中国科学: 信息科学 2019 年 第 49 卷 第 5 期: 599–612
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
无人机自主飞行技术专题 • 论文

信任节点机制下的异构多智能体系统安全一致性控制

黄锦波[1], 伍益明[2*], 常丽萍[1], 何熊熊[1]

1. 浙江工业大学信息工程学院, 杭州 310023
2. 杭州电子科技大学网络空间安全学院, 杭州 310018
* 通信作者. E-mail: ymwu@hdu.edu.cn

收稿日期: 2018–12–30; 接受日期: 2019–03–10; 网络出版日期: 2019–05–09

国家自然科学基金 (批准号: 61873239, 61803135, 61473262)、浙江省公益技术应用研究计划 (批准号: LGG18F020015) 和浙江省自然科学基金 (批准号: LY18F010023) 资助项目

摘要 本文研究了一类由一阶二阶智能体组成的异构系统安全一致性分析与设计问题. 首先从拓扑结构角度, 通过设立信任节点机制, 显著提升了系统网络拓扑的稳健性. 然后, 针对邻居中敌对节点的攻击行为, 分别设计了一阶二阶智能体的控制策略, 并给出了系统实现安全一致性目标的充分条件. 最后, 通过仿真实例验证了理论结果的有效性.

关键词 异构系统, 多智能体系统, 安全一致性, 安全控制, 信任节点

1 引言

近些年来, 多智能体系统协同控制技术作为系统控制领域的研究热点, 是当前网络化控制和群体智能领域最有活力的研究方向之一, 并在交通流量控制、无人机编队、电网调控等众多领域得到了广泛应用 [1~5]. 其中, 一致性问题作为分布式协同控制领域的代表性问题, 其主要目的是通过设计合适的分布式控制协议来确保各智能体在某个状态量上渐进地或者有限时间内趋于一致. 研究者们通过代数图论、矩阵理论、李雅普诺夫 (Lyapunov) 函数等方法, 目前已在一致性控制问题上取得了丰硕的成果 [6~13].

然而伴随着网络安全形势日益严峻, 多智能体系统中安全一致性控制问题成为一个新兴且重要的研究问题, 逐渐被国内外专家学者所重视 [14~18]. 所谓的安全一致性控制, 是指针对系统中存在敌对个体的情况, 通过设计合适的一致性控制协议 (算法), 有效抵御敌对节点的攻击行为, 确保系统状态始终保持在一个可容许范围内变化并最终实现一致. 为去除敌对个体对整个系统一致性进程的影响, 研究者们先后提出了许多有针对性的安全一致性控制方法. 文献 [14] 考虑在系统中存在不超过 F 个敌对

引用格式: 黄锦波, 伍益明, 常丽萍, 等. 信任节点机制下的异构多智能体系统安全一致性控制. 中国科学: 信息科学, 2019, 49: 599–612, doi: 10.1360/N112018-00343
Huang J B, Wu Y M, Chang L P, et al. Secure consensus control for heterogeneous multi-agent systems with trusted nodes (in Chinese). Sci Sin Inform, 2019, 49: 599–612, doi: 10.1360/N112018-00343

© 2019《中国科学》杂志社

个体的情况下, 设计了相应的分布式控制算法, 作者指明系统网络拓扑在满足 $(2F+1)$- 连通度的条件下能够实现一致, 然而该算法需每个智能体获取网络拓扑结构的全局信息. 文献 [19] 在图论的基础上, 针对网络攻击, 有别于传统的网络连通性, 首次提出了一种称为网络稳健性 (network robustness) 的概念, 并基于此概念, 仅利用邻居个体传输的局部信息作为控制输入, 设计了相应的安全算法, 实现系统的安全一致. 大致地讲, 上述算法本质上是通过消除邻居个体中的极端值来保证系统的安全性, 此类算法最早应用在计算机领域, 被称为 Mean Subsequence Reduced (MSR) 系列算法 [20]. 文献 [21] 针对带有通信时延的多智能体网络, 提出一种安全有效的控制策略, 使得系统状态在拜占庭攻击节点影响下达成一致. 文献 [22] 通过将迭代学习控制方法与分布式控制相结合, 提出了一种基于节点中间值状态的一致性更新策略, 不但保证了系统实现安全一致的目标, 而且有效降低了节点的计算负担. 还有研究者考虑了一阶多智能体系统在量化通信下的安全一致性 [23, 24]. 此外, 文献 [25∼27] 则将现有的一阶多智能体系统安全一致性理论成果推广到了二阶系统.

小结而言, 上述研究工作主要针对同构系统, 即系统中所有个体都具有相同的动力学模型. 但在实际工程中由于约束不同, 智能体个体间的动力学模型和行为存在一定的差异. 因此考虑由一阶二阶混合异构系统的安全一致性问题具有一定的理论和工程价值. 另外, 值得注意的一点, 传统的安全一致性算法对网络拓扑连通性提出了较高的要求, 传统的方法是通过增设网络节点和通信链路来提升网络连通度, 这一方法虽然可以有效应对敌节点的攻击行为, 但同时会给整个系统带来更大的资源开销. 众所周知, 对于一个大型的分布式网络, 系统中单个智能体的计算能力和信息处理能力往往十分有限. 为此, 如何在不盲目增设通信链路的同时, 提升整个多智能体系统的容侵能力也成为一些学者的研究重点. 文献 [28] 给出了一种全新的解决策略, 作者发现通过在网络中设立部分节点或链路为信任节点或信任链路, 可有效地提升网络拓扑结构的健壮性. 更进一步, 文中指出若设立的信任节点能够彼此构成一个无向连通子图, 则整个多智能体系统在抵御恶意节点攻击的表现上得到显著提升.

本文的主要贡献如下: (1) 以一类由一阶与二阶智能体组成的异构系统为研究对象, 考虑部分节点为敌对节点的情况, 建立相应数学模型并提出了一种基于节点本地信息的分布式安全一致性控制协议; (2) 受文献 [28] 启发, 通过设立系统中部分节点为信任节点, 放宽了传统文献 [15, 17, 19, 27] 对系统达成安全一致性收敛所需要较高拓扑连通性的条件.

