2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Secure Communication via Cluster Synchronization of Chaotic Systems

Zekeriya Sarı† and Serkan Günel‡

† The Graduate School of Natural and Applied Sciences, Department of Electrical and Electronics Engineering,
Dokuz Eylül University, 35160 Buca, İzmir, Turkey
‡Faculty of Engineering, Department of Electrical and Electronics Engineering, Dokuz Eylül University
35160 Buca, İzmir, Turkey
Email: zekeriya.sari@deu.edu.tr, serkan.gunel@deu.edu.tr

Abstract—In this paper, conceptual design of a secure communication system based on the cluster synchronization of chaotic systems has been proposed. Dividing the network into two sub-networks as transmitter and receiver, the symbols to be transmitted are signified by the cluster modes of the corresponding node groups. Numerical simulations have been presented to illustrate the basic concept.

1. Introduction

The discovery of synchronization of two or more chaotic systems without changing their dynamical characteristics (strange attractors peculiar to chaotic systems, sensitivity to initial conditions, etc.) and direct observations of this phenomenon in physical and biological systems have led to careful investigation of the synchronization of the nonlinear dynamical systems over the past decades [1]. It is well known that due to their sensitive dependence on initial conditions, the chaotic systems are capable of producing unpredictable outputs, characteristically. The idea of using them in secure data transmission has been studied extensively [5, 6, 7, 8].

The problem of under what conditions the interacting dynamical systems are able to synchronize has much more variety of results than expected at a first glance [2, 3, 4]. Depending on the network topology and coupling strength, all the nodes can synchronize to a common (periodic, quasi-periodic or chaotic) dynamical behavior resulting in full synchronization. The nodes of the network can also synchronize in groups forming clusters but there can be no synchronization in between the groups resulting in cluster synchronization [2, 3, 4]. Each cluster can have a different dynamical behavior or can loose synchronization totally.

In this paper, conceptual design of a secure communication system via the cluster synchronization of the chaotic systems has been proposed. In the proposed system, one or more controllable parameters allow cluster synchronization of the different node groups. The symbols to be transmitted are represented by the cluster synchronization modes. The paper is organized as follows: In section 2, design of arbitrary clusters in networks of chaotic systems has been summarized. Section 3 presents the main idea of using cluster synchronization of the chaotic systems to design secure communication systems. The concept has been illustrated through an example in Section 4.

2. Arbitrary Clusters of Networks of Chaotic Systems

Consider the network given as,

$$\dot{x}_i = f(x_i) + \sum_{j=1}^{N} \epsilon_{ij}(t) c_{ij} \boldsymbol{P} x_j, \quad i = 1, 2, \ldots, N \qquad (1)$$

consisting of identical chaotic oscillators where $x_i \in \mathbb{R}^d$ is the state vector of the i^{th} node, $f : \mathbb{R}^d \mapsto \mathbb{R}^d$ is the vector function defining individual node dynamics, $\epsilon_{ij}(t) \in \mathbb{R}$ is the coupling strength at time t between the i^{th} and j^{th} nodes, N is the number of the nodes. The diagonal matrix $\boldsymbol{P} = diag(p_1, p_2, \ldots, p_d) \in \mathbb{R}^{d\times d}$, where $p_k > 0$ for $k = 1, \ldots, s$ and $p_k = 0$ for $k = s+1, \ldots, d$ determines by which state variables of the nodes are coupled. The symmetric matrix with zero row sums $\boldsymbol{C} = [c_{ij}] \in \mathbb{R}^{N\times N}$ determines the network topology, i.e. $c_{ij} \neq 0$ if there exists coupling between the i^{th} and j^{th} node and $c_{ij} = 0$, otherwise.

Following the formalism in [4], assume that the network is divided into n clusters as $G_1 = \{1, \ldots, m_1\}, \ldots, G_n = \{\sum_{i=1}^{n-1} m_i+1, \ \ldots, \ \sum_{i=1}^{n} m_i = N\}$, where m_j is the number of nodes in the j^{th} cluster and $m_1 \leq \ldots \leq m_n$ can be assumed without any loss of generality. "$i \sim j$" denotes that the i^{th} and j^{th} nodes are in the same cluster. $\overline{G}_{\bar{k}}$ is the number of nodes that are in the same cluster with k^{th} node.

The design of arbitrary clusters and assurance of the stability of them require solution of two problems consequently; constructing the coupling matrix $\boldsymbol{C}$ and adjusting the coupling strength among the nodes [4].

Assuming that the individual system $\dot{x}_i = f(x_i)$ is eventually dissipative, which implies there exists compact sets $B_i = \{x_i \mid \|x_i\| \leq b_1\}$ attracting all the trajectories outside of it, then it can be shown that the coupled network in (1) is eventually dissipative [4].

