Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Distributed Tracking Control for Multi-Agent Systems Under Two Types of Attacks ⋆

Zhi Feng and Guoqiang Hu

Abstract: This paper studies a distributed consensus tracking control problem for a class of stochastic linear multi-agent systems subject to two types of attacks. The problem boils down to how to achieve robust consensus tracking of multi-agent systems with switching connected and disconnected directed topologies under attacks. The attacks on the edges instead of nodes lead to the loss of consensus tracking security. Based on a multi-step design procedure for designing a distributed secure algorithm, sufficient conditions on robust mean-square exponential consensus tracking are derived via the idea of average dwell time switching between some stable and unstable subsystems obtained from graph theory analysis. An applicaton to a practical power system is considered. It is proved that each distributed generator (DG) modeled as an agent in a microgrid can successfully synchronize their terminal voltage amplitude to a prespecified reference value under these two types of attacks.

Keywords: Distributed consensus tracking; Linear stochastic agents; Mean-square exponential convergence; Lyapunov function method; Microgrid under attacks.

1. INTRODUCTION

Distributed cooperative control has received increasing attention from various scientific communities due to its broad applications in real-world multi-agent systems, such as transportation, multi-vehicle systems, sensor networks and so on (e.g. see [1, 2, 3], just name a few). The main idea behind this is to obtain an emerging behavior using only local information interactions to eventually achieve an agreement. Surveys of most recent advances can be found in [3, 4]. As an effective consensus seeking approach, consensus tracking problem has attracted important interest [5, 6, 7, 8]. By employing a variable structure approach, [5] investigated the consensus tracking problem for both first and second-order multi-agent systems. The cooperative output regulation problem was addressed in [6] via an internal model method. An identifier-dependent consensus tracking protocol was developed in [7] to achieve robust consensus tracking. Note that the above results mostly focus on multi-agent systems with only single/double-integrator dynamics.

Multi-agent systems usually evolve in uncertain real-world communication environments, like networks with random noises. In reality, the agents might be subject to some Gaussian white noises with certain noise intensity. In this case, the agents are not only affected by the interaction among neighboring agents, but also by its own intrinsic stochastic dynamics. Consensus problems with noise communications have been studied (e.g., see [9, 10], just name a few), while few results on consensus tracking were published, especially for high-order linear multi-agent systems. Recently, a distributed tracking control scheme with distributed estimators has been proposed in [10] to achieve stochastic consensus tracking.

⋆ Z. Feng and G. Hu are with EXQUISITUS, Centre for E-City, School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798. E-mail: zfeng001@e.ntu.edu.sg, gqhu@ntu.edu.sg.

The system security of multi-agent systems is an interesting and important problem. Multi-agent systems, like all large-scale spatially distributed systems, are vulnerable to cyber attacks due to the development of network information and communication technologies. Typically, there are two different attack scenarios in a multi-agent system: dynamic behavior (or closed-loop dynamics) of the agents and communication among the agents. Both of these attacks can dramatically affect the consensus properties of the whole team of agents. Some of the literature concerning this problem has been reported [11, 12, 13, 14, 15]. The authors in [11] studied the design of distributed attack (or fault) detection via a branks of unknown input observers (UIO) for network systems. In [12], a consensus problem was considered for networked multi-agent systems with adversaries. Under the assumption that the network is complete. An attack detection and identification algorithm based on distributed filter was investigated for cyber-physical systems in [14]. In reality, it is more general to consider the second attack scenario that only a number of edges are attacked in the multi-agent systems. In such a case, it is important to study how to design an effective cyber-security control algorithm.

In this paper, a distributed cyber-security control problem is addressed for stochastic linear multi-agent systems under two types of attacks. Relating to the communications (more specifically the connectivity of the communication links) among the agents, the attacks on the edges may lead to the loss of consensus tracking security. By assuming that the paralyzed topologies can be recovered into any connected topologies after a communication restoration mechanism, sufficient conditions on robust mean-square exponential consensus tracking are established if the attack frequency and unavailability length rate of different attacks satisfy certain conditions. A multi-step design procedure is developed for designing the distributed algorithm. Moreover, an application to power system is given to show the effectiveness of the proposed method.

Copyright © 2014 IFAC

2. NOTATION AND PRELIMINARIES

Graph theory[16]: Let $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, A\}$ represent a connected directed graph of order n with the set of nodes $V = \{v_1, v_2, \cdots, v_n\}$, $E \in V \times V$ is the set of edges and $A = [a_{ij}] \in \mathbb{R}^{n\times n}$ denotes the adjacency matrix of $\mathcal{G}$, where $a_{ij} > 0$ if and only if $(j, i) \in E$ else $a_{ij} = 0$. The node indexes belong to a finite index set $N = \{1, 2, \cdots, n\}$. An edge of $\mathcal{G}$ is an ordered pair $(i, j) \in E$ if agent j can be directly supplied with information from agent i. The set of neighbors of node v_i is denoted by $N = \{v_i \in \mathcal{V}, (v_i, v_j) \in \mathcal{E}\}$. Graph $\mathcal{G}$ contains a directed spanning tree if there is a node which can reach all the other nodes through a directed path. A matrix $A = [a_{ij}] \in \mathbb{R}^{n\times n}$ denotes the adjacency matrix of $\mathcal{G}$, where $a_{ij} > 0$ if and only if $(j, i) \in E$ else $a_{ij} = 0$. The Laplacian matrix of a graph $\mathcal{G}$ is defined as $L(A) = D - A \in \mathbb{R}^{n\times n}$, where $D = [d_{ii}]$ is a diagonal matrix with $d_{ii} = \sum_{j=1}^{N} a_{ij}$.