2 预备知识

2.1 图论知识

考虑多智能系统由 n 个智能体组成, 其关系拓扑可以用一个无向的带权图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$ 表示, 其中 $\mathcal{V}=\{1,2,\ldots,n\}$ 表示节点集, $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ 表示边集. 在无向图 $\mathcal{G}$ 中, 节点 i 与 j 之间传递的信息等同于节点 j 与 i 之间传递的信息, 即 $(i,j)=(j,i)$. 两个节点之间的连接关系用邻接矩阵 $A=[a_{ij}]\in\mathbb{R}^{n\times n}$ 表示, 若两个节点之间存在连接, 则 $a_{ij}\in(\gamma,1)$, 其中 $\gamma>0$ 为固定下界; 若两个节点之间无连接, 则 $a_{ij}=0$. 这里规定 $a_{ii}=0$, 即图中节点无自环. 与节点 i 相连的节点为邻居节点, 用集合 $\mathcal{N}_i=\{j\in\mathcal{V}:(i,j)\in\mathcal{E}\}$ 表示. Laplacian 矩阵定义为 $L=D-A$, 其中度矩阵:

$$D=\operatorname{diag}\left\{\sum_{j=1}^{n}a_{1j},\sum_{j=1}^{n}a_{2j},\ldots,\sum_{j=1}^{n}a_{nj}\right\}.$$

基于上述图论知识, 本文引入以下关于网络稳健性的相关定义, 这些定义来源于文献 [19], 并进行

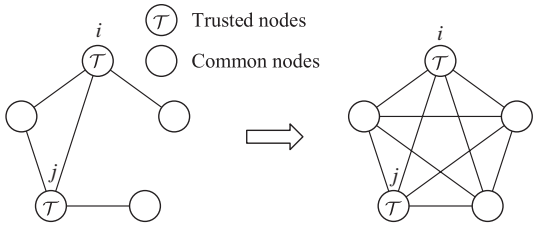

图 1 图 $\mathcal{G}$ (左) 设置信任节点后得到等效拓扑图 $\mathcal{G}'$ (右)

Figure 1 The left graph $\mathcal{G}$ with set of trusted nodes and the resulting graph $\mathcal{G}'$

了适当修改, 具体如下:

定义1 (r- 可达集) 对于一个图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$ 以及其中一个非空节点集合 $\mathcal{S}\subset\mathcal{V}$, 如果集合 $\mathcal{S}$ 中至少有一个节点 i 在集合 $\mathcal{N}_i\setminus\mathcal{S}$ 存在不少于 r 个节点, 称集合 $\mathcal{S}$ 为 r- 可达集.

定义2 (r- 稳健性 (r-robustness)) 对于一个图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$, 如果存在一对非空子集 $\mathcal{S}_1,\mathcal{S}_2\subset\mathcal{V}$, $\mathcal{S}_1\bigcap\mathcal{S}_2=\emptyset$, 其中至少一个子集为 r- 可达集, 称图 $\mathcal{G}$ 具备 r- 稳健性.

由上述 r- 可达集和 r- 稳健性的概念可以得到这样一个集合 $\mathcal{X}_{\mathcal{S}}^r$, 该集合为 $\mathcal{S}$ 的子集, 其所有的节点在集合 $\mathcal{S}$ 之外存在至少 r 个邻居节点, 即

$$\mathcal{X}_{\mathcal{S}}^r=\{i\in\mathcal{S}:|\mathcal{N}_i\setminus\mathcal{S}|\geqslant r\}. \tag{1}$$

用集合 $\mathcal{T}$ 表示网络中的信任节点, 信任节点是通过软硬件加强等方式使其较普通节点具有更高安全性的一类节点. 本文假设信任节点面对来自攻击者的信息篡改、注入、拦截等多种攻击形式, 都不会受到影响. 对于节点集的一个非空子集 $\mathcal{S}\subset\mathcal{V}$, 我们假设它的一个子集中所有节点在集合 $\mathcal{S}$ 之外至少存在一个信任节点, 用 $\mathcal{Y}_{\mathcal{S}}$ 表示, 关系如下:

$$\mathcal{Y}_{\mathcal{S}}=\{i\in\mathcal{S}:(\mathcal{N}_i\setminus\mathcal{S})\cap\mathcal{T}\neq\emptyset\}. \tag{2}$$

基于 (1) 和 (2), 令 $\mathcal{Z}_{\mathcal{S}}^r=\mathcal{X}_{\mathcal{S}}^r\cup\mathcal{Y}_{\mathcal{S}}$, 可知 $\mathcal{Z}_{\mathcal{S}}^r$ 作为集合 $\mathcal{S}$ 的一个子集, 其包含的所有节点在集合 $\mathcal{S}$ 之外至少存在 r 个邻居节点或者至少有一个信任节点. 如果集合 $\mathcal{Z}_{\mathcal{S}}^r$ 为非空集合, 我们称集合 $\mathcal{S}$ 为包含信任节点的 r- 可达集. 下面给出包含信任节点的 r- 稳健性定义.

定义3 (r- 稳健性 (含信任节点)) 对于一个图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$, 如果存在一对非空子集 $\mathcal{S}_1,\mathcal{S}_2\subset\mathcal{V}$, $\mathcal{S}_1\bigcap\mathcal{S}_2=\emptyset$, 其中至少一个子集为包含信任节点的 r- 可达集, 即 $\mathcal{Z}_{\mathcal{S}_1}^r$ 或者 $\mathcal{Z}_{\mathcal{S}_2}^r$ 为非空集合, 则称图 $\mathcal{G}$ 具备 r- 稳健性 (含信任节点).

信任节点最大的作用是在不需要添加额外通信边的情况下能够提升网络中节点之间信息交换的冗余度, 从而提高网络拓扑的容侵能力. 引入信任节点后, 原先不相邻的两个节点如果分别与一个信任节点相连或者两个节点之间存在一条信任节点路径, 则在这两个节点之间将形成一条虚拟路径 [28]. 信任路径表示一条路径中所有的节点都为信任节点. 举例说明, 图 1 左图 $\mathcal{G}$ 中节点 i 与 j 为信任节点, 其他节点与信任节点相邻或者存在一条信任路径, 因此可以得到如图 1 右图中的等效拓扑图 $\mathcal{G}'$.

