

doi: 10.12052/gdutxb.210078

两种不同脉冲欺骗攻击下随机多智能体系统的均方拟一致性

曾梓贤, 彭世国, 黄昱嘉, 谷志华, 冯万典
(广东工业大学 自动化学院, 广东 广州 510006)

摘要: 考虑实际应用中多智能体系统所处环境的复杂性及相关通信网络的开放性, 主要研究了一类随机多智能体系统在受到两种不同脉冲欺骗攻击情况下实现均方拟一致性问题。所考虑的两种脉冲欺骗攻击包括替代攻击和虚假数据注入攻击, 而攻击发生的概率则是通过引入服从伯努利分布的随机变量加以描述。结合随机过程相关知识和李雅普诺夫稳定性理论, 给出系统实现均方拟一致性充分条件。条件表明, 系统在遭受两种不同攻击的情况下, 误差能保持在一定的范围内。最后, 数值仿真验证了结果的有效性。

关键词: 多智能体系统; 随机噪声干扰; 替代攻击; 虚假数据注入攻击; 均方拟一致性
中图分类号: TP273 **文献标志码:** A **文章编号:** 1007-7162(2022)01-0071-07

Mean Square Quasi-consensus of Stochastic Multi-agent Systems Under Two Different Impulsive Deception Attacks

Zeng Zi-xian, Peng Shi-guo, Huang Yu-jia, Gu Zhi-hua, Feng Wan-dian
(School of Automation, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Considering the complexity of the environment and the openness of related communication networks, the problem of mean square quasi-consensus for a class of stochastic multi-agent systems under two different impulsive deception attacks is studied. The impulsive deception attacks considered here include replacement attack and false data injection attack, while the probabilities of attacks are described by introducing random variables that obey Bernoulli distribution. By employing the knowledge of stochastic process and Lyapunov stability theory, the sufficient conditions of quasi-consensus are given. The conditions show that the error of systems can be kept in a certain range under two different attacks. Finally, a numerical simulation is given to verify the effectiveness of the results.

Key words: multi-agent systems; random noise disturbances; replacement attacks; false data injection attacks; mean square quasi-consensus

随着网络技术的不断发展, 多智能体系统一致性问题深受学者的关注^[1-2], 并逐渐被应用到实际生活中, 如无人机编队、电网能源分配等^[3-4]。在实际应用中, 多智能体系统难免会遭受到如随机干扰、网络攻击等外部因素的干扰, 而这对其一致性有重要影响^[4-5]。

一般地, 随机干扰对多智能体系统的影响主要反映在系统动态特性或信息传输的信道中。前者可

表现为随机噪声和随机出现不确定项等干扰, 如文献[6]通过设计新颖的脉冲控制协议, 并基于广义伊藤公式与李雅普诺夫稳定性理论得到了系统实现均方一致性的充分条件; 文献[7]研究了一类具有随机出现不确定项的非线性多智能体系统的均方一致性问题。后者则一般体现在信息丢包和信道堵塞的建模中^[8]。

另一方面, 考虑到多智能体系统应用中环境的

收稿日期: 2021-05-21

基金项目: 国家自然科学基金资助项目(61973092); 广东省基础与应用基础研究基金资助项目(2019A1515012104)

作者简介: 曾梓贤(1997-), 男, 硕士研究生, 主要研究方向为多智能体系统一致性问题、非线性系统和欺骗攻击, E-mail: zzxian1007@163.com

通信作者: 彭世国(1967-), 男, 教授, 博士生导师, 主要研究方向为随机系统分析与控制、多智能体系统的分析与综合, E-mail: psg7202@126.com

复杂性及其通信网络的开放性,由网络攻击所引起的网络安全问题也不容忽视。由文献[9-11]可知,攻击会导致多智能体一致性性能达不到理想的要求,并可能进一步导致智能体间的通信瘫痪。一般地,网络攻击主要分为两大类:拒绝服务性攻击和欺骗攻击^[12]。在文献[13]中,作者指出在一般情况下,拒绝服务性攻击的目标可以是传感器、控制器或智能体间的传输数据,从而导致信号在传输过程中发生数据丢包或延时的问题。相比之下,欺骗攻击则可能会绕过系统的检测技术并进入系统内部,进而操控控制指令或篡改传输数据,致使系统性能下降甚至变得不稳定^[14]。

欺骗攻击可进一步分为虚假数据注入攻击和替代欺骗攻击等类型。虚假数据注入攻击主要是向控制器加入错误数据来破坏系统数据的完整性和准确性,如文献[15]将虚假数据引起的偏差加入到系统中来得到攻击下的系统动力学方程;文献[16]考虑了在传感器的数据传输通道中注入虚假数据情况下非线性多智能体系统一致性问题;文献[17]引入了伯努利变量来描述控制信号是否会受到虚假数据欺骗攻击。替代欺骗攻击则是指控制器受到攻击后会使控制信号被替代为相应的攻击信号,已有的关于欺骗攻击下的多智能体系统一致性的研究主要集中在传感器到控制器信道上的加性攻击,很少考虑替代攻击,文献[3]考虑替代攻击下利普希兹型非线性系统的一致性问题。值得注意的是,目前文献仅仅考虑虚假数据注入攻击或替代攻击^[17-19],而同时考虑两者对一致性问题的影响则还未得到相应的研究。如何设计两种攻击下控制器的模型以及如何进一步得到系统实现一致性的条件是一个待解决的问题。

基于上述分析,本文主要研究了一类领导跟随随机多智能体系统在受到两种不同脉冲欺骗攻击情况下实现均方拟一致性问题。利用李雅普诺夫稳定性理论,本文给出了系统实现均方拟一致性的充分条件及相应的误差上界。