Lemma 1. Denote the Laplacian matrix $L = [l_{ij}]$ where

$$l_{ij} = \begin{cases} \sum\limits_{k=1,k\neq i}^{n} a_{ik} & i = j \\ -a_{ij} & i \neq j. \end{cases}$$

Then, the following statements are true:

(i) Zero is a simple eigenvalue of L, and $\mathbf{1}_n$ is the corresponding eigenvector, that is $L\mathbf{1}_n = 0$.

(ii) If $\mathcal{G}$ has a directed spanning tree, then the eigenvalue 0 is algebraically simple for its Laplacian matrix, and all the other eigenvalues have positive real parts.

Lemma 2. [8] Suppose that matrix $A = [a_{ij}] \in \mathbb{R}^{n\times n}$ has $a_{ij} \leq 0$ for all $i \neq j$, $i, j \in \{1, \cdots, n\}$. Then, the following statements are equivalent:

1) A is a nonsingular M-matrix.

2) There exists a positive definite diagonal matrix $\Theta = diag\{\theta_1^{-1}, \theta_2^{-1}, \cdots, \theta_n^{-1}\}$ such that $Q = A^T\Theta + \Theta A > 0$.

3) All the eigenvalues of A have positive real parts.

3. PROBLEM FORMULATION

Consider a class of $It\hat{o}$ stochastic linear multi-agent systems with the ith agent described as

$$dx_i(t) = [Ax_i(t) + Bu_i(t)]\, dt + f(x_i(t), t)dw_i(t), \quad (1)$$

where $x_i(t) \in \mathbb{R}^l$ is the system state, $u_i(t) \in \mathbb{R}^p$ is the control input, $i = 1, 2, \cdots, n,$, $w_i(t)$ denotes a one-dimensional Brownian motion satisfying $E\{dw_i(t)\} = 0$ and $E\{dw_i^2(t)\} = dt$, $f : \mathbb{R}^l \times [0, +\infty) \to \mathbb{R}$ is a continuously differentiable function, and A and B are constant matrices with compatible dimensions. For simplification, let $f(x_i(t), t) = (f_1(x_i(t), t), f_2(x_i(t), t), \ldots, f_l(x_i(t), t))^T$.

The objective is to design a distributed protocol $u_i(t)$ for system (1) such that all the followers track the leader under two types of attacks. The leader for consensus tracking, labeled as $i = 0$, is generated as

$$dx_0(t) = Ax_0(t)dt + f(x_0(t), t)dw_0(t), \quad (2)$$

where $x_0(t) \in \mathbb{R}^l$ is the state of the leader.

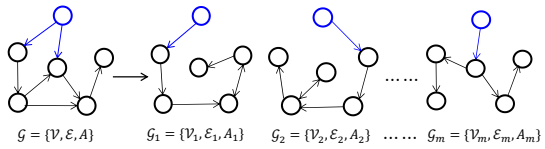

Fig. 1. Examples of the network topology under connectivity-maintained attacks.

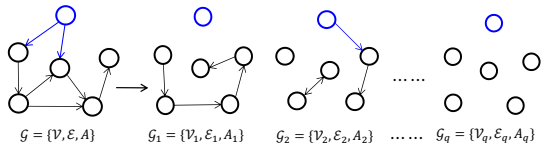

Fig. 2. Examples of the network topology under connectivity-broken attacks.

Consider the information exchange between the n agents and the leader. A diagonal matrix $\Delta = diag\{\Lambda_1, \Lambda_2, \cdots, \Lambda_n\}$ is used to represent the access of agents to the desired trajectory. If Λ_i, $i \in \{1, 2, \cdots, n\}$ is equal to 1, then the ith agent has access to the desired trajectory, and 0 otherwise. For further analysis, we denote a matrix H as $H = L + \Delta$, which is named as the information-exchange matrix.

Assumption 1. The pair (A, B) is stabilizable.

Assumption 2. There exists a constant $\rho > 0$, such that

$$\| f(y, t) - f(z, t) \| \leq \rho \| y - z \|;\ \forall y, z \in \mathbb{R}^l, t \geq 0. \quad (3)$$

In this paper, we consider attacks on the links but not on the nodes. That is, an attack removes or adds edges instead of nodes in the network. It is known that an edge can fail either due to a random fault or a strategic attack. We will consider the attacks on the edges which may cause the loss of consensus tracking security. To start, let us define two types of attacks.

Definition 1. (*Connectivity-maintained attacks*) Under connectivity-maintained attacks, the original network topology with a directed spanning tree still possesses a directed spanning tree, even though the topology changes due to link failures or creation of new links.

