Distributed Secure Coordinated Control for Multi-Agent Systems Under Strategic Attacks

Zhi Feng, *Student Member, IEEE,* Guanghui Wen, *Member, IEEE,* and Guoqiang Hu, *Member, IEEE*

***Abstract*— This paper studies a distributed secure consensus tracking control for multi-agent systems subject to strategic cyber attacks modeled by a random Markov process. A hybrid stochastic secure control framework is established for designing a distributed secure control law such that mean-square exponential consensus tracking is achieved. A connectivity restoration mechanism is considered and the properties on attack frequency and attack length rate are investigated, respectively. Based on the solutions of an algebraic Riccati equation and an algebraic Riccati inequality, a procedure to select the control gains is provided and stability analysis is studied by using Lyapunov method. The effect of strategic attacks on discrete-time systems is also studied. Finally, numerical examples are provided to illustrate the effectiveness of theoretical analysis.**

***Index Terms*— Cyber system; Network system; Distributed secure control; Strategic attack; Attack frequency; Mean-square exponential convergence.**

I. Introduction

Recent years have witnessed an increasing attention on distributed cooperative control of real-world multi-agent systems due to its widespread applications in various fields such as distributed control of team robots, design of sensor networks, formation control of vehicles, rendezvous of mobile agents, and synchronization of coupled chaotic oscillators [1]–[5]. A fundamental yet interesting issue on this topic is to develop distributed controllers using only relative local information such that as time goes on, all the agents eventually achieve state consensus of the whole group. As an effective consensus seeking approach, consensus tracking problem has been widely studied for linear multi-agent systems [6]–[13].

Distributed secure coordinated control 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: attack on the dynamic behaviors (or closed-loop dynamics) of the agents and attack on the communications among the agents. Both of attacks can dramatically affect the consensus properties of the whole team. Under the assumption that the network is complete, consensus problem was studied in [14] for multi-agent systems with adversaries. [15], [16] considered distributed attack detection using unknown input observers for double integrator multi-agent systems. In [17], a distributed attack detection and identification algorithm via a distributed filter was investigated for cyber-physical systems. Note that [14]–[17] show that an attack on a specific node is identical to node removal on network graphs. In reality, it is more general to consider the second attack scenario that a number of edges are attacked [18]–[20]. In addition, the aforementioned detection techniques and control algorithms are always separated, which implies that there is no feedback to the control parameters when the attacks are detected or identified. Recently, [21] proposed a distributed receding-horizon control method for secure control of multi-agent systems by limiting the actions of the adversaries. [24] and [25] modeled attacker-defender interactions as a stochastic game and developed the game-theoretic resilient control schemes for cyber-physical systems. So far, how to design effective resilient algorithms is still challenging and of great significance to the distributed secure control problem of multi-agent systems.

In previous work [26], two types of attacks: connectivity-maintained and connectivity-broken attacks were studied and a hybrid secure control scheme was provided to achieve distributed secure control of a leader-follower multi-agent system. However, on the one hand, the attacks on graphs are modeled by using a deterministic switching signal that determines the switching among various network topologies. That is, it is assumed that the system has complete access to the attacker moves. This similar switching attacks are also considered in [29] from the perspective of sliding mode. On the other hand, sufficient conditions for existence of consensus algorithms are established by solving two linear matrix inequalities (LMIs) to get a common solution for designing Lyapunov functions afterwards. The set of LMIs are dependent on the eigenvalues of the Laplacian matrix of all the information graph topologies. Besides, the time-complexity of solving an LMI is $O(N^2s^4)$, where N and s are the number of agents and the dimension number of agent dynamics, respectively. Overall, it is conservative via LMI techniques.

In this work, a distributed secure coordinated control problem is addressed for linear multi-agent systems under strategic attacks in cyber space whose dynamics are captured by a random Markov process. Exponential consensus tracking in mean-square sense is achieved based on a novel hybrid stochastic secure control approach, provided that two conditions are satisfied with respect to the attack frequency and attack length rate. A piecewise quadratic Lyapunov function is explored, which is determined by solving an algebraic Riccati equation and an algebraic Riccati inequality and the existence of solutions can be guaranteed [30], [31].

This work was supported by Singapore Economic Development Board under EIRP grant S14-1172-NRF EIRP-IHL. Z. Feng and G. Hu are with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798. G. Wen is with Research Center for Complex Systems and Network Sciences, Department of Mathematics, Southeast University, Nanjing 210096, P. R. China. (E-mail: zfeng001@e.ntu.edu.sg; gqhu@ntu.edu.sg; wenguanghui@gmail.com).

The main contributions of this work are summarized as follows. 1). In contrast to consensus (or consensus tracking) problems for lower-order multi-agent systems in [1]–[5], [9]–[25], continuous-time and discrete-time linear dynamics are considered in this paper. Furthermore, the open-loop system matrix of the linear agent dynamics may not contain stable eigenvalues as required in [6]–[8]. 2). Different from deterministic attacks in [26], this paper studies strategic attacks, whose dynamics are captured by a random Markov process. A connectivity restoration mechanism is assumed such that after a short period of time, the networks can recover from attacks. The problem is formulated from a switching perspective and a switching sequence forms a random Markov chain to model strategic attacks. 3). An explicit analysis of the attack frequency and length rate is provided to achieve secure consensus tracking. By virtue of the slowly switching mechanism with a piecewise Lyapunov function, the upper bounds of the attack frequency and attack length rate are obtained to ensure that the attacks do not occur frequently and the average recovery time is not too large. Under these two conditions, the designed distributed secure control laws guarantee that all the agents can achieve mean-square exponential consensus tracking. 4). Different from solving two LMIs to obtain a common solution in [26], the distributed control laws can be designed by solving the algebraic Riccati equation and inequality, respectively, with the time-complexity of $O(s^4)$ [30], which are independent of all the information topologies under strategic attacks.

This paper is organized to provide mathematical development and stability analysis along with numerical simulations. Specifically, in Section II, a distributed secure coordinated control problem is formulated. In Section III, the distributed design and stability analysis are first developed for continuous-time multi-agent systems under attacks. Then, an extension to discrete-time case is studied. Section IV gives the numerical stimulations, followed by conclusions in Section V.

The following notations are used throughout this paper. Let $\mathbb{R}$ ($\mathbb{R}_{\geq 0}$) be the set of reals (greater than or equal to 0), $\mathbb{R}^{N\times N}$ be the set of $N\times N$ real matrices, I_N be the $N\times N$ identity matrix, and $\mathbf{1}$ be the $N\times 1$ vector with all ones. $\mathbb{N}$ denotes the set of natural numbers and $\mathbb{N}_0=\{\mathbb{N}\cup 0\}$. Notations $\otimes$ and $\|\cdot\|$ denote, respectively, the Kronecker product and the Euclidean norm. For a real symmetric matrix A, $\lambda_{\min}(A)$ and $\lambda_{\max}(A)$ represent its smallest and maximum eigenvalues, respectively.

II. Problem Formulation

Consider a group of N agents modeled by the following continuous-time linear dynamics:

$$\dot{x}_i(t)=Ax_i(t)+Bu_i(t),\ t\in\mathbb{R}_{\geq 0}, \tag{1}$$

and its discrete-time counterpart is given by

$$x_i(t+1)=\tilde{A}x_i(t)+\tilde{B}u_i(t),\ t\in\mathbb{N}_0, \tag{2}$$

where $x_i(t)\in\mathbb{R}^n$ and $u_i(t)\in\mathbb{R}^l$, $i=1,\,2,\,\cdots,\,N$, are the state and control input, respectively, and $A,\,\tilde{A}\in\mathbb{R}^{n\times n}$, and $B,\,\tilde{B}\in\mathbb{R}^{n\times l}$ are the system and input matrices of (1) and (2), respectively. We assume that A is not Hurwitz stable and $\tilde{A}$ is not Schur stable, while (A,B) and $(\tilde{A},\tilde{B})$ are stabilizable. That is, there exists a control gain $K\in\mathbb{R}^{l\times n}$ such that $A+BK$ is Hurwitz stable and $\tilde{A}+\tilde{B}K$ is Schur stable, respectively.

Cooperative team objectives are prescribed in terms of local neighborhood consensus tracking error $\delta_i(t)$ defined as

$$\delta_i(t)=\sum_{j=1}^{N}a_{ij}(x_i(t)-x_j(t))+b_i(x_i(t)-x_0(t)), \tag{3}$$

where $x_0(t)\in\mathbb{R}^n$ is the state of a leader, labeled as $i=0$, satisfying the linear dynamics: $\dot{x}_0(t)=Ax_0(t)$.

The objective of distributed coordination is to design

$$u_i(t)=-cK\delta_i(t),\ i=1,\,2,\,\cdots,\,N, \tag{4}$$

with coupling gain $c>0$ and control gain matrix $K\in\mathbb{R}^{l\times n}$, such that $x_i(t)$ of the followers track $x_0(t)$ of the leader.

A. Attack Model

In [26], two types of attacks, connectivity-maintained and connectivity-broken attacks, are studied. These attacks on graphs are modeled by using a deterministic switching signal to determine switchings among various network topologies. The model in [26] assumes that the system has complete access to the attacker moves. In this work, we study the following new attack model partly motivated by [24] and [25].

1) Cyber System: Different from the results in [26], the state of the cyber system in this paper is described by $\theta(t)$. The evolution of $\theta(t)$ depends on the attacker's action a and the cyber defense action d, which are also functions of time. For a given pair (a,d), $\theta(t)$ is modeled as a right-continuous, time-homogeneous, ergodic, random Markov process. $\mathcal{S}=\{1,2,...,s\}$ is the finite state space corresponding to all possible topologies under attacks. Let the infinitesimal generator of Markov process be $\Upsilon=(\gamma_{pq})$, which is given by

$$\begin{aligned}\mathrm{P}_{pq}(t) &= \Pr\mathrm{ob}\{r(t+h)=q|r(t)=p\}\\ &= \begin{cases}\gamma_{pq}h+o(h),\ p\neq q,\\ 1+\gamma_{pp}h+o(h),\ p=q,\end{cases}\end{aligned} \tag{5}$$

where for the switching signal $r(t)$, $\gamma_{pq}\geq 0$ is the transition rate from state p to state q if $p\neq q$ while $\gamma_{pp}=-\sum_{q=1,p\neq q}\gamma_{pq}$, and $o(h)$ denotes an infinitesimal of higher order than h, i.e. $\lim_{h\to 0}o(h)/h=0$. Note that Υ is the transition rate matrix, whose row summation is zero and all off-diagonal elements are nonnegative.