本文主要创新点如下:建立了同时受到两种脉冲欺骗攻击和随机噪声干扰下系统的模型;引入服从伯努利分布的随机变量来解决攻击类型的描述及其攻击成功与否的问题。

1 问题描述与预备知识

1.1 图论

在多智能体系统中,智能体之间可以相互传递数据,而图论则是能够较好地描述上述关系的工具。

一般地,一个图可表示为 $G = (V, E, \bar{A})$,其中 V, E 和 $\bar{A} = [a_{ij}]_{N \times N}$ 分别表示图 G 的节点集、边集与连接矩阵,其中, N 是一个正整数。图中节点表示智能体,边则表示智能体间传递数据的关系,连接矩阵为反映智能体间的邻接权重矩阵。假设图 $\hat{G} = (\hat{V}, \hat{E}, \hat{A})$ 为无向图,包括 N 个跟随者和一个领导者,则有 $\hat{V} = \{\hat{v}_1, \hat{v}_2, \dots, \hat{v}_N\}$, $\hat{E} \subseteq \hat{V} \times \hat{V}$ 以及 $\hat{A} = [a_{ij}]_{N \times N}$ 。若智能体 i 与智能体 j 间可传递数据,则节点 $\hat{v}_i$ 与 $\hat{v}_j$ 间存在的一条边 $(i, j) \in \hat{E}$ 。若边 $(i, j) \in \hat{E}$,则有 $a_{ij} = a_{ji} > 0$,否则, $a_{ij} = 0$ 。此外,假设 $a_{ii} = 0$ 。图 $\hat{G}$ 的拉普拉斯矩阵表示为 $\hat{L} = [l_{ij}]_{N \times N}$,且有 $l_{ii} = \sum_{j \in N_i} a_{ij}$, $l_{ij} = -a_{ij}$, $i \neq j$ 。令 $N_i = \{v_j | (i, j) \in \hat{E}\}$,表示智能体 i 的邻居节点集。图 $\hat{G}$ 中领导者的标签用 0 表示。领导者与跟随者间的连接关系可由矩阵 C 所反映,其中 $C = \text{diag}\{c_1, c_2, \dots, c_N\}$ 是一个对角矩阵。若节点 $\hat{v}_i$ 与 $\hat{v}_0$ 间存在的一条边,则有 $c_i = 1$,否则 $c_i = 0$ 。此外,定义 $H = [h_{ij}]_{N \times N} = \hat{L} + C$,则有 $h_{ii} = l_{ii} + c_i$ 与 $h_{ij} = l_{ij}$, $i \neq j$ 。

1.2 问题描述及协议设计

考虑一类含有 N 个跟随者的多智能体系统,其中各跟随者的动力学特性描述如式(1)所示。

$$\begin{aligned} dx_i(t) = & [Ax_i(t) + p(t)f(t, x_i(t)) + \hat{u}_i(t)]dt + \\ & \bar{\sigma}(t, x_i(t))d\omega(t), t \geq t_0, i \in \mathcal{N} \end{aligned} \quad (1)$$

式中: $\mathcal{N} = \{1, 2, \dots, N\}$ 是一个有限集, $x_i(t) \in \mathbb{R}^n$ 与 $\hat{u}_i(t) \in \mathbb{R}^n$ 分别表示智能体 i 的状态变量与控制输入,其中, $\mathbb{R}^n$ 是 n 维欧几里得空间;函数 $f: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ 表示智能体 i 的非线性特性,其中, $\mathbb{R} = (-\infty, +\infty)$ 表示一个实数集;函数 $\bar{\sigma}: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^{n \times m}$ 为噪声强度函数; $\omega(t) \in \mathbb{R}^m$ 是定义在概率空间 $(\Omega, \mathcal{F}, \text{Pr})$ 上的 m 维维纳过程,且 $\omega_i(t)$ 与 $\omega_j(t)$, $i \neq j$ 相互独立; A 是已知合适维数的常数矩阵;随机变量 $p(t)$ 服从伯努利分布,与 $\omega(t)$ 相互独立且满足

$$\begin{cases} \text{Pr}(p(t) = 1) = \bar{p} \\ \text{Pr}(p(t) = 0) = 1 - \bar{p} \end{cases} \quad (2)$$

式中: $\bar{p} \in [0, 1]$ 是已知常数,且有 $E[p(t) - \bar{p}] = 0$,其中, $E[\cdot]$ 表示随机变量的数学期望。

另一方面,领导者智能体的状态量假设为 $x_0(t) \in \mathbb{R}^n$,其动力学特性描述为

$$\begin{aligned} dx_0(t) = & [Ax_0(t) + p(t)f(t, x_0(t))]dt + \\ & \bar{\sigma}(t, x_0(t))d\omega(t), \quad t \geq t_0 \end{aligned} \quad (3)$$

考虑控制协议同时遭受两种脉冲欺骗攻击即虚假数据注入脉冲攻击和替代脉冲攻击的影响。此外,引入两个伯努利随机变量来分别描述两种欺骗攻击成功与否。具体脉冲控制协议设计如式(4)所示。

$$\hat{\mathbf{u}}_i(t) = \sum_{k=1}^{\infty} [(1-\alpha_i(t))\eta_k(\sum_{j \in \mathcal{N}_i} a_{ij}(\mathbf{x}_i(t) - \mathbf{x}_j(t)) + c_i(\mathbf{x}_i(t) - \mathbf{x}_0(t))) + \alpha_i(t)d_k\xi_i(t) + \beta_i(t)\psi_k(\mathbf{x}_i(t) - \mathbf{x}_0(t))]\delta(t-t_k), i \in \mathcal{N} \quad (4)$$

式中: η_k, d_k 和 ψ_k 分别表示脉冲增益、替代攻击的强度和虚假数据注入攻击的强度, 且 η_k 与 ψ_k 需要满足条件一定的条件, 详见备注3. $\delta(\cdot)$ 表示狄拉克函数. $\{t_k, k \in \mathbb{N}^+\}$ 表示脉冲序列, 其中, $\mathbb{N}^+$ 是正整数集, 该序列满足 $0 = t_0 < t_1 < t_2 < \dots < t_k < \dots, \lim_{k \rightarrow \infty} t_k = +\infty$. $\xi_i(t)$ 表示替代攻击信号. 服从伯努利分布的随机变量 $\alpha_i(t)$ 与 $\beta_i(t)$ 分别用于描述替代攻击和虚假数据注入攻击是否发生. 若 $\alpha_i(t) = 1$, 则发生替代攻击; 若 $\beta_i(t) = 1$, 则发生虚假数据注入攻击; 否则不发生攻击. 此外, 假设 $\alpha_i(t)$ 与 $\beta_i(t)$ 相互独立, 且满足

$$\begin{cases} \Pr(\alpha_i(t) = 1) = \bar{\alpha}, \Pr(\alpha_i(t) = 0) = 1 - \bar{\alpha} \\ \Pr(\beta_i(t) = 1) = \bar{\beta}, \Pr(\beta_i(t) = 0) = 1 - \bar{\beta} \end{cases} \quad (5)$$

式中: $\bar{\alpha}, \bar{\beta} \in [0, 1]$ 为已知常数.

此外, 假设由式(1)和(3)所组成的领导跟随随机多智能体系统状态初值为 $\phi(t_0) = (\mathbf{x}_0^T(t_0), \mathbf{x}_1^T(t_0), \dots, \mathbf{x}_N^T(t_0))^T$, 其中 $t_0 \geq 0$ 为初始时刻.