Definition 2. (*Connectivity-broken attacks*) Under connectivity-broken attacks, the original network topology with a directed spanning tree become disconnected due to attack-caused link failures.

Examples of the network topology under the two types of attacks are shown in Figs. 1 and 2.

Remark 1. Definition 1 implies that each possible topology with a directed spanning tree provides the possibility to guarantee consensus tracking of the overall multi-agent systems, while in Definition 2, each topology under connectivity-broken attacks without any directed spanning trees will bring negative in$f$luence and might totally destroy the consensus tracking performance.

4. ROBUST MEAN-SQUARE EXPONENTIAL CONSENSUS TRACKING UNDER CONNECTIVITY-MAINTAINED/BROKEN ATTACKS

A switching signal $\sigma(t) : [0,\ \infty) \to \Xi = \{1, 2, \cdots, m, m+1, \cdots, l\}$, $m \geq 1$, $l \geq 2$ is introduced to describe the evolution of the underlying topologies subject to the m and

b ($b = l - m$) connectivity-maintained/broken attacks, respectively. Let $G_{\sigma(t)}$ be the interaction graph of system (1) at time $t \geq 0$. Obviously, $\{\mathcal{G}_1, \mathcal{G}_2, \cdots, \mathcal{G}_m, \mathcal{G}_{m+1}, \cdots, \mathcal{G}_l\}$ denote the set of all possible directed interaction graphs under these two types of attacks. The information-exchange matrix for consensus tracking is denoted as $H_1, H_2, \cdots, H_m, H_{m+1}, \cdots, H_l$. Corresponding to the switching signal $\sigma(t)$, we have the switching sequence $\{(i_0, t_0), (i_1, t_1), \cdots, (i_k, t_k), \cdots, k = 0, 1, 2, ..., Z\}$, which means that the i_k^{th} subsystem is activated when $t \in [t_k, t_{k+1})$ under which each of the possible topologies are all time-invariant.

For notational convenience, some notations are introduced, which will be used later for system (1) subject to both connectivity-maintained/broken attacks. First, the index set Ξ of the switching signal $\sigma(t)$ is divided into two subsets Ξ_m and Ξ_b ($\Xi_m \cup \Xi_b = \Xi$), where Ξ_m and Ξ_b are used to index the sets of the connectivity-maintained/broken attacks, respectively. Furthermore, T_m and T_b denote the total activation time of the connectivity-maintained/broken attacks on the time interval $[t_0, t)$, respectively. Denoting t_k ($k = 0, 1, 2, ..., Z$) as the switching instants in $[t_0, t)$, and letting $t_{Z+1} = t$, one gets

$$T_m(t_0, t) = \sum_{\substack{k=0, \\ \sigma(t_k) \in \Xi_m}}^{Z} (t_{k+1} - t_k), \tag{4}$$

$$T_b(t_0, t) = \sum_{\substack{k=0, \\ \sigma(t_k) \in \Xi_b}}^{Z} (t_{k+1} - t_k). \tag{5}$$

From Definitions 1 and 2, the following assumptions hold.

Assumption 3. Each possible communication topology $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_m$ under the connectivity-maintained attacks contains a directed spanning tree with the leader as the root, while all the other paralyzed topology $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_b$ under the connectivity-broken attacks does not contain any directed spanning trees.

Assumption 4. The paralyzed topology $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_b$ can be recovered into any of the possible connectivity-maintained topologies $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_m$ after a communication restoration mechanism (e.g., the sensing devices are able to recover through some backup or repairing efforts).

Remark 2. The paralyzed topology $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_b$ can be recovered into any of possible connectivity-maintained topology $\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in \Xi_m$ through the internal recovery/tolerance capacities of the system or repairing efforts, even though it may take a short period of time.

Based on Lemma 2 and Assumption 3, the following lemma can be obtained.

Lemma 3. Suppose that Assumption 3 holds. Then, there exist positive definite diagonal matrices $\Theta_{\sigma(t)} = diag\{\theta_{\sigma(t),1}^{-1}, \cdots, \theta_{\sigma(t),n}^{-1}\}$, $\sigma(t) \in \Xi_m$, such that the symmetric positive definite matrix $Q_{\sigma(t)} = H_{\sigma(t)}^T \Theta_{\sigma(t)} + \Theta_{\sigma(t)} H_{\sigma(t)} > 0$, where $\theta_{\sigma(t)} = [\theta_{\sigma(t),1}, \theta_{\sigma(t),2}, \cdots, \theta_{\sigma(t),n}] = H_{\sigma(t)}^{-1} \mathbf{1}_n$.

To achieve consensus tracking, the following distributed consensus tracking protocol is proposed for system (1) under these connectivity-maintained/broken attacks as

$$u_i(t) = \begin{cases} \gamma K \{ \sum_{j=1}^{n} a_{ij}^{\sigma(t)} (x_j(t) - x_i(t)) \\ + \Lambda_i^{\sigma(t)} (x_0(t) - x_i(t)) \}, \ \sigma(t) \in \Xi, \end{cases} \tag{6}$$

where $\Xi = (\Xi_m \cup \Xi_b)$, $a_{ij}^{\sigma(t)}$ is the adjacency element of $\mathcal{G}_{\sigma(t)}$, $\Lambda_i^{\sigma(t)}$ is equal to 1 when agent i has access to the leader, and 0 otherwise, and $\gamma > 0$ denotes the scalar coupling strength gain and K is the feedback controller gain matrix.