2) Cyber Strategy: Denote by $a\in\mathcal{A}$ a cyber-attack chosen by the attacker from its attack space $\mathcal{A}:=\{a_1,a_2,\cdots,a_m\}$ composed of all m possible actions. $d\in\mathcal{D}$ is the cyber defense mechanism employed by the network administrator, which includes possible defense actions from $\mathcal{D}:=\{d_1,d_2,\cdots,d_n\}$. Thus, one can consider the following mixed strategies of the defender and the attacker:

$$f(k) = [f_p(k)]_{p=1}^{n}\in\mathcal{F}_k,\ g(k)=[g_q(k)]_{q=1}^{m}\in\mathcal{G}_k, \tag{6}$$

$$\tilde{\mathcal{F}}_k :=\{f(k)\in[0,1]^n:\ \sum_{p=1}^{n}f_p(k)=1\}, \tag{7}$$

$$\tilde{\mathcal{G}}_k :=\{g(k)\in[0,1]^m:\ \sum_{q=1}^{m}g_q(k)=1\}, \tag{8}$$

where k denotes the time scale on which cyber events occur, $f_p(k)$ and $g_q(k)$ are the probabilities of choosing $d_p\in\mathcal{D}$ and $a_q\in\mathcal{A}$, respectively, and $\tilde{\mathcal{F}}_k$ and $\tilde{\mathcal{G}}_k$ are two sets of admissible strategies provided for the defender and the attacker.

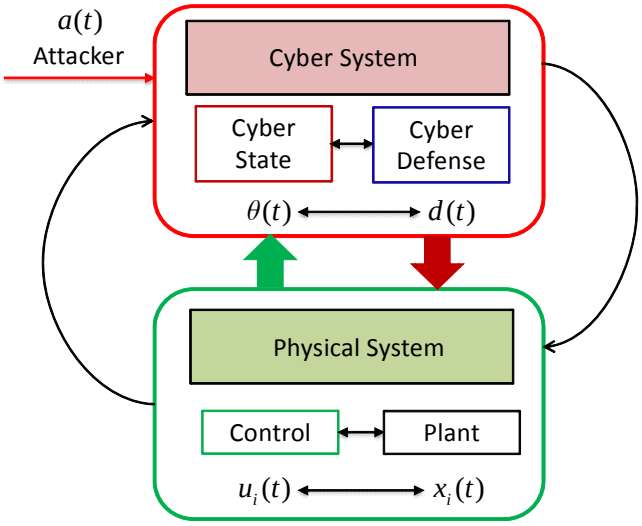

Fig. 1. Hybrid stochastic secure control framework in a multi-agent system.

Therefore, the transition law of the cyber system state $\theta(k)$ at time k depends on the actions of the attacker as well as the defense mechanism employed by the network administrator. More precisely, the rate matrix satisfies

$$\text{Prob}\{\theta(k+\Delta)=q|\theta(k)=p\}=\begin{cases}\gamma_{pq}(f(k),\ g(k)),\ q\neq p,\\ \gamma_{pp}(f(k),\ g(k)),\ q=p,\end{cases}$$

where $\Delta>0$ is on the same scale as k, $\gamma_{pq}(f(k),\ g(k))$ are the average transition rates in terms of the transition rates $\tilde{\gamma}_{pq}(k)=\tilde{\gamma}_{pq}(a_q(k),d_p(k))$, $p,q\in S$, defined by

$$\gamma_{pq}(f(k),g(k))=\sum_{p=1}^{n}\sum_{q=1}^{m}f_p(k)g_q(k)\tilde{\gamma}_{pq}(k). \tag{9}$$

B. Hybrid Stochastic Secure Control Framework

In a networked multi-agent system, an interaction between the physical space and cyber space is captured by their dynamics. Clearly, equations (1) and (5) describe a hybrid system with continuous-time and discrete-time states. The multi-agent physical system state $x_i(t)$ is controlled by a distributed secure controller $u_i(t)$. In cyber space under attacks modeled by a random Markov jump process, the cyber system state $\theta(t)$ is controlled by a cyber defense mechanism d used by the network administrator as well as the attacker's action a. The attacker intends to remove the connection edges in a networked multi-agent system by launching strategic attacks on graphs, which results in all kinds of new possible graph topologies. These topologies are paralyzed when the graph connectivity is broken. A distributed resilient control algorithm will be developed such that the network won't lose the secure consensus tracking performance. The hybrid nature of the multi-agent system leads to the adoption of a class of hybrid systems model. Therefore, a framework of this hybrid stochastic secure control for a networked multi-agent system is illustrated in Fig. 1.

C. Control Objective

The objective is to design a distributed secure control law $u_i(t)$ for multi-agent systems (1) with strategic attacks on communication graphs modeled by a random Markov jump process. Therefore, a distributed secure consensus tracking control problem is defined as follows.

Definition 1: (Mean-Square Consensus Tracking Under Strategic Attacks) The distributed secure control law $u_i(t)$ is said to solve a secure consensus tracking problem in mean-square sense for multi-agent systems (1) under strategic attacks, if there exist a scalar $\kappa>0$ and a decay rate $\rho>0$ such that for all $t>t_0$, $i\in\mathcal{V}$,

$$E\left\{\|x_i(t)-x_0(t)\|^2\right\}\leq\kappa e^{-\rho(t-t_0)}E\left\{\|x_i(t_0)-x_0(t_0)\|^2\right\}.$$

III. Mean-Square Exponential Consensus Tracking under Strategic Attacks

In this section, based on the attack model in subsection II-A, a distributed secure consensus tracking control problem will be studied for multi-agent systems (1) under strategic attacks. In the context of multi-agent systems, the initial connectivity graph of the agents often meets some connection conditions [5]. Thus, motivated by this observation, we assume that the initial graph without being attacked by any strategic attacks contains a directed spanning tree with the leader being the root. However, strategic attacks satisfying a random Markov jump process may make the networks paralyzed as the graph communication connectivity is broken, which results in the loss of secure consensus tracking performance for the entire multi-agent systems. Before deriving the main results, the following graph description under attacks is presented.

A. Time-varying Markovian Graph

Based on descriptions of attack model in Section II-A, let $\mathcal{G}_{r(t)}=\{\mathcal{V},\mathcal{E}_{r(t)},A_{r(t)}\}$ represent a directed time-varying graph of order N with the set of nodes $\mathcal{V}$, $\mathcal{E}_{r(t)}$ is the set of edges and $A_{r(t)}=\left[a_{ij}^{r(t)}\right]\in\mathbb{R}^{N\times N}$ denotes the adjacency matrix of $\mathcal{G}_{r(t)}$, where $a_{ij}^{r(t)}>0$ if and only if $(j,i)\in\mathcal{E}_{r(t)}$ else $a_{ij}^{r(t)}=0$. An edge of $\mathcal{G}_{r(t)}$ is an ordered pair $(i,j)\in\mathcal{E}_{r(t)}$ if agent j can be directly supplied with information from agent i. The set of neighbors of node v_i is denoted by $\mathcal{N}_{r(t)}=\{v_i\in\mathcal{V},(v_j,v_i)\in\mathcal{E}_{r(t)},j\neq i\}$. Graph $\mathcal{G}_{r(t)}$ contains a directed spanning tree if there is a node which can reach all the other nodes through a directed path. The Laplacian matrix of a graph $\mathcal{G}_{r(t)}$ is defined as $\mathcal{L}_{r(t)}=D_{r(t)}-A_{r(t)}\in\mathbb{R}^{N\times N}$, where $D_{r(t)}=\text{diag}\{d_1^{r(t)},d_2^{r(t)},\cdots,d_N^{r(t)}\}$ with $d_i^{r(t)}=\sum_{j=1}^{N}a_{ij}^{r(t)}$. Thus, an information-exchange matrix for consensus tracking is written as $H_{r(t)}=\mathcal{L}_{r(t)}+\mathcal{B}_{r(t)}$, where $\mathcal{B}_{r(t)}=\text{diag}\{b_1^{r(t)},\ b_2^{r(t)},\cdots,\ b_N^{r(t)}\}$ represents the access of followers to the leader under attacks. If $b_i^{r(t)}=1$, the ith agent accesses to leader, and $b_i^{r(t)}=0$, otherwise.

B. Connectivity Restoration Mechanism

In order to achieve secure consensus tracking for systems (1) under strategic attacks, the following assumption introduces a connectivity recovery mechanism.

Assumption 1: $\mathcal{G}_{r(t)}$ can be recovered into connectivity-maintained topologies after a connectivity restoration mechanism (i.e, the sensing and communication devices are able to recover through some backup or repairing efforts).

Remark 1: Although the initial graph without being attacked can provide the possibility of consensus tracking for system (1), each paralyzed topology $\mathcal{G}_{r(t)}$ under strategic attacks might totally destroy the secure consensus performance of the whole multi-agent systems. Thus, Assumption 1 implies that the secure consensus tracking problem can be solved if there exists a connectivity restoration mechanism through internal recovery/tolerance capacities of the system or repairing efforts, even though it may take a short period of time.

C. Distributed Secure Control Law Design

Without loss of generality, one may suppose that there exists an infinite sequence $k = 0, 1, 2, \cdots$, for $[t_{2k}, t_{2(k+1)})$, such that when $t = t_{2k+1}$, the multi-agent system is subject to strategic attacks. That is, the multi-agent network $\mathcal{G}_{r(t)}$ is paralyzed during $[t_{2k+1}, t_{2(k+1)})$, while it works well during $[t_{2k}, t_{2k+1})$ for an initial graph $\mathcal{G}_0$ without being attacked by any strategic attacks. Based on the recovery mechanism in Assumption 1, when $t = t_{2k}^{+}$, the multi-agent network is recovered to a connectivity-maintained topology.

The objective is to construct a distributed resilient control law to achieve secure consensus tracking for system (1) under strategic attacks. Specifically, based on the above analysis the protocol (4) can be designed as

$$u_i(t) = \begin{cases} \varrho K[\sum_{j=1}^{N} a_{ij}^0(x_j(t) - x_i(t)) + b_i^0(x_0(t) - x_i(t))], \\ \qquad t \in [t_{2k}, t_{2k+1}), \\ \\ \vartheta F[\sum_{j=1}^{N} a_{ij}^{r(t)}(x_j(t) - x_i(t)) + b_i^{r(t)}(x_0(t) \\ \qquad -x_i(t))],\ t \in [t_{2k+1}, t_{2(k+1)}), \end{cases} \tag{10}$$

where $k \in \mathbb{N}_0$, $i = 1, 2, \cdots, N$, ϱ, $\vartheta > 0$ represent the coupling strengths, K, $F \in \mathbb{R}^{l \times n}$ are the feedback control gain matrices to be designed, a_{ij}^0, b_i^0 are the adjacency elements of the initial network $\mathcal{G}_0$, while $a_{ij}^{r(t)}$, $b_i^{r(t)}$ represent the adjacency elements of $\mathcal{G}_{r(t)}$ under strategic attacks modeled by a random Markov jump process.

