# A SURVEY OF CHAOTIC SYNCHRONIZATION AND SECURE COMMUNICATION

*Aziz-Alaoui M.A.*

Laboratoire de Mathématiques Appliquées,
Université du Havre, BP 540, 76058 Le Havre Cedex, France

## ABSTRACT

With the rapid development of personal communications and the Internet, information security has become an increasingly important issue of telecommunication industry. Recently, there has been tremendous worldwide interest in exploiting chaos in communication systems, which has applications in the encryption of information for secure communications. Chaotic synchronization of transmitters and receivers has been studied during the last decade, and still remains an interesting research topic. In this paper we give a rapide survey on this subject, focusing on identical synchronization which is the best way to explain chaos synchornization.

## 1. INTRODUCTION

Synchronization is a ubiquitous phenomenon characteristic of many processes in natural systems and (nonlinear) science, it has permanently remained an objectif of intensive research and is today considered as one of the basic nonlinear phenomena studied in mathematics, physics, engineering or life science. Synchronization of two dynamical systems generally means that one system somehow traces the motion of another. Indeed, it is well known that many coupled oscillators have the ability to adjust some common relation that they have between them due to weak interaction, which yields to a situation in which a synchronization-like phenomenon takes place, see [1].

Since this discovery, periodic synchronization has found numerous applications in various domains, for instance in biological systems and living nature where synchronization is encountered on differents levels. Examples range from the modeling of the heart to the investigation of the circardian rhythm, phase locking of respiration with a mechanical ventilator, synchronization of oscillations of human insulin secretion and glucose infusion, neuronal information processing within a brain area and communication between different brain areas. Also synchronization plays an important role in several neurological diseases such as epilepsies and pathological tremors, or in differents forms of cooperative behavior of insects, animals or humans. For more details, see [9].

Author Email : aziz.alaoui@univ-lehavre.fr

This process may also be encountered in other areas, celestical mechanics or radio engineering and acoustics.

But, even though original notion and theory of synchronization implies periodicity of oscillators, during the last decades, the notion of synchronization has been generalized to the case of interacting chaotic oscillators.

Roughly speaking, a system is chaotic if it is deterministic, has a long-term aperiodic behavior, and exhibits sensitive dependence on initial conditions on a closed invariant set.

Despite the instability and the limited predictability in time of chaotic oscillators, in the two last decades, the search for synchronization has moved to chaotic systems. A lot of research has been done and, as a result, researchers showed that two chaotic systems could be synchronized by coupling them : synchronization of chaos is actual and chaos could then be expoitable, see [7], and for a review see [1]. Ever since, many researchers have discussed the theory, the design or applications of synchronized motion in coupled chaotic systems. A broad variety of applications have emerged, for example to increase the power of lasers, to synchronize the output of electronic circuits, to control oscillations in chemical reactions or to encode electronic messages for secure communications. Moreover, in the topics of coupled chaotic systems, many different phenomena, which are usually referred to as *synchronization*, exist and have been studied now for over a decade.

## 2. SYNCHRONIZATION AND STABILITY

### 2.1. Definitions

For the basic *master-slave* configuration where an autonomous chaotic system (the master) :

$$\frac{dX}{dt} = F(X), \quad X \in \mathbb{R}^n \tag{1}$$

drives another system (the slave) :

$$\frac{dY}{dt} = G(X, Y), \quad Y \in \mathbb{R}^m, \tag{2}$$

synchronization takes place when $Y$ asymptotically copies, in a certain manner, a subset $X_p$ of $X$. That is, there exists a relation between the two coupled systems, which could

be a smooth invertible function $\psi$, the last carries trajectories on the attractor of a first system on the attractor of a second system. In other words, if we know, after a transient regime, the state of the first system, it allows us to predict the state of the second : $Y(t) = \psi(X(t))$. Generally, it is assumed $n \geq m$, however, for the sake of easy readability, we will reduce, even if this is not a necessary restriction, to the case $n = m$, and thus $X_p = X$. Henceforth, if we denote the difference $Y - \psi(X)$ by $X_\perp$, in order to arrive at a synchronized motion, it is expected to have :

$$||X_\perp|| \longrightarrow 0, \quad as \quad t \longrightarrow +\infty. \tag{3}$$

If $\psi$ is the identity function, the process is called *identical synchronization* (IS hereafter).

**Definition of IS.** System (2) synchronizes with system (1), if the set $M = \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n, Y = X\}$ is an attracting set with a basin of attraction $B$ ($M \subset B$) such that $\lim_{t\to} \infty||X(t) - Y(t)|| = 0$, forall $(X(0), Y(0)) \in B$.

