A COMMUNICATION SCHEME BY USING SYNCHRONIZED CHAOTIC SYSTEMS

Ömer Morgül and Moez Feki
Bilkent University, Dept. of Electrical and Electronics Engineering
06533, Bilkent, Ankara, Turkey
e-mail : morgul@bilkent.edu.tr moez@ee.bilkent.edu.tr

Abstract

A method to synchronize systems with chaotic behavior, in a master-slave configuration adapted to communication systems, is discussed. This work is motivated by the need for secure communication. In this method, the synchronization and message transmission phases are separated, and while the synchronization is achieved in the synchronization phases, the message is only sent in the message transmission phases.

I. INTRODUCTION

Recently the idea of synchronization of chaotic systems has received a great deal of attention, see e.g. [1]-[4]. One of the motivations for synchronization is the possibility of sending messages through chaotic systems for secure communication, see e.g. [8], [6], [5]. Such synchronized systems usually consist of two parts : a generator of chaotic signals (drive system), and a receiver (response system). The response system is usually a duplicate of a part (or the whole) of the drive system. It has been shown in [2] that by driving the duplicate with signal(s) from the original system, both drive and response systems will have their common signals synchronized.

In this work, we present a method for message transmission using synchronized chaotic systems. In this approach, the synchronization and the message sending phases are alternated. While in one interval, drive and response systems are synchronized (synchronization phase (**SP**)), in the next one, the response system is switched to an autonomous system(transmission phase (**TP**)). Then, at the transmitter, the information-bearing signal(message) is added to the chaotic signal, and at the receiver the masking is removed.

II. COMMUNICATION SCHEME

Assume the following chaotic drive system:

$$\dot{u} = f(u) \ , \ (u \in \mathbf{R}^n)$$

($f(.)$ is differentiable).
Knowing that the solutions of the chaotic system are bounded in a region, and since $f(.)$ is differentiable then the following Lipscitz condition is also satisfied

$$\|f(u) - f(w)\| \leq k\|u - w\| \ , \quad u, w \in \mathbf{R}^n \quad , \qquad (1)$$

where $k > 0$ is a Lipschitz constant and the norm $\|\cdot\|$ is the standard Euclidean norm in $\mathbf{R}^n$.

For the response system we consider the following :

$$\dot{w} = g(u_p, w) \ , \ w \in \mathbf{R}^n \ , u_p \in \mathbf{R}^p \ ,$$

where $g(\cdot) : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^n$ is a differentiable function. Note that the response uses signals of the drive as an input for synchronization. We assume both systems to be exponentially synchronized, hence there exists constants $M > 0$ and $\alpha > 0$ such that for any $u(0)$ and $w(0)$ the following holds :

$$\|u(t) - w(t)\| \leq Me^{-\alpha t}\|u(0) - w(0)\| \ . \qquad (2)$$

Let $m(t)$ be the message to be sent. Let $T_s > 0$ and $T_m > 0$ denote the intervals for synchronization and message transmission, respectively. Our scheme is as given below :

i : (*Synchronization phase*) For $0 \leq t < T_s$, send the synchronization signal to the response system.

ii : (*Message transmission phase*) For $T_s \leq t < T_s + T_m$, send the masked message $u(t) + m(t)$, and for the response system use $\dot{w} = g(w, w) = f(w)$.

iii : (*Message recovery*) For $T_s \leq t < T_s + T_m$, the recovered message is

$$m_r(t) = u(t) + m(t) - w(t) \quad . \tag{3}$$

Note that in the above formulation, it is desirable to have p, the dimension of the synchronizing signal, to be as small as possible. Also, the number of messages to be sent should not exceed the dimension of that portion of the drive system used for synchronization, because the sent message in the **TP** is simply their sum. Since the error decays to zero in the **SP** (see [5]), at the end of this phase these errors become extremely small, provided that T_s is sufficiently large.

It can be easily shown using (1) and (2) that the relation between T_s and T_m should satisfy the following relation:

$$T_s > \frac{kT_m + \ln \frac{Mr}{\epsilon}}{\alpha} \quad . \tag{4}$$

where r is the initial error magnitude and ϵ is the precision number, (i.e. maximum error magnitude in the **TP**).

III. SYNCHRONISATION

We consider the following well-known Lorenz system for the drive system, see e.g. [2] :

$$\begin{aligned} \dot{x} &= \sigma(y - x) \ , \\ \dot{y} &= -xz + rx - y \ , \\ \dot{z} &= xy - bz \ . \end{aligned} \tag{5}$$

with $\sigma = 10$, $r = 20$ and $b = 1$. The solution $x(t)$ will be used to synchronize the following response system,

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r) \ , \\ \dot{y}_r &= -xz_r + rx - y_r \ , \\ \dot{z}_r &= xy_r - bz_r \ . \end{aligned} \tag{6}$$

It can be proved that if the matrix A of the system $\dot{w} = Aw + f(t)$ is Hurwitz-stable and that $f(t)$ decreases exponentially to zero, i.e. for some $M_1 > 0$ and $\alpha_1 > 0$, $\|f(t)\| \leq M_1 e^{-\alpha_1 t}, t \geq 0$, then for any $w(0) \in \mathbf{R}^n$, $w(t)$ also decays exponentially to zero.

