Paper:

Synchronization of positive networks with impulsive control under false data deception attacks

Kai Zhou*, Yijun Zhang, Zhiqiang Chen*****

School of Automation, Nanjing University of Science and Technology, Nanjing 210094, P.R. China.
Email:*zhoukainjust@163.com, **zhangyijun@njust.edu.cn, ***zqchen@njust.edu.cn

[Received 2022/05/13; accepted 2022/07/22]

The aim of this paper is to investigate the synchronization of a network, which consists of a set of positive systems. The false data deception attacks are involved in the communication channels which will destroy the data completeness of the considered network. Distinguished from general networks, the condition retaining positivity of the interconnected positive systems is firstly considered. Considering constraints on the positivity of the systems, a distributed impulsive control approach is proposed to solve the synchronization issue of the network. A data detector is designed as well in the sensor. By rigorous mathematical analysis, a sufficient condition for the mean-square bounded synchronization of continuous-time positive systems is provided. Finally, the effectiveness of main results is illustrated by a specific numerical example.

Keywords: Bounded synchronization, positive systems, false data deception attacks, impulsive controller, data detector

1. Introduction

In practice, there exist many industrial processes that can be modeled as dynamic systems. These dynamic systems complete information transmission by a communication network to fulfill some control tasks such as synchronization, formation, collaboration. Therefore, these industrial processes are also called as complex networks. Interestingly, some dynamic systems can be considered as positive systems. A positive system is one in which both initial state and control input are non-negative, as well as output variables and state variables. In addition, because of the property of these dynamic systems, it is required that the state of the system be guaranteed to be positive at all times while satisfying the control requirements. Therefore, it is worth discussing that using the properties of the positive system copes with the control problem of the network composed of positive systems.

The modeling and theoretical analysis of positive systems are different from regular systems because of the properties of positive systems. The necessary and sufficient conditions of asymptotic stability of nonnegative and compartmental dynamical systems with time delay are presented in [1] by using linear Lyapunov-krasovskii functionals. This linear co-positive Lyapunov function has received considerable attention [2–6], because it brings convenience in the calculation, compared with the conventional quadratic Lyapunov function. Besides, scholars have become very interested in the observer design of the positive system, and a co-positive Lyapunov function has also been well applied. Based on a linear programming method, a positive observer design of linear positive systems was designed in [7]. At the same time, the observer error system is exponentially stable, due to new design approaches for positive observers of linear positive systems.

A network-based filter system model [8] was proposed to estimate the variables of a positive system for the L_1-gain filtering problem of positive linear continuous-time systems, which includes event-triggered network communication channels. Similarly, using the linear Lyapunov method, a sufficient condition to ensure the existence of the L_1-gain filter was derived. Furthermore, the resilient estimation of a positive system was investigated. A linear programming approach was also constructed to achieve the demand of the desired distributed estimators. Positive nonlinear semi-Markovian switching systems (MSSs) was studied and a positive observer was designed further in [9]. Different from the LP method, the expansion of Taylor formula and the fuzzy Lyapunov function approach was proposed, which led to a solution to problems about semi-Markovian switching parameters, positivity, Takagi-Sugeno (T-S) fuzzy, and external disturbance in a unified framework. On the other hand, the synchronization problem of positive multi-agent systems has also been concerned. Each agent of the positive system communicates through the network to realize data transmission and construct a positive multi-agent systems network further. When the state of each agent in the network tends to be the same, it indicates that the multi-agent is synchronized with the system. In [10], the positive consistency problem of multi-agent systems with directed communication topology was studied. According to the properties of the linear positive system and spectral theory, using linear matrix inequality (LMI) techniques, some necessary and sufficient conditions for positive consistency of directed multi-agent systems are derived. For the case of sector input nonlinearities in the positive system, Su [11] made use of the nonlinear input and convex optimization method to

obtain feedback matrices, which is solved by quadratic matrix inequalities. In addition, based on the definition and topology of the line graph, Su also investigated the positive edge-consensus problem and then studied problems related to constraint conditions of positive systems themselves [12–14]. However, in these studies, linear systems are usually in the majority. Conversely, nonlinear positive systems are seldom considered, which leads to lacking accurate dynamical models of nonlinear positive systems and corresponding theorem of positivity and synchronization. Due to the positivity of multi-agent positive systems, it is difficult to design the controller, thus realizing synchronization.