Thus, this regime corresponds to the situation where all the variables of two (or more) coupled chaotic systems converge.

If $\psi$ is not the identity function, the phenomenon is more general and is referred to as *generalized synchronization* (GS).

**Definition of GS.** System (2) synchronizes with system (1), in the generalized sense, if there exists a transformation $\psi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$, a manifold $M = \{(X, Y) \in \mathbb{R}^{n+m}, Y = \psi(X)\}$ and a subset $B$ ($M \subset B$), such that for all $(X_o, Y_o) \in B$, the trajectory based on the initial conditions $(X_o, Y_o)$ approaches $M$ as time goes to infinity.

Henceforth, in the case of identical synchronization, equation (3) above means that a certain hyperplane $M$, called *synchronization manifold*, within $\mathbb{R}^{2n}$, is asymptotically stable. Consequently, for the sake of synchrony motion, we have to prove that the origin of the transverse system $X_\perp = Y - X$ is asymptotically stable. That is, to prove that the motion transversal to the synchronization manifold dies out.

The Lyapunov exponents associated with the variational equation corresponding to the tranverse system $X_\perp$ :

$$\frac{dX_\perp}{dt} = DF(X)X_\perp \tag{4}$$

where $DF(X)$ is the Jacobian of the vector field evaluated onto the driving trajectory $X$, are referred to as transverse or conditional Lyapunov exponents (CLE hereafter).

In the case of IS it appears that the condition $L^\perp_{max} < 0$, is sufficient to insure synchronization, where $L^\perp_{max}$ is the largest CLE. Indeed, Equation (4) gives the dynamics of the motion transverse to the synchronization manifold, therefore CLE will tell us if this motion die out or not, and hence, whether the synchronization state is stable or not. Consequently, if $L^\perp_{max}$ is negative, it will insure the stability of the synchronized state. This will be best explained using two examples below.

### 2.2. Identical synchronization

Thet simplest form of chaos synchronization and the best way to explain it, is *identical synchronization* (IS), also referred to as *Conventional* or *Complete synchronization* (see [2]). It is also the most typical form of chaotic synchronization often observable in two identical systems.

There are various processes leading to synchronization, depending on the used particular coupling configuration they could be very different. So, one has to distinguish between the two following main situations, even if they are, in some sense, similar : the **uni-directional** and the **bi-directional** coupling. Indeed, synchronization of chaotic systems is often studied for schemes of the form :

$$\begin{aligned} \frac{dX}{dt} &= F(X) + kN(X - Y) \\ \frac{dY}{dt} &= G(Y) + kM(X - Y) \end{aligned} \tag{5}$$

where $F$ and $G$ act in $\mathbb{R}^n$, $(X, Y) \in (\mathbb{R}^n)^2$, $k$ is a scalar and $M$ and $N$ are coupling matrices belonging to $\mathbb{R}^{n\times n}$. If $F = G$ the two subsystems $X$ and $Y$ are identical. Moreover, when both matrices are nonzero then the coupling is called *bi-directional*, while it is referred to as *uni-directional* if one is the zero matrix, and the other being nonzero.

Other names were given in the litterature of this type of synchronization, such as *one-way diffusive* coupling, *drive-response* coupling, *master-slave* coupling or *negative feedback control*.

System (5) above with $F = G$ and $N = 0$ becomes uni-directionlly coupled, and reads :

$$\begin{aligned} \frac{dX}{dt} &= F(X) \\ \frac{dY}{dt} &= F(Y) + kM(X - Y) \end{aligned} \tag{6}$$

$M$ is then a matrix that determines the linear combination of $X$ components that will be used in the difference, and $k$ determines the strength of the coupling.

In uni-directional synchronization, the evolution of the first system (the drive) is unaltered by the coupling, the second system (the response) is then constrained to copy the dynamics of the first.

In contrast to the uni-directional coupling, for the bi-directionally (also called *mutual* or *two-way*) coupling, both drive and response systems are connected in such a way that they mutually influence each other's behavior. Many biological or physical systems consist of bi-directionally interacting elements or components, examples range from cardiac and respiratory systems to coupled lasers with feedback.

In the following, we give an example, and for the sake of simplicity, let us develop the idea on the following 3-dimensional simple autonomous system, which belongs to the class of dynamical systems called *generalized Lorenz systems*, see [5] and references therein :

$$\begin{cases} \dot{x} &= -9x - 9y \\ \dot{y} &= -17x - y - xz \\ \dot{z} &= -z + xy\,. \end{cases} \tag{7}$$

The signs used differentiate system (7) from the well-known Lorenz system :

$$\dot{x} = -10x + 10y,\ \dot{y} = 28x - y - xz,\ \dot{z} = -\frac{8}{3}z + xy.$$

From previous observations, it was shown that system (7) oscillate chaotically, its Lyapunov exponents are $+0.601$, $0.000$ and $-16.470$, it exhibits the chaotic attractor of figure 1, with a 3D feature very similar to that of Lorenz attractor.