Considering the case $\epsilon_{ij}(t) = \epsilon_1, \ i, j = 1 \ldots, N, \ \forall t$ and denoting the error between the i^{th} and j^{th} node as e_{ij}

$$e_{ij} = x_j - x_i, \quad i, j = 1, \ldots, N, \ i \sim j \qquad (2)$$

the error dynamics is governed by,

$$\dot{e}_{ij} = f(x_j) - f(x_i) + \epsilon_1 \sum_{k=1}^{N} \Big(c_{jk} \boldsymbol{P} e_{jk} - c_{ik} \boldsymbol{P} e_{ik} \Big) \quad (3)$$

where $i, j = 1, \ldots, N,\ i \sim j$. Let Df denote the Jacobi matrix of f, then (3) can be written as,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta x_j + (1-\beta) x_i) d\beta \right] e_{ij} + \epsilon_1 \sum_{k=1}^{N} \Big(c_{jk} \boldsymbol{P} e_{jk} - c_{ik} \boldsymbol{P} e_{ik} \Big) \quad i, j = 1, \ldots, N,\ i \sim j \quad (4)$$

Adding and subtracting the term $\boldsymbol{A} e_{ij}$ to (4) to avoid instabilities caused by the positive eigenvalues of Df, where $\boldsymbol{A} = diag(a_1, \ldots, a_d),\ a_k > 0$ for $k = 1, \ldots, s$ and $a_k = 0$ for $k = s+1, \ldots, d$ (recall that s is the number of nonzero elements in diagonal matrix $\boldsymbol{P}$), we have,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta x_j + (1-\beta) x_i) d\beta - \boldsymbol{A} \right] e_{ij} + \boldsymbol{A} e_{ij} + \epsilon_1 \sum_{k=1}^{N} \Big(c_{jk} \boldsymbol{P} e_{jk} - c_{ik} \boldsymbol{P} e_{ik} \Big) \quad i, j = 1, \ldots, N,\ i \sim j \quad (5)$$

Considering the auxilary system,

$$\dot{e}_{ij} = \left[\int_0^1 Df(\beta x_j + (1-\beta) x_i) d\beta - \boldsymbol{A} \right] e_{ij} \quad i, j = 1, \ldots, N,\ i \sim j \quad (6)$$

we assume Lyapunov functions of the form,

$$W_{ij} = \frac{1}{2} e_{ij}^T \boldsymbol{H} e_{ij}, \quad i, j = 1, \ldots, N, \quad i \sim j \quad (7)$$

where $\boldsymbol{H} = diag(h_1, \ldots, h_s, \boldsymbol{H_1}),\ h_1 > 0, \ldots, h_s > 0$ and $\boldsymbol{H_1} \in \mathbb{R}^{(d-s)\times(d-s)}$ is a positive definite matrix, whose time derivative along the trajectories of (6) is negative, i.e.

$$\dot{W}_{ij} = e_{ij}^T \boldsymbol{H} \left[\int_0^1 Df(\beta x_j + (1-\beta) x_i) d\beta - \boldsymbol{A} \right] e_{ij} < 0 \quad i, j = 1, \ldots, N,\ i \sim j,\ e_{ij} \neq 0 \quad (8)$$

Theorem 2.1. *Under the eventual dissipativeness of (1) and assumption (8) and with the coupling matrix,*

$$\boldsymbol{C} = \begin{bmatrix} 3\boldsymbol{C}_{11} & \boldsymbol{C}_{12} & \boldsymbol{0} & \boldsymbol{0} & \ldots & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{C}_{21} & 5\boldsymbol{C}_{22} & \boldsymbol{C}_{23} & \boldsymbol{0} & \ldots & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{C}_{32} & 5\boldsymbol{C}_{33} & \ddots & \ldots & \boldsymbol{0} & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \ldots & 5\boldsymbol{C}_{n-1,n-1} & \boldsymbol{C}_{n-1,n} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \ldots & \boldsymbol{C}_{n,n-1} & 3\boldsymbol{C}_{n,n} \end{bmatrix} \quad (9)$$