2.2 问题描述

本小节给出一阶与二阶智能体构成的异构系统模型, 为了更好地描述异构多智能体系统的动力学方程关系, 暂不考虑敌对攻击节点的影响. 假设图 $\mathcal{G}$ 由 n 个节点组成, 每一个节点代表一个智能体. 为便于叙述, 假设前 m 个节点代表二阶智能体, 随后的 $n-m$ 个节点代表一阶智能体.

本文考虑离散时间异构多智能体系统, 二阶智能体的动态方程如下:

$$\begin{cases} x_i(k+1) = x_i(k) + Tv_i(k) + \dfrac{T^2}{2}u_i(k), \\ v_i(k+1) = v_i(k) + Tu_i(k), \quad i = 1, 2, \ldots, m, \end{cases} \tag{3}$$

其中 $x_i(k) \in \mathbb{R}$, $v_i(k) \in \mathbb{R}$ 和 $u_i(k) \in \mathbb{R}$ 分别表示二阶智能体 i 的位置, 速度和控制输入, T 为采样周期.

一阶智能体的动态方程如下:

$$x_i(k+1) = x_i(k) + Tu_i(k), \quad i = m+1, \ldots, n, \tag{4}$$

其中 $x_i(k) \in \mathbb{R}$, $u_i(k) \in \mathbb{R}$ 分别表示一阶智能体 i 的位置和控制输入, T 为采样周期.

线性一致性控制协议广泛应用于多智能体系统的一致性问题中, 因此本文为异构系统中二阶智能体和一阶智能体分别设计如下一致性控制协议:

$$u_i(k) = \begin{cases} \sum\limits_{j \in \mathcal{N}_i} a_{ij}(x_{ij}(k) - x_i(k)) - \alpha v_i(k), \ i = 1, 2, \ldots, m, \\ \sum\limits_{j \in \mathcal{N}_i} a_{ij}(x_{ij}(k) - x_i(k)), \qquad\qquad i = m+1, \ldots, n. \end{cases} \tag{5}$$

其中 $x_{ij}(k)$ 表示节点 i 在 k 时刻从邻居节点 j 那里接收到的信息, 边权值 $a_{ij} \geqslant 0$ 且 $\sum_{j=1}^{n} a_{ij} \leqslant 1$, 令 α 为一个大于零的标量.

本文考虑的多智能体网络中假设存在两类节点: 正常节点与敌对节点, 分别用 N 和 $\mathcal{M}$ 表示. 正常节点完全按照系统设计的控制协议进行状态更新, 而敌对节点因被攻击者劫持而无法正常工作, 甚至发送虚假信息扰乱系统达到一致状态. 敌对节点的攻击方式有击停攻击、共谋攻击及拜占庭攻击等, 其中拜占庭攻击为最具破坏力的攻击方式. 具有拜占庭攻击方式的节点被称为拜占庭节点, 这类节点不受系统控制协议的约束, 可随意改变自身状态, 在同一时刻发送不同的信息给邻居节点. 本文考虑的敌对节点同样不受控制协议的约束, 但在同一时刻下发送给邻居节点的信息是相同的.

考虑攻击者攻击能力的限制, 本文对敌对节点的部署范围给出如下假设:

假设1 对于系统中任一节点的邻居节点集合, 其含有敌对节点的个数至多为 F个, 即 $|\mathcal{N}_i \backslash \mathcal{M}| \leqslant F$.

值得注意的是, 上述假设条件同样在文献 [15, 17, 19, 27] 中被采用, 这类攻击节点的部署方式通常被称作 F- 本地 (F-local) 攻击模型.

定义4 (异构系统安全一致性) 由式 (3) 和 (4) 描述的异构多智能体系统, 若满足下列两个条件, 则称系统达成安全一致性.

- 一致性: 随着时间的推移, 系统中所有正常节点最终达到一致状态, 即存在一个常数 $c \in \mathbb{R}$, 当 $k \to \infty$ 时, 满足 $x_i(k) \to c$ 以及 $v_i(k) \to 0$.
- 有效性: 系统中所有正常节点的状态量大小始终局限在一个由初始状态构成的有界区间中, 即 $A \leqslant x_i(k) \leqslant B, \forall k \geqslant 0, i \in N$, 其中 A 和 B 分别表示正常节点在初始时刻状态的最小值与最大值.

定义 4 中的有效性条件又称为多智能体系统的安全性条件, 其要求所有正常节点的状态在任意时刻下都处于一个指定的安全区间中, 该安全区间通常由系统初始时刻所有正常节点的最小值和最大值决定. 与仅包含一阶智能体的同构系统不同, 本文研究的多智能体系统除了一阶智能体还包含二阶智能体. 智能体在初始状态下的最大最小值由所有正常节点的位置信息以及二阶节点的速度信息共同决定, 因此用 A 和 B 表示, 具体形式会在后面的章节中给出.

3 安全一致性算法

本文假设系统中的正常智能体节点无法辨识邻居节点是否为敌对节点, 仅知道邻居中敌对节点个数的上限为 F. 为实现异构系统的安全一致性, 本文设计了一种仅依靠本地信息进行状态更新的安全算法, 具体步骤如下:

步骤 1. 系统中的一阶节点与二阶节点在任一 k 时刻都会接收来自邻居节点的位置与速度信息, 将接收到的位置信息按数值大小进行降序排序.

步骤 2. 信息值处理. 如果节点 i 的邻居节点中存在至少 F 个节点的数值严格大于节点 i 的自身状态值 $x_i(k)$, 那么移除序列中前 F 个节点的信息, 如果不足 F 个节点的数值严格大于 $x_i(k)$, 那么将这些值大于 $x_i(k)$ 的节点全部移除; 同样地, 如果存在至少 F 个节点的数值严格小于节点 i 的自身状态值 $x_i(k)$, 那么移除序列中后 F 个节点的信息, 如果不足 F 个值严格小于 $x_i(k)$, 那么将这些节点全部移除.

