Optics Communications 418 (2018) 41–45

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Secure remote synchronization and secure key distribution in electro-optic networks revealed by symmetries

Mingfeng Xu, Wei Pan, Liyue Zhang *

Center for Information Photonics and Communications, Southwest Jiaotong University, Chengdu, Sichuan 611756, China

ARTICLE INFO

Keywords:
Remote synchronization
Cluster synchronization
Secure key distribution

ABSTRACT

Despite the intuition that synchronization of different nodes in coupled oscillator networks results from information exchange between them, it has recently been shown that remote nodes could be partially synchronous even when they are separated by intermediately unsynchronized nodes. Here based on electro-optic system, we report on a more stronger form of such synchronization pattern that is termed as secure remote synchronization, in which two remotely separated nodes could have identically synchronized dynamical behaviors while the rest of the network are both statistically and information-theoretically incoherent relative to the two synchronized nodes. The generalized form of mirror symmetry in the network structure is identified to be a key mechanism allowing for secure remote synchronization. Moreover, this synchronization mode is robust against a wild range of system parameters and noise perturbing the intermediary dynamics. The lack of information about the synchronized dynamics in the rest of the network suggests that our results could potentially lead to network-based solutions for secure key distribution and secure communication.

1. Introduction

The use of complex networks to model the underlying topology of 'real-world' complex systems from social interaction networks, such as scientific collaboration networks, to biological regulatory networks and technological networks, such as the internet, has attracted much current research interest. The synchronization in complex networks plays an important role in the proper functioning of a wide variety of these 'real-world' systems [1–3]. Complete and isochronous synchronization of coupled chaotic units in which all the nodes in the network evolve into the same dynamics have been extensively studied [4,5]. Moreover, there also exist some more complicated synchronization modes such as cluster synchronization, in which novel patterns of synchronized elements are emergent [6,7]. On the other hand, the characterization of stability of cluster synchronization can be predicted by computational group theory to reveal the hidden symmetries of a network [8]. Based on these symmetries in networks, remote isochronous synchronization could be achieved despite the distance between the nodes in the same cluster, which means that two nodes could be completely synchronized even though there is no direct coupling between them [9,10]. However, there exist a serious problem in the above-mentioned networks is that, most of time, the clusters in the networks are highly coherent and thus they will share their respective dynamical information with each other. The possibility of synchronization without synchronized intermediaries is fascinating, it means that two nodes in the same cluster could be synchronized and be incoherent with all the other parts of the network. This special scheme suggests applications to new forms of secure communication technologies or new scheme for simultaneous generation and distribution of secret encryption keys [11–14].

In this letter, based on symmetries and cluster synchronization of network, we present a configuration scheme to realize secure remote synchronization. In this mirror-symmetric network, nodes separated far away from each other are designed to be in the same cluster, and remote isochronous synchronization could be achieved between these nodes while all the intermediaries in the network remains dynamically and statistically incoherent with respect to the two synchronized nodes. Based on the secure remote synchronization, secure key distribution in nonlinear networks is explored and moreover the performance analysis is presented. Our results suggest a new network-based solution for secure key distribution directly built on physical principle.

2. The network model

Mathematically, a network could be described as a graph $g = (V(g), E(g))$ with vertex set $V(g)$ and edge set $E(g)$, where vertices are called to be adjacent if there is an edge between them. The symmetry is

[*] Corresponding author.
E-mail addresses: liyuezhang1989@126.com, liyuezhang@my.swjtu.edu.cn (L. Zhang).

https://doi.org/10.1016/j.optcom.2018.02.057
Received 9 December 2017; Received in revised form 23 February 2018; Accepted 24 February 2018