Denote the consensus tracking error as $e_i(t) = x_i(t) - x_0(t)$ and the stochastic error as $\omega_i(t) = w_i(t) - w_0(t)$. Then, combining (1), (2), with (6) gives the following switched stochastic closed-loop error system in a compact form as

$$de_i(t) = \begin{cases} [(I_n \otimes A)e(t) - \gamma (H_{\sigma(t)} \otimes BK)e(t)]dt \\ + \tilde{f}(x(t), t) dw(t), \ \sigma(t) \in \Xi. \end{cases} \tag{7}$$

Next, two concepts on mean-square exponential consensus tracking and average dwell time (ADT) are introduced.

Definition 3. The proposed distributed protocol (6) is said to solve the robust, mean-square, exponential, consensus tracking problem for system (1) under the connectivity-maintained/broken attacks if there exist a scalar $\kappa > 0$ and a decay rate $\lambda > 0$ such that the solution of (7) satisfies

$$E\{\|x_i(t) - x_0(t)\|^2\} \leq \kappa e^{-\lambda(t - t_0)} \|x_i(t_0) - x_0(t_0)\|^2. \tag{8}$$

Definition 4. [17] For a switching signal $\sigma(t) \in \Xi$ and $T_2 > T_1 \geq 0$, let $N_a(T_1, T_2)$ denote the number of $\sigma(t)$ over $[T_1, T_2)$. If there exist $N_0 \geq 0$ and $T_a > 0$ such that $N_a(T_1, T_2) \leq N_0 + (T_2 - T_1)/T_a$ holds, then T_a and N_0 are called the average dwell time and the chattering bound, respectively. As commonly used in the literature, for simplicity here, we choose $N_0 = 0$ in this paper.

Inspired by the above definition of ADT in [17] and controller failure in [18], we will introduce the following new definitions to study consensus tracking security under the connectivity-maintained/broken attacks.

Definition 5. *(Connectivity-broken attack frequency)* For a switching signal $\sigma(t) \in \Xi$ and $\forall T_2 > T_1 \geq 0$, let $N_f(T_1, T_2)$ denote the number of connectivity-broken attacks over (T_1, T_2). $F_f(T_1, T_2) = \frac{N_f(T_1, T_2)}{T_2 - T_1}$ is defined as the connectivity-broken attack frequency over (T_1, T_2).

Definition 6. *(Connectivity-broken attack length rate)* For a switching signal $\sigma(t) \in \Xi$ and $\forall t > 0$, T_m and T_b defined in (4) and (5) represent the total activation time of the connectivity-maintained/broken attacks during $[t_0, t)$, respectively. $\frac{T_b(t_0, t)}{t - t_0}$ is defined as the connectivity-broken length rate over $[t_0, t)$.

Before moving on, a multi-step design procedure is developed for selecting the control parameters of the distributed consensus tracking protocol (6).

Algorithm 1. Under Assumptions 1-4, a distributed consensus tracking protocol (6) can be constructed as follows.

(1) Solve an LMI

$$AP + PA^T - c\tilde{\theta}_0 BB^T + \rho^2 P + \beta P < 0, \tag{9}$$

to get a matrix $P > 0$ and scalars β, $c > 0$. In (9), ρ satisfies Assumption 2 and $\tilde{\theta}_0 = \min_{s,i} \theta_{s,i}$, $s \in \{1, \cdots, m\}$, $i = 1, 2, \cdots, n$ is defined in Lemma 3.

(2) Solve an LMI

$$AP + PA^T + \varepsilon BB^T + \rho^2 P - \alpha P < 0, \tag{10}$$

to get scalars ε, $\alpha > 0$.

(3) Design the feedback gain matrix K of (6) as

$$K = B^T P^{-1}. \tag{11}$$

(4) Choose the coupling strength γ satisfying:

$$\varepsilon / \left|\bar{\lambda}_0\right| \geq \gamma \geq c/\lambda_0, \tag{12}$$

where ε and c are defined in (9) and (10), $\lambda_0 = \min\{\lambda_{\min}(Q_{\sigma(t)}), \sigma(t) \in \Xi_m\}$ and $\bar{\lambda}_0 = \min\{\lambda_{\min}(H^T_{\sigma(t)} + H_{\sigma(t)}) : \sigma(t) \in \Xi_b\}$, respectively.