步骤 3. 执行步骤 2 后系统中被移除的所有节点用集合 $\mathcal{R}_i$ 表示, 考虑到信任节点的高安全性, 倘若被移除的节点中包含信任节点, 那么在节点的状态更新过程中仍然考虑信任节点的作用, 该信任节点集合用 $\mathcal{T}_i$ 表示. 剩余被移除节点以及节点 i 的边权重设置为 0. 为系统中二阶节点设计如下一致性控制协议:

$$u_i(k)=\sum_{j\in(\mathcal{N}_i\backslash\mathcal{R}_i)\cup\mathcal{T}_i}a_{ij}(x_{ij}(k)-x_i(k))-\alpha v_i(k),\quad i=1,2,\ldots,m. \tag{6}$$

系统中一阶智能体的一致性控制协议为

$$u_i(k)=\sum_{j\in(\mathcal{N}_i\backslash\mathcal{R}_i)\cup\mathcal{T}_i}a_{ij}(x_{ij}(k)-x_i(k)),\quad i=m+1,\ldots,n. \tag{7}$$

现在考虑存在敌对节点情况的异构多智能体系统. 首先需要对系统中的节点序号进行重新编排. 令前 n_1 个节点为二阶正常节点, 第 n_1+1 个节点到 n_2 个节点为一阶正常节点, 剩下的节点为恶意节点, 包括一阶和二阶节点. 与之对应的节点集合分别用 $N_s=[1,\ldots,n_1]$, $N_f=[n_1+1,\ldots,n_2]$ 和 $\mathcal{M}=[n_2+1,\ldots,n]$ 表示. 值得注意的是, 为节点编排序号只为了便于叙述, 而真实系统中所有节点只接收到邻居的状态值, 该值不包含任何的序号信息. 下面给出多智能体系统所有状态量的向量形式, $X(k)=[x_1(k),\ldots,x_{n_1}(k),\ldots,x_{n_2}(k),\ldots,x_n(k)]^{\mathrm{T}}$ 表示所有节点位置的向量形式, $\boldsymbol{v}(k)=[v_1(k),\ldots,v_{n_1}(k)]^{\mathrm{T}}$ 表示所有正常二阶节点的向量形式, $\boldsymbol{u}_s(k)=[u_1(k),\ldots,u_{n_1}(k)]^{\mathrm{T}}$ 和 $\boldsymbol{u}_f(k)=[u_{n_1+1}(k),\ldots,u_{n_2}(k)]^{\mathrm{T}}$ 分别表示二阶节点和一阶节点的控制输入的向量形式. 系统的初始条件为

$$\begin{aligned}&X(0)=[x_1(0),x_2(0),\ldots,x_n(0)]^{\mathrm{T}},\\&\boldsymbol{v}(0)=[v_1(0),v_2(0),\ldots,v_{n_1}(0)]^{\mathrm{T}}.\end{aligned}$$

为了便于标记, 初始条件不考虑敌对节点中二阶节点的速度状态.

基于上述各个状态量的向量形式, 二阶智能体系统的动态方程可用如下矩阵形式表示:

$$X_s(k+1)=X_s(k)+T\boldsymbol{v}(k)+\frac{T^2}{2}\boldsymbol{u}_s(k), \tag{8}$$

$$\boldsymbol{v}(k+1)=\boldsymbol{v}(k)+T\boldsymbol{u}_s(k), \tag{9}$$

其中 $X_s(k)=[x_1(k),\ldots,x_{n_1}(k)]^{\mathrm{T}}$ 表示二阶节点在 k 时刻的位置向量.

同样, 一阶智能体的动态方程可用如下矩阵形式表示:

$$X_f(k+1)=X_f(k)+T\boldsymbol{u}_f(k), \tag{10}$$

其中 $X_f(k)=[x_{n_1+1}(k),\ldots,x_{n_2}(k)]^{\mathrm{T}}$ 表示一阶节点在 k 时刻的位置向量.

根据式 (6) 和 (7), 控制输入 $\boldsymbol{u}_s(k)$ 和 $\boldsymbol{u}_f(k)$ 的矩阵形式如下所示:

$$\boldsymbol{u}_s(k)=-\alpha\boldsymbol{v}(k)-L_s(k)X(k), \tag{11}$$

$$\boldsymbol{u}_f(k)=-L_f(k)X(k), \tag{12}$$

其中 $L_s(k)\in\mathbb{R}^{n_1\times n}$ 表示 Laplacian 矩阵 $L(k)$ 前 n_1 行的元素, $L_f(k)\in\mathbb{R}^{(n_2-n_1)\times n}$ 则表示 Laplacian 矩阵 $L(k)$ 第 n_1+1 行到 n_2 行的元素.

将式 (11) 代入到式 (8) 得到二阶智能体系统闭环形式的矩阵表达式:

$$X_s(k+1)=\left([\,I_{n_1}\ 0\,]-\frac{T^2}{2}L_s(k)\right)X(k)+\left(T-\frac{\alpha T^2}{2}\right)\boldsymbol{v}(k), \tag{13}$$

$$\boldsymbol{v}(k+1)=-TL_s(k)X(k)+(1-\alpha T)\boldsymbol{v}(k). \tag{14}$$

将式 (12) 代入到式 (10) 可得一阶智能体系统闭环形式的矩阵表达式:

$$X_f(k+1)=([\,0\ I_{(n_2-n_1)}\ 0\,]-TL_f(k))X(k). \tag{15}$$

假设2 在二阶智能体系统 (13) 和 (14) 中, α 和 T 的参数设计满足下述条件:

$$1+\frac{T^2}{2}\leqslant\alpha T\leqslant 2-\frac{T^2}{2}. \tag{16}$$

上述条件在文献 [29] 中被应用于二阶智能体系统的一致性问题中, 是接下来引理 1 中矩阵 $[\,\phi_1\ \phi_2\,]$ 实现相关性质的充分条件.