On the other hand, cyber attacks in complex networks are worth being considered. Generally, network attackers can be divided into three types from the perspective of engineering: 1) deception attack, which destroys data integrity by tampering with packets; 2) a denial of service (DoS) attack, which damages data availability by blocking the flow of information between different components of a network system; 3) A replay attack. A replay attack is a natural strategy in which a valid data transfer is maliciously or fraudulently repeated or delayed. Scholars have also made many contributions to the above cyber attacks. In [15], the multi-agent systems under DoS attacks from different adversaries were considered and the secure consensus of these systems was also dealt with. From the perspective of the defenders to consider, the event-triggered mechanism has been chosen as one of the means to resist cyber attacks, such as [16–18]. Besides, adaptive strategies have been also applied to counter cyber attacks. For example, in [19], an adaptive strategy was used to update coupling weights and gains for ensuring cluster synchronization under DoS attack in the control channels. [20] designed an adaptive stochastic attacks detector to detect the stochastic attack signals acting on the actuator. Interestingly, some scholars tried to impose impulsive control, solving the synchronization of complex networks with cyber attacks. The event-triggered impulsive control [21] was studied to realize the stability of complex networks under the DoS attacks and deception attacks, which are independent. However, the dynamical model of complex networks composed of positive systems under cyber attacks is not still investigated and a corresponding design to achieve synchronization is not proposed as well. It is noteworthy that false data deception attacks tend to destroy the positivity of the positive systems in the above networks.

The issue studied in this paper is on the synchronization problem of complex networks composed of positive systems under the deception attacks. In the complex networks, the dynamic models of the deception attacks are described by Bernoulli distribution stochastic variables. Aiming at protecting the destruction of positivity of the above systems by deception attacks, a data detector is designed in the sensor. Besides, the distributed impulsive controller is designed, and mean-square bounded synchronization under deception attacks is studied. The sufficient conditions of this problem are also given by using the quadratic Lyapunov function.

The remainder of this article is organized as follows. Section 2 gives the problem formulation of a complex network composed of positive systems and description of deception attacks in a communication network. In Section 3, a sufficient condition realizing mean-square bounded synchronization is proposed, and crucial proof about it is given. In Section 4, a concrete numerical example is presented to demonstrate the effectiveness of the conclusion. Finally, Section 5 sums up this article.

Notations: $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. $\|\cdot\|$ stands for either Euclidean vector norm or its induced matrix 2-norm. For the matrix $A=[a_{ij}]_{n\times m}\in\mathbb{R}^{n\times m}$, the notation $A>0(A\geq 0)$ means the matrix A is positive define (nonnegative define). The notation $A\succ 0(A\succeq 0)$ means $a_{ij}>0(a_{ij}\geq 0)$. $\lambda_{max}(A)$ represents the maximum eigenvalue of the matrix A. $|A|$ represents $|A|=[|a_{ij}|]_{n\times m}$. $\otimes$ represents the Kronecker product. Prob{a} and $\mathscr{E}\{a\}$ are the probability and the expectation of the stochastic variable a, respectively. For matrix $B=[a_{ij}]_{N\times N}\in\mathbb{R}^{N\times N}$, it is a Metzler matrix if the off-diagonal elements of B are nonnegative.

2. Preliminaries And Problem Formulation

2.1. A complex network composed of positive systems

First, some basic concepts and significant results from algebraic graph theory are introduced.

The interaction topology of the sensors is described by an undirected graph $\mathscr{G}=(\mathscr{V},\varepsilon,\mathscr{A})$, where vertices set $\mathscr{V}=\{1,2,\cdots,N\}$ denotes the index set of distributed sensors and $\varepsilon\subseteq\mathscr{V}\times\mathscr{V}$ denotes the set of edges connecting the paired sensor nodes. $\mathscr{A}=[a_{ij}]_{N\times N}\in\mathbb{R}^{N\times N}$ is called the adjacency matrix of $\mathscr{G}$, which is defined as $a_{ij}=1$ if $(i,j)\in\varepsilon$, otherwise $a_{ij}=0$. The Laplacian matrix of graph $\mathscr{G}$ is denoted as $\mathscr{L}\triangleq\mathscr{D}-\mathscr{A}$, where $\mathscr{D}\triangleq\text{diag}\{\deg(1),\deg(2),\ldots,\deg(N)\}$ and $\deg(i)=\sum_{j=1}^{N}a_{ij}$.

A complex network with internal nonlinear dynamic characteristics consists of n agents, which models are described as:

$$\dot{x}_i(t)=Ax_i(t)+Wf(x_i(t))+u_i(t) \quad .\ .\ .\ .\ . \quad (1)$$

where $x_i(t)\in\mathbb{R}^m$ is state vector of the ith agent; $u_i(t)\in\mathbb{R}^m$ is input control of the ith agent, and $f:\mathbb{R}^m\to\mathbb{R}^m$ is a nonlinear function. A,W are the known system matrices of appropriate dimensions.

Definition 1: [22] The system (1) is a positive system if the output and state of system are non-negative for every non-negative $x_i(0)$ and $u_i(0)$ and for every $f(x_i(0))\geq 0$.

Lemma 1: [22] The system (1) is said to be positive if and only if A is a Metzler matrix and W is a nonnegative matrix.