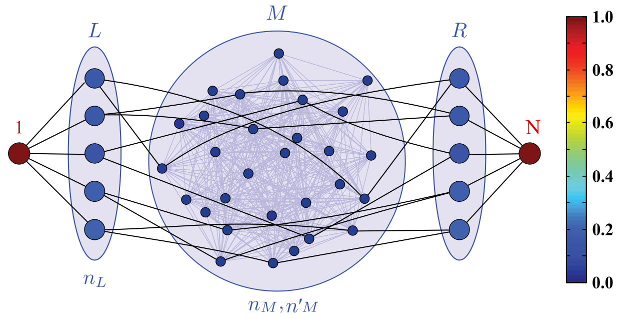

Fig. 1. Structure for mirror-symmetric networks allowing secure remote synchronization.

a permutation of the vertices of the network which preserves adjacency. Once all the symmetries of the network are identified, one can partition the nodes of the graph to clusters by finding the orbits of the symmetry group. The orbit of the symmetry group are the disjoint sets of nodes that when all of the symmetry operations are applied permute among one another, and the nodes had same orbits are defined in the same cluster. As shown in Fig. 1, the topology of network for secure remote synchronization is mirror-symmetric, and the nodes are designed to be in the same cluster to realize remote synchronization. Given n_M, n_L, (and $n_R = n_L$) nodes in M, L, and R, respectively, the generating algorithm of networks are provided as follows. We firstly generate a random network M with n_M nodes with probability p. Then, all nodes in L will be connected node 1 and all the other nodes in R are connected to node N. After that the nodes in L and nodes in R will be paired up. Finally, we connect each of pair of these nodes to n'_M nodes randomly chosen from M. Such network has a mirror symmetry, groups (1, L) and (N, R) are "mirror images" of each other. More precisely, the network structure is invariant under a node permutation that serves the role of a "reflection" and maps each node in groups (1, L) to a unique node in groups (N, R) , but does not move any nodes in M.

3. Theoretical results and discussion

To illustrate secure remote synchronization, we use the electro-optic system [15,8] and focus on the mirror-symmetric network model defined above with specific parameters. The system dynamics is governed by

$$\theta_i^{t+1} = \left[\beta I\left(\theta_i^t\right) + \sigma \sum_{j=1}^{N} A_{ij} I\left(\theta_j^t\right) + \delta\right] \bmod 2\pi, \tag{1}$$

where θ_i^t is the phase shift in time step t for the ith component of the spatial light modulator array, σ is the overall coupling strength, $A = (A_{ij})_{1\leq i,j\leq N}$ is the coupling matrix representing an undirected unweighted network topology of the type illustrated in Fig. 1, β is the strength of self-feedback coupling for the array components, and the offset δ is introduced to suppress the trivial solution, $\theta_i^t \equiv 0$. We set $\delta = 0.525$ for all computations for this system. The intensity of light is related to spatially dependent phase shift θ through the nonlinear function $I(\theta) = [1 - \cos(\theta)]/2$.

Within this framework, we define remote synchronization as a state in which $\theta_1(t) = \theta_N(t)$ for all t, nodes 1 and N are not directly connected, and the time series $\theta_i(t)$ and $\theta_j(t)$ are statistically incoherent with each other for all combinations of $i = 1, N$ and $j = 2, \ldots, N-1$. Any such state can always be written as cluster synchronous state, $s_k(t)_{1\leq k\leq K}$, where $\theta_i(t) = s_k(t)$ for all t if node i belongs to cluster C_k, $k = 1, \ldots, K$, with nodes 1 and N forming C_1. Note that some clusters among $C_2, \ldots, C_K$ may consist of a single node. The color of nodes in Fig. 1 represents the cross correlation function between each node and the reference node 1. As the node N is in the same cluster with node 1, and they are complete synchronized, the color of node N is red, indicating that the cross correlation function between these two nodes equals to be 1. The cluster synchronization stability of node 1 and N is verified for a given network structure using the method in [10]. We first identify clusters C_k in the network using computational group theory, and then compute the maximum transverse Lyapunov exponent λ_{C_1}, which is associated with the modes of perturbation that destroys the synchronization of cluster C_1. And if $\lambda_{C_1} < 0$, synchronization between nodes 1 and N will be stable.