Theorem 1. Consider a class of *Itô* stochastic linear multi-agent system (1) which are subject to connectivity-maintained/broken attacks. Suppose Assumptions 1-4 hold and the LMIs (9) and (10) have feasible solutions. Then under the distributed protocol (6) constructed by Algorithm 1, the agents modeled by (1) can achieve robust mean-square exponential consensus tracking for the switching signal $\sigma(t)$, $\sigma(t) \in \Xi$, provided that the following two conditions are satisfied:

1. For a positive constant $\eta^* \in (0, \beta)$, the connectivity-broken attack length rate of attacks satisfies:

$$\frac{T_b(t_0, t)}{t - t_0} \leq \frac{\beta - \eta^*}{\alpha + \beta}. \tag{13}$$

2. For a positive constant $\eta \in (0, \eta^*)$, the connectivity-broken attack frequency $F_f(t_0, t)$ for the whole time interval satisfies:

$$F_f(t_0, t) = \frac{N_f(t_0, t)}{t - t_0} \leq F_f^* = \frac{\eta^* - \eta}{2\ln(\mu)}, \tag{14}$$

where $\mu = \frac{\bar{\theta}_0}{\tilde{\theta}_0} \geq 1$, $\tilde{\theta}_0 = \min_{s,i} \theta_{s,i}$, $\bar{\theta}_0 = \max_{s,i} \theta_{s,i}$, $s \in \{1, \cdots, m\}$, $i = 1, 2, \cdots, n$.

Moreover, the state decay estimation of consensus tracking error is given as

$$E\{\|e_i(t)\|^2\} \leq \varphi e^{-\eta(t - t_0)} E\{\|e_i(t_0)\|^2\}, \tag{15}$$

where $\varphi = \frac{b}{a}$, $b = \max\{\lambda_{\max}(\theta_{s,i}^{-1} P^{-1}), \lambda_{\max}(P^{-1})\}$, $a = \min\{\lambda_{\min}(\theta_{s,i}^{-1} P^{-1}), \lambda_{\min}(P^{-1})\}$, $s \in \{1, \cdots, m\}$, $i = 1, 2, \cdots, n$.

Proof: The following piecewise multiple Lyapunov functional candidate is chosen for the switched stochastic closed-loop error system (7) under the switching signal $\sigma(t) \in \Xi = (\Xi_m \cup \Xi_b)$:

$$V(\sigma(t), t) = \begin{cases} e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1})e(t), & \sigma(t) \in \Xi_m, \\ e^T(t)(I_n \otimes P^{-1})e(t), & \sigma(t) \in \Xi_b. \end{cases} \tag{16}$$

The detailed proof procedure is given as follows.

Step (I): The multi-agent system (1) is subject to m connectivity-maintained attacks denoted by a switching signal $\sigma(t) \in \Xi_m$.

When $\sigma(t) \in \Xi_m$, it follows from the *Itô* formula that the stochastic derivative of (16) along system (7) is given by

$$\begin{aligned} d(V(\sigma(t), t) = {} & LV(\sigma(t), t)dt + 2e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1}) \\ & \times \tilde{f}(x(t), t)dw(t), \end{aligned} \tag{17}$$

where the infinitesimal generator $LV_m(t)$ is

$$\begin{aligned} LV(\sigma(t), t) = {} & 2e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1})[(I_n \otimes A) \\ & -\gamma(H_{\sigma(t)} \otimes BK)e(t)] + \tilde{f}^T(x(t), t) \\ & \times (\Theta_{\sigma(t)} \otimes P^{-1})\tilde{f}(x(t), t). \end{aligned} \tag{18}$$

According to Algorithm 1 and Assumption 2, substituting (11) into (18) yields

$$\begin{aligned} LV(\sigma(t), t) = {} & 2e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1}A)e(t) - 2\gamma e^T(t) \\ & \times (\Theta_{\sigma(t)} H_{\sigma(t)} \otimes P^{-1}BB^T P^{-1})e(t) \\ & + \tilde{f}^T(x(t), t)(\Theta_{\sigma(t)} \otimes P^{-1})\tilde{f}(x(t), t) \\ \leq {} & e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1}A + \Theta_{\sigma(t)} \otimes A^T P^{-1} \\ & + \rho^2 P^{-1})e(t) - \gamma e^T(t)[(\Theta_{\sigma(t)} H_{\sigma(t)} \\ & + H^T_{\sigma(t)} \Theta_{\sigma(t)}) \otimes P^{-1}BB^T P^{-1}]e(t). \end{aligned} \tag{19}$$

Let $\varsigma(t) = (\varsigma_1^T(t), \cdots, \varsigma_n^T(t))^T$, where $\varsigma_i(t) = P^{-1}e_i(t), i = 1, \cdots, n$. Obviously, $e(t) = (I_n \otimes P)\varsigma(t)$. It thus follows from Assumption 3, Lemma 3, and (19) that

$$\begin{aligned} LV(\sigma(t), t) = {} & \varsigma^T(t)[\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ & -\gamma \varsigma^T(t)(Q_{\sigma(t)} \otimes BB^T)\varsigma(t) \\ \leq {} & \varsigma^T(t)[\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ & -\gamma \lambda_0 \varsigma^T(t)(I \otimes BB^T)\varsigma(t), \end{aligned} \tag{20}$$

where $\lambda_0 = \min\{\lambda_{\min}(Q_{\sigma(t)}) : \sigma(t) \in \Xi_m\}$ with $Q_{\sigma(t)}$ defined in Lemma 3. Since $\gamma > \frac{c}{\lambda_0}$ in Algorithm 1, the expression in (20) can be rewritten as