Assumption 1: [23] Positive nonlinear function $f(\cdot)$ in (1), which means $f(x)\geq 0,\forall x\geq 0$, satisfies Lipschitz conditions , i.e., $\forall x_1,x_2\in\mathbb{R}^n$

$$(x_1-x_2)^T(f(x_1)-f(x_2))\leq\vartheta(x_1-x_2)^T(x_1-x_2),(2)$$

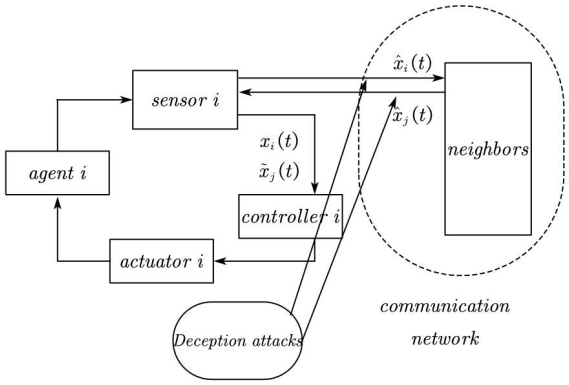


Fig. 1. : Deception attacks in the communication network

where $\vartheta > 0$ is a known constant.

2.2. Deception attack in communication network

Deception attacks refer to injecting or tampering with the signal in communication channels in most cases. In this paper, the information transmission between sensors is carried out by a communication network. Assume that deception attacks, satisfying the Bernoulli distribution, occur during information transmission, as shown in Fig.1. The Bernoulli distributed random variable $\beta_j(t)$ ($j = 1,2,\ldots,N$) associated with deception attack from sensor j is also proposed. The deception attack is defined as follow:

$$\beta_j(t) = \begin{cases} 1, & \text{with deception attacks} \\ 0, & \text{without deception attacks} \end{cases} \quad . \; . \quad (3)$$

Furthermore, the probability of $\beta_j(t)$ satisfies the following conditions: $\text{Prob}\{\beta_j(t) = 1\} = \beta$, $\text{Prob}\{\beta_j(t) = 0\} = 1-\beta$, with the known constant $\beta \in [0,1]$.

Assumption 2: The stochastic variables $\beta_j(t)$ ($j = 1,2,\ldots,N$) are independent.

Define $\zeta(t) \in \mathbb{R}^m$ is the attack signal from cyber attackers. Based on the energy limitation of attackers, it is reasonable to assume that $\|\zeta(t)\|^2 \le \ell$ where ℓ is a known positive constant. Under the deception attack, the data $\hat{x}_j(t)$ from sensor j to sensor i can be written as:

$$\hat{x}_j(t) = \alpha_j(t)x_j(t) + \beta_j(t)\zeta_j(t) \quad . \; . \; . \; . \; . \; . \quad (4)$$

where $\alpha_j(t) = 1-\beta_j(t)$. Similarly, $\text{Prob}\{\alpha_j(t) = 1\} = \alpha = 1-\beta$, $\text{Prob}\{\alpha_j(t) = 0\} = 1-\alpha = \beta$. Because of the existence of deception attack, the nonnegativity of the data $\hat{x}_j(t)$ can not be guaranteed, and system (1) dissatisfies Definition 1 further. Consequently, a data detector is designed in the sensor. The data detector in sensor i is used to guarantee the positivity of data $\hat{x}_j(t)$. The effect of the data detector can be described as:

$$\tilde{x}_j(t) = \begin{cases} \hat{x}_j(t), & \hat{x}_j(t) \succeq 0 \\ |\hat{x}_j(t)|, & \text{others} \end{cases} \quad . \; . \; . \; . \; . \; . \; . \quad (5)$$

Define $\hat{\zeta}_j(t) = |\zeta_j(t)|$, and $\tilde{x}_j(t)$ can be written as : $\tilde{x}_j(t) = \alpha_j(t)x_j(t) + \beta_j(t)\hat{\zeta}_j(t)$. Then, data $\tilde{x}_j(t)$ in sensor i is sent to the controller i. A distributed impulsive controller is designed as:

$$u_i(t) = \sum_{k=1}^{\infty} K\left(\sum_{j=1}^{n} a_{ij}\left(\alpha_j(t)x_j(t) + \beta_j(t)\hat{\zeta}_j(t) - x_i(t)\right)\right) \times \delta(t-t_k) \quad . \; . \; . \; . \; . \; . \; . \; . \quad (6)$$

where $\delta(\cdot)$ is the Dirac function which will take effect at the instance $t = t_k$, and periodic impulsive sequence $\{t_k\}_{k=1}^{\infty}$ satisfies $t_k = kT, k \in \mathbb{N}^+$, with known sampling period T and $t_0 = 0$. $K \in \mathbb{R}^{m\times m}$ is a control matrix.

The following lemma and definition are needed to conclude our main results.