Denote the state tracking error between the followers and the leader as $e_i(t) = x_i(t) - x_0(t)$ and let $e(t) = (e_1^T(t), e_2^T(t), \cdots, e_N^T(t))^T$. Then, substituting (10) into the multi-agent system (1) yields the following closed-loop error dynamic system in a compact form

$$\dot{e}(t) = \begin{cases} [I_N \otimes A - \varrho(H_0 \otimes BK)]e(t),\ t \in [t_{2k}, t_{2k+1}), \\ \\ [I_N \otimes A - \vartheta(H_{r(t)} \otimes BF)]e(t), t \in [t_{2k+1}, t_{2(k+1)}), \end{cases}$$

where H_0 and $H_{r(t)}$ are the information-exchange matrices of the initial graph $\mathcal{G}_0$ and graph $\mathcal{G}_{r(t)}$ under malicious cyber-attacks, respectively. Here H_0 is a nonsingular matrix.

D. Attack Frequency and Attack Length Rate

Based on [26], it is obvious that the attack amount is not arbitrary and suitable conditions must be imposed. Motivated by a slowly switching mechanism in [27], the following definitions are introduced to solve the studied problem.

Definition 2: (Attack Frequency) For any $T_2 > T_1 \geq t_0$, let $N_f(T_1, T_2)$ denote the number of attacks taking place over $[T_1, T_2)$. Thus, $F_f(T_1, T_2) = \frac{N_f(T_1, T_2)}{T_2 - T_1}$ is defined as the attack frequency over $[T_1, T_2)$ for all $T_2 > T_1 \geq t_0$.

Definition 3: (Attack Length Rate) For any $t > 0$, denote $T_a(t_0, t)$ as the total time interval for multi-agent systems under attacks during $[t_0, t)$. Thus, $\frac{T_a(t_0,t)}{t - t_0}$ is defined as the attack length rate over $[t_0, t)$.

Remark 2: Note that H_0 is a nonsingular matrix, while $H_{r(t)}$ may be a reducible matrix. Even though H_0 provides the possibility of consensus tracking, the existence of paralyzed topologies $H_{r(t)}$ may totally destroy the secure consensus tracking performance. To overcome this difficulty, suitable conditions must be imposed on both attack frequency and length rate as it is important to determine the amount of attacks that a system can tolerate before undergoing instability.

Remark 3: As defined in [26] for a multi-agent system under attacks, Definitions 2 and 3 can specify the class of attack signals in terms of their frequency and length rate.

E. Stability Analysis

The following two lemmas are provided as a basis for the development of the main result.

Lemma 1: For multi-agent systems (1) without being attacked by any strategic attacks, if there exists a unique symmetric positive definite matrix $P > 0$ such that the following algebraic Riccati equation (ARE) is satisfied

$$PA + A^T P - PBR^{-1}B^T P + Q = 0, \tag{11}$$

where $R > 0$ and $Q > I$ are two symmetric positive definite matrices. Then, under the proposed distributed controller (10), for a selected Lyapunov function $V_a(e(t))$ and a positive constant $\alpha = \lambda_{\min}(Q)/\lambda_{\max}(P) > 0$, it holds that

$$V_a(e(t)) \leq e^{-\alpha(t - t_0)} V_a(e(t_0)). \tag{12}$$

Proof: Choose a Lyapunov function candidate as:

$$V_a(e(t)) = \sum_{i=1}^{N} e_i^T(t)\theta_i^{-1} P e_i(t),\ i = 1,\ 2,\ \cdots,\ N, \tag{13}$$

where θ_i^{-1} is similarly given as in Lemma 4 [28] such that $\Phi = \Theta H_0 + H_0^T \Theta > 0$. One such Θ is given by $\mathrm{diag}\{\theta_1^{-1}, \cdots, \theta_N^{-1}\}$ where $\theta = [\theta_1^{-1}, \cdots, \theta_N^{-1}]^T = (H_0^T)^{-1}\mathbf{1}$.

Taking the time derivative of $V_a(e(t))$ along the closed-loop systems yields the following equality in a compact form

$$\begin{aligned} \dot{V}_a(e(t)) &= e^T(t)(\Theta \otimes PA + \Theta \otimes A^T P)e(t) \\ &\quad -\varrho e^T(t)((\Theta H_0 + H_0^T \Theta) \otimes PBK)e(t). \end{aligned} \tag{14}$$

Substituting $K = R^{-1}B^T P$ into (14) yields

$$\begin{aligned} \dot{V}_a(e(t)) &= e^T(t)(\Theta \otimes PA + \Theta \otimes A^T P)e(t) \\ &\quad -\varrho e^T(t)((\Theta H_0 + H_0^T \Theta) \otimes PBR^{-1}B^T P)e(t) \\ &\leq e^T(t)(\Theta \otimes (PA + A^T P))e(t) \\ &\quad -\varrho\lambda_{\min} e^T(t)(I_N \otimes PBR^{-1}B^T P)e(t) \\ &\leq e^T(t)(\Theta \otimes (PA + A^T P))e(t) - \varrho\lambda_{\min}\theta_{\min} \\ &\quad \times e^T(t)(\Theta \otimes PBR^{-1}B^T P)e(t), \end{aligned} \tag{15}$$

where $\theta_{\min} = \min_i \theta_i$, $i = 1, 2, \cdots, N$, and $\lambda_{\min} = \lambda_{\min}(\Phi)$.

Provided the coupling strength $\varrho > (\lambda_{\min}\theta_{\min})^{-1}$, it follows from (11) that the expression in (15) can be rewritten as

$$\begin{aligned}\dot{V}_a(e(t)) &\leq e^T(t)[\Theta \otimes (PA + A^TP - PBR^{-1}B^TP)]e(t)\\ &= -e^T(t)(\Theta \otimes Q)e(t). \end{aligned} \quad (16)$$

Given that $-Q \leq -\lambda_{\min}(Q)I = -\alpha\lambda_{\max}(P)I \leq -\alpha P$ and $\alpha = \lambda_{\min}(Q)/\lambda_{\max}(P)$, (16) is further rewritten as

$$\dot{V}_a(e(t)) \leq -\alpha e^T(t)(\Theta \otimes P)e(t) = -\alpha V_a(e(t)). \quad (17)$$

Integrating both sides of (16) over $[t_0, t)$ leads to

$$V_a(e(t)) \leq e^{-\alpha(t-t_0)}V_a(e(t_0)).$$

Thus, the proof is completed. ■

Next, we consider that the multi-agent system (1) is subject to strategic attacks satisfying a random Markov process. Before presenting the result, the following assumption is given on possible graphs under strategic attacks.

Assumption 2: The paralyzed topology $\mathcal{G}_{r(t)}$ under strategic attacks are balanced and the union of all digraphs consisting of the leader and the N followers contains a spanning tree rooted at the leader.

Lemma 2: For multi-agent systems (1), if there exists a symmetric positive definite matrix $S > 0$ such that the following algebraic Riccati inequality (ARI) is satisfied

$$SA + A^TS - SBT^{-1}B^TS - \beta S < 0, \quad (18)$$

where $T > 0$ is a symmetric positive definite matrix, then, under the proposed distributed controller (10) with Assumption 2, for a selected Lyapunov function $V_b(e(t))$ and a constant $\beta > 0$, the following expression can be obtained:

$$E\{V_b(e(t))\} \leq e^{\beta(t-t_0)}E\{V_b(e(t_0))\}. \quad (19)$$

Proof: Choose a Lyapunov function candidate as

$$V_b(e(t)) = \sum_{i=1}^{N} e_i^T(t)Se_i(t),\ i = 1, 2, \cdots, N. \quad (20)$$

Based on Lemma 4.2 in [32], the stochastic Lyapunov function candidate of (20) w.r.t the Markov jump process is

$$V_b^p(e(t)) = E[e^T(t)(I_N \otimes S)e(t)\boldsymbol{\chi}_{\{r(t)=p\}}], \forall p \in \mathcal{S}, \quad (21)$$

where $r(t)$ used to model the strategic attacks on graphs is given in Section II-A, and for a real function $r(t)$, its indicator function of event $r(t) = p$ is defined by

$$\boldsymbol{\chi}_{\{r(t)=p\}} = \begin{cases} 1, \text{ if } r(t) = p, \\ 0, \text{ if } r(t) \neq p. \end{cases} \quad (22)$$

Based on Lemma 4.2 in [32], the stochastic derivative of $V_b^p(e(t))$ along the closed-loop error system is expressed as

$$\begin{aligned} V_b^p(e(t)) &= E[(de(t))^T(I_N \otimes S)e(t)\boldsymbol{\chi}_{\{r(t)=p\}}]\\ &\quad +E[e^T(t)(I_N \otimes S)de(t)\boldsymbol{\chi}_{\{r(t)=p\}}]\\ &\quad + \sum_{q=1}^{s} \gamma_{qp}V_b^q(e(t))dt + o(dt)\\ &= E\{e^T(t)[I_N \otimes SA + I_N \otimes A^TS\\ &\quad -\vartheta(H_p \otimes SBF + (H_p \otimes SBF)^T)]e(t)\\ &\quad + \sum_{q=1}^{s} \gamma_{qp}V_b^q(e(t))dt + o(dt)\}, \end{aligned} \quad (23)$$

where $V_b^q(e(t))$ denotes the Lyapunov function for $r(t) = q$.