The dynamics of an isolated oscillator indicated by Lyapunov exponent is shown in Fig. 2(a). For small β, the dynamics of oscillator will converge to a fixed point with $\lambda_{iso} < 0$, and it will become chaotic as $\lambda_{iso} > 0$ with the increment of β. The stability of cluster synchronization for nodes 1 and N is presented in Fig. 2(b), from which we could find that stable cluster synchronization can be achieved with $\lambda_{C1} < 0$ when β is relatively small where the dynamics of isolated oscillator is stable point or periodic. Moreover, Fig. 2(c) shows that, even when we start with oscillators that are not chaotic in isolation, the dynamics of clusters can always be chaotic with relative strong coupling strength, wherein λ is the maximum Lyapunov exponent parallel to the synchronization manifold (associated with perturbations that do not destroy synchronization of any cluster C_k), and if $\lambda > 0$, the dynamics of these nodes are chaotic. The stability of cluster synchronization and the dynamics of clusters as the function of coupling strength σ are presented in Fig. 2(d–e), and it is shown that stable chaotic cluster synchronization can be achieved with the increment of σ. It is clear that there is a wide range of the parameters for which the network could realize stable chaotic cluster synchronization.

Using the specific setting of parameters, such as $\beta = 1.5$ and $\sigma = 1.5$, the secure remote synchronization in the electro-optic networks could be demonstrated as shown in Fig. 3. The statistical coherence between cluster C_1 (nodes 1 and N) and all the other nodes in network is measured by cross correlation and mutual information, accounting for possible coherence with a time lag Δt. We use $C_{i,j}$ to denote the absolute value of the correlation coefficient between $\theta_i(t)$ and $\theta_j(t + \Delta t)$ over a range of t, maximized over a range of Δt [16]. Likewise, we use $I_{i,j}$ to denote the mutual information between $\theta_i(t)$ and $\theta_j(t + \Delta t)$ over t, maximized over Δt [16–18]. The mathematical forms of $C_{i,j}$ and $I_{i,j}$ are given as follows:

$$C(\triangle(t)) = \frac{\left\langle \left[S_i(t) - \langle S_i(t)\rangle\right] \cdot \left[S_j(t+\triangle(t)) - \left\langle S_j(t+\triangle(t))\right\rangle\right]\right\rangle}{\sqrt{\left\langle \left[S_i(t) - \langle S_i(t)\rangle\right]^2\right\rangle \cdot \left\langle \left[S_j(t+\triangle(t)) - \left\langle S_j(t+\triangle(t))\right\rangle\right]^2\right\rangle}} \tag{2}$$

$$H(\triangle(t)) = \mathbb{E}\left(log\left(\frac{f_{XY}(x,y)}{f_X(x) f_Y(y)}\right)\right) \tag{3}$$

where $\langle\cdot\rangle$ denotes time average, $\mathbb{E}$ is the expectancy operator and f is the probability density function. The two variables X and Y are obtain from the chaotic dynamics of clusters in the network and can be represented as $S_i(t)$ and $S_j(t + \triangle t)$. For a given value $\triangle t$, the $C(\triangle(t))$ measures the tendency of cloud of points $(S_i, S_j(t + \triangle t))$ to be aligned along a straight line and thus measures a linear relationship between S_i and S_j. And $C_{i,j} = |\max\{C(\triangle t)\}|$ represents the maximum linear coherence in the whole range of $\triangle t$ for all clusters. On the other hand, the mutual information corresponds intuitively to the quantity of information that the two random variables are sharing, and $C_{i,j}$, $I_{i,j} = \max_j\{H(\triangle t)\}$ represents the maximum nonlinear coherence in the whole range of $\triangle t$.

As shown in Fig. 3(a), zero-lag synchronization between the phase of the nodes 1 and 42 is achieved, which could be selected as communicate cluster to realize remote key distribution. The absolute maximum of cross-correlation function and mutual information are 1 and 8.436 at $\Delta t_{max} = 0$, which are shown in Fig. 3(d) and (g), respectively. Moreover, the correlation between nodes in communicate cluster and the other parts of network are shown in the other subfigures of Fig. 3. As shown