where $\boldsymbol{C}_{ii} \in \mathbb{R}^{m_i \times m_i},\ \boldsymbol{C}_{ii} = [c_{jk}],\ c_{jk} = 1$ *for* $j \neq k$ *and* $c_{jj} = -\sum_{k=1, k\neq j}^{m_i} c_{jk}$. $\boldsymbol{C}_{i,i+1} \in \mathbb{R}^{m_i, m_{i+1}}$. $\boldsymbol{C}_{i+1,i}^T = \boldsymbol{C}_{i,i+1} = (\boldsymbol{C}_{ii}, \boldsymbol{0})$ *if* $m_i < m_{i+1}$ *or* $\boldsymbol{C}_{i+1,i}^T = \boldsymbol{C}_{i,i+1} = \boldsymbol{C}_{ii}$ *if* $m_i = m_{i+1}$, *the cluster synchronization invariant manifold* $M = \{x_1 = \ldots x_{m_1}, \ldots, x_{m_1+\ldots+m_{n-1}+1} = \ldots = x_N\}$ *is globally asymptotically stable, if the following inequality holds:*

$$\epsilon_1 \sum_{i=1}^{N} \sum_{j\sim i} \overline{G}_{\overline{j}} e_{ji}^T \boldsymbol{H} \boldsymbol{P} e_{ji} \geq \sum_{i=1}^{N} \sum_{j\sim i} e_{ji}^T \boldsymbol{H} \boldsymbol{A} e_{ji} \quad (10)$$

Proof. See [4] for the proof. □

Corollary 2.1.1. *Since* $\overline{G}_{\overline{1}} = \ldots = \overline{G}_{\overline{m}_1} = m_1 \leq \ldots \leq \overline{G}_{\overline{N}} = m_n$, *we have,*

$$\epsilon_1 \sum_{i=1}^{N} \sum_{j\sim i} \overline{G}_{\overline{j}} e_{ji}^T \boldsymbol{H} \boldsymbol{P} e_{ji} \geq \epsilon_1 \sum_{i=1}^{N} \sum_{j\sim i} m_1 e_{ji}^T \boldsymbol{H} \boldsymbol{P} e_{ji} \quad (11)$$

Then, if

$$\epsilon_1 \sum_{i=1}^{N} \sum_{j\sim i} m_1 e_{ji}^T \boldsymbol{H} \boldsymbol{P} e_{ji} \geq \sum_{i=1}^{N} \sum_{j\sim i} e_{ji}^T \boldsymbol{H} \boldsymbol{A} e_{ji} \quad (12)$$

holds, which implies,

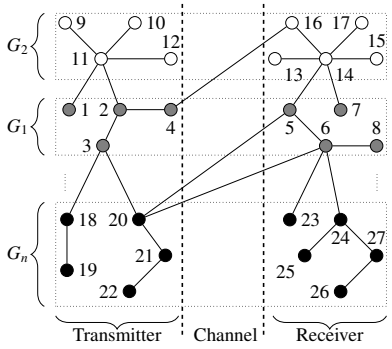
$$\epsilon_1 \geq \frac{1}{m_1} \max_{1\leq h\leq s} \frac{a_h}{p_h} \quad (13)$$

the Theorem (2.1) is satisfied.

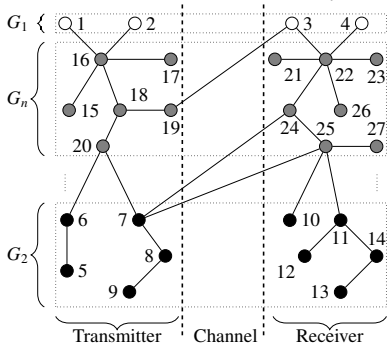
3. Secure Communication via Cluster Synchronization

In an attempt to use cluster synchronization in networks of oscillators in a communication system in which the information to be sent is encoded into symbols $s_i,\ i = 0, \ldots, M-1$, consider an arbitrary network of N identical oscillators that can be partitioned into n clusters. The network evolves with the dynamics in (1). All the oscillators are in their chaotic regime. The whole network is divided into two sub-networks as transmitter and receiver in such a way that the nodes connecting the transmitter side and the receiver side are not in the same cluster. Since the change of cluster mode in the transmitter side also changes the dynamics in the receiver side, the symbols to be transmitted are represented by the absence or the presence of the cluster synchronization of the corresponding node groups. The coupling strengths in the transmitter side are adjusted to assure the cluster mode corresponding to the symbol to be transmitted.

Figure 1a shows the case when the coupling strengths in the transmitter side are adjusted so that the symbol, say, s_j is to be transmitted. Note, since all the nodes are in their chaotic regime, and the nodes connecting the transmitter side and receiver side are not in the same cluster, the transmitted signals through the channel are always chaotic and cannot be resolved without the knowledge of the transmitter and the receiver internal topologies. Figure 1b shows the case when the couplings in the transmitter side is adjusted so that another symbol, say, s_k is to be transmitted. The spatiotemporal behavior of the network changes when different symbols are to be transmitted.