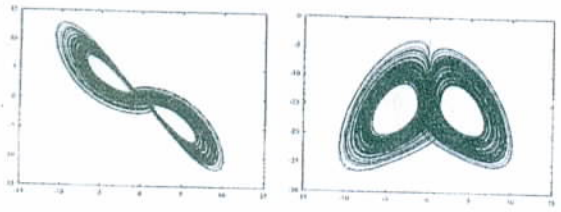

**Figure 1.** The chaotic attractor of system (7) : $xy$ and $xz$-plane projections.

**Unidirectional identical synchronization**

Let us consider an example with two copies of system (7), and for

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{8}$$

that is, by adding a damping term to the first equation of the response system, we get a following uni-directionally coupled system, coupled through a linear term $k > 0$ according to variables $x_{1,2}$ :

$$\begin{cases} \dot{x_1} &= -9x_1 - 9y_1 \\ \dot{y_1} &= -17x_1 - y_1 - x_1 z_1 \\ \dot{z_1} &= -z_1 + x_1 y_1 \\ \dot{x_2} &= -9x_2 - 9y_2 - k(x_2 - x_1) \\ \dot{y_2} &= -17x_2 - y_2 - x_2 z_2 \\ \dot{z_2} &= -z_2 + x_2 y_2 \end{cases} \tag{9}$$

For $k = 0$ the two subsystems are uncoupled, for $k > 0$ both subsystems are uni-directionally coupled. Our numerical computations yield the optimal value $\tilde{k}$ for the synchronization, we found that for $k \geq \tilde{k} = 4.999$ both subsystems of (9) synchronize. That is, starting from random initial conditions, and after some transient time, system (9) generates the same attractor as for system (7), see figure 1. Consequently, all the variables of the coupled chaotic subsystems converge, that are $x_2$ converges to $x_1$, $y_2$ to $y_1$ and $z_2$ to $z_1$, see figure 2. Thus, the second system (the response) is locked to the first one (the drive). One

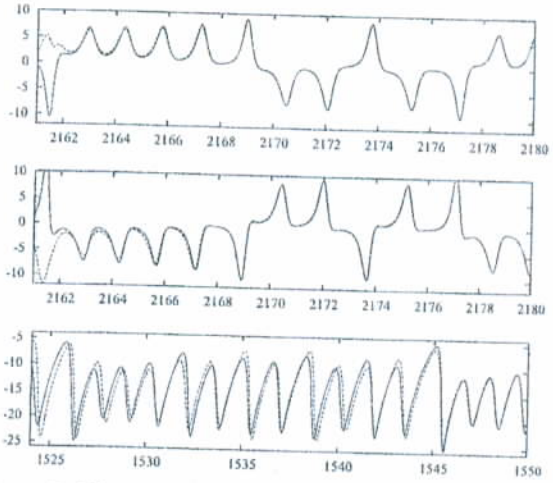


**Figure 2.** Time series for $x_i(t)$, $y_i(t)$ and $z_i(t)$ in system (9), $(i = 1, 2)$, for the coupling constant k = 5.0, that is beyond the threshold necessary for synchronization. After transients die down, the two subsystems synchronize perfectly.

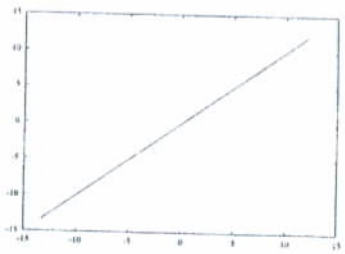

**Figure 3.** Regular behavior emerges from chaotic behaviors. The plot of amplitudes $y_1$ against $y_2$, after transients die down, shows a diagonal line, which also indicates that the receiver and the transmitter are maintaining synchronization. The plot of $z_1$ against $z_2$ shows a similar figure.

also could give correlation plots that are the amplitudes $x_1$ against $x_2$, $y_1$ against $y_2$ and $z_1$ against $z_2$, and observe diagonal lines, meaning also that the system synchronizes.

For an example of bidirectional identical synchronization, see [1].

## 3. APPLICATION TO TRANSMISSION SYSTEMS AND SECURE COMMUNICATION

Synchronization principles work in practical applications as those pointed out in the introduction, and the use of chaotic signals to transmit information has been a very active research topic in the last decade. Thus, it has been established that chaotic circuits may be used to transmit

information by synchronization. As a result, several proposals for secure communications schemes have been advanced, see for instance [4]. The first laboratory demonstration of a secure communication system which uses a chaotic signal for *masking* purposes, and which exploits the chaotic synchronization techniques to recover the signal, has been reported in [6].