备注1 如图1所示, 两种不同欺骗攻击发生在传感器到控制器或控制器到执行器的信道上, 且是相互独立的. 当替代攻击成功发生时, 控制信号将会被篡改为欺骗攻击信号; 当虚假数据注入攻击成功发生时, 虚假数据则会附加到控制信号中.

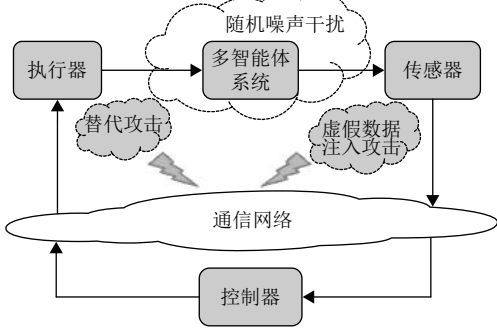


图1 两种不同欺骗攻击的攻击原理图

Fig.1 Configuration of two different deception attacks

将控制协议(4)代入系统(1)中, 可得到遭受两种欺骗攻击下跟随者的状态方程如下.

$$\begin{cases} d\mathbf{x}_i(t) = [\mathbf{A}\mathbf{x}_i(t) + p(t)\mathbf{f}(t, \mathbf{x}_i(t))]dt + \bar{\sigma}(t, \mathbf{x}_i(t))d\omega(t), \quad t \geq t_0, \quad t \neq t_k, \\ \Delta\mathbf{x}_i(t) = \mathbf{x}_i(t_k^+) - \mathbf{x}_i(t_k^-) = \beta_i(t_k)\psi_k(\mathbf{x}_i(t_k^-) - \mathbf{x}_0(t_k^-)) + \alpha_i(t_k)d_k\xi_i(t_k) + (1 - \alpha_i(t_k))\eta_k\left(\sum_{j \in \mathcal{N}_i} a_{ij}(\mathbf{x}_i(t_k^-) - \mathbf{x}_j(t_k^-)) + c_i(\mathbf{x}_i(t_k^-) - \mathbf{x}_0(t_k^-))\right), \quad t = t_k \end{cases} \quad (6)$$

式中: $\mathbf{x}_i(t_k^-) = \lim_{\Delta \rightarrow 0^-} \mathbf{x}_i(t_k + \Delta)$, $\mathbf{x}_i(t_k^+) = \lim_{\Delta \rightarrow 0^+} \mathbf{x}_i(t_k + \Delta)$. 此外, 假设 $\mathbf{x}_i(t)$ 在 $t = t_k, k \in \mathbb{N}^+$ 时刻是右连续的, 即 $\mathbf{x}_i(t_k^+) = \mathbf{x}_i(t_k)$.

为实现式(1)与式(3)所组成的领导跟随随机多智能体系统在两种欺骗攻击情况下的均方拟一致性, 构建如下误差系统.

$$\begin{cases} d\mathbf{e}_i(t) = [\mathbf{A}\mathbf{e}_i(t) + p(t)\bar{\mathbf{f}}(t, \mathbf{e}_i(t))]dt + \bar{\sigma}(t, \mathbf{e}_i(t))d\omega(t), \quad t \geq t_0, \quad t \neq t_k, \\ \Delta\mathbf{e}_i(t) = \mathbf{e}_i(t_k^+) - \mathbf{e}_i(t_k^-) = \beta_i(t_k)\psi_k\mathbf{e}_i(t_k^-) + \alpha_i(t_k)d_k\xi_i(t_k) + (1 - \alpha_i(t_k))\eta_k\left(\sum_{j \in \mathcal{N}_i} a_{ij}(\mathbf{e}_i(t_k^-) - \mathbf{e}_j(t_k^-)) + c_i\mathbf{e}_i(t_k^-)\right), \\ t = t_k \end{cases} \quad (7)$$

式中: $\mathbf{e}_i(t) = \mathbf{x}_i(t) - \mathbf{x}_0(t)$, $\bar{\mathbf{f}}(t, \mathbf{e}_i(t)) = \mathbf{f}(t, \mathbf{x}_i(t)) - \mathbf{f}(t, \mathbf{x}_0(t))$, $\bar{\sigma}(t, \mathbf{e}_i(t)) = \bar{\sigma}(t, \mathbf{x}_i(t)) - \bar{\sigma}(t, \mathbf{x}_0(t))$.

备注2 两种欺骗攻击是相互独立的, 也就是说它们的攻击时刻可以是不一样的, 但均属于脉冲序列 $\{t_k, k \in \mathbb{N}^+\}$. 不同欺骗攻击具体出现的攻击时刻由 $\{t_k, k \in \mathbb{N}^+\}$ 、 $\alpha_i(t_k)$ 与 $\beta_i(t_k)$ 共同决定.

此外, 令 $\mathbf{e}(t) = [\mathbf{e}_1^T(t), \mathbf{e}_2^T(t), \dots, \mathbf{e}_N^T(t)]^T$, $\bar{\mathbf{F}}(t, \mathbf{e}(t)) = [\bar{\mathbf{f}}^T(t, \mathbf{e}_1(t)), \bar{\mathbf{f}}^T(t, \mathbf{e}_2(t)), \dots, \bar{\mathbf{f}}^T(t, \mathbf{e}_N(t))]^T$ 与 $\bar{\sigma}(t, \mathbf{e}(t)) = [\bar{\sigma}^T(t, \mathbf{e}_1(t)), \bar{\sigma}^T(t, \mathbf{e}_2(t)), \dots, \bar{\sigma}^T(t, \mathbf{e}_N(t))]^T$. 利用克罗内克积可将误差系统(7)改写如下.

$$\begin{cases} d\mathbf{e}(t) = [(\mathbf{I}_N \otimes \mathbf{A})\mathbf{e}(t) + p(t)\bar{\mathbf{F}}(t, \mathbf{e}(t))]dt + \bar{\sigma}(t, \mathbf{e}(t))d\omega(t), \quad t \geq t_0, \quad t \neq t_k \\ \Delta\mathbf{e}(t) = [(\eta_k\mathbf{H} - \eta_k\mathbf{G}(t_k)\mathbf{H} + \psi_k\mathbf{A}(t_k)) \otimes \mathbf{I}_n]\mathbf{e}(t_k^-) + d_k(\mathbf{G}(t_k) \otimes \mathbf{I}_n)\xi(t_k), \quad t = t_k \end{cases} \quad (8)$$

式中: $\mathbf{G}(t_k) = \text{diag}\{\alpha_1(t_k), \alpha_2(t_k), \dots, \alpha_N(t_k)\} \in \mathbb{R}^{N \times N}$, $\mathbf{A}(t_k) = \text{diag}\{\beta_1(t_k), \beta_2(t_k), \dots, \beta_N(t_k)\} \in \mathbb{R}^{N \times N}$ 及 $\xi(t_k) = [\xi_1^T(t_k), \xi_2^T(t_k), \dots, \xi_N^T(t_k)]^T$.