(a) Cluster mode for symbol s_j.



(b) Cluster mode for symbol s_k.

Figure 1: An arbitrary network of identical oscillators. The oscillators are illustrated by circles and the oscillators with the same gray level are in the same cluster. Figure 1a and Figure 1b show the cluster mode for the symbol s_j and s_k, respectively.

4. An Example for Binary Communication

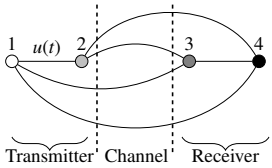
Consider the network of identical Lorenz oscillators given in Figure 2 with the network dynamics in (1). The Lorenz system defined by,

$$\begin{aligned} \dot{x}^{(1)} &= \sigma(x^{(2)} - x^{(1)}) \\ \dot{x}^{(2)} &= x^{(1)}(r - x^{(3)}) - x^{(2)} \\ \dot{x}^{(3)} &= x^{(1)}x^{(2)} - bx^{(3)} \end{aligned} \tag{14}$$

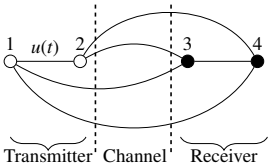
is chaotic for the parameter values $\sigma = 10.0$, $b = 8.0/3.0$, $r = 28.0$ [4]. All the oscillators in the network are coupled to each other through their $x^{(1)}$ states, i.e. $\boldsymbol{P} = diag(1, 0, 0)$.

Consider that the network is to be used in a binary communication system where the information to be sent is encoded into symbols 0 and 1. Assume that the symbols 0 and 1 are signified by the spatiotemporal behavior in Figure 2a and Figure 2b, respectively. Note that for the symbol 1 transmission the clusters $G_1 = \{1, 2\}$, $G_2 = \{3, 4\}$ are formed while for the symbol 0 transmission all the nodes are out of synchrony. The coupling strength between the node 1 and node 2 is to be used as the control parameter during the symbol transmission.

Considering Theorem (2.1) and denoting $\tilde{\boldsymbol{C}}_{ij}(t) = [\epsilon_{ij}(t)c_{ij}]$, we have a time varying coupling matrix for the network in Figure 2,



(a) Cluster mode for symbol 0.



(b) Cluster mode for symbol 1.

Figure 2: A network of identical Lorenz oscillators for a binary communication system. The oscillators are illustrated by circles and the oscillators with the same gray level are in the same cluster. Figure 2a and Figure 2b show the cluster mode for the symbol 0 and 1, respectively.

$$\tilde{\boldsymbol{C}}(t) = \begin{bmatrix} -3u(t) & 3u(t) & -\epsilon_1 & \epsilon_1 \\ 3u(t) & -3u(t) & \epsilon_1 & -\epsilon_1 \\ -\epsilon_1 & \epsilon_1 & -3\epsilon_1 & 3\epsilon_1 \\ \epsilon_1 & -\epsilon_1 & 3\epsilon_1 & -3\epsilon_1 \end{bmatrix} \tag{15}$$

Here, $u(t) = (1 - s_j)\epsilon_0 + s_j\epsilon_1$ which is the pulse modulated waveform of the information signal where s_j is the symbol to be transmitted at time t.

Note that during the symbol 1 transmission $u(t) = \epsilon_1$ and (13) must be satisfied for predefined clusters. During symbol 0 transmission, $u(t) = \epsilon_0$ and must be a non-zero value such that all the oscillators in the network are not synchronous.

Assuming that the transmitted signals through the channel are disturbed by independent additive white Gaussian noise, the network in Figure 2 has been numerically integrated with Euler-Maruyama method for 500 seconds with a step size of 0.005 seconds, signal-to-noise ratio of 20 dB, bit rate of 0.1 bps and $\epsilon_1 = 10.0$, $\epsilon_0 = 1.0$. Figure 3a shows pulse modulated waveform of the information signal. Figures 3b, 3c and 3d show the time waveforms of the errors between the nodes. Figure 3b and 3d shows the existence of $G_1 = \{1, 2\}$, $G_2 = \{3, 4\}$ clusters during symbol 1 transmission and their disappearance during symbol 0 transmission. Figure 3c shows that since node 1 and node 2 are not in the same cluster, there is no change in the temporal behavior of $e_{23}(t)$, which is one of the error signals through the channel, during any symbol transmission and $e_{23}(t)$ is always chaotic. Figure 3e shows the spectrogram of $e_{23}(t)$ in logarithmic scale plotted with the pulse modulated waveform of the information signal and it can be seen that there is no apparent correlation between the time-frequency properties of $e_{23}(t)$ and the information to be transmitted, which implies no information can be extracted from the time-frequency properties of the signals transmitted through the channel by a third party, directly, although the system needs to be checked toughly against known attacks.