引理1 根据式 (6) 和 (13), 系统中二阶正常智能体的位置状态矩阵形式在任意时刻 $k\geqslant 1$, 可用如下形式表示:

$$X_s(k+1)=\begin{bmatrix}\phi_1 & \phi_2\end{bmatrix}\begin{bmatrix}X(k)\\ X(k-1)\end{bmatrix}, \tag{17}$$

其中

$$\phi_1=(2-\alpha T)[I_{n_1}\quad 0]-\frac{T^2}{2}L_s(k),$$

$$\phi_2=(-1+\alpha T)[I_{n_1}\quad 0]-\frac{T^2}{2}L_s(k-1).$$

证明 根据假设 2 中 α 和 T 的关系以及 Laplacian 矩阵每一行元素和为 0 的性质, 可知 $[\,\phi_1\ \phi_2\,]$ 中每一个元素都为非负元素且每一行元素和为 1. 当 $k\geqslant 1$ 时, 根据二阶智能体速度状态的更新方程 (14), 可以得到如下关系:

$$\boldsymbol{v}(k)-(1-\alpha T)\boldsymbol{v}(k-1)=-TL_s(k-1)X(k-1). \tag{18}$$

根据二阶智能体位置状态的更新方程 (13), 进行如下计算:

$$\begin{aligned} X_s(k+1)-(1-\alpha T)X_s(k) = {} & X_s(k)-(1-\alpha T)X_s(k-1)-\frac{T^2}{2}L_s(k)X(k) \\ & +\frac{T^2}{2}(1-\alpha T)L_s(k-1)X(k-1) \\ & +\left(T-\frac{\alpha T^2}{2}\right)\left(\boldsymbol{v}\left(k\right)-(1-\alpha T)\,\boldsymbol{v}\left(k-1\right)\right). \end{aligned} \tag{19}$$

将式 (18) 代入式 (19), 可得到如下关系:

$$\begin{aligned} X_s(k+1) = {} & \left((2-\alpha T)[I_{n_1} \quad 0]-\frac{T^2}{2}L_s(k)\right)X(k) \\ & +\left((-1+\alpha T)[I_{n_1} \quad 0]-\frac{T^2}{2}L_s(k-1)\right)X(k-1) \\ = {} & \phi_1 X(k)+\phi_2 X(k-1), \end{aligned}$$

整理后即可得到式 (17).

由引理 1 可知, 系统中的二阶节点其更新后的状态值是当前时刻以及上一时刻所有节点的状态值所组成的凸组合. 类似地, 式 (15) 中系数矩阵 $[\,0 \;\; I_{(n_2-n_1)} \;\; 0\,]-TL_f(k)$ 中每一行元素和为 1, 可以得到一阶节点状态更新值为当前时刻所有节点状态值的凸组合.

4 主要结果

首先给出定义 4 中有效性条件的安全区间 S. 该安全区间由所有正常节点的位置和速度初始状态决定, 如下所示:

$$\begin{aligned} S = \Bigg[& \min x^N(0)+\min\left\{0,\left(T-\frac{\alpha T^2}{2}\right)\boldsymbol{v}(0)\right\}, \\ & \max x^N(0)+\max\left\{0,\left(T-\frac{\alpha T^2}{2}\right)\boldsymbol{v}(0)\right\}\Bigg], \end{aligned} \tag{20}$$

其中上标 N 表示正常节点包括一阶与二阶节点, $\boldsymbol{v}(0)$ 表示正常二阶节点的速度初始状态集.

系统中所有正常节点位置状态的最大值最小值分别用 $M(k)$ 和 $m(k)$ 表示:

$$M(k) := \max_{i\in N} x_i(k), \tag{21}$$

$$m(k) := \min_{i\in N} x_i(k). \tag{22}$$

根据引理 1, 定义如下两个变量:

$$\overline{M}(k) := \max(M(k), M(k-1)), \tag{23}$$

$$\underline{m}(k) := \min(m(k), m(k-1)). \tag{24}$$

下面给出本文的主要结论.

定理1 对于由一阶与二阶智能体组成的系统模型 (3) 和 (4), 在控制协议 (6) 和 (7) 下, 系统攻击模型满足假设 1, 如果系统的网络拓扑满足 $(2F+1)$- 稳健性 (含信任节点), 则系统最终能实现安全一致.

证明 首先证明系统在任意时刻满足安全一致性定义中的有效性条件. 在初始时刻, 即 $k=0$ 时, 正常节点的位置状态量 $x_i(0)$ 显然满足条件. 由式 (13) 可知所有二阶正常节点状态更新后位置信息的状态值 $X_s(1)$:

$$X_s(1)=\left([I_{n_1}\ 0]-\frac{T^2}{2}L_s(0)\right)X(0)+\left(T-\frac{\alpha T^2}{2}\right)\boldsymbol{v}(0). \tag{25}$$

又由式 (15) 可知所有一阶正常节点状态更新后位置信息的状态值 $X_f(1)$:

$$X_f(1)=([0\ I_{(n_2-n_1)}\ 0]-TL_f(0))X(0). \tag{26}$$

由式 (25) 可知, 二阶正常节点主要基于邻居节点的位置状态信息及其自身的速度状态信息进行状态更新. 此时, 恶意攻击节点的速度状态量不会对二阶正常节点的状态更新造成影响. 如果邻居节点中存在敌对节点且该节点的位置状态值在区间 $[\min x_i(0),\max x_i(0)]$ 外, 那么在控制算法运行到第 3 节所提算法的步骤 2 时将会被移除. 由假设 1 可知邻居节点中最多存在 F 个敌对节点, 而算法在执行过程中总是会移除具有极端值的部分节点. 又由矩阵 $[I_{n_1}\ 0]-\frac{T^2}{2}L_s(0)$ 每一行元素和为 1, 表明向量 $([I_{n_1}\ 0]-\frac{T^2}{2}L_s(0))X(0)$ 是一个值落在区间 $[\min x_i(0),\max x_i(0)]$ 内的各节点状态值的凸组合, 由此可得 $x_i(1)\in S,\ i\in N_s$. 类似地, 如果式 (26) 中的一阶节点其邻居节点值的大小超出区间 $[\min x_i(0),\max x_i(0)]$ 的范围, 那么这些邻居节点的值在算法执行第 3 节所提算法的步骤 2 时会被移除. 因此保证了矩阵 $[0\ I_{(n_2-n_1)}\ 0]-TL_f(0)$ 每一行元素的和为 1. 由此, 式 (26) 中各一阶正常节点的位置状态为所有节点的凸组合, 也就表明了 $x_i(1)\in S, i\in N_f$.