The work described here doesn't pretend to be complete, there are many competing methods that are well-established and tested.

The main idea of the communication shemes is to encode a message by means of a chaotic dynamical system (the transmitter), and to decode it using a second dynamical system (the receiver) that synchronizes with the first. In general, secure communication applications assume additionally that the used coupled systems are identical.

Different methods can be used to hide the useful information, for example chaotic masking, chaotic switching or direct chaotic modulation, see (Hasler, 1998). For instance, in the chaotic masking method, an analog information carrying signal $s(t)$ is added to the output $y(t)$ of the chaotic system in the transmitter. The receiver tries to synchronize with component $y(t)$ of the transmitted signal $s(t)+y(t)$. If synchronization takes place, the information signal can be retrieved by substraction, see figure 4. It is

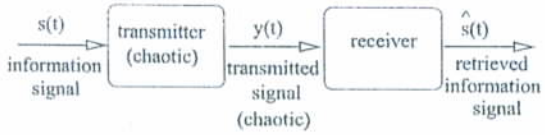


**Figure 4**. A typical communication setup

interesting to note that, in all proposed schemes for secure communications using the idea of synchronization (experimental realization or computer simulation), there is an inevitable noise degrading the fidelity of the original message. Robustness to parameter mismatch was addressed by many authors, see [1] for references.

Furtheremore, different implementations of chaotic secure communication have been proposed during the last decades, as well as methods for cracking this encoding. The methods used to crack such a chaotic encoding, make use of the low dimensionality of the chaotic attractors. Indeed, since the properties of low dimensional chaotic systems, with one positive Lyapunov exponent, can be reconstruted by analysis of the signal, such as through the delay time reconstruction methods, it seems unlikely that these systems might provide a secure encryption method. The hidden message can often be retrieved easily by an eavesdropper without having to have the receiver. But, chaotic masking and encoding are difficult to break, using the state of the art analysis tools, if sufficiently high dimensional chaos generators, with multiple positive Lyapunov exponents, that are hyperchaotic systems, are used, see references within [8].

## 4. REFERENCES


[1] M.A. Aziz-Alaoui, "Synchronization of Chaos," *Encyclopedia of Mathematical Physics*, Elsevier, 2006.

[2] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares and C. Zhou, The synchronization of chaotic systems. *Physics Reports* Vol. 366: pp. 1-101, 2002.

[3] G. Chen and X. Dong, *From chaos to order*, Singapore: World Scientific, 1998.

[4] Cuomo K, Oppenheim A and Strogatz S (1993) Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst.* 40, 623-633.

[5] S. Derivière and M.A. Aziz-Alaoui, "Estimation of attractors and synchronization of generalized Lorenz systems", *Dynamics of Continuous, Discrete and Impulsive Systems series B: Applications and Algorithms* Vol. 10(6), pp. 833-852, 2003.

[6] Kocarev Lj, Halle K, Eckert K and Chua LO (1992) Experimental demonstration of secure communication via chaotic synchronization. *International Journal of Bifurcation and Chaos* 2(3): 709-713.

[7] L. Pecora and T. Carroll, Synchronization in chaotic systems. *Physical Review letters* Vol. 64, pp. 821-824, 1990.

[8] Pecora L, Carroll T, Johnson G and Mar D (1997) Fundamentals of synchronization in chaotic systems, concepts and applications. *Chaos* 7(4): 520-543.

[9] A. Pikovsky, M. Rosenblum and J. Kurths, *Synchronization, A Universal Concept in Nonlinear Science*, Cambridge University Press, 2001.

[10] N. Rulkov, M. Sushchik, L. Tsimring, and H. Abarbanel, Generalized synchronization of chaos in directionally coupled chaotic systems, *Phys. Rev. E* Vol. 51(2), pp. 980-994, 1995.

# 12TH IEEE INTERNATIONAL CONFERENCE ON ELECTRONICS, CIRCUITS AND SYSTEMS

PROCEEDINGS
VOLUME 2

EDITED BY:

NOUREDDINE BOUDRIGA
MOHAMMAD S. OBAIDAT

SPONSORED BY:

IEEE

IEEE CIRCUITS AND SYSTEMS SOCIETY

Tunisian Telecommunications Scientific Society

ICECS 2005 ICECS 2005 ICECS 2005 ICECS 2005 ICECS 2005 ICECS 2005 ICECS 2005 ICECS 2005 ICECS

December 11-14, 2005
Gammarth, Tunisia