5. Conclusion

A conceptual design of a secure communication system based on the cluster synchronization of chaotic systems has been proposed. Numerical simulations including time-frequency properties of the designed system has been presented through an example to illustrate the basic concept. Obtaining the bit error rate of the system, comparing the designed system with the conventional communication systems, investigation of different network topologies and unidirectional coupling are among further research.

References

[1] L. M. Pecora, T. L. Carroll, "Synchronization in chaotic systems", *Physical Review Letters*, vol.64, pp.821-824, 1990.

[2] V. N. Belykh, I. N. Belykh, M. Hasler, "Connection graph stability method for synchronized coupled chaotic systems", *Physica D*, vol.195, pp.159-187, 2004.

[3] V. N. Belykh, I. N. Belykh, M. Hasler, "Hierarchy and stability of partially synchronous oscillations of diffusively coupled dynamical systems", *Physical Review E*, vol.62, pp.6332-6345, 2000.

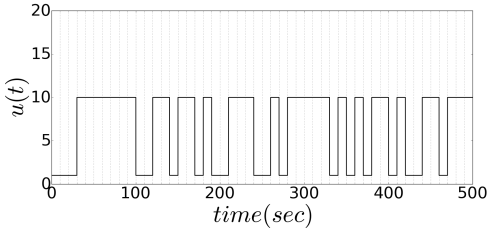
[4] Z. Ma, Z. Liu, G. Zhang, "A new method to realize cluster synchronization in connected chaotic networks", *Chaos: An Interdisciplinary Journal of Nonlinear Sciences*, vol.16, pp.023103, 2006.

[5] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, A. Shang, "Transmission of digital signals by chaotic synchronization", *International Journal of Bifurcation and Chaos*, vol.2, pp.973-977, 1992.

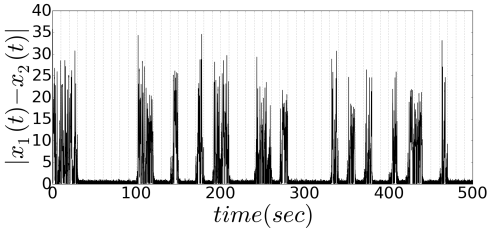
[6] K. M. Cuomo, A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications", *Physical Review Letters*, vol.71, pp.65-68, 1993.

[7] H. Dedieu, M. P. Kennedy, M. Hasler, "Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits", *IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing*, vol.40, pp.634-642, 1993.

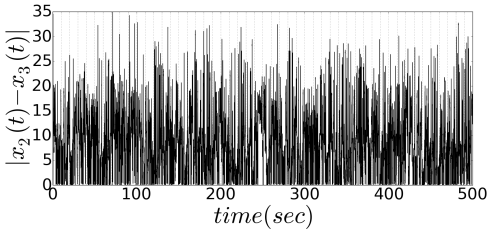
[8] Y. C. Kouomou, P. Woafo, "Cluster synchronization in coupled chaotic semiconductor lasers and application to switching in chaos-secured communication networks", *Optics communications*, vol.223, pp.283-293, 2003.



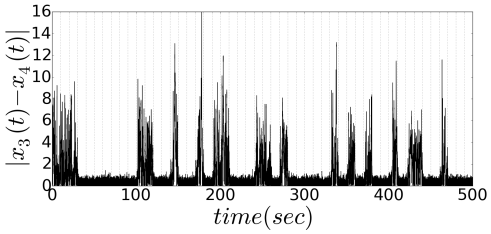
(a) Pulse modulated waveform of the information signal.



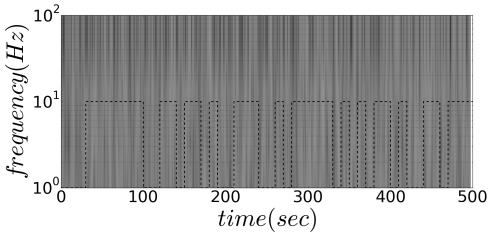
(b) Absolute value of $e_{12}(t)$.



(c) Absolute value of $e_{23}(t)$.



(d) Absolute value of $e_{34}(t)$.



(e) Spectrogram of $e_{23}(t)$ in logarithmic scale.

Figure 3: Simulation results of the network in Figure 2. Figure 3a shows the information signal. Figure 3b, Figure 3c, Figure 3d show the absolute values of the errors $e_{12}(t), e_{23}(t), e_{34}(t)$, respectively. Figure 3e shows the spectrogram of $e_{23}(t)$ in logarithmic scale.