备注3 当 $\alpha_i(t_k) = 0, \beta_i(t_k) = 1$ 时, 即控制信号仅受到虚假数据注入攻击时, η_k 与 ψ_k 需要满足条件 $\inf_{k \in \mathbb{N}^+} |\lambda_{\max}(\mathbf{I}_N + \eta_k\mathbf{H} - \eta_k\mathbf{G}(t_k)\mathbf{H} + \psi_k\mathbf{A}(t_k))| \geq 1$, 其中, $\lambda_{\max}(\cdot)$, $\lambda_{\min}(\cdot)$ 分别表示对称矩阵特征值的最大值和最小值. 这是因为如果 $\mu = \inf_{k \in \mathbb{N}^+} |\lambda_{\max}(\mathbf{I}_N + \eta_k\mathbf{H} - \eta_k\mathbf{G}(t_k)\mathbf{H} + \psi_k\mathbf{A}(t_k))| \leq 1$, 有 $\mathbf{e}(t_k) \leq \mu\mathbf{e}(t_k^-)$, 则此时攻击依然起到脉冲控制作用, 与攻击的定义相违背.

以下是本文用到的引理、假设及定义.

引理1 令向量 $\zeta, \mathbf{Y} \in \mathbb{R}^n, \varepsilon > 0$, 则有

$$\zeta^T \mathbf{Y} + \mathbf{Y}^T \zeta \leq \varepsilon \zeta^T \zeta + \varepsilon^{-1} \mathbf{Y}^T \mathbf{Y}.$$

假设1 非线性函数 $\mathbf{f}: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ 和 $\bar{\sigma}: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^{n \times m}$ 满足如下的李普希兹条件

$$\|\mathbf{f}(t, v) - \mathbf{f}(t, w)\| \leq \|\bar{\mathbf{J}}(v - w)\|, \quad \forall v, w \in \mathbb{R}^n$$

$$\|\bar{\sigma}(t, q) - \bar{\sigma}(t, u)\| \leq \|\Phi(q - u)\|, \forall q, u \in \mathbb{R}^n$$

式中: $\tilde{J}$ 与 Φ 均是已知适合维度的常数矩阵。

假设2 替代攻击信号 $\xi(t_k), k \in \mathbb{N}^+$ 有界且满足如下条件:

$$\|\xi(t_k)\|^2 \leq \xi$$

式中: $\xi < +\infty$ 是一个已知非负实数。

定义1 对于任意给定的系统初值 $\phi(t_0)$, 如果存在一个闭集 $\bar{\mathcal{B}}$ 和常数 $\bar{\Pi} \geq 0$ 使 $e(t)$ 满足条件

$$\bar{\mathcal{B}} = \left\{ e(t) \mid \lim_{t \rightarrow +\infty} \mathbb{E}[\|e(t)\|^2] \leq \bar{\Pi} \right\}$$

则称由式(1)和式(3)组成的领导跟随随机多智能体系统实现均方拟一致性, 且具有均方误差极限的上界 $\bar{\Pi}$; 若 $\bar{\Pi} = 0$, 则称系统可实现均方一致性。

定义2 对函数 $V: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^+$, 定义运算符 $\mathcal{L}$:

$$\begin{aligned} \mathcal{L}V(t, y) = & V_t(t, y) + V_y(t, y)f(t, y) + \\ & \frac{1}{2} \text{tr}[\mathbf{h}^T(t, y)V_{yy}(t, y)\mathbf{h}(t, y)] \end{aligned}$$

式中: $\text{tr}[\cdot]$ 表示矩阵的迹。此外, $V_t(t, y), V_{yy}(t, y)$ 与 $V_y(t, y)$ 分别定义为

$$\begin{aligned} V_t(t, y) = & \frac{\partial V(t, y)}{\partial t}, V_{yy}(t, y) = \left(\frac{\partial^2 V(t, y)}{\partial y_i \partial y_j} \right)_{n \times n}, \\ V_y(t, y) = & \left(\frac{\partial V(t, y)}{\partial y_1}, \frac{\partial V(t, y)}{\partial y_2}, \dots, \frac{\partial V(t, y)}{\partial y_n} \right) \end{aligned}$$

2 一致性分析

定理1 在假设1~2成立的情况下, 若存在 $\varepsilon > 0$ 满足以下条件

$$\varsigma = \kappa(\kappa + d\varepsilon\bar{\alpha}) \in (0, 1) \quad (9)$$

$$0 \leq \tau_{\sup} < -\frac{\ln \varsigma}{\lambda_{\max}(\Xi)} \quad (10)$$

式中: $\kappa = 1 + \eta\theta(1 - \bar{\alpha}) + \psi\bar{\beta}$, $\psi = \max_{k \in \mathbb{N}^+} \{\psi_k\}$, $d = \max_{k \in \mathbb{N}^+} \{d_k\}$, $\eta = \max_{k \in \mathbb{N}^+} \{\eta_k\}$, $\theta = \lambda_{\max}(\mathbf{H})$, $\Xi = \mathbf{I}_N \otimes (\mathbf{A}^T + \mathbf{A}) + 2\bar{p}\|\tilde{J}\|\mathbf{I}_{nN} + \mathbf{I}_N \otimes (\Phi^T \Phi)$, $\tau_{\sup} = \sup_{k \in \mathbb{N}^+} \{t_{k+1} - t_k\}$ 表示脉冲间隔的上确界。则由式(1)和式(3)组成随机多智能体系统在控制协议(4)下可实现均方拟一致性, 且具有均方误差极限的上界

$$\bar{\Pi} = \frac{d\bar{\alpha}\xi(\varepsilon^{-1}\kappa + d)}{\varepsilon^{-\lambda_{\max}(\Xi)\tau_{\sup}} - \varsigma}$$