To prove the synchronization, let us define the synchronization error terms as follows:

$$e_x = x - x_r \ , \quad e_y = y - y_r \ , \quad e_z = z - z_r \ . \tag{7}$$

Remark 1 : Since in the **TP** the synchronization error diverge exponentially, it is quite important to show that these errors decay exponentially in the SP. Our analysis will emphasize this fact using Lyapunov function and the above statement.

$$\dot{e}_y = -xe_z - e_y \quad , \dot{e}_z = xe_y - be_z \quad . \tag{8}$$

Let us define the Lyapunov function V:

$$V = \frac{1}{2}e_y^2 + \frac{1}{2}e_z^2 \quad . \tag{9}$$

Simple differentiation of V along the solutions of (8) results in :

$$\dot{V} = -e_y^2 - be_z^2 \quad . \tag{10}$$

Since $b > 0$, this shows that all solutions of (8) globally asymptotically decay to zero, see e.g. [9]. Moreover, from (9) and (10) it easily follows that $V(t) \leq e^{-kt}V(0)$, where $k = 2\min\{1, b\}$. Moreover, since $b = 1$, we have $\dot{V} \leq -2V$, which implies that $V(t) \leq e^{-2t}V(0)$, hence the errors $e_y(t)$ and $e_z(t)$ in fact decay exponentially to zero. This in particular implies that $\mid e_y(t) \mid \leq e^{-t}\|e(0)\|$ where $\|e(t)\| = \sqrt{e_x^2(t) + e_y^2(t) + e_z^2(t)}$. Then, we have:

$$\dot{e}_x = -\sigma e_x + \sigma e_y \quad . \tag{11}$$

Since $\sigma > 0$ and e_y decays exponentially to zero, it follows from the statment that e_x also decays exponentially to zero. The solution of (11) is given as

$$e_x(t) = e^{-\sigma t}e_x(0) + \int_0^t \sigma e^{-\sigma(t-\tau)}e_y(\tau)d\tau \quad .$$

Hence, by taking norms, using the facts given above and $\sigma > 1$, we obtain

$$\|e(t)\| \leq \sqrt{2 + \frac{8\sigma^2}{(\sigma - 1)^2}}e^{-t}\|e(0)\| \quad ,$$

which implies that (2) is satisfied. □

IV. SIGNAL TRANSMISSION

Consider the systems given by (5) and (6). Let $m(t)$ be the message to be sent. If, in addition to synchronization signal $x(t)$ we could send another signal, say $y(t)$, then by sending, say $y(t)+m(t)$ we could recover the message by subtracting $y_r(t)$ from this signal. In this case, the message can be recovered asymptotically since $e_y(t)$ decays to zero exponentially fast. However, this scheme requires the transmission of two messages, one for synchronization and one for message. Alternatively, we could separate the **SP** and the **TP**, and at each phase send only one message. For successful synchronization, T_s should be sufficiently large, and this depends on the exponential decay rate. Our method for synchronization and message sending is as follows:

i : (*Synchronization phase*) For $0 \leq t < T_s$, send the synchronization signal $x(t)$, and for the response system use (6).

ii : (*Message transmission phase*) For $T_s \leq t < T_s + T_m$, send $x(t) + m(t)$, and for the response system use the following :

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r) \ , \\ \dot{y}_r &= -x_r z_r + r x_r - y_r \ , \\ \dot{z}_r &= x_r y_r - b z_r \ . \end{aligned} \tag{12}$$

iii : (*Message recovery*) For $T_s \leq t < T_s + T_m$, the recovered message $m_r(t)$ is :

$$m_r(t) = x(t) + m(t) - x_r(t) \ . \tag{13}$$

Note that, the response system becomes an autonomous system in the **TP**. Since in the **SP**, the errors e_x, e_y, e_z decay to zero exponentially fast, at the end of this phase these errors become extremely small, provided that T_s is sufficiently large. Hence, for the **TP** we could use the variable x_r instead of x, which is the rationale behind using (12) instead of (6). Since $e_x(T_s) \neq 0$, however small, the solutions of (6) and (12) start diverging exponentially fast, and this increase in synchronization error terms depends on an appropriate Lyapunov exponent. However, if T_m is sufficiently small, which now depends on this Lyapunov exponent, at the end of message transmission phase the synchronization error still could remain at a negligible level. Hence by using (13) we could recover the message. This idea suggests that by making T_s larger, we could also be able to choose larger T_m for successful message transmission. Our simulations reveal that the ratio T_m/T_s should be made smaller than a constant, which depends on the decay rate in the synchronization phase and the associated Lyapunov exponent of the drive system. However, the determination of optimum ratio for T_m/T_s requires further research.