Lemma 2: [24] Let $\mathscr{D}$ and $\mathscr{S}$ be real matrices of appropriate dimensions and a constant ε be positive, then for any vectors x and y with appropriate dimensions, it has :

$$2x^T\mathscr{D}^T\mathscr{S}y \le \varepsilon x^T\mathscr{D}^T\mathscr{D}x + \frac{1}{\varepsilon}y^T\mathscr{S}^T\mathscr{S}y \quad . \; . \; . \quad (7)$$

Definition 2: [25] (Mean-square Bounded Synchronization under Deception Attack) The complex network (10) are said to achieve mean-square bounded synchronization if there exists a positive constant $\hbar > 0$ and a compact set $\mathscr{C}$, for $\forall x_i(0)$, let $e_i(t) = x_i(t) - x_1(t), i = 2,\ldots,n$ converge to the set:

$$\mathscr{C} = \left\{e(t) \in \mathbb{R}^{(n-1)m} | \mathscr{E}\{\|e(t)\|^2\} \le \hbar\right\} \quad . \; . \; . \quad (8)$$

as $t \to \infty$, where $e(t) = [e_2^T(t),\cdots,e_n^T(t)]^T$.

3. Main Results

The theorem given in this section will guarantee the positivity of the complex network (10) and achieve synchronous control.

We consider the positivity of the systems in the network firstly. With the above-proposed control protocol (6), the system (1) can be written as :

$$\begin{cases} \dot{x}_i(t) = Ax_i(t) + Wf(x_i(t)), t \ne t_k \\ \Delta x_i(t_k) = x_i\left(t_k^+\right) - x_i\left(t_k^-\right) = \\ K\sum_{j=1}^{n} a_{ij}(\alpha_j(t)x_j(t) + \beta_j(t)\hat{\zeta}_j(t) - x_i(t)), t = t_k \end{cases} \quad (9)$$

where $x_i(t_k^+) = \lim_{h\to 0+} x_i(t_k+h)$, $x_i(t_k^-) = \lim_{h\to 0-} x_i(t_k+h)$, and $x_i(t)$ is right-hand continuous at $t = t_k$. Denote $x(t) = [x_1^T(t), x_2^T(t),\cdots,x_n^T(t)]^T$, $f(x(t)) = [f^T(x_1(t)), f^T(x_2(t)),\cdots,f^T(x_n(t))]^T$ and $\hat{\zeta}(t) = [\hat{\zeta}_1^T(t),\hat{\zeta}_2^T(t),\cdots,\hat{\zeta}_n^T(t)]$. Similarly, the dynamic models of the complex network can be described as :

$$\begin{cases} \dot{x}(t) = \\ I_n \otimes Ax(t) + I_n \otimes Wf(x(t)), t \ne t_k \\ \Delta x(t_k) = \\ (\bar{\mathscr{A}} - D) \otimes Kx(t_k^-) + \check{\mathscr{A}} \otimes K\hat{\zeta}(t), t = t_k \end{cases} \quad . \; . \quad (10)$$

where $\bar{\mathscr{A}} = [a_{ij}\alpha_j]_{n\times n}$, $\check{\mathscr{A}} = [a_{ij}\beta_j]_{n\times n}$. It can be seen

that the systems in (10) are positive, if $\Delta x(t_k) \succeq 0$.

Remark 1: In the previous design of a multi-agent synchronization controller, the data of the adjacent agent is usually used to achieve synchronization control. But for the complex network (10), when considering the synchronous control of the system, we also need to consider whether the synchronous controller will damage the positivity of the systems in the network. In (10), through the data detector, the data false deception attack is separated. Positivity of the systems in the network is ensured by constraints on the control matrix K, and the proof is given further.

Theorem 1: Considering all cases of $\bar{\mathscr{A}}$ and $\check{\mathscr{A}}$ resulting from the stochastic variables $\beta_j(t)$, the systems in the complex network (10) are positive if satisfying the following inequalities:

$$\begin{cases} I_n \otimes I_m - D \otimes K \succeq 0 \\ K \succeq 0 \end{cases} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (11)$$

Proof: It is easy to check that, if $t \neq t_k$, the systems in the complex network (10) are positive according to Lemma 1.

We consider the boundary case. For the case $t = t_k$, the complex network can be written as:

$$\begin{aligned} x(t_k) = &((\bar{\mathscr{A}} - D) \otimes K + I_n \otimes I_m) x(t_k^-) \\ &+ I_n \otimes W f(x(t_k^-)) + \check{\mathscr{A}} \otimes K \hat{\xi}(t_k) \quad . \quad . \quad (12) \end{aligned}$$