证明 考虑以下李雅普诺夫函数

$$V(t, e(t)) = e^T(t)e(t) \quad (11)$$

由伊藤公式可知, 当 $t \in [t_{k-1}, t_k], k \in \mathbb{N}^+$, 有

$$dV(t, e(t)) = \mathcal{L}V(t, e(t))dt + 2e^T(t)\bar{\sigma}(t, e(t))d\omega(t) \quad (12)$$

$$\begin{aligned} \mathcal{L}V(t, e(t)) = & 2e^T(t)[(\mathbf{I}_N \otimes \mathbf{A})e(t) + \\ & p(t)\bar{F}(t, e(t))] + \text{tr}[\bar{\sigma}^T(t, e(t))\bar{\sigma}(t, e(t))] \end{aligned} \quad (13)$$

由假设1可得

$$\begin{aligned} 2e^T(t)p(t)\bar{F}(t, e(t)) \leq & 2\bar{p}\|\tilde{J}\|e^T(t)e(t) + \\ & 2(p(t) - \bar{p})\|\tilde{J}\|e^T(t)e(t) \end{aligned} \quad (14)$$

$$\text{tr}[\bar{\sigma}^T(t, e(t))\bar{\sigma}(t, e(t))] \leq e^T(t)(\mathbf{I}_N \otimes (\Phi^T \Phi))e(t) \quad (15)$$

当 $t \in [t_{k-1}, t_k], k \in \mathbb{N}^+$, 令 $\iota > 0$ 足够小且满足 $t + \iota \in [t_{k-1}, t_k]$, 有

$$\begin{aligned} \mathbb{E}[V(t + \iota, e(t + \iota))] - \mathbb{E}[V(t, e(t))] = \\ \int_t^{t+\iota} \mathbb{E}[\mathcal{L}V(v, e(v))]dv \end{aligned}$$

由此可知, 有 $D^+ \mathbb{E}[V(t, e(t))] = \mathbb{E}[\mathcal{L}V(t, e(t))]$ 。

当 $t \in [t_{k-1}, t_k], k \in \mathbb{N}^+$, 结合式(14)与(15), 有

$$D^+ \mathbb{E}[V(t, e(t))] \leq \lambda_{\max}(\Xi)\mathbb{E}[V(t, e(t))] \quad (16)$$

式中, $\Xi = \mathbf{I}_N \otimes (\mathbf{A}^T + \mathbf{A}) + 2\bar{p}\|\tilde{J}\|\mathbf{I}_{nN} + \mathbf{I}_N \otimes (\Phi^T \Phi)$ 。进一步可得

$$\mathbb{E}[V(t, e(t))] \leq \mathbb{E}[V(t_{k-1}, e(t_{k-1}))]e^{\lambda_{\max}(\Xi)(t-t_{k-1})} \quad (17)$$

当 $t = t_k, k \in \mathbb{N}^+$ 时, 由误差系统(8)可知

$$\begin{aligned} e(t_k) = & (\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{G}(t_k) \mathbf{H} + \\ & \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n [e(t_k^-) + d_k(\mathbf{G}(t_k) \otimes \mathbf{I}_n)\xi(t_k)] \end{aligned} \quad (18)$$

根据式(11)与式(18)可知

$$\begin{aligned} \mathbb{E}[V(t_k^+, e(t_k^+))] = & \mathbb{E}[e^T(t_k)e(t_k)] = \\ & \mathbb{E}[(e^T(t_k^-)\mathbf{M}^T(t_k) + \xi^T(t_k)\mathbf{W}^T(t_k)) \times \\ & (\mathbf{M}(t_k)e(t_k^-) + \mathbf{W}(t_k)\xi(t_k))] = \\ & \mathbb{E}[e^T(t_k^-)\mathbf{M}^T(t_k)\mathbf{M}(t_k)e(t_k^-) + \\ & e^T(t_k^-)\mathbf{M}^T(t_k)\mathbf{W}(t_k)\xi(t_k) + \\ & \xi^T(t_k)\mathbf{W}^T(t_k)\mathbf{M}(t_k)e(t_k^-) + \\ & \xi^T(t_k)\mathbf{W}^T(t_k)\mathbf{W}(t_k)\xi(t_k)] \end{aligned} \quad (19)$$

式中 $\mathbf{W}(t_k) = d_k \mathbf{G}(t_k) \otimes \mathbf{I}_n$, $\mathbf{M}(t_k) = (\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{G}(t_k) \mathbf{H} + \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n$ 。

对于式(19)中的第一项, 有

$$\begin{aligned} \mathbb{E}[e^T(t_k^-)\mathbf{M}^T(t_k)\mathbf{M}(t_k)e(t_k^-)] = \\ \mathbb{E}[e^T(t_k^-)((\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{H}\mathbf{G}(t_k) + \\ \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n)(\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{G}(t_k) \mathbf{H} + \\ \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n e(t_k^-)] \leq \\ (1 + \eta\theta(1 - \bar{\alpha}) + \psi\bar{\beta})^2 \mathbb{E}[V(t_k^-, e(t_k^-))] \leq \\ \kappa^2 \mathbb{E}[V(t_k^-, e(t_k^-))] \end{aligned} \quad (20)$$

式中: $\kappa = 1 + \eta\theta(1 - \bar{\alpha}) + \psi\bar{\beta}$, $\eta = \max_{k \in \mathbb{N}^+} \{\eta_k\}$ 以及 $\psi = \max_{k \in \mathbb{N}^+} \{\psi_k\}$ 。

对式(19)中的第二项和第三项, 结合引理1,

$$\begin{aligned}
& \mathbb{E}[\mathbf{e}^T(t_k^-) \mathbf{M}^T(t_k) \mathbf{W}(t_k) \boldsymbol{\xi}(t_k) + \\
& \boldsymbol{\xi}^T(t_k) \mathbf{W}^T(t_k) \mathbf{M}(t_k) \mathbf{e}(t_k)] = \\
& \mathbb{E}[\mathbf{e}^T(t_k^-)((\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{H} \mathbf{G}(t_k) + \\
& \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n)(d_k \mathbf{G}(t_k) \otimes \mathbf{I}_n) \boldsymbol{\xi}(t_k) + \\
& \boldsymbol{\xi}^T(t_k)(d_k \mathbf{G}(t_k) \otimes \mathbf{I}_n)((\mathbf{I}_N + \eta_k \mathbf{H} - \\
& \eta_k \mathbf{G}(t_k) \mathbf{H} + \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n) \mathbf{e}(t_k^-)] \leq \\
& d_k \bar{\alpha} \mathbb{E}[\mathbf{e}^T(t_k^-)((\mathbf{I}_N + \eta_k \mathbf{H} - \eta_k \mathbf{H} \mathbf{G}(t_k) + \\
& \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n) \boldsymbol{\xi}(t_k) + \boldsymbol{\xi}^T(t_k)((\mathbf{I}_N + \\
& \eta_k \mathbf{H} - \eta_k \mathbf{G}(t_k) \mathbf{H} + \\
& \psi_k \mathbf{A}(t_k)) \otimes \mathbf{I}_n) \mathbf{e}(t_k^-)] \leq \\
& d_k \bar{\alpha} \kappa \mathbb{E}[\mathbf{e}^T(t_k^-) \boldsymbol{\xi}(t_k) + \boldsymbol{\xi}^T(t_k) \mathbf{e}(t_k^-)] \leq \\
& d_k \bar{\alpha} \kappa \mathbb{E}[\varepsilon \mathbf{e}^T(t_k^-) \mathbf{e}(t_k^-) + \varepsilon^{-1} \boldsymbol{\xi}^T(t_k) \boldsymbol{\xi}(t_k)] \leq \\
& d \varepsilon \bar{\alpha} \kappa \mathbb{E}[V(t_k^-, \mathbf{e}(t_k^-))] + d \bar{\alpha} \kappa \varepsilon^{-1} \bar{\xi}
\end{aligned} \quad (21)$$