这里需要指出的是, 式 (23) 和 (24) 中的 $\overline{M}(k)$ 和 $\underline{m}(k)$ 分别为单调非增函数和单调非减函数. 首先证明 $\overline{M}(k)$ 是一个随时间变化的非增函数. 由引理 1 可知时刻 k 下二阶节点 i 的位置状态 $x_i(k)$ 为 $X(k-1)$ 以及 $X(k-2)$ 中所有元素的凸组合, 因此有 $x_i(k)\leqslant\max(M(k-1),M(k-2))$. 与此同时, 考虑到时刻 k 中一阶节点 j 的位置状态 $x_j(k)$ 为 $X(k-1)$ 中所有元素的凸组合, 因此有 $x_j(k)\leqslant M(k-1)$. 结合两者可知 $M(k)\leqslant\max(M(k-1),M(k-2))$, 又根据式 (23) 可得到如下关系:

$$\begin{aligned}\overline{M}(k)&=\max(M(k),M(k-1))\\&\leqslant\max(M(k-1),M(k-2))\\&\leqslant\overline{M}(k-1).\end{aligned} \tag{27}$$

上述过程表明, $\overline{M}(k)$ 为一个随着时间变化的非增函数, 类似地, 可以证明 $\underline{m}(k)$ 为一个随时间变化的非减函数. 再根据 $\overline{M}(k)$ 和 $\underline{m}(k)$ 的单调性, 可以得到 $x_i(k)\in S,\ i\in N$, 即系统的有效性得证.

接下来, 证明系统满足安全一致性定义中的一致性条件. 根据单调收敛理论, $\overline{M}(k)$ 和 $\underline{m}(k)$ 分别存在有限上界和有限下界, 用 M^* 和 m^* 表示. 为证明正常节点能够在位置状态空间中达到一致状态, 系统则必须满足 $M^*=m^*$. 这里我们采用反证法.

假设 $M^*>m^*$, β 为矩阵 $[\phi_1\ \phi_2]$ 以及矩阵 $[0\ I_{(n_2-n_1)}\ 0]-TL_f(0)$ 中所有元素的最小系数. $\epsilon>0$ 和 $\epsilon_0>0$ 都足够小, 因此有

$$m^*+\epsilon_0<M^*-\epsilon_0,\quad \epsilon<\frac{\beta^{n_2}\epsilon_0}{1-\beta^{n_2}}. \tag{28}$$

假设序列 $\{\epsilon_l\}$ 存在如下关系:

$$\epsilon_l=\beta\epsilon_{l-1}-(1-\beta)\epsilon,\quad l=1,2,\ldots,n_2. \tag{29}$$

可以看出对于所有的 l 都存在 $0<\epsilon_{l+1}<\epsilon_l$, 结合式 (28) 可知所有的 ϵ_l 都为正数, 因此可得出下列关系:

$$\begin{aligned}\epsilon_{n_2} &= \beta^{n_2}\epsilon_0-\sum_{l=0}^{n_2-1}\beta^l(1-\beta)\epsilon\\ &=\beta^{n_2}\epsilon_0-(1-\beta^{n_2})\epsilon>0,\end{aligned}$$

从上式中可以看出 ϵ_{n_2} 的最小值大于零.

由于 $\overline{M}(k)$ 和 $\underline{m}(k)$ 都为收敛函数, 那么必定存在一个 k_ϵ, 使得任意 $k\geqslant k_\epsilon$, 有 $\overline{M}(k_\epsilon)<M^*+\epsilon$ 和 $\underline{m}(k_\epsilon)>m^*-\epsilon$. 结合序列 $\{\epsilon_l\}$, 给出如下两个集合:

$$\mathcal{X}_M(k_\epsilon+l,\epsilon_l)=\{j\in\mathcal{V}:x_j(k_\epsilon+l)>M^*-\epsilon_l\},\tag{30}$$

$$\mathcal{X}_m(k_\epsilon+l,\epsilon_l)=\{j\in\mathcal{V}:x_j(k_\epsilon+l)<m^*+\epsilon_l\}.\tag{31}$$

下面证明以上两个集合伴随着系统状态更新至少有一个集合将不再包含正常节点. $\overline{M}(k)$ 的上界 M^* 表明集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 和 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 中至少存在一个正常节点. 假设存在这样一个二阶节点 i 位于集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 之外, 那么就有 $x_i(k_\epsilon)\leqslant M^*-\epsilon_0$. 节点 i 的位置状态为 $X(k_\epsilon)$ 和 $X(k_\epsilon-1)$ 中所有元素的凸组合. 又因为 β 是系统中所有系数的最小值, 节点 i 的位置状态更新后为

$$\begin{aligned}x_i(k_\epsilon+1)&\leqslant(1-\beta)\overline{M}(k_\epsilon)+\beta(M^*-\epsilon_0)\\&\leqslant(1-\beta)(M^*+\epsilon)+\beta(M^*-\epsilon_0)\\&\leqslant M^*-\epsilon_1.\end{aligned}\tag{32}$$

类似地, 假设一个一阶节点 i 其位置状态大小在集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 之外, 可知 $x_i(k_\epsilon)\leqslant M^*-\epsilon_0$. 从邻居节点中接收到的位置信息其值上界为 $\overline{M}(k_\epsilon)$, 考虑到一阶节点的状态更新过程得到与式 (32) 相同的关系, 如下所示:

$$x_i(k_\epsilon+1)\leqslant(1-\beta)\overline{M}(k_\epsilon)+\beta(M^*-\epsilon_0).\tag{33}$$

式 (32) 和 (33) 表明当前时刻 k 落在集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 之外的正常节点进行系统状态更新后其值仍落在集合 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 之外. 类似地, 落在集合 $\mathcal{X}_m(k_\epsilon,\epsilon_0)$ 之外的正常节点在系统更新后的下一时刻其状态值同样落在集合 $\mathcal{X}_m(k_\epsilon+1,\epsilon_1)$ 之外.