Suppose that the signal $\gamma(t)$ starts at an invariant distribution $\pi = [\pi_1,\ \pi_2,\ \cdots,\ \pi_s]$ as given in [33], selecting the coupling strength $\vartheta \geq (2\pi_{\min}\lambda_{\min}(\hat{H}_{un}))^{-1}$ with $\pi_{\min} = \min_{p\in\mathcal{S}}\{\pi_p\}$, $\mathcal{S} = \{1, 2, ..., s\}$, and substituting the controller gain matrix $F = T^{-1}B^TS$ into (23) yield the following expression by bearing in mind that $\pi_p \geq \pi_{\min}$,

$$\begin{aligned}\frac{dV_b(e(t))}{dt} &\leq E[e^T(t)(I_N \otimes SA + I_N \otimes A^TS)e(t)]\\ &\quad - E[e^T(t)(\tilde{H} \otimes SBT^{-1}B^TS)e(t)], \end{aligned} \quad (24)$$

where $\tilde{H} = (H_{un} + H_{un}^T)/(2\lambda_{\min}(\hat{H}_{un}))$, $H_{un} = \sum_{p=1}^{s} H_p$ is the information-exchange matrix of the union of all digraphs $\mathcal{G}_p$, $p \in \mathcal{S}$ and $\hat{H}_{un}$ is its corresponding information-exchange of the mirror of the union of $\mathcal{G}_p$, $p \in \mathcal{S}$.

Take a unitary matrix $\Psi = [\psi_1, \psi_2, \cdots, \psi_N]$, where ψ_i is an orthonormal eigenvector of $\hat{H}_{un}$ associated with eigenvalue $\lambda_i(\hat{H}_{un})$, i.e., $\psi_i^T\hat{H}_{un} = \lambda_i(\hat{H}_{un})\psi_i^T$ for all $i = 1, 2, \cdots, N$. Similarly, defining $\tilde{e}(t) = (\Psi^T \otimes I_N)e(t)$ gives

$$\begin{aligned} &e^T(t)[I_N \otimes (SA + A^TS) - \tilde{H} \otimes SBT^{-1}B^TS]e(t)\\ =& \sum_{j=1}^{N} \tilde{e}_j^T(t)(SA + A^TS - \frac{\lambda_j(\hat{H}_{un})}{\lambda_{\min}(\hat{H}_{un})}SBT^{-1}B^TS)\tilde{e}_j(t)\\ \leq& \sum_{j=1}^{N} \tilde{e}_j^T(t)(SA + A^TS - SBT^{-1}B^TS)\tilde{e}_j(t). \end{aligned} \quad (25)$$

Since $SA+A^TS-SBT^{-1}B^TS-\beta S < 0$ in (18), it follows from (25) that (24) can be rewritten as

$$E\{\dot{V}_b(e(t))\} \leq \beta E\{e^T(t)(I_N \otimes S)e(t)\} \leq \beta E\{V_b(e(t))\},$$

which yields (19) and the proof is completed. ■

Next, a multi-step design procedure is developed for selecting the control parameters of (10).

Algorithm 1: Under Assumptions 1 and 2, the proposed distributed control law (10) can be constructed as follows.

(1) Solve the following algebraic Riccati equation (ARE)

$$PA + A^TP - PBR^{-1}B^TP + Q = 0, \quad (26)$$

to get a matrix $P > 0$.

(2) Solve the following algebraic Riccati inequality (ARI)

$$SA + A^TS - SBT^{-1}B^TS - \beta S < 0, \quad (27)$$

to get a matrix $S > 0$ for a given positive scalar β.

(3) Design the feedback control gains of (10) as

$$K = R^{-1}B^TP,\ F = T^{-1}B^TS, \quad (28)$$

where $R > 0$ and $T > 0$ are two given symmetric positive definite matrices, P and S are obtained by solving ARE (26) and ARI (27), respectively.

(4) Choose the coupling strength satisfying:

$$\varrho > (\lambda_{\min}\theta_{\min})^{-1},\ \vartheta \geq (2\pi_{\min}\lambda_{\min}(\hat{H}_{un}))^{-1}, \quad (29)$$

where $\lambda_{\min} = \lambda_{\min}(\Phi)$, $\theta_{\min} = \min_i \theta_i$, $i = 1, 2, \cdots, N$, and $\pi_{\min} = \min_{p\in\mathcal{S}}\{\pi_p\}$, $\mathcal{S} = \{1, 2, ..., s\}$.

Next, according to this designed Algorithm 1, sufficient conditions on secure consensus tracking are developed for multi-agent systems (1) subject to strategic attacks. The main result is thus described as follows.

Theorem 2: Consider the multi-agent systems (1) subject to strategic attacks. Suppose that Assumptions 1 and 2 hold. Under the proposed control law $u_i(t)$ in (10), all the agents can achieve secure consensus tracking in mean-square sense, provided that the following two conditions are satisfied:

1. There exists a constant $\eta^* \in (0, \alpha)$ such that the *attack length rate* satisfies

$$\frac{T_a(t_0,t)}{t-t_0} \leq \frac{\alpha-\eta^*}{\alpha+\beta}. \tag{30}$$

2. There exists a constant $\eta \in (0, \eta^*)$ such that the *attack frequency* $F_f(t_0,t)$ satisfies

$$F_f(t_0,t) = \frac{N_f(t_0,t)}{t-t_0} \leq F_f^* = \frac{\eta^*-\eta}{2\ln(\mu)}, \tag{31}$$

where $\mu = \max\{\frac{\theta_{\max}\lambda_{\max}(P)}{\lambda_{\min}(S)}, \frac{\lambda_{\max}(S)}{\theta_{\min}\lambda_{\min}(P)}\} \geq 1$, $\theta_{\min} = \min_i \theta_i$, and $\theta_{\max} = \max_i \theta_i$, $i = 1, 2, \cdots, N$.

Moreover, the state decay estimation is given by

$$E\{\|e_i(t)\|^2\} \leq \phi e^{-\eta(t-t_0)} E\{\|e_i(t_0)\|^2\}, \tag{32}$$

where $\phi = \frac{a}{b}$, $a = \max\{\lambda_{\max}(\theta_i^{-1}P),\ \lambda_{\max}(S)\}$, $b = \min\{\lambda_{\min}(\theta_i^{-1}P),\ \lambda_{\min}(S)\}$, $i = 1, 2, \cdots, N$.

Proof: Based on Lemmas 1 and 2, the following piecewise Lyapunov-like functional candidate is defined as $V(t) = V_{\sigma(t)}(e(t))$, where $\sigma(t) = a$ or b is a switching signal, specifically, to activate the running time of the controller.

$$V(t) = \begin{cases} V_a(e(t)), \text{ if } t \in [t_{2k}, t_{2k+1}), \\ V_b(e(t)), \text{ if } t \in [t_{2k+1}, t_{2(k+1)}), \end{cases} \tag{33}$$

where the Lyapunov functions $V_a(e(t))$ and $V_b(e(t))$ are defined in (13) and (20), respectively.

Suppose V_a is activated in $[t_{2k}, t_{2k+1})$ and V_b is activated in $[t_{2k+1}, t_{2(k+1)})$. It follows from Lemmas 1 and 2 that

$$\begin{aligned} & E\{V(t)\} \\ \leq\ & \begin{cases} e^{-\alpha(t-t_{2k})} E\{V_a(t_{2k})\}, \text{ if } t \in [t_{2k}, t_{2k+1}), \\ e^{\beta(t-t_{2k+1})} E\{V_b(t_{2k+1})\}, \text{ if } t \in [t_{2k+1}, t_{2(k+1)}). \end{cases} \end{aligned} \tag{34}$$

Note that the closed-loop error system is switched at $t = t_{2k}^+$ and $t = t_{2k+1}^+$. Next, we discuss two cases for $t \in [t_{2k}, t_{2k+1})$ and $t \in [t_{2k+1}, t_{2(k+1)})$, respectively.

Case I: if $t \in [t_{2k}, t_{2k+1})$, it follows from (34) that

$$\begin{aligned} & E\{V(t)\} \\ \leq\ & e^{-\alpha(t-t_{2k})} E\{V_a(t_{2k})\} \leq \mu e^{-\alpha(t-t_{2k})} E\{V_b(t_{2k}^-)\} \\ \leq\ & \mu e^{-\alpha(t-t_{2k})} [e^{\beta(t_{2k}-t_{2k-1})} E\{V_b(t_{2k-1})\}] \\ \leq\ & \mu e^{-\alpha(t-t_{2k})} [e^{\beta(t_{2k}-t_{2k-1})} \mu E\{V_a(t_{2k-1}^-)\}] \\ =\ & \mu^2 e^{-\alpha(t-t_{2k})} e^{\beta(t_{2k}-t_{2k-1})} E\{V_a(t_{2k-1}^-)\} \\ \leq\ & \mu^2 e^{-\alpha(t-t_{2k})} e^{\beta(t_{2k}-t_{2k-1})} \\ & \times [e^{-\alpha(t_{2k-1}-t_{2(k-1)})} E\{V_a(t_{2(k-1)})\}] \\ \leq\ & \cdots \\ \leq\ & \mu^{2k} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V_a(t_0)\}. \end{aligned} \tag{35}$$

Case II: if $t \in [t_{2k+1}, t_{2(k+1)})$, it follows from (34) that

$$\begin{aligned} & E\{V(t)\} \\ \leq\ & e^{\beta(t-t_{2k+1})} E\{V_b(t_{2k+1})\} \leq \mu e^{\beta(t-t_{2k+1})} E\{V_a(t_{2k+1}^-)\} \\ \leq\ & \mu e^{\beta(t-t_{2k+1})} [e^{-\alpha(t_{2k+1}-t_{2k})} E\{V_a(t_{2k})\} \\ \leq\ & \cdots \\ \leq\ & \mu^{2k+1} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V_a(t_0)\}. \end{aligned} \tag{36}$$

According to Definition 2, $N_f(t_0,t) = k$ for $t \in [t_{2k}, t_{2k+1})$ and $N_f(t_0,t) = k+1$ for $t \in [t_{2k+1}, t_{2(k+1)})$. Thus, for $\forall t \geq t_0$, it follows from (35) and (36) that

$$E\{V(t)\} \leq \mu^{2N_f(t_0,t)} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V(t_0)\}. \tag{37}$$

Based on (30), it holds that

$$-\alpha(t-t_0-T_a(t_0,t)) + \beta T_a(t_0,t) \leq -\eta^*(t-t_0), \tag{38}$$

which implies that

$$e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} \leq e^{-\eta^*(t-t_0)}. \tag{39}$$

Based on (31), it is clear that

$$e^{2N_f(t_0,t)\ln(\mu)} \leq e^{(\eta^*-\eta)(t-t_0)}. \tag{40}$$

Thus, substituting (38)-(40) into (37) yields

$$E\{V(t)\} \leq e^{-\eta(t-t_0)} E\{V_0(t_0)\}. \tag{41}$$

From (33), it is not difficult to obtain that

$$bE\{\|e_i(t)\|^2\} \leq E\{V(t)\},\ E\{V(t_0)\} \leq aE\{\|e_i(t_0)\|^2\}. \tag{42}$$

Thus, combining (41) and (42) yields the following state decay estimation of consensus tracking error

$$E\{\|e_i(t)\|^2\} \leq \phi e^{-\eta(t-t_0)} E\{\|e_i(t_0)\|^2\}. \tag{43}$$

According to (43), $e_i(t) \to 0$ as $t \to +\infty$, which indicates that $x_i(t) \to x_0(t)$ as $t \to +\infty$. ■

F. Extension to Discrete-time Case

The objective is to design a distributed controller $u_i(k)$ for a discrete-time linear multi-agent system (2) under strategic attacks satisfying a random discrete-time Markov process with a transition probability matrix $\Lambda = (\Lambda_{pq})$, which is given by

$$\Lambda_{pq} = \Pr\text{ob}\{r(k+1) = q | r(k) = p\},\ k \in \mathbb{N}_0. \tag{44}$$

Thus, a distributed secure consensus tracking control problem for discrete-time systems (2) is defined as follows.