式中: $d = \max_{k \in \mathbb{N}^+} \{d_k\}$ 。

对式(19)中的最后一项,有

$$\begin{aligned}
& \mathbb{E}[\boldsymbol{\xi}^T(t_k) \mathbf{W}^T(t_k) \mathbf{W}(t_k) \boldsymbol{\xi}(t_k)] = \\
& \mathbb{E}[\boldsymbol{\xi}^T(t_k)(d_k \mathbf{G}(t_k) \otimes \mathbf{I}_n) \times \\
& (d_k \mathbf{G}(t_k) \otimes \mathbf{I}_n) \boldsymbol{\xi}(t_k)] \leq \\
& d_k^2 \bar{\alpha} \mathbb{E}[\boldsymbol{\xi}^T(t_k) \boldsymbol{\xi}(t_k)] \leq d^2 \bar{\alpha} \bar{\xi}
\end{aligned} \quad (22)$$

将式(20)~(22)代入式(19)中,有

$$\begin{aligned}
& \mathbb{E}[V(t_k^+, \mathbf{e}(t_k^+))] \leq \\
& \kappa^2 \mathbb{E}[V(t_k^-, \mathbf{e}(t_k^-))] + d \varepsilon \bar{\alpha} \kappa \mathbb{E}[V(t_k^-, \mathbf{e}(t_k^-))] + \\
& d \bar{\alpha} \kappa \varepsilon^{-1} \bar{\xi} + d^2 \bar{\alpha} \bar{\xi} \leq \\
& \varsigma \mathbb{E}[V(t_k^-, \mathbf{e}(t_k^-))] + \bar{m}
\end{aligned} \quad (23)$$

式中: $\varsigma = \kappa(\kappa + d \varepsilon \bar{\alpha})$, $\bar{m} = d \bar{\alpha} \xi(\varepsilon^{-1} \kappa + d)$ 。

对 $t \in [t_0, t_1)$, 由式(17)可知,

$$\mathbb{E}[V(t, \mathbf{e}(t))] \leq \varsigma e^{\lambda_{\max}(\Xi)(t-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))]$$

由此可知, 当 $t = t_1$ 时, 有

$$\begin{aligned}
& \mathbb{E}[V(t_1, \mathbf{e}(t_1))] \leq \varsigma \mathbb{E}[V(t_1^-, \mathbf{e}(t_1^-))] + \bar{m} \leq \\
& \varsigma e^{\lambda_{\max}(\Xi)(t_1-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] + \bar{m}
\end{aligned}$$

对 $t \in [t_1, t_2)$, 同理有

$$\mathbb{E}[V(t, \mathbf{e}(t))] \leq \varsigma^2 e^{\lambda_{\max}(\Xi)(t-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] + \varsigma e^{\lambda_{\max}(\Xi)(t-t_1)} \bar{m}$$

由此可知, 当 $t = t_2$ 时, 有

$$\begin{aligned}
& \mathbb{E}[V(t_2, \mathbf{e}(t_2))] \leq \\
& \varsigma^2 e^{\lambda_{\max}(\Xi)(t_2-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] + \varsigma \bar{m} e^{\lambda_{\max}(\Xi)(t_2-t_1)} + \bar{m}
\end{aligned}$$

通过迭代法, 当 $t \in [t_k, t_{k+1})$, 有

$$\begin{aligned}
& \mathbb{E}[V(t, \mathbf{e}(t))] \leq \\
& \varsigma^k e^{\lambda_{\max}(\Xi)(t-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] + \\
& \varsigma^{k-1} \bar{m} e^{\lambda_{\max}(\Xi)(t-t_1)} + \varsigma^{k-2} \bar{m} e^{\lambda_{\max}(\Xi)(t-t_2)} + \dots + \\
& \bar{m} e^{\lambda_{\max}(\Xi)(t-t_k)} \leq \\
& \varsigma^k e^{\lambda_{\max}(\Xi)(t-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] + \\
& \frac{\bar{m} e^{\lambda_{\max}(\Xi) \tau_{\text{sup}}} (1 - (e^{\lambda_{\max}(\Xi) \tau_{\text{sup}}} + \ln \varsigma)^{\bar{k}})}{1 - \varsigma e^{\lambda_{\max}(\Xi) \tau_{\text{sup}}}}
\end{aligned} \quad (24)$$

式中: $\bar{k} \geq \frac{t-t_0}{\tau_{\text{sup}}} - 1$, $k \in \mathbb{N}^+$ 。

令 $\rho = \frac{\ln \varsigma}{\tau_{\text{sup}}} + \lambda_{\max}(\Xi) < 0$, 由式(24)可得

$$\begin{aligned}
& \mathbb{E}[V(t, \mathbf{e}(t))] \leq \frac{1}{\varsigma} e^{\rho(t-t_0)} \mathbb{E}[V(t_0, \mathbf{e}(t_0))] - \\
& \frac{\bar{m} e^{-\ln \varsigma e^{\rho(t-t_0)}}}{1 - \varsigma e^{\lambda_{\max}(\Xi) \tau_{\text{sup}}}} + \frac{\bar{m}}{e^{-\lambda_{\max}(\Xi) \tau_{\text{sup}}} - \varsigma}
\end{aligned} \quad (25)$$