Considering that $x(t_k^-) \geq 0$ and $\hat{\xi}(t_k) \geq 0$, to ensure $x(t_k) \geq 0$, the terms $(\bar{\mathscr{A}} - D) \otimes K + I_n \otimes I_m$, $\check{\mathscr{A}} \otimes K$ and $I_n \otimes W$ should be positive. For the matrix $\check{\mathscr{A}} \otimes K$, it can be seen that $K \succeq 0$ is sufficient to ensure $\check{\mathscr{A}} \otimes K \succeq 0$. For the randomness caused by $\beta_j(t)$, we consider the critical case. $(\bar{\mathscr{A}} - D) \otimes K + I_n \otimes I_m \succeq 0$ is satisfied if K guarantees $-D \otimes K + I_n \otimes I_m \succeq 0$. From (11), we conclude that the systems in the complex network (10) are positive. □

Remark 2: A continuous synchronous controller has been proved in [26], but it requires the ideal network communication. However, according to the author's research, there are few conclusions for the discontinuous controller. Therefore, the impulsive control not only ensures the positivity of the system but also provides a controller selection for the follow-up study of the positive systems.

Since $e_i(t) = x_i(t) - x_1(t)$, the error system of the complex network (10) under deception attacks is rearranged as:

$$\begin{cases} \dot{e}(t) = I_{n-1} \otimes Ae(t) + I_{n-1} \otimes W\eta(t), t \neq t_k \\ \Delta e(t) = (\bar{\mathscr{L}}_{22} + 1_{n-1}\bar{\alpha}) \otimes Ke(t_k^-) \\ \quad + (\check{\mathscr{A}}_{22} - 1_{n-1}\check{\alpha}) \otimes K\hat{\xi}(t_k^-), t = t_k \end{cases} . \quad (13)$$

where $1_{n-1} = [1]_{(n-1)\times 1}$, and

$$\begin{aligned} &\eta(t) = [f^T(x_2(t)) - f^T(x_1(t)), \cdots, \\ &f^T(x_n(t)) - f^T(x_1(t))]^T, \\ &\bar{L} = \bar{\mathscr{A}} - D = [\bar{l}_{ij}]_{n\times n}, \\ &\bar{\alpha} = [\bar{l}_{12}, \bar{l}_{13}, \cdots, \bar{l}_{1n}], \\ &\check{\alpha} = [a_{11}\beta_1, a_{12}\beta_2, \cdots, a_{1n}\beta_n], \end{aligned}$$

$$\bar{\mathscr{L}}_{22} = \begin{pmatrix} \bar{l}_{22} & \bar{l}_{23} & \cdots & \bar{l}_{2n} \\ \bar{l}_{32} & \bar{l}_{33} & \cdots & \bar{l}_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ \bar{l}_{n2} & \bar{l}_{n3} & \cdots & \bar{l}_{nn} \end{pmatrix},$$

$$\check{\mathscr{A}}_{22} = \begin{pmatrix} a_{21}\beta_1 & a_{22}\beta_2 & \cdots & a_{2n}\beta_n \\ a_{31}\beta_1 & a_{32}\beta_2 & \cdots & a_{3n}\beta_n \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}\beta_1 & a_{n2}\beta_2 & \cdots & a_{nn}\beta_n \end{pmatrix},$$

Denote $\mathscr{F} = \bar{\mathscr{L}}_{22} + 1_{n-1}\bar{\alpha}$, $\mathscr{Q} = \check{\mathscr{A}}_{22} - 1_{n-1}\check{\alpha}$, and denote $\tilde{\mathscr{F}} = \mathscr{E}\{\mathscr{F}\}$, $\tilde{\mathscr{Q}} = \mathscr{E}\{\mathscr{Q}\}$. The error system (13) can be rewritten as :

$$\begin{cases} \dot{e}(t) = I_{n-1} \otimes Ae(t) + I_{n-1} \otimes W\eta(t), t \neq t_k \\ \Delta e(t) = \mathscr{F} \otimes Ke(t_k^-) + \mathscr{Q} \otimes K\hat{\zeta}(t_k^-), t = t_k \end{cases} . \quad (14)$$

Theorem 2: On the premise of Theorem 1, under Assumption 1 and 2, for given nonnegative scalars T, the complex network (10) is said to achieve a mean-square bounded synchronization, if there exists $\varepsilon > 0$ in (4), ϑ in (2), satisfying the following inequality:

$$2\lambda_1 T + \ln\mu < 0 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (15)$$

where

$$\begin{aligned} &\lambda_1 = \lambda_{max}(A + \vartheta W), \\ &\mu = (\varepsilon + 1)\lambda_{\mathscr{F}}, \\ &\xi = \frac{n}{2}(1 + \frac{1}{\varepsilon})\lambda_{\mathscr{Q}}\ell, \\ &\lambda_{\mathscr{F}} = \\ &\lambda_{max}((\tilde{\mathscr{F}} \otimes K + I_{(n-1)m})^T(\tilde{\mathscr{F}} \otimes K + I_{(n-1)m})), \\ &\lambda_{\mathscr{Q}} = \lambda_{max}((\tilde{\mathscr{Q}} \otimes K)^T\tilde{\mathscr{Q}} \otimes K). \end{aligned} \quad (16)$$

Remark 3: In this paper, with parameters ϑ and ε determined, the value of the controller K can be constrained using the above inequalities (11) and (15), and can be further calculated.