$$\begin{aligned} LV(\sigma(t), t) \leq {} & \varsigma^T(t)[\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ & -c\varsigma^T(t)(\Theta_{\sigma(t)} \otimes BB^T)\varsigma(t) \\ \leq {} & \varsigma^T(t)[\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P \\ & -c\tilde{\theta}_0 BB^T)]\varsigma(t) \\ \leq {} & -\beta \varsigma^T(t)(\Theta_{\sigma(t)} \otimes P)\varsigma(t) \\ = {} & -\beta e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1})e(t). \end{aligned} \tag{21}$$

where $\tilde{\theta}_0 = \min_{s,i} \theta_{s,i}$, $s \in \{1, \cdots, m\}$, $i = 1, 2, \cdots, n$.

Combining (17) to (21) leads to

$$\begin{aligned} d(V(\sigma(t), t)) \leq {} & -\beta V(\sigma(t), t)dt + 2e^T(t)(\Theta_{\sigma(t)} \otimes P^{-1}) \\ & \times \tilde{f}(x(t), t)dw(t). \end{aligned} \tag{22}$$

Integrating both sides of (22) over $t \in [t_k, t_{k+1})$ and then taking expectation yield

$$E\{V_m(t)\} \leq e^{-\beta(t - t_k)} E\{V_m(t_k)\}. \tag{23}$$

Step (II): The multi-agent system (1) is subject to the b connectivity-broken attacks.

When $\sigma(t) \in \Xi_b$, the stochastic derivative of (16) along system (7) is shown in (21) with the infinitesimal generator $LV(\sigma(t), t)$ is is given by

$$LV(\sigma(t),t) = e^T(t)[I_n \otimes (P^{-1}A + A^T P^{-1})]e(t) - 2\gamma e^T(t)(I_n \otimes P^{-1})(I_n \otimes BK)e(t) + \tilde{f}^T(x(t),t)(I_n \otimes P^{-1})\tilde{f}(x(t),t)dw(t). \quad (24)$$

Similar to (19)-(21) in Step (I), it follows from Algorithm 1 that

$$\begin{aligned} LV(\sigma(t),t) &\le \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ &\quad - \gamma\varsigma^T(t)[(H_{\sigma(t)} + H_{\sigma(t)}^T) \otimes BB^T]\varsigma(t) \\ &\le \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ &\quad + \gamma\left|\bar{\lambda}_0\right|\varsigma^T(t)[I_n \otimes BB^T]\varsigma(t) \\ &\le \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P + \varepsilon BB^T)]\varsigma(t), \end{aligned}$$

where $\varepsilon \ge \gamma\left|\bar{\lambda}_0\right|$ and $\bar{\lambda}_0 = \min\{\lambda_{\min}(H_{\sigma(t)}^T + H_{\sigma(t)})$.

Based on the design (10) in Algorithm (1), it is not difficult to obtain

$$LV(\sigma(t),t) \le \alpha e^T(t)(I_n \otimes P^{-1})e(t). \quad (25)$$

Similar to (21) to (23), it follows from (25) that

$$E\{V(\sigma(t),t)\} \le e^{\alpha(t-t_k)}E\{V(\sigma(t_0),t_0)\}. \quad (26)$$

Step (III): Synthesizing the above circumstances (I)-(II) into one, during the period $[t_k, t)$, $t \in [t_k, t_{k+1})$, it is true from (23) and (26) that under the switching signal $\sigma(t) \in \Xi = (\Xi_m \cup \Xi_b)$,

$$\begin{aligned} &E\{V(\sigma(t),t)\} \\ &\le \begin{cases} e^{-\beta(t-t_k)}E\{V_m(\sigma(t_k),t_k)\}, & \sigma(t) \in \Xi_m, \\ e^{\alpha(t-t_k)}E\{V_b(\sigma(t_k),t_k)\}, & \sigma(t) \in \Xi_b. \end{cases} \end{aligned} \quad (27)$$

Therefore, it further yields for $t \in [t_k, t_{k+1})$,

$$E\{V(e(t),\sigma(t))\} \le e^{\alpha T_m(t_k,t) - \beta T_{\bar{m}}(t_k,t)}E\{V(e(t_k),\sigma(t_k))\}. \quad (28)$$

When $t = t_k$, we assume that the switching signal $\sigma(t_k)$ is activated during $t \in [t_k, t_{k+1})$, and $\sigma(t_{k-1})$ is identified at the switching instant t_{k-1}. Besides, it is assumed that for system (1), there is no jump in the state $x_i(t)$ at the switching instant, i.e., $x_i(t_k) = x_i(t_k^-)$. Thus, it follows from (16) that

$$E\{V(e(t_k),\sigma(t_k))\} \le \mu E\{V(e(t_k^-),\sigma(t_k^-))\}. \quad (29)$$