因此, 当 $t \rightarrow \infty$ 时, 由(25)可得

$$\lim_{t \rightarrow \infty} \mathbb{E}[\|\mathbf{e}(t)\|^2] \leq \frac{\bar{m}}{e^{-\lambda_{\max}(\Xi) \tau_{\text{sup}}} - \varsigma}$$

根据式(25)与定义1, 取 $\bar{l} = \frac{\bar{m}}{e^{-\lambda_{\max}(\Xi) \tau_{\text{sup}}} - \varsigma}$, 从而式

(1)与式(3)所组成的领导跟随随机多智能体系统在同时受到替代攻击和虚假数据注入攻击时, 在控制协议(4)作用下可实现均方拟一致性, 且具有均方误差极限的上界 $\bar{l}$ 和收敛率 $-\rho$ 。

3 数字仿真

为验证本文结果的有效性, 本节考虑由5个3维智能体所组成的蔡氏循环电路组合, 其中包含1个领导者和4个跟随者。系统通信拓扑如图2所示。

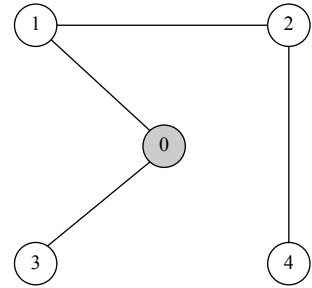


图2 循环电路组回路拓扑图

Fig.2 Topological diagram of each sub loop in the cycle circuit combination

由图2可知, 矩阵 $\hat{\mathbf{L}}$, $\mathbf{C}$ 与 $\mathbf{H}$ 分别为

$$\hat{\mathbf{L}} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ -1 & 2 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{bmatrix},$$

$$\mathbf{H} = \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$$

设跟随者动力学方程(1)和领导者动力学方程(3)中状态为 $\mathbf{x}_i(t) = [\mathbf{x}_{i1}(t), \mathbf{x}_{i2}(t), \mathbf{x}_{i3}(t)]^T$, $i \in \mathcal{N} \cup \{0\}$, 其他参数的选择为

$$\mathbf{A} = \begin{bmatrix} -2.2(1-0.14) & 2.2 & 0 \\ 1 & -1 & 1 \\ 0 & -0.8 & 0 \end{bmatrix}$$

非线性函数选择 $f(t, \mathbf{x}_i(t)) = [0.4\text{sat}(\mathbf{x}_{i1}(t)), 0, 0]^T$, $\bar{\sigma}(t, \mathbf{x}_i(t)) = 0.4|\text{sat}(\mathbf{x}_i(t))|\mathbf{I}_3$, $\text{sat}(\mathbf{x}_i(t)) = 0.5(|\mathbf{x}_i(t) + 1| - |\mathbf{x}_i(t) - 1|)$, $\text{sat}(\cdot)$ 为饱和函数, $i = 1, 2, 3$ 。同时, 由假设 1 可以得到 $\|\bar{\mathbf{J}}\| = 0.4$ 与 $\Phi = \text{diag}\{0.4, 0.4, 0.4\}$ 。此外, 选择 $\bar{\rho} = 0.5$ 。

考虑式(4)所设计的控制协议, 其中控制增益选择为 $\eta \equiv -0.32$, 攻击强度为 $d \equiv 0.2$ 。替代攻击的攻击信号 $\xi_i = (0.1, 0.14, -0.14)^T$, 同时由假设2可得 $\xi = 0.0492$ 。同理, 设虚假数据注入攻击的攻击信号 $\mathbf{x}_i = (0.1, 0.15, -0.15)^T$, 攻击强度 $\psi \equiv 0.43$ 。同时, 选择 $\bar{\alpha} = 0.2$ 与 $\bar{\beta} = 0.5$ 。

系统(1)采用的脉冲序列如图3所示, 设最大控制脉冲间隔 $\tau_{\text{sup}} = \sup_{k \in \mathbb{N}^+} \{t_{k+1} - t_k\} = 2$, 令仿真步长为0.1, 结合给定的初始条件与本节所选择和计算得到的参数在MATLAB中仿真得到图4。由图4可知, 由式(1)与式(3)所组成的领导跟随随机多智能体系统受到两种不同脉冲欺骗攻击时, 在控制协议(4)作用下可实现均方拟一致性, 即误差保持在所计算的误差界限内。若不发生脉冲欺骗攻击时, 可得到系统的均方一致性, 如图5所示。

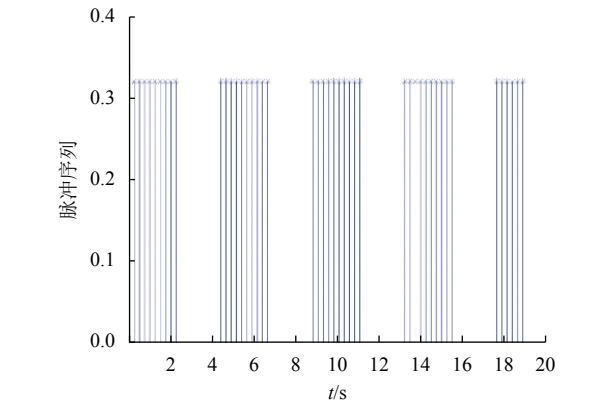


图 3 系统(1)脉冲控制信号

Fig.3 The impulse control signal of system (1)

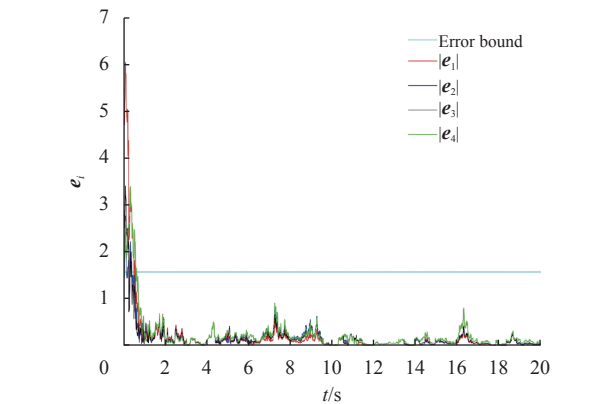


图 4 受到两种欺骗攻击时系统的误差轨迹图

Fig.4 The errors' trajectories of the system with two different deception attacks