We chose the Lyapunov function as follows:

$$V(t) = \frac{1}{2}e^T(t)e(t) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (17)$$

For $t \in [t_{k-1}, t_k)$, the derivative of $V(t)$ can be obtained:

$$\begin{aligned} \dot{V}(t) &= e^T(t)[I_{n-1} \otimes Ae(t) + I_{n-1} \otimes W\eta(t)] \\ &\leq e^T(t)(I_{n-1} \otimes A + I_{n-1} \otimes \vartheta W)e(t) \\ &\leq \lambda_1 e^T(t)e(t) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (18) \end{aligned}$$

According to the above inequality (18), we can get:

$$\mathscr{E}\{\dot{V}(t)\} \leq 2\lambda_1 \mathscr{E}\{V(t)\} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (19)$$

Integrating the above inequality from t_{k-1} to t_k, we have :

$$\begin{aligned} &\mathscr{E}\{V(t)\} \\ &\leq \exp(2\lambda_1(t - t_{k-1}))\mathscr{E}\{V(t_{k-1})\}, t \in [t_{k-1}, t_k) \end{aligned} \quad (20)$$

Through some analysis and derivation, it can be obtained for $t \in [t_{k-1}, t_k)$, (The details are omitted here due to the page limitation.)

$$\begin{aligned} &\mathscr{E}\{V(t)\} \\ &\leq \frac{1}{\mu}\exp((2\lambda_1 + \frac{\ln\mu}{T})(t - t_0))\mathscr{E}\{V(t_0)\} \end{aligned}$$

$$
\begin{aligned}
&+\frac{\xi\exp(2\lambda_1(t-t_{k-1}))}{1-\exp(2\lambda_1 T+\ln\mu)}\\
&-\frac{\xi\exp(2\lambda_1(t-t_0)+(k-1)\ln\mu)}{1-2\exp(2\lambda_1 T+\ln\mu)}\\
\le\ &\frac{1}{\mu}\exp((2\lambda_1+\frac{\ln\mu}{T})(t-t_0))\mathscr{E}\{V(t_0)\}\\
&+\frac{\xi\exp(2\lambda_1 T)-\xi\exp((2\lambda_1 T+\ln\mu)(k-1))}{1-\exp(2\lambda_1 T+\ln\mu)}
\end{aligned}
$$

When $k\to\infty$, if (15) is satisfied, the following results can be further obtained:

$$
\begin{aligned}
&\lim_{k\to\infty}\frac{1}{\mu}\exp((2\lambda_1+\frac{\ln\mu}{T})(t-t_0))\mathscr{E}\{V(t_0)\}=0\\
&\lim_{k\to\infty}\frac{-\xi\exp((2\lambda_1 T+\ln\mu)(k-1))}{1-\exp(2\lambda_1 T+\ln\mu)}=0
\end{aligned}
\qquad (21)
$$

Therefore, with $\mathscr{E}\{\|e(t)\|^2\}=2\mathscr{E}\{V(t)\}$, the error system (14) will converge to the ball

$$
\begin{aligned}
&\mathscr{C}=\{e(t)\in\mathbb{R}^{(n-1)m}|\\
&\mathscr{E}\{\|e(t)\|^2\}\le\frac{2\xi\exp(2\lambda_1 T)}{1-\exp(2\lambda_1 T+\ln\mu)}\}
\end{aligned}
\qquad \ldots (22)
$$

From Definition 2, we come the the conclusion that the complex network (10) achieves a mean-square bounded synchronization.

4. Numerical Examples

Consider the complex network (1) coupled by six nodes. The undirected topology $\mathscr{G}$ is shown in Fig.2. Its adjacency matrix $\mathscr{A}$ is

$$
\begin{bmatrix}
0 & 1 & 0 & 1 & 1 & 0\\
1 & 0 & 1 & 0 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 1\\
1 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 0 & 1 & 0 & 1\\
0 & 1 & 1 & 0 & 1 & 0
\end{bmatrix}
$$

For $i=1,2,\ldots,6$, the dynamic model of the ith node is described as,

$$
\begin{aligned}
\dot{x}_i(t)=&\begin{bmatrix}-0.5 & 0.2\\ 0.1 & -0.2\end{bmatrix}x_i(t)+u_i(t)\\
&+\begin{bmatrix}0.1 & 0.2\\ 0.3 & 0.1\end{bmatrix}\begin{bmatrix}\tanh 0.015x_{i1}\\ \tanh 0.015x_{i2}\end{bmatrix}
\end{aligned}
\qquad \ldots (23)
$$