Definition 4: The distributed resilient control law $u_i(k)$ solves a secure consensus tracking problem in mean-square sense for discrete-time linear multi-agent system (2) under strategic attacks, if there exists a scalar $c > 0$ and a decay rate $0 < \upsilon < 1$ such that for all $k > k_0$,

$$E\left\{\|x_i(k) - x_0(k)\|^2\right\} \leq c\upsilon^{(k-k_0)} E\left\{\|x_i(k_0) - x_0(k_0)\|^2\right\}.$$

Similar to Section III-C, the following distributed control law is proposed to achieve secure consensus tracking

$$u_i(k) = \begin{cases} \tilde{\varrho}\tilde{K}\delta_i^0(k),\ k \in [k_{2m}, k_{2m+1}), \\ \tilde{\vartheta}\tilde{F}\delta_i^{r(k)}(k),\ k \in [k_{2m+1}, k_{2(m+1)}), \end{cases} \tag{45}$$

where $m \in \mathbb{N}_0$ and $\delta_i^\hbar(k) = \sum_{j=1}^N a_{ij}^\hbar (x_i(k) - x_j(k)) + b_i^\hbar (x_i(k) - x_0(k))$, $\hbar = 0, r(k)$.

Thus, substituting (45) into system (2) yields the following closed-loop error systems in a compact form

$$e(k+1) = \begin{cases} [I_N \otimes \tilde{A} - \tilde{\varrho}(H_0 \otimes \tilde{B}\tilde{K})]e(k), \text{ if } k \in \Omega_1, \\ [I_N \otimes \tilde{A} - \tilde{\vartheta}(H_{r(k)} \otimes \tilde{B}\tilde{F})]e(k), \text{ if } k \in \Omega_2, \end{cases} \tag{46}$$

where $\Omega_1 = [k_{2m}, k_{2m+1})$ and $\Omega_2 = [k_{2m+1}, k_{2(m+1)})$.

Algorithm 3: Under Assumptions 1 and 2, the proposed distributed control law (45) can be constructed as follows.

(1) Solve the following algebraic Riccati equation (ARE)

$$\tilde{A}^T\tilde{P}\tilde{A}-\tilde{P}-\tilde{A}^T\tilde{P}\tilde{B}(\tilde{B}^T\tilde{P}\tilde{B}+\tilde{R})^{-1}\tilde{B}^T\tilde{P}\tilde{A}+\tilde{Q}=0, \quad (47)$$

to get a matrix $\tilde{P}>0$.

(2) Solve the following algebraic Riccati inequality (ARI)

$$\tilde{A}^T\tilde{S}\tilde{A}-\lambda_+\tilde{S}-\gamma\tilde{A}^T\tilde{S}\tilde{B}(\tilde{B}^T\tilde{S}\tilde{B}+\tilde{T})^{-1}\tilde{B}^T\tilde{S}\tilde{A}<0, \quad (48)$$

to get a matrix $\tilde{S}>0$ for constants $\lambda_+>1$ and $\gamma\in[0,1)$.

(3) Design the feedback control gains of (45) as

$$\tilde{K}=(\tilde{B}^T\tilde{P}\tilde{B}+\tilde{R})^{-1}\tilde{B}^T\tilde{P}\tilde{A}, \ \tilde{F}=(\tilde{B}^T\tilde{S}\tilde{B}+\tilde{T})^{-1}\tilde{B}^T\tilde{S}\tilde{A}, \quad (49)$$

where $\tilde{R}>0$ and $\tilde{T}>0$ are two given matrices.

(4) Choose the coupling strength satisfying

$$|\tilde{\varrho}\lambda_i(H_0)-1|<\gamma_0, \ \tilde{\vartheta}\in\Im, \quad (50)$$

where $\lambda_i(H_0)$ is the nonzero eigenvalues of H_0, $\gamma_0=[\sigma_{\max}(\tilde{Q}^{-\frac{1}{2}}\tilde{A}^T\tilde{P}\tilde{B}(\tilde{B}^T\tilde{P}\tilde{B}+\tilde{R})^{-1}\tilde{B}^T\tilde{P}\tilde{A}\tilde{Q}^{-\frac{1}{2}})]^{-\frac{1}{2}}$, and $\Im=\{\tilde{\vartheta}\in\mathbb{R}|\tilde{\vartheta}^2\lambda_{\max}(\sum_{p=1}^s H_p^TH_p)-2\tilde{\vartheta}\tilde{\pi}_{\min}\lambda_{\min}(\hat{H}_{un})=-\gamma(\tilde{\vartheta})<-\gamma_1<0\}$ with $\gamma_1<1$ and $\tilde{\pi}_{\min}\lambda_{\min}(\hat{H}_{un})>(\gamma_1\lambda_{\max}(\sum_{p=1}^s H_p^TH_p))^{1/2}$, $\tilde{\pi}_{\min}=\min_{p\in\mathcal{S}}\{\tilde{\pi}_p\}$.

Next, sufficient conditions on secure consensus tracking are developed for systems (2) subject to strategic attacks.

Theorem 4: Consider the multi-agent system (2) subject to strategic attacks. Suppose that Assumptions 1 and 2 hold. Under the proposed $u_i(k)$ in (45), all the agents can achieve secure consensus tracking in mean-square sense, provided that the following two conditions are satisfied:

1. There exists a constant $\lambda_*\in(\lambda_-,\lambda_+)$ such that the *attack length rate* satisfies

$$\frac{T_a(k_0,k)}{k-k_0}\le\frac{\ln\lambda_*-\ln\lambda_-}{\ln\lambda_+-\ln\lambda_-}. \quad (51)$$

2. There exists a constant $\lambda_d^2\in(\lambda_*,1)$ such that the *attack frequency* $F_f(k_0,k)$ satisfies

$$F_f(k_0,k)=\frac{N_f(k_0,k)}{k-k_0}\le F_f^*=\frac{2\ln\lambda_d-\ln\lambda_*}{2\ln(\tilde{\mu})}, \quad (52)$$

where $\tilde{\mu}=\max\{\frac{\lambda_{\max}(\tilde{P})}{\lambda_{\min}(\tilde{S})},\frac{\lambda_{\max}(\tilde{S})}{\lambda_{\min}(\tilde{P})}\}\ge1$.

Moreover, the state decay estimation is given by

$$E\{\|e_i(k)\|^2\}\le\tilde{\phi}\upsilon^{(k-k_0)}E\{\|e_i(k_0)\|^2\}, \quad (53)$$

where $\upsilon=\lambda_d^2$, $\tilde{\phi}=\frac{\tilde{a}}{\tilde{b}}$, $\tilde{a}=\max\{\lambda_{\max}(\tilde{P}),\lambda_{\max}(\tilde{S})\}$, $\tilde{b}=\min\{\lambda_{\min}(\tilde{P}),\lambda_{\min}(\tilde{S})\}$.

Proof: Without loss of generality, suppose that there exists an infinite sequence $m=0,1,2,\cdots$, for $[k_{2m},k_{2(m+1)})$ such that when $k=k_{2m+1}$ the multi-agent system is subject to strategic attacks. That is, the multi-agent network $\mathcal{G}_{r(t)}$ is paralyzed during $[k_{2m+1},k_{2(m+1)})$, while it works well during $[k_{2k},k_{2m+1})$ for an initial graph $\mathcal{G}_0$. Choose the following piecewise Lyapunov-like function candidate as

$$\tilde{V}(k)=\begin{cases}\tilde{V}_a(e(k))=\sum_{i=1}^N e_i^T(k)\tilde{P}e_i(k), \text{if } k\in\Omega_1,\\ \tilde{V}_b(e(k))=\sum_{i=1}^N e_i^T(k)\tilde{S}e_i(k), \text{if } k\in\Omega_2,\end{cases}$$

where $i=1,2,\cdots,N$, Ω_1 and Ω_2 are given in (46).

Next, the proof will be presented with the following steps.