下面讨论落在集合 $\mathcal{X}_M(k_\epsilon+l,\epsilon_l)$ 或者 $\mathcal{X}_m(k_\epsilon+l,\epsilon_l)$ 内的正常节点进行系统状态更新后的情况.

假设集合 $\mathcal{Z}_M^{2F+1}(k_\epsilon,\epsilon_l)\subseteq\mathcal{X}_M(k_\epsilon,\epsilon_l)$, 该集合中的每一个节点在集合 $\mathcal{V}\setminus\mathcal{X}_M(k_\epsilon,\epsilon_l)$ 中至少存在 $2F+1$ 个邻居节点, 或者存在至少一个信任邻居节点. 类似地, 给出集合 $\mathcal{Z}_m^{2F+1}(k_\epsilon,\epsilon_l)\subseteq\mathcal{X}_m(k_\epsilon,\epsilon_l)$.

由于 $\mathcal{X}_M(k_\epsilon,\epsilon_0)\cap\mathcal{X}_m(k_\epsilon,\epsilon_0)=\emptyset$ 且系统的网络拓扑满足 $(2F+1)$- 稳健性 (含信任节点), 那么集合 $\mathcal{Z}_M^{2F+1}(k_\epsilon,\epsilon_0)$ 和 $\mathcal{Z}_m^{2F+1}(k_\epsilon,\epsilon_0)$ 其中至少有一个集合不为空集. 假设节点 $i\in\mathcal{Z}_M^{2F+1}(k_\epsilon,\epsilon_0)$ 是这样一个节点: 它在集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 外至少存在 $2F+1$ 个邻居节点, 或者至少存在一个信任节点. 考虑到节点 i 的邻居节点中至多有 F 个恶意节点, 那么在集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 之外至少有 $F+1$ 个正常节点或者至少有一个信任节点. 执行算法操作后, 节点 i 至少还有一个邻居节点 (包括信任节点), 其最大值为 $M^*-\epsilon_0$, 同时节点 i 的最大值为 $\overline{M}(k_\epsilon)$. 那么在状态更新后节点 i 具有如下关系:

$$x_i(k_\epsilon+1)\leqslant(1-\beta)\overline{M}(k_\epsilon)+\beta(M^*-\epsilon_0).$$

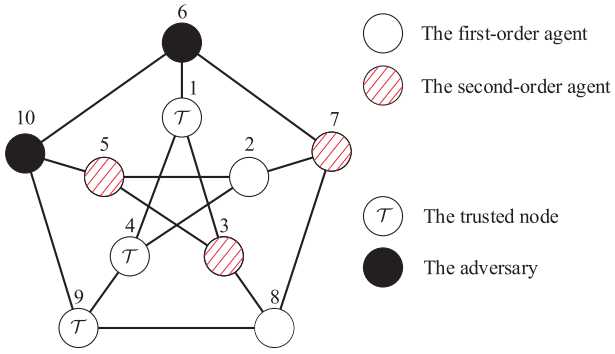

图 2 (网络版彩图) 由 10 个节点组成的无向图

Figure 2 (Color online) Undirected graph with 10 agents

由式 (32) 可知, $x_i(k_\epsilon+1)$ 的值要小于 $M^*-\epsilon_1$, 这表明节点 i 在系统更新状态后便不再包含在集合 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 上. 同样地, 若 $\mathcal{Z}_m^{2F+1}(k_\epsilon,\epsilon_0)$ 不为空集, 那么落在集合 $\mathcal{X}_m(k_\epsilon,\epsilon_0)$ 内的一个正常节点在状态更新后不再包含在集合 $\mathcal{X}_m(k_\epsilon+1,\epsilon_1)$ 上. 由此可得, $|\mathcal{X}_M(k_\epsilon+1,\epsilon_1)|<|\mathcal{X}_M(k_\epsilon,\epsilon_0)|$ 以及 $|\mathcal{X}_m(k_\epsilon+1,\epsilon_1)|<|\mathcal{X}_m(k_\epsilon,\epsilon_0)|$.

序列 ϵ_l 为一递减序列, 因此有 $\epsilon_1<\epsilon_0$. 由此保证状态更新后的两个集合 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 和 $\mathcal{X}_m(k_\epsilon+1,\epsilon_1)$ 为不相邻集合. 只要集合 $\mathcal{X}_M(k_\epsilon+l,\epsilon_l)$ 和 $\mathcal{X}_m(k_\epsilon+l,\epsilon_l)$ 内存在正常节点, 那么在任意时刻 $k_\epsilon+l$ 下重复上述分析过程, 可以得到 $|\mathcal{X}_M(k_\epsilon+l+1,\epsilon_{l+1})|<|\mathcal{X}_M(k_\epsilon+l,\epsilon_l)|$ 或者 $|\mathcal{X}_m(k_\epsilon+l+1,\epsilon_{l+1})|<|\mathcal{X}_m(k_\epsilon+l,\epsilon_l)|$. 由于正常节点的个数是固定的, 假设某一个时刻 τ 下集合 $\mathcal{X}_M(k_\epsilon+\tau,\epsilon_\tau)$ 和 $\mathcal{X}_m(k_\epsilon+\tau,\epsilon_\tau)$ 中至少有一个集合不再包含正常节点. 那么对于 $l\geqslant\tau$, 集合 $\mathcal{X}_M(k_\epsilon+l,\epsilon_l)$ 或者 $\mathcal{X}_m(k_\epsilon+l,\epsilon_l)$ 其中一个集合会变为空集. 这与 M^* 和 m^* 的存在性矛盾. 由此, 得出 $M^*=m^*$ 成立.

当系统中所有正常节点都聚集到空间中的某一个位置, 即位置状态收敛于一个常数时, 我们可以得到 $x_i(k+1)\to x_i(k)$. 又根据式 (5) 可知 $u_i(k)\to-\alpha v_i(k), k\to\infty$. 代入到二阶节点的动态方程 (3) 中则有 $x_i(k+1)\to x_i(k)+(T-\frac{\alpha T^2}{2})v_i(k), k\to\infty$. 再通过式 (2) 中给出的 α 和 T 的约束关系, 得到 $v_i(k)\to 0, k\to\infty$. 由此定理得证.