Note that for longer messages, instead of choosing sufficiently large synchronization intervals, we could divide the message into smaller intervals if possible, and then send each part in a message transmission phase, followed by a synchronization phase until all the message is sent.

V. SIMULATIONS

Next we present some numerical simulation results which indicate that the suggested method can be used for successful message transmission and recovery. Since the state variables in (5) vary in a wide dynamical range, for simulation purposes following [7], we use the scaling $x/10$, $y/10$ and $z/20$ which results in the following "scaled" Lorenz system :

$$\dot{x} = \sigma(y - x) \ ,$$

$$\dot{y} = -20xz + rx - y \ ,$$

$$\dot{z} = 5xy - bz \ .$$

and we changed the response systems accordingly.

In the first simulation, as the message to be sent, we used the speech signals corresponding the sounds of letters "A" and "B". This message is recovered with good listening quality. In the second simulation, the message to be sent is "wish you good luck" using the standard international alphabet code no. 2, see [10]. Figure 2 depicts the message recovery success. In this experiment, we choose smaller amplitude for the message to show that using our approach there is no restrictions on message amplitude.

VI. CONCLUSION

In this work, we presented a method for the signal recovery for the synchronized chaotic systems.

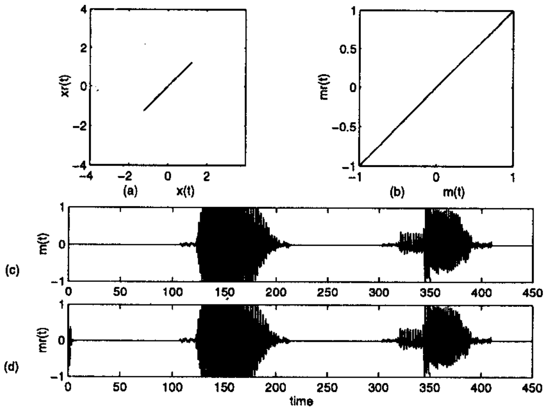

Fig. 1. Transmission of sounds "A" and "B".(a)Drive vs Response signals.(b)Transmitted vs recovered messages.(c)Transitted message.(d)Received message.

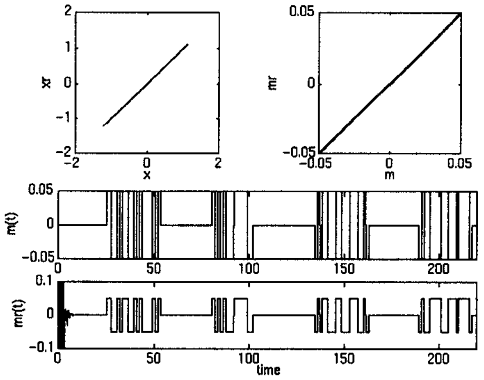

Fig. 2. Transmission of coded message.(a)Drive vs Response signals.(b)Transmitted vs recovered messages.(c)Transitted message.(d)Received message.

In this method, the synchronization and the message sending phases are alternated. This approach has the advantage of using only one transmission channel, in addition to providing freedom for the message magnitude.

References

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821-824, Feb. 1990.

[2] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, no. 4, pp. 2374-2383, Aug. 1991.

[3] L. O. Chua, L. Kocarev, and K. Eckert, "Experimental chaos synchronization in Chua's circuit," *Int. J. Bifurcation Chaos*, vol. 2, pp. 705-708, 1992.

[4] M. J. Ogorzalek, "Taming chaos - Part 1 : synchronization," *IEEE Trans. Circuits Syst.*, vol. 40, pp. 693-699, Oct. 1993.

[5] L. Kocarev, K. S. Halle, K. Eckert, and L. O. Chua, "Experimental demonstration of secure communication via chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, pp. 709-713, 1992.

[6] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcation Chaos*, vol. 3, pp. 469-477, 1993.

[7] K. M. Cuomo, and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65-68, 1993.

[8] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, " Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst.*, vol. 40, pp. 626-633, 1993.

[9] M. Vidyasagar, M. Vidyasagar, *Nonlinear Systems Analysis*, Prentice-Hall, Englewood Cliffs, 2nd. ed, 1993, p. 292, p. 153.

[10] W. D. Gegg, *Analog and Digital Communication*, John Wiley, New York, 1977, p. 526.