(I) The system (2) is not subject to any attacks. When $k\in\Omega_1$, calculating the difference of $\tilde{V}(k)$ in terms of

$$\Delta\tilde{V}_a(e(k))=\tilde{V}_a(e(k+1))-\tilde{V}_a(e(k)),$$

which is written as the following expression in a compact form

$$\begin{aligned}&\tilde{V}_a(e(k+1))-\tilde{V}_a(e(k))\\ =\ & e^T(k+1)(I_N\otimes\tilde{P})e(k+1)-e^T(k)(I_N\otimes\tilde{P})e(k)\\ =\ & e^T(k)[I_N\otimes\tilde{A}-\tilde{\varrho}(H_0\otimes\tilde{B}\tilde{K})]^T(I_N\otimes\tilde{P})\\ \times\ & [I_N\otimes\tilde{A}-\tilde{\varrho}(H_0\otimes\tilde{B}\tilde{K})]e(k)-e^T(k)(I_N\otimes\tilde{P})e(k)\\ =\ & e^T(k)[I_N\otimes\tilde{A}^T\tilde{P}\tilde{A}-2\tilde{\varrho}H_0\otimes\tilde{A}^T\tilde{P}\tilde{B}\tilde{K}]e(k)\\ +\ & \tilde{\varrho}^2e^T(k)[(H_0\otimes\tilde{B}\tilde{K})^T(I_N\otimes\tilde{P})(H_0\otimes\tilde{B}\tilde{K})]e(k)\\ -\ & e^T(k)(I_N\otimes\tilde{P})e(k). \end{aligned} \quad (54)$$

Substituting $\tilde{K}=(\tilde{B}^T\tilde{P}\tilde{B}+\tilde{R})^{-1}\tilde{B}^T\tilde{P}\tilde{A}$ into (54) and it follows from Algorithm 3 and Theorem 2 in [31] that $\Delta\tilde{V}_a(e(k))\le-e^T(k)\tilde{Q}e(k)\le-\lambda_a\tilde{V}_a(e(k))$, $\lambda_a=\lambda_{\min}(\tilde{Q})/\lambda_{\max}(\tilde{P})\in(0,1)$, which implies that

$$\tilde{V}_a(k+1)\le\lambda_-\tilde{V}_a(k), \ \lambda_-=1-\lambda_a<1. \quad (55)$$

(II) The system (2) is subject to strategic attacks on graphs. When $k\in\Omega_2$, similar to that in part (I), it is obtained that

$$\Delta\tilde{V}_b(e(k))=\tilde{V}_b(e(k+1))-\tilde{V}_b(e(k)), \quad (56)$$

where the stochastic Lyapunov function candidate of $\tilde{V}_b(e_i(k))$ w.r.t the Markov jump process is

$$\tilde{V}_b^p(e_i(k))=E[e^T(k)(I_N\otimes\tilde{S})e(k)\boldsymbol{\chi}_{\{r(k)=p\}}],\forall p\in\mathcal{S}, \quad (57)$$

where $r(k)$ is used to model the strategic attacks on graphs, and its indicator function of event $r(k)=p$ is defined by

$$\boldsymbol{\chi}_{\{\gamma(k)=p\}}=\begin{cases}1, \text{ if } r(k)=p,\\ 0, \text{ if } r(k)\ne p.\end{cases} \quad (58)$$

Based on Lemma 4.2 in [32], the stochastic difference of $\tilde{V}_b^p(e(t))$ is expressed as

$$\begin{aligned}\Delta\tilde{V}_b^p(e(k)) &= V_b^p(e(k+1))-\tilde{V}_b^p(e(k))\\ &= E[e^T(k+1)(I_N\otimes\tilde{S})e(k+1)\boldsymbol{\chi}_{\{r(k)=p\}}]\\ &\quad -E[e^T(k)(I_N\otimes\tilde{S})e(k)\boldsymbol{\chi}_{\{r(k)=p\}}]\\ &\quad +\sum_{q=1}^s\gamma_{qp}\tilde{V}_b^q(e(k))+o(k), \end{aligned} \quad (59)$$

which implies that for a positive constant $\lambda_b=\lambda^+-1>0$

$$\begin{aligned}&\Delta\tilde{V}_b^p(e(k))-\lambda_b\tilde{V}_b^p(e(k))\\ =\ & E\{e^T(k)[(I_N\otimes\tilde{A}-\tilde{\vartheta}(H_p\otimes\tilde{B}\tilde{F}))^T(I_N\otimes\tilde{S})\\ &\times(I_N\otimes\tilde{A}-\tilde{\vartheta}(H_p\otimes\tilde{B}\tilde{F}))-\lambda^+(I_N\otimes\tilde{S})]e(k)\}\\ &+\sum_{q=1}^s\gamma_{qp}\tilde{V}_b^q(e(k))+o(k). \end{aligned} \quad (60)$$

Since $\gamma(k)$ starts at the invariant distribution $\tilde{\pi}$, it follows from (59) and $\tilde{\pi}\ge\tilde{\pi}_{\min}$ that

$$\begin{aligned}&\Delta\tilde{V}_b(e(k))-\lambda_b\tilde{V}_b(e(k))\\ \le\ & E\{e^T[I_N\otimes\tilde{A}^T\tilde{S}\tilde{A}+\tilde{\vartheta}^2(\sum_{p=1}^s H_p^TH_p)\otimes\tilde{F}^T\tilde{B}^T\tilde{S}\tilde{B}\tilde{F}\\ &-2\tilde{\vartheta}\tilde{\pi}_{\min}\lambda_{\min}(\hat{H}_{un})\frac{H_{un}+H_{un}^T}{2\lambda_{\min}(\hat{H}_{un})}\otimes\tilde{A}^T\tilde{S}\tilde{B}\tilde{F})]e(k)\}\\ &-\lambda^+E\{e^T(k)(I_N\otimes\tilde{S})e(k)\}. \end{aligned} \quad (61)$$

Substituting $\tilde{F} = (\tilde{B}^T\tilde{S}\tilde{B} + \tilde{T})^{-1}\tilde{B}^T\tilde{S}\tilde{A}$ into (61) and it follows from Algorithm 3 and Theorem 1 in [31] that $\Delta\tilde{V}_b(e(k)) - \lambda_b\tilde{V}_b(e(k)) \leq 0$ holds, which implies that

$$E\{\tilde{V}_b(k+1)\} \leq \lambda_+ E\{\tilde{V}_b(k)\},\ \lambda_+ = 1 + \lambda_b > 1. \quad (62)$$

(III) Synthesizing the above two circumstances (I)-(II) into one, it follows from (55) and (62) that for any $k > 0$,

$$E\{\tilde{V}(k)\} \leq \begin{cases} \lambda_-^{k-k_{2m}} E\{\tilde{V}_a(k_{2m})\},\ \text{if } k \in \Omega_1, \\ \lambda_+^{k-k_{2m+1}} E\{\tilde{V}_b(k_{2m+1})\},\ \text{if } k \in \Omega_2, \end{cases} \quad (63)$$

where $0 < \lambda_- = 1 - \lambda_a < 1$ and $\lambda_+ = 1 + \lambda_b > 1$ imply that the Lyapunov function along the closed-loop systems (46) has an exponential decay rate λ_- or increase rate λ_+.

Similar to (35) and (36) in Theorem 2, we can obtain

Case I: if $k_{2m+1} \leq k \leq k_{2(m+1)}$,

$$\begin{aligned} & E\{\tilde{V}(k)\} \\ \leq\ & \lambda_+^{k-k_{2m+1}} E\{\tilde{V}_b(k_{2m+1})\} \leq \tilde{\mu}\lambda_+^{k-k_{2m+1}} E\{\tilde{V}_a(k_{2m+1}^-)\} \\ \leq\ & \tilde{\mu}\lambda_+^{k-k_{2m+1}}\lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_a(k_{2m})\} \\ \leq\ & \tilde{\mu}^2\lambda_+^{k-k_{2m+1}}\lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_b(k_{2m}^-)\} \\ \leq\ & \tilde{\mu}^3\lambda_+^{k-k_{2m+1}+k_{2m}-k_{2m-1}}\lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_a(k_{2m-1}^-)\} \\ \leq\ & \cdots \\ \leq\ & \tilde{\mu}^{2m+1}\lambda_+^{T_a(k_0,k)}\lambda_-^{k-k_0-T_a(k_0,k)} E\{\tilde{V}_a(k_0)\}. \end{aligned} \quad (64)$$

Case II: if $k_{2m} \leq k \leq k_{2m+1}$, similarly

$$E\{\tilde{V}(k)\} \leq \tilde{\mu}^{2m}\lambda_+^{T_a(k_0,k)}\lambda_-^{k-k_0-T_a(k_0,k)} E\{\tilde{V}_a(k_0)\}. \quad (65)$$

Thus, it follows from $N_f(k_0,k) = m$ for $k \in [t_{2m}, t_{2m+1})$ and $N_f(k_0,k) = m+1$ for $t \in [t_{2m+1}, t_{2(m+1)})$ that

$$E\{\tilde{V}(k)\} \leq \tilde{\mu}^{2N_f(k_0,k)}\lambda_+^{T_a(k_0,k)}\lambda_-^{k-k_0-T_a(k_0,k)} E\{\tilde{V}_a(k_0)\}. \quad (66)$$

Based on (51), it holds that

$$(\ln\lambda_- - \ln\lambda_+)T_a(k_0,k) \geq (\ln\lambda_- - \ln\lambda_*)(k-k_0), \quad (67)$$

which implies that

$$\lambda_+^{T_a(k_0,k)}\lambda_-^{k-k_0-T_a(k_0,k)} \leq (\lambda_*)^{k-k_0}. \quad (68)$$

Based on (52), it is clear that

$$\tilde{\mu}^{2N_f(k_0,k)} \leq e^{(2\ln\lambda_d - \ln\lambda_*)(k-k_0)} = (\frac{\lambda_d^2}{\lambda_*})^{k-k_0}. \quad (69)$$

Thus, substituting (67)-(68) into (66) yields

$$E\{\tilde{V}(k)\} \leq \lambda_d^{2(k-k_0)} E\{\tilde{V}(k_0)\}. \quad (70)$$

Thus, it gives

$$\tilde{b}E\{\|e_i(k)\|^2\} \leq E\{\tilde{V}(k)\},\ E\{\tilde{V}(k_0)\} \leq \tilde{a}E\{\|e_i(k_0)\|^2\}. \quad (71)$$

Combining (70) and (71) yields the following state decay estimation of consensus tracking error

$$E\{\|e_i(k)\|^2\} \leq \tilde{\phi}\upsilon^{(k-k_0)} E\{\|e_i(k_0)\|^2\},$$

where $\tilde{\phi} = \frac{\tilde{a}}{\tilde{b}}$ and υ are shown in Theorem 4. Thus, $e_i(k) \to 0$ as $k \to +\infty$, which that $x_i(k) \to x_0(k)$ as $k \to +\infty$. This completes the proof. ■

Remark 4: Theorems 2 and 4 show mean-square exponential consensus tracking for continuous-time and discrete-time multi-agent systems under strategic attacks, respectively. The divergence of tracking errors with the exponential increasing rates β in (19) and λ_+ in (62) are caused by strategic attacks. Fortunately, it follows from conditions (30) and (31) for continuous-time case and conditions (51) and (52) for discrete-time case that exponential convergence with decay rates η and υ are eventually obtained in (32) and (53), respectively.

IV. Numerical Simulations

Two numerical examples are provided to demonstrate the theoretical effectiveness for continuous-time and discrete-time linear multi-agent systems under strategic attacks.

