993

12 A·V·Oppenheim et al"Signal processing in the context of the chaotic signals "in Proc· IEEE ICASSP, pp, IV-117IV-120 , 1992

13 T·C·Newell "Synchronization of chaotic resonators based on control theory"Physical Rev· E, vol·51, Mar·1995

14 M·J·Ogorzalek" Taming Chaos-Part Ⅰ: Synchronization"IEEE Trans· Circuits SYst·, vol·40, No, 10, Oct·1993

15 H·Dedieu"Chaos shift keying: Modulation and demodulation of a chaotic carrier using selfsynchronizing Chua's circuits "IEEE Trans· Circuits Syst·, vol·40, No·10, Oct·1993

16 P·L·Carroll"Communication with use of filtered, synchronized, chaotic signals", IEEE Trans· Circuits Syst, vol 42, No3, Mar·1995

17 Chaos / Edited by A·V·Holden , Manchester, Manchester Univ·Pr, ·1986

18 高金峰等·同步混沌保密通信系统的同步性能研究·待发

19 Tao Yang L·O·Chua"Secure communication via Chaotic parameter modulation"IEEE Trans· Circuits Syst· Ⅰ:Fundamental theory and applications, vol·43, No·9, Sep·1996

20 L·O·Chua et al "Synchro nization of Chua's circuits with time-varying channel and parameters"IEEE Trans· Circuits Syst· Ⅰ:Fundamental theory and applications, vol·43, No·10, Oct·1996

21 P·Celda"Synchronization of chaotic optical dynamically systems through 700m of single mode fiber "IEEE Trans· Circuits Syst· Ⅰ: Fundamental theory and applications, vol·43, No·10, Oct·1996

22 钟国群·蔡氏电路混沌同步保密通信·电路与系统学报·第一卷·1996·3

23 Bifurcation Sights Sounds, and Mathematics / edited by T·Matsumoto et al , Springer-Verlag , Tokyo , 1993

24 李春生·混沌振荡在保密通信中的应用研究·郑州工业大学硕士研究生论文·1997

The Research-based Chaos with Application to Secure Communications

Li Chunsheng　Gao Jinfen　Wang Junkun

(*ZhenZhou university of technology*)

Abstract　Chaos with application to secure communications is one of research aspects of chaotic theroy · In this paper , we combine with our research results on secure communication via chaos, having a reviews about chaotic theory's application to secure communication·

keywords　chaos;secure communication ; synchronization