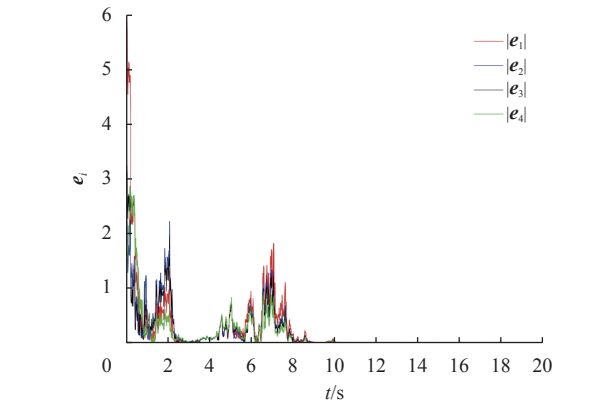


图 5 无欺骗攻击时系统的误差轨迹图

Fig.5 The errors' trajectories of the system without deception attacks

假设系统初始时刻为 $t_0 = 0$, 其初始状态值随机选择为

$$[\mathbf{x}_0(t_0), \mathbf{x}_1(t_0), \mathbf{x}_2(t_0), \mathbf{x}_3(t_0), \mathbf{x}_4(t_0)] = \begin{bmatrix} 1 & -0.5 & -0.5 & -1.5 & 2.5 \\ 1 & 2 & -1 & -2 & 1 \\ -2 & -2.5 & 2.5 & 2 & -1 \end{bmatrix}$$

此外, 令 $\varepsilon = 1$ 。根据上述所选择的参数, 可计算得到误差上界为 $\bar{\eta} = 1.566$ 。据此可知, 上述参数可满足定理1中的条件, 故由式(1)与式(3)所组成的领导跟随随机多智能体系统在两种不同的欺骗攻击作用下可实现均方拟一致性, 且其收敛率为 $-\rho = 1.8$ 。

4 结论

基于脉冲控制方法, 本文研究了一类领导跟随随机多智能体系统在遭受替代攻击和虚假数据注入攻击下的均方拟一致性问题。不同于已有文献, 本文同时考虑了两种不同脉冲欺骗攻击对系统均方拟一致性的影响, 其中攻击模型采用两个服从伯努利分布的随机变量来描述不同攻击的成功与否, 更适用于模拟现实应用中的情形。基于李雅普诺夫稳定性理论和相关随机过程知识, 本文给出了两种不同脉冲欺骗攻击下系统实现均方拟一致性的充分条件, 同时也给出了误差极限的上界。最后, 通过数值仿真例子验证了研究结果的有效性。

参考文献:

[1] 周琪, 陈广登, 鲁仁全, 等. 基于干扰观测器的输入饱和和多智能体系统事件触发控制[J]. 中国科学: 信息科学, 2019, 49(11): 1502-1516.

ZHOU Q, CHEN G D, LU R Q, et al. Disturbance observer-based event triggered control for input saturated multi-agent systems [J]. Chinese Science: Information Science, 2019, 49(11): 1502-1516.

- [2] 张弘烨, 彭世国. 基于模型简化法的含有随机时延的多智能体系统一致性研究[J]. *广东工业大学学报*, 2019, 36(2): 86-90, 96.
- ZHANG H Y, PENG S G. A research on the consensus problem of multi-agent systems with random time delays based on model reduction [J]. *Journal of Guangdong University of Technology*, 2019, 36(2): 86-90, 96.
- [3] HE W, MO Z, Han Q L, *et al.* Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks [J]. *IEEE/CAA Journal of Automatica Sinica*, 2020, 7(5): 1326-1334.
- [4] ZHOU Q, XU S, CHEN B, *et al.* Stability analysis of delayed genetic regulatory networks with stochastic disturbances [J]. *Physics Letters A*, 2009, 373(41): 3715-3723.
- [5] HU M, GUO L, HU A, *et al.* Leader-following consensus of linear multi-agent systems with randomly occurring nonlinearities and uncertainties and stochastic disturbances [J]. *Neurocomputing*, 2015, 149: 884-890.
- [6] ZHANG Z H, PENG S G, CHEN T. Leader-following mean square consensus of stochastic multi-agent systems with ROUs and RONs under periodically variable impulse time windows [J]. *Neurocomputing*, 2020, 412: 276-286.
- [7] WANG F, ZHANG Y, ZHANG L, *et al.* Finite-time consensus of stochastic nonlinear multi-agent systems [J]. *International Journal of Fuzzy Systems*, 2020, 22(1): 77-88.
- [8] GONG X, PAN Y J, LI J N, *et al.* Leader-following consensus for multi-agent systems with stochastic packet dropout[C]//2013 10th IEEE International Conference on Control and Automation (ICCA). Hangzhou: IEEE, 2013: 1160-1165.
- [9] YE D, YANG X. Distributed event-triggered consensus for nonlinear multi-agent systems subject to cyber attacks [J]. *Information Sciences*, 2019, 473: 178-189.
- [10] ZUO Z, CAO X, WANG Y. Security control of multi-agent systems under false data injection attacks [J]. *Neurocomputing*, 2020, 404: 240-246.
- [11] FENG J, XIE J, WANG J, *et al.* Secure synchronization of stochastic complex networks subject to deception attack with nonidentical nodes and internal disturbance [J]. *Information Sciences*, 2021, 547: 514-525.
- [12] HE W, QIAN F, HAN Q L, *et al.* Almost sure stability of nonlinear systems under random and impulsive sequential attacks [J]. *IEEE Transactions on Automatic Control*, 2020, 65(9): 3879-3886.
- [13] ZHAO L, YANG G H. Cooperative adaptive fault-tolerant control for multi-agent systems with deception attacks [J]. *Journal of the Franklin Institute*, 2020, 357(6): 3419-3433.
- [14] LI X M, ZHOU Q, LI P, *et al.* Event-triggered consensus control for multi-agent systems against false data-injection attacks [J]. *IEEE Transactions on Cybernetics*, 2019, 50(5): 1856-1866.
- [15] HE W, GAO X, ZHONG W, *et al.* Secure impulsive synchronization control of multi-agent systems under deception attacks [J]. *Information Sciences*, 2018, 459: 354-368.
- [16] DING D, WANG Z, HO D W C, *et al.* Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks [J]. *IEEE Transactions on Cybernetics*, 2016, 47(8): 1936-1947.
- [17] MA L, WANG Z, YUAN Y. Consensus control for nonlinear multi-agent systems subject to deception attacks[C]//2016 22nd International Conference on Automation and Computing (ICAC). Colchester: IEEE, 2016: 21-26.
- [18] 伍益明. 恶意攻击下的多智能体系统安全一致性问题研究[D]. 杭州: 浙江工业大学, 2016.
- [19] 常盛. 考虑虚假数据攻击的电力信息物理系统检测方法研究[D]. 秦皇岛: 燕山大学, 2020.

(责任编辑: 赵少飞)