It is easy to check that the nonlinear function $f(\cdot)$ satisfies Assumption 1 with $\vartheta=0.015$. Let $T=0.05s$, $\mathrm{Prob}\{\beta_j=1\}=0.2$, $\mathrm{Prob}\{\beta_j=0\}=0.8$, $\varepsilon=0.01$. We assume the deception attack signal to be $\zeta_j(t)=[0.2\sin t;\ 0.1+0.4\sin t]$ and $\ell=0.29$. It can be checked that (11) is satisfied. According to Theorem 1, the positivity of the systems (23) is ensured. We further check that (15) is satisfied as well, which implied that the complex network achieves the bounded synchronization in accordance with Theorem 2. Mean while, the control matrix K can be gained as

$$
K=10^{-3}\begin{bmatrix}0.9550 & 0\\ 0 & 0.9545\end{bmatrix}.
$$

The following parameters can be calculated, i.e., $\lambda_1=-0.1394$; $\mu=1.0129$; $\xi=4.064\times10^{-5}$. Substituting these parameters into (22), the radius of compact set $\mathscr{C}$ is achieved as $\hbar=0.0696$. It can be concluded that the system (23) can achieve the bounded synchronization.

In addition, the numerical simulation of the system (23) also confirms Theorem 1 and 2. Simulation results are as follows. The state $x_{i1}(t)$ with time varying is described in Fig.3. From Fig.3, the systems (23) in the complex network still stay positive under the false data deception attacks. Fig.4 shows the evolutions of $\|e(t)\|^2$ with the initial conditions $x_1(0)=[3,\ 2]$, $x_2(0)=[1,\ 3]$, $x_3(0)=[2,\ 5]$, $x_4(0)=[3,\ 1]$, $x_5(0)=[4,\ 3]$, $x_6(0)=[2,\ 4]$. Through Fig.4, it can be seen that the considered complex network arrives the bounded synchronization under the false data deception attacks.

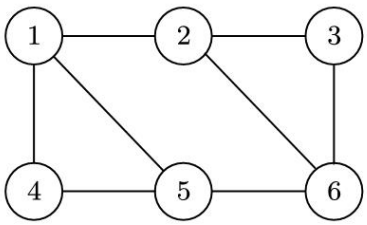


Fig. 2. : Network topology

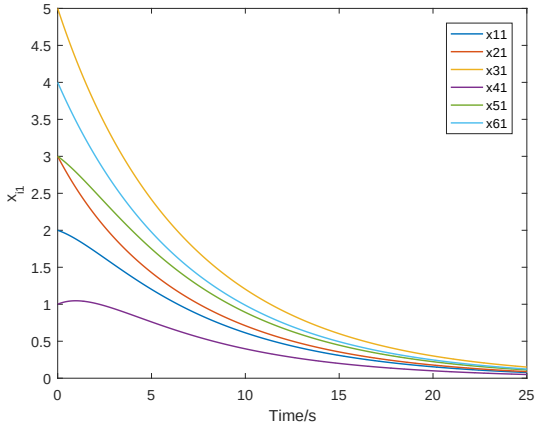


Fig. 3. : State trajectories of $x_{i1}(t)$ under the impulsive control

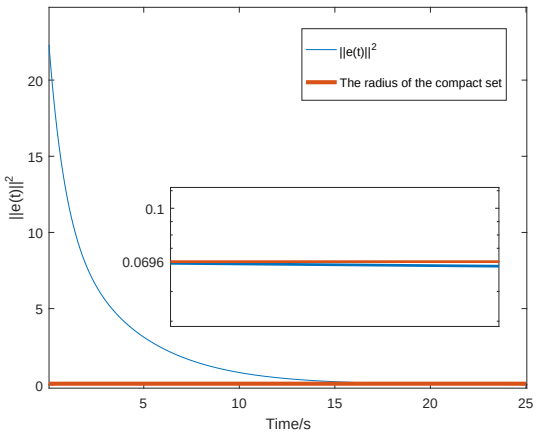


Fig. 4. : The evolution curves of the error system

5. Conclusions

In this paper, the dynamic model of a complex network composed of positive systems under the impulsive control is constructed. Based on the analytical and experimental investigations presented in this paper, the data detector in the sensor ensures the positivity of the systems, although the complex network suffers from the false data deception attacks in sensor-to-sensor channels. Moreover, sufficient conditions of positivity of the systems in the complex network under the periodic impulsive control are proposed. By using the quadratic Lyapunov function, it is feasible for the distributed periodic impulsive controller to achieve the bounded synchronization of the complex network. A specific example is also given aiming at support the theorem. In our future work, under different cyber attacks, the network performance of the complex network composed of positive systems could be investigated. Furthermore, facing the more covert network attacks, it is an interesting topic for researchers to design controllers to ensure the synchronization of networks.

Acknowledgements

This work is supported in part by National Natural Science Foundation of China under grants numbers 61973166.

References:

[1] W. M. Haddad and V. Chellaboina, "Stability theory for nonnegative and compartmental dynamical systems with time delay," *Systems & Control Letters*, vol. 51, no. 5, pp. 355–361, 2004.