Example 1: (Continuous-time consensus tracking)

In this example we consider a cooperative tracking problem with 1 leader agent and 6 follower agents. Each agent is a two–mass–spring system with a single force input, except for the leader agent, which is unforced. The dynamics of the ith agent are given in the form of (1) as provided in [34]:

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t),\ t \in \mathbb{R}_{\geq 0}, \quad (72)$$

where $x_i(t) = [x_{i1}(t), x_{i2}(t), x_{i3}(t), x_{i4}(t)]^T$ is the state vector for agent $i = 0, 1, \cdots, 6$ with $u_0(t) = 0$, and the system and input matrices A and B, respectively, are given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ \frac{-k_1-k_2}{m_1} & 0 & \frac{k_2}{m_1} & 0 \\ 0 & 0 & 0 & 1 \\ \frac{k_2}{m_2} & 0 & \frac{-k_2}{m_1} & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ \frac{1}{m_1} \\ 0 \\ 0 \end{bmatrix},$$

where m_1 and m_2 are masses, k_1 and k_2 are spring constants, and u_i is the force input of the ith mass, $i = 1, \cdots, 6$.

Let these agents receive information from their neighbors according to a communication topology. As described in Section II-A, we consider two cases:

(1) When the cyber system is not subject to an attack, the communication topology is shown in Fig. 2.

(2) When the cyber system is under strategic attacks modeled by a random Markov jump process, the communication topologies are shown in Fig. 3. It can be seen that each topology $\mathcal{G}_{r(t)},\ r(t) = 1, 2, 3$, is paralyzed while the union of $\mathcal{G}_{r(t)}$ has a spanning tree satisfying Assumption 2.

The objective of the secure consensus tracking control problem in mean-square sense is to design a resilient distributed controller $u_i(t)$ for system (72) under strategic attacks modeled by a random Markov jump process.

In simulations, choose the dynamic parameters $m_1 = 1.1$kg, $m_2 = 0.9$kg, $k_1 = 1.5$N/m, and $k_2 = 1$N/m. It is easy to check that (A, B) is stabilizable. To generate the attack model, the generator matrix is chosen as

$$\Upsilon = \begin{bmatrix} -0.1 & 0.02 & 0.08 \\ 0.3 & -0.5 & 0.2 \\ 0.1 & 0.1 & -0.2 \end{bmatrix}, \quad (73)$$

where the probabilities of choosing the attacker and defender strategies $f_p(k) = g_q(k) = 1/3,\ p, q = 1, 2, 3$, are used and the initial distribution of the random Markov jump process is given by its invariant distribution $\pi = [0.5882, 0.1500, 0.3235]$.

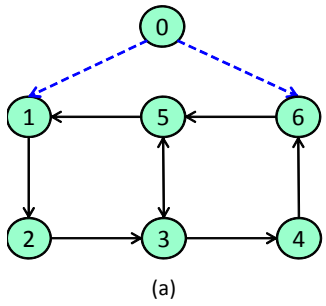

Fig. 2. Initial communication topologies $\mathcal{G}_0$ in Example 1.

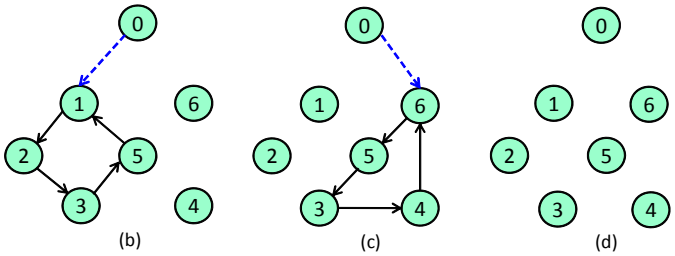

Fig. 3. Topologies under strategic attacks $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ in Example 1.

Based on Algorithm 1, constructing the controller (10) with $R = 2$, $T = 0.05$, $Q = 10I$, I is a 4×4 identity matrix, $\alpha = 4.31$, and $\beta = 0.19$ yields $K = [3.2477,\ 3.4850,\ -1.2477,\ 2.4193]$ and $F = [0.0386,\ 0.0873,\ -0.0155,\ 0.0272]$. Some calculations give the parameters $\lambda_{\min} = 0.0842$, $\theta_{\min} = 2.5$, $\lambda_{\min}(\hat{H}_{un}) = 0.1433$, $\mu = 11.1843$. According to Algorithm 1, set the coupling strength $\varrho = 15$ and $\vartheta = 25$. It follows from Theorem 2 that mean-square consensus tracking for system (72) with protocol (10) can be achieved if two conditions in (30) and (31) are satisfied. The switching signal is shown in Fig. 4, where $r(t) = 1, 2, 3$ is to describe the evolution of the cyber state under $\mathcal{G}_{r(t)}$ and $\sigma(t)$ is to describe the switching in high level to activate the running time of the designed controller. The total activation time of attacks is 3.2 seconds, which implies that (30) and (31) are satisfied. The state trajectories of the multi-agent systems are shown in Fig. 5 which imply that the agents can achieve consensus and track the leader. Use $E_c(t) = (1/6)\sqrt{\sum_{j=1}^{6} \|x_j(t) - x_0(t)\|}$ in Fig. 6 to denote the consensus tracking error of systems. This simulation demonstrates that secure consensus tracking can be achieved. The details on (30) and (31) are provided.

As given in (31), the *attack frequency* $F_f(t_0, t)$ satisfies

$$F_f(t_0, t) \leq \frac{\eta^* - \eta}{2\ln(\mu)} = \frac{3.31 - 0.31}{2\ln(11.1843)} = 0.6058,$$

which means that in a statistical sense, the attacks cannot occur more than 0.6058 times during a unit of time.

It follows from (30) that the *attack length rate* satisfies

$$\frac{T_a(t_0, t)}{t - t_0} \leq \frac{\alpha - \eta^*}{\alpha + \beta} = \frac{4.31 - 3.31}{4.31 + 0.19} = 0.2222, \qquad (74)$$

which means that in a statistical sense, average recovery time is less than $(\alpha - \eta^*)/((\alpha + \beta)F_f(t_0, t)) = 0.3665$ time unit.

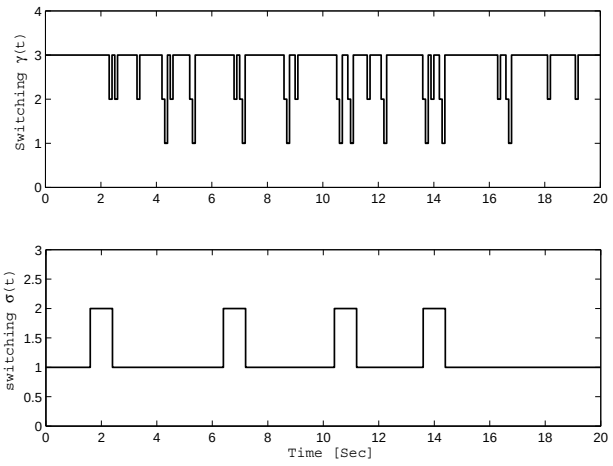

Fig. 4. Switching signal $\gamma(t)$ and $\sigma(t)$ in Example 1.

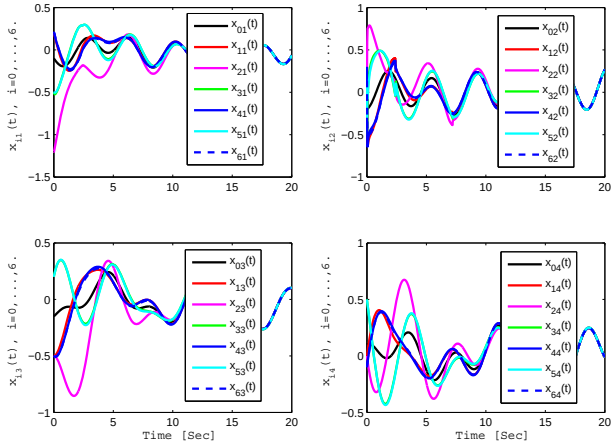

Fig. 5. State trajectories $x_{ij}(t)$ under the distributed control law (10).

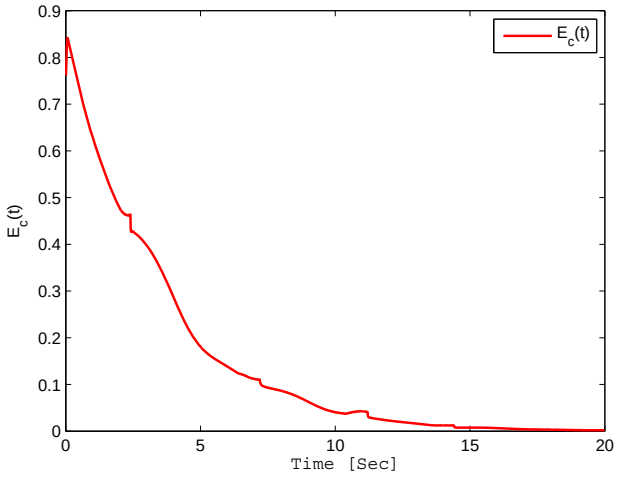

Fig. 6. Consensus tracking errors $E_c(t)$.

Example 2: (Discrete-time consensus tracking)
Consider the discrete-time dynamics of the ith agent as

$$x_i(k+1) = \tilde{A}x_i(k) + \tilde{B}u_i(k),\ k \in \mathbb{N}_0, \tag{75}$$

where the system and input matrices $\tilde{A}$ and $\tilde{B}$, respectively, are given by

$$\tilde{A} = \begin{bmatrix} -1.5 & 2.5 & 0 & 0 \\ -0.5 & -1 & 0.5 & 0 \\ 0 & 0 & 0 & 1 \\ 1.5 & 0 & -2 & 0 \end{bmatrix},\ \tilde{B} = \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}.$$

The communication topologies in cyber space are the same as that in Example 1. However, the transition probability matrix to generate the attack model for system (75) is

$$\Lambda = \begin{bmatrix} 0.1 & 0.4 & 0.5 \\ 0.2 & 0.5 & 0.3 \\ 0.3 & 0.3 & 0.4 \end{bmatrix}, \tag{76}$$

and the discrete-time Markov process starts at its invariant distribution $\tilde{\pi} = [0.2165, 0.4021, 0.3814]$.

Based on Algorithm 3, we construct the distributed control law (45) with the parameters selected as $\tilde{R} = 0.5$, $\tilde{T} = 0.8$, $\tilde{Q} = 0.4I$, $\lambda_- = 0.0035$, $\lambda_* = 0.6$, $\lambda_+ = 1.6$. According to Theorem 4, the simulation results are shown in Figs. 7-9. Use $E_d(k) = (1/6)\sqrt{\sum_{j=1}^{6} \|x_j(k) - x_0(k)\|}$ in Fig. 9 to denote the consensus tracking errors of the closed-loop discrete-time multi-agent system. This simulation demonstrates that secure consensus tracking can be achieved for systems under strategic attacks. The details on the conditions provided in Theorem 4 are shown as follows.