For the whole switching interval, (28) and (29) give

$$\begin{aligned} &E\{V(e(t),\sigma(t))\} \\ &\le \mu e^{\alpha T_m(t_k,t) - \beta T_b(t_k,t)}E\{V(e(t_k^-),\sigma(t_k^-))\} \\ &\le \mu e^{\alpha T_m(t_{k-1},t) - \beta T_b(t_{k-1},t)}E\{V(e(t_{k-1}),\sigma(t_{k-1}))\} \\ &\le \cdots \le \mu^{N_{\sigma(t)}(t_0,t)}e^{\alpha T_m(t_0,t) - \beta T_b(t_0,t)}V(e(t_0),\sigma(t_0)) \\ &= e^{N_{\sigma(t)}(t_0,t)\ln(\mu) + \alpha T_m(t_0,t) - \beta T_b(t_0,t)}V(e(t_0),\sigma(t_0)). \end{aligned} \quad (30)$$

Based on the condition (13), it holds that

$$-\beta T_m(t_0,t) + \alpha T_b(t_0,t) \le -\eta^*(t - t_0). \quad (31)$$

From the condition (14), it is clear that

$$e^{N_{\sigma(t)}(t_0,t)\ln(\mu)} \le e^{2N_f(t_0,t)\ln(\mu)} \le e^{(\eta^* - \eta)(t-t_0)}. \quad (32)$$

Hence, it follows from (30)-(32) that

$$E\{V(e(t),\sigma(t))\} \le e^{-\eta(t-t_0)}E\{V(e(t_0),\sigma(t_0))\}. \quad (33)$$

Combining (16) with (33) yields

$$E\{\|e_i(t)\|^2\} \le \varphi e^{-\eta(t-t_0)}E\{\|e_i(t_0)\|^2\}, \quad (34)$$

where $\varphi = \frac{b}{a}$ as shown in Theorem 1.

According to (34), one concludes that $e_i(t) \to 0$ as $t \to +\infty$, which means that $x_i(t) \to x_0(t)$, as $t \to +\infty$. Thus, the proposed protocol (6)can solve the consensus tracking problem for (1) under the two types of attacks. This completes the proof. □

5. SIMULATIONS: APPLICATION IN POWER SYSTEMS UNDER TWO TYPES OF ATTACKS

In this section, a practical power system example is provided to demonstrate the effectiveness of the results. A microgrid can be regarded as a multi-agent system, where each DG is an agent. In such a case, the distributed cooperative secondary control of microgrids can be formulated as a consensus tracking problem, where all DGs try to synchronize their terminal voltage amplitude to a reference value. However, this system is vulnerable to cyber attacks as the communication lines connected among the different DGs might be subject to attacks.

The following six DGs are presented to describe the communication network of a microgrid under two types of attacks, respectively. Figs. 3 and 4 show the communication topologies under two different connectivity-maintained/broken attacks, respectively. The parameters of the DGs, lines, and loads are adopted from [15]. The goal is to design a distributed algorithm such that $y_i \to y_0$

$$\begin{aligned} \dot{y}_i &= Ay_i + Bu_i, \\ \dot{y}_0 &= Ay_0, \end{aligned} \quad (35)$$

where $y_i = [v_{o,magi}, \dot{v}_{o,magi}]^T$, $i = 1, 2, \cdots 6$, $y_0 = [v_{ref}, 0]^T$, $B = [0, 1]^T$, and $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

According to Algorithm 1, some simple calculations give $\tilde{\theta}_0 = 2$, $\mu = 1.5$, $\lambda_0 = 0.2039$, and $\bar{\lambda}_0 = -0.4142$. In simulations, constructing the distributed controller (11)

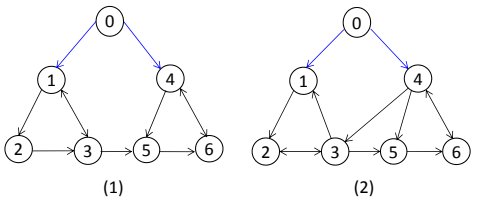

Fig. 3. Topologies under connectivity-maintained attacks

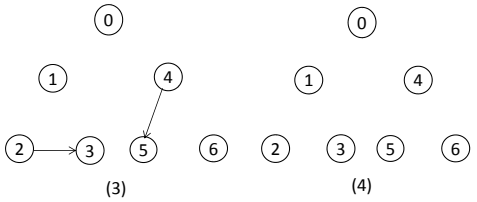

Fig. 4. Topologies under connectivity-broken attacks

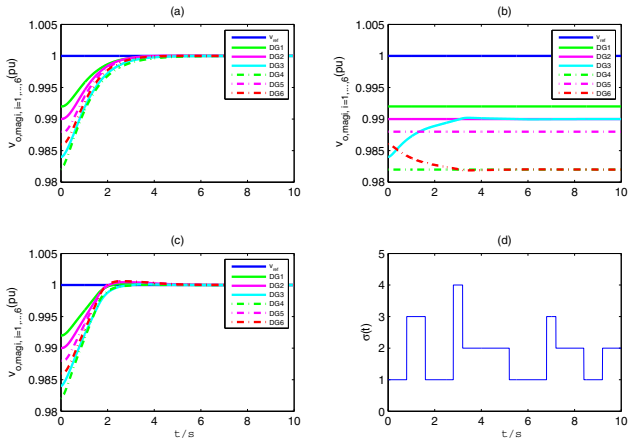

Fig. 5. (a), (b), and (c) represent DG output voltage magnitudes under connectivity-maintained attacks, connectivity-broken attacks, and a mix of two types of attacks. (d) shows the switching signal $\sigma(t)$.