[2] F. Blanchini, P. Colaneri, and M. E. Valcher, "Co-positive lyapunov functions for the stabilization of positive switched systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 12, pp. 3038–3050, 2012.

[3] Y. Li and H. Zhang, "New results on stability analysis and estimator design for switched positive linear systems: A reverse-timer-dependent linear co-positive lyapunov function approach," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 697–701, 2021.

[4] P. Wang and J. Zhao, "Feedback dissipativity and stabilization for switched positive systems with a combined switching law," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 11, pp. 2572–2576, 2020.

[5] Y. Ju, X. Zhu, and Y. Sun, "Stability analysis of continuous-time positive switched linear systems," in *2018 18th International Conference on Control, Automation and Systems (ICCAS)*, pp. 1062–1065, 2018.

[6] R. Oubah and A. Benzaouia, "Stability and stabilization of positive takagi-sugeno fuzzy continuous systems with delay by linear programming," in *2016 5th International Conference on Systems and Control (ICSC)*, pp. 90–96, 2016.

[7] L.-J. Liu, X. Zhao, X.-M. Sun, and W. Wang, "New approaches to positive observer design of linear positive systems," in *2017 Chinese Automation Congress (CAC)*, pp. 7195–7198, 2017.

[8] S. Xiao, Y. Zhang, Q. Xu, and B. Zhang, "Event-triggered network-based l_1-gain filtering for positive continuous-time systems," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, pp. 5356–5361, 2016.

[9] W. Qi, J. H. Park, G. Zong, J. Cao, and J. Cheng, "A fuzzy lyapunov function approach to positive L_1 observer design for positive fuzzy semi-markovian switching systems with its application," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 775–785, 2021.

[10] J. J. R. Liu, N. Yang, K.-W. Kwok, and J. Lam, "Positive consensus of directed multi-agent systems," *IEEE Transactions on Automatic Control*, pp. 1–1, 2021.

[11] H. Wu and H. Su, "Observer-based consensus for positive multiagent systems with directed topology and nonlinear control input," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 7, pp. 1459–1469, 2019.

[12] H. Su, H. Wu, and J. Lam, "Positive edge-consensus for nodal networks via output feedback," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1244–1249, 2019.

[13] H. Wu, J. Lam, and H. Su, "Global consensus of positive edge system with sector input nonlinearities," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, pp. 4057–4066, July 2021.

[14] H. Su, H. Wu, X. Chen, and M. Z. Q. Chen, "Positive edge consensus of complex networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 12, pp. 2242–2250, 2018.

[15] S. Du, Q. Yan, L. Dong, and J. Qiao, "Secure consensus of multiagent systems with input saturation and distributed multiple DoS attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, pp. 1–1, 2021.

[16] P. Liu, Z. Huang, and X. Guo, "Event-triggered secure group consensus of second-order multi-agent systems under periodic DoS attacks," in *2021 IEEE 10th Data Driven Control and Learning Systems Conference (DDCLS)*, pp. 1007–1012, 2021.

[17] Y. Yang, Y. Li, D. Yue, Y.-C. Tian, and X. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 6, pp. 2916–2928, 2021.

[18] J. Liu, Y. Wang, J. Cao, D. Yue, and X. Xie, "Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack," *IEEE Transactions on Cybernetics*, vol. 51, no. 8, pp. 4000–4010, 2021.

[19] D. Liu and D. Ye, "Cluster synchronization of complex networks under denial-of-service attacks with distributed adaptive strategies," *IEEE Transactions on Control of Network Systems*, pp. 1–1, 2021.

[20] L. Dong and H. Xu, "Adaptive fuzzy detector-based secure correct control for cyber-physical systems subject to heterogeneous physical attacks," in *2020 39th Chinese Control Conference (CCC)*, pp. 7632–7636, 2020.

[21] Z. Hu and X. Mu, "Event-triggered impulsive control for stochastic networked control systems under cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–10, 2021.

[22] Y. Ohta, "Positive linear systems: theory and applications," *John Wiley*, New York, 2000.

[23] D. Ding, Z. Tang, Y. Wang, and Z. Ji, "Secure synchronization of complex networks under deception attacks against vulnerable nodes," *Applied Mathematics and Computation*, vol. 399, p. 126017, 2021.

[24] J. Wu and L. Jiao, "Synchronization in complex dynamical networks with nonsymmetric coupling," *Physica D: Nonlinear Phenomena*, vol. 237, no. 19, pp. 2487–2498, 2008.

[25] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Information Sciences*, vol. 459, pp. 354–368, 2018.

[26] C. Chen, J. Liang, and A. M. Dobaie, "Synchronization control for multi-linear positive systems," in *2017 Chinese Automation Congress (CAC)*, pp. 5715–5720, 2017.