As given in (31), the *attack frequency* $F_f(k_0, k)$ satisfies

$$F_f(k_0, k) \le \frac{2\ln\lambda_d - \ln\lambda_*}{2\ln(\tilde{\mu})} = \frac{-0.1951 + 0.5108}{2 \times 0.2624} = 0.2298,$$

which means that in a statistical sense, the attacks cannot occur more than 0.2298 times during a unit of time.

It follows from (30) that the *attack length rate* satisfies

$$\frac{T_a(k_0, k)}{k - k_0} \le \frac{\ln\lambda_+ - \ln\lambda_*}{\ln\lambda_+ - \ln\lambda_-} = \frac{-0.5108 + 0.5108}{0.4700 + 5.6550} = 0.8399, \tag{77}$$

which means that in a statistical sense, the average recovery time is less than $\frac{\ln\lambda_+ - \ln\lambda_*}{(\ln\lambda_+ - \ln\lambda_-)F_f(k_0,k)}$ =3.6549 time unit.

V. Conclusions

In this paper, a distributed secure consensus tracking problem is studied for both continuous-time and discrete-time linear multi-agent systems under strategic attacks in cyber system whose dynamics are captured by a random Markov process. We formulate this problem from the perspective of a switched system with two-level switching sequences. Under the proposed hybrid stochastic secure control framework, a distributed resilient control law is developed to achieve exponential consensus tracking in mean square sense, provided that two conditions on the attack frequency and attack length rate are satisfied. Based on the solutions of the ARE and ARI, a design methodology is proposed to properly select the controller gains and the stability analysis is studied by using Lyapunov analysis together with graph theory.

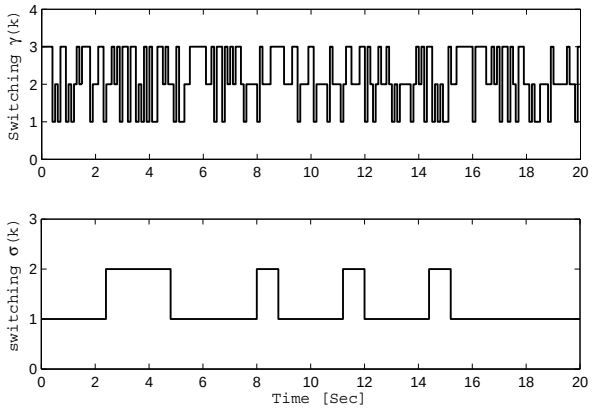

Fig. 7. Switching signal $\gamma(k)$ and $\sigma(k)$ in Example 2.

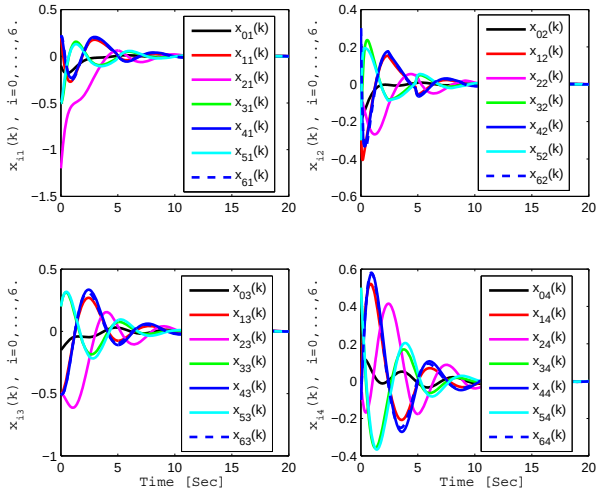

Fig. 8. State trajectories $x_{ij}(k)$ under the distributed control law (45).

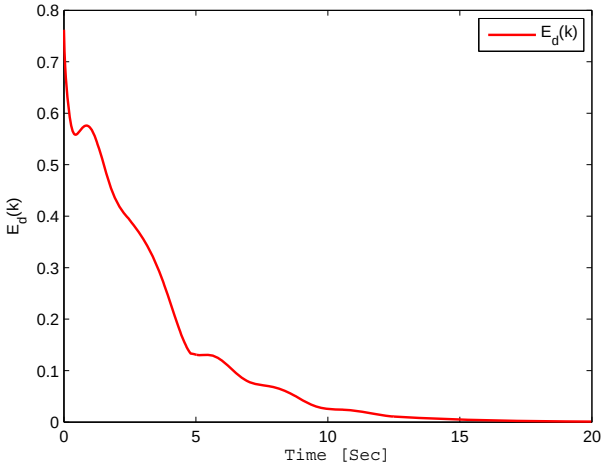

Fig. 9. Consensus tracking errors $E_d(k)$.

REFERENCES

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

[2] W. Ren, "Synchronization of coupled harmonic oscillators with local interaction", *Automatica*, 44(12): 3195–3200, 2008.

[3] M. Cao, C. Yu, B. Anderson, "Formation control using range-only measurements", *Automatica*, 47(4): 776–781, 2011.

[4] Z. Feng, C. Sun, G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," *IEEE Trans. Control Netw. Syst., to be published*, 2016, DOI:10.1109/TCNS.2016.2545869.

[5] Y. Dong, J. Huang, "A leader-following rendezvous problem of double integrator multi-agent systems", *Automatica*, 49(5): 1386–1391, 2013.

[6] L. Scardovi, R. Sepulchre, "Synchronization in networks of identical linear systems", *Automatica*, 45(11): 2557–2562, 2009.

[7] Y. Su, J. Huang, "Two consensus problems for discrete-time multi-agent systems with switching topology", *Automatica*, 48(9): 1988–1997, 2012.

[8] H. Su, Michael. Z. Q. Chen, J. Lam, Z. Lin, "Semi-global consensus of linear multi-agent systems with input saturation via low gain feedback", *IEEE Trans. Circuits Syst. I, Reg. Papers*, 60(7): 1881–1889, 2013.

[9] G. Hu, "Robust consensus tracking of a class of second-order multi-agent dynamic systems", *Syst. Control Lett.*, 61(1): 134–142, 2012.

[10] G. Wen, G. Hu, W. Yu, G. Chen, "Distributed H-infinity consensus of higher-order multi-agent systems with switching topologies", *IEEE Trans. Circuits Syst. II: Exp. Briefs*, 61(5): 359-363, 2014.

[11] C. Sun, G. Hu, L. Xie, "Robust consensus tracking for high-order multi-agent systems," *Int. J. Robust. Nonlinear Control*, 26(3): 578–598, 2015.

[12] S. Chen, Daniel W. C. Ho, L. Li, M. Liu, "Fault-tolerant consensus of multi-agent system with distributed adaptive protocol", *IEEE Trans. Cybern.*, 44(10): 2142–2155, 2015.

[13] D. Wang, N. Zhang, J. Wang, W. Wang, "A PD-like protocol with a time delay to average consensus control for multi-agent systems under an arbitrarily fast switching topology", *IEEE Trans. Cybern., to be published, 2016*, DOI:10.1109/TCYB.2016.2532898.

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

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

[16] I. Shames, A. Teixeira, H. Sandberg, K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties", *IEEE Trans. Cybern*, 44(11): 2024–2037, 2014.

[17] F. Pasqualetti, R. Carli, F. Bullo, "Attack Detection in cyber-physical systems", *IEEE Trans. Autom. Control*, 58(11): 2715–2729, 2013.

[18] L. Zhao, K. Park, Y. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown", *Phys. Rev. E*, 70(3), 035101(R), 2004.

[19] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, "Attack vulnerability of complex networks", *Phys. Rev. E*, 65(5), 056109, 2009.

[20] A. N. Bishop, I. Shames, "Link operations for slowing the spread of disease in complex networks", *Europhys. Lett.*, 95(1), 18005, 2011.

[21] M. Zhu, S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks", *IEEE Trans. Autom. Control*, 59(3): 804–808, 2014.

[22] W. Zeng, M. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems", *IEEE Trans. Cybern.*, 44(11): 2038–2049, 2014.

[23] D. Meng, K. Moore, "Studies on resilient control through multiagent consensus networks subject to disturbances", *IEEE Trans. Cybern.*, 44(11): 2050–2064, 2014.

[24] J. Moon, T. Basar, "Control over lossy networks: A dynamic game approach", *American Control Conference*, June 4–6, Portland, 2014.

[25] Q. Zhu, T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems", *IEEE Trans. Syst. Mag.*, 35(1): 46–65, 2015.

[26] Z. Feng, G. Hu, G. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks", *Int. J. Robust. Nonlinear Control*, 26(5): 896–918, 2015.

[27] J. Lian, Z. Feng, P. Shi, "Observer design for switched recurrent neural networks: An average dwell time approach", *IEEE Trans. Neural Netw.*, 22(10): 547–1556, 2011.

[28] Z. Li, G. Wen, Z. Duan, W. Ren, "Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs", *IEEE Trans. Autom. Control*, 60(6): 1152–1157, 2015.

[29] S. Liu, B. Chen, T. Zourntos, D. Kundur, K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid", *IEEE Trans. Smart Grid*, 5(3): 1183–1195, 2014.

[30] D. A. Bini, B. Iannazzoa, F. Poloni, "A fast newton's method for anonsymmetric algebraic Riccati equation", *SIAM J. Matrix Anal. Appl.*, 30(1): 276–290, 2008.

[31] K. H. Movric, K. You, F. Lewis, L, Xie, "Synchronization of discrete-time multi-agent systems on grphs using Riccati design", *Automatica*, 49(2): 414–423, 2013.

[32] M. D. Fragoso, O. L. V. Costa, "A unified approach for stochastic and mean square stability of continuous-time linear systems with Markovian jumping parameters and additive disturbances", *SIAM J. Control Optim.*, 44(4): 1165–1191, 2005.

[33] W. Li, Z. Wu, "Output tracking of stochastic high-order nonlinear systems with Markovian switching", *IEEE Trans. Autom. Control*, 58(6): 1585–1590, 2013.

[34] H. Zhang, F. Lewis, Z. Qu, "Lyapunov, adaptive, and optimal design techniques for cooperative systems on directed communication graphs", *IEEE Trans. Ind. Electronics*, 59(7): 3026–3041, 2012.

[35] M. Ye, G. Hu, "Game design and analysis for price based demand response: an aggregate game approach," *IEEE Trans. Cybern., to be published*, 2016, DOI:10.1109/TCYB.2016.2524452.