with parameters $\rho = 0.1$, $\alpha = 5.2$, and $\beta = 1.6$ yields $K = [0.82621,\ 1.0185]$ and $\mu = 1.5$. It is assumed that the microgird is islanded from the main grid at $t = 0$, while the secondary control is active. Figs. 5 show the DG terminal voltage amplitudes under different attacks and the reference voltage value is set to 1 p.u. Fig. 5 (a) implies that the distributed control can regulate the DG terminal voltage amplitude to a reference value under the connectivity-maintained attacks, while Fig. 5 (b) shows that it fails under the connectivity-broken attacks. Fortunately, Fig. 5 (c) presents that under a mix of the connectivity-maintained/broken attacks, it works if the conditions in Theorem 1 are satisfied. Fig. 5 (d) shows the switching singal $\sigma(t) \in \Xi$, which implies that the above conditions (13) and (14) are satisfied.

6. CONCLUSIONS

In this paper, a distributed coordinated cyber-security control problem is studied for stochastic linear multi-agent systems under connectivity-maintained/broken attacks. We formulate this problem from the perspective of switching systems subject to connected and disconnected topologies caused by attacks. A mild assumption is needed where only each possible topology by the connectivity-maintained attacks contains a directed spanning tree with the leader as the root. Under a multi-step distributed algorithm, sufficient conditions on exponential convergence are established via the tools from M-matrix, switched system theory, and graph theory. A practical power system example is studied to show the effectiveness of the proposed method.

REFERENCES

[1] R. Olfati-Saber, R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays", *IEEE Transactions on Automatic Control,* 2004, 49(9):1520–1533.

[2] W. Ren, R. W. Beard, "Consensus seeking in multi-agent systems under dynamically changing interaction topologies", *IEEE Transactions on Automatic Control,* 2005, 50(5):655–661.

[3] R. Olfati-Saber, J. A. Fax, R. M. Murray, "Consensus and cooperation in networked multi-agent systems", *Proceedings of the IEEE,* 2007, 95(1):215-233.

[4] Y. Cao, W. Yu, W. Ren, G. Chen, "An overview of recent progress in the study of distributed multi-agent coordination", *IEEE Transactions on Industrial informatics,* 2013, 9(1):427–438.

[5] Y. Cao, W. Ren, "Distributed coordinated tracking with reduced interaction via a variable structure approach", *IEEE Transactions on Automatic Control,* 2012, 57(1):33-48.

[6] X. Wang, Y. Hong, J. Huang, Z. Jiang, "A distributed control approach to a robust output regulation problem for multi-agent linear systems", *IEEE Transactions on Automatic Control,* 2010, 55(12):2891-2895.

[7] G. Hu, "Robust consensus tracking of a class of second-order multi-agent dynamic systems", *Systems and Control Letters,* 2012, 61(1):134-142.

[8] Q. Song, F. Liu, J. Cao, W. Yu, "Pinning-controllability analysis of complex networks: An M-matrix approach", *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2012, 59: 2692–2701.

[9] L. Cheng, Z. Hou, M. Tan, X. Wang, "Necessary and sufficient conditions for consensus of double-integrator multi-agent systems with measurement noises", *IEEE Transactions Automatic Control,* 2011, 56(8):1958–1963.

[10] J. Hu, G. Feng, "Distributed tracking control of leader-follower multiagent systems under noisy measurements", *Automatica*, 2010, 46(8):1382-1387.

[11] I. Shames, A. Teixeira, H. Sandberg, K. H. Johansson, "Distributed fault detection for interconnected second-order systems", *Automatica*, 2011, 47(12):2757-2764.

[12] H. J. LeBlanc, X. D. Koutsoukos, "Consensus in networked multi-agent systems with adversaries", *Proceedings of the 14th International Conference on Hybrid systems: Computation and Control, Chicago, IL,* 2011.

[13] F. Pasqualetti, R. Carli, F. Bullo, "A distributed method for state estimation and false data detection in power networks", *In IEEE International Conference on Smart Grid Communications* 2011.

[14] F. Pasqualetti, R. Carli, F. Bullo, "Attack Detection and identification in cyber-physical systems", *IEEE Transactions Automatic Control,* 2013, 58(11):2715-2729.

[15] A.Bidram, A. Davoudi, F. L. Lewis, J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization", *IEEE Transactions Power Systems,* 2013, 28(3):3462–3470.

[16] R. Diestel, Graph Theory. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[17] J. P. Hespanha, A. S. Morse, "Stability of switched systems with average dwell time", *Proceedings of the 38th IEEE Conference on Decision and Control, Phoenix, AR,* 1999, 2655-2660.

[18] X. Sun, G. Liu, D. Rees, W. Wei, "Stability of systems with controller failure and time-varying delay", *IEEE Transactions Automatic Control,* 2008, 53: 2391–2396.