5 数值仿真

考虑一个由 10 个节点组成的异构多智能体系统, 其通信拓扑如图 2 所示. 图中节点由一阶与二阶节点混合构成, 其中节点 1, 2, 3, 4, 9 为一阶节点, 节点 5, 7, 8 为二阶节点, 节点 6, 10 为敌对节点. 设置节点 1, 4, 9 为信任节点. 方便起见, 假设系统的初始状态值为 $X(0)=[1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10]^{\mathrm{T}}$, 二阶节点的初始速度状态皆设置为 1. 式 (2) 中 α 和 T 设为 $\alpha=5, T=0.3$ s. 由式 (20) 得到系统的安全区间 $S=[1,9.075]$.

若不设置信任节点, 根据定义 2, 可以验证图 2 中节点之间的拓扑并不具备 3- 稳健性. 若设置信任节点, 根据定义 3, 图 2 节点之间的拓扑具备 3- 稳健性 (含信任节点). 假设敌对节点 6, 10 的动态方程分别为

$$\begin{cases} x_6(k+1)=0.5\sin(0.3k)+6, \\ v_6(k+1)=0.8v_6(k)+1.6, \end{cases} \tag{34}$$

$$x_{10}(k+1)=0.8x_{10}(k)+0.5, \tag{35}$$

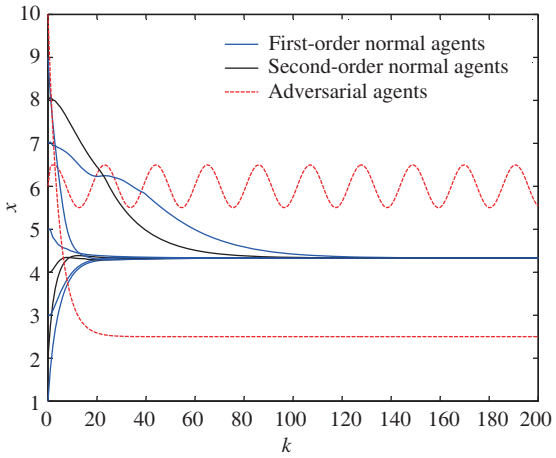

图 3 (网络版彩图) 满足 3- 稳健性 (含信任节点) 的图中各节点的状态轨迹

Figure 3 (Color online) State trajectories of agents under graph satisfying 3-robust with trusted nodes

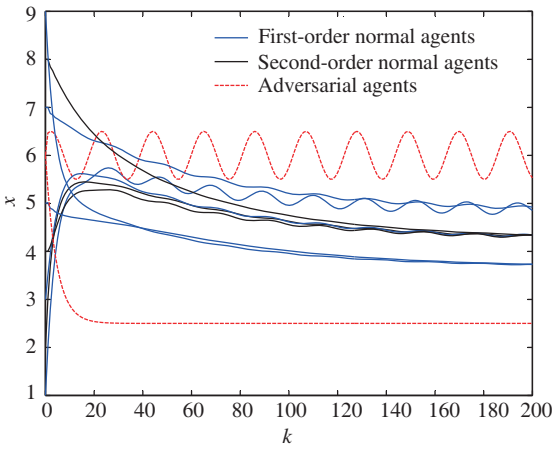

图 4 (网络版彩图) 不包含信任节点的图中各节点的状态轨迹

Figure 4 (Color online) State trajectories of agents under graph without trusted nodes

其中敌对攻击节点 6 为二阶节点, 节点 10 为一阶节点. 图 2 中各正常节点在任意时刻邻居节点中的最大敌对节点数为 1. 根据定理 1 可知, 若图 2 中节点采用本文提出的控制协议, 那么系统状态在上述拓扑条件下能够实现安全一致.

系统的状态轨迹如图 3 所示, 从图中可以看出, 即便遭受到了两个敌对节点的攻击, 各正常节点的状态值仍在安全区间内变化, 且最终达到一致状态. 若考虑将图 2 中节点 1, 4, 9 设置为普通节点, 致使图 2 拓扑不再具备 3- 稳健性. 此时各节点的状态轨迹如图 4 所示, 从图中可以看到, 在敌对节点的影响下, 系统的状态无法达成一致.

6 结论

本文针对一阶二阶异构多智能体系统的安全一致性问题进行了研究, 得到了系统中各正常智能体

状态达到安全一致的充分条件. 同时, 通过将系统中部分节点设置为信任节点, 显著提升了网络稳健性. 在设置与不设置信任节点拓扑下的数值实例验证了所提方法的有效性.

参考文献

1 Lin X, Stephen B, Sanjay L. A scheme for robust distributed sensor fusion based on average consensus. In: Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, Boise, 2005. 63–70

2 Lin Z Y, Francis B, Maggiore M. Necessary and sufficient graphical conditions for formation control of unicycles. IEEE Trans Automat Contr, 2005, 50: 121–127

3 Ren W. Consensus strategies for cooperative control of vehicle formations. IET Control Theor Appl, 2007, 1: 505–512

4 Li T, Fu M, Xie L, et al. Distributed consensus with limited communication data rate. IEEE Trans Automat Contr, 2011, 56: 279–292

5 Rao S, Ghose D. Sliding mode control-based autopilots for leaderless consensus of unmanned aerial vehicles. IEEE Trans Contr Syst Technol, 2014, 22: 1964–1972

6 Zheng Y S, Zhao Q, Ma J, et al. Second-order consensus of hybrid multi-agent systems. Syst Contr Lett, 2019, 125: 51–58

7 Olfati-Saber R, Murray R M. Consensus problems in networks of agents with switching topology and time-delays. IEEE Trans Automat Contr, 2004, 49: 1520–1533

8 Ren W, Beard R W. Consensus seeking in multiagent systems under dynamically changing interaction topologies. IEEE Trans Automat Contr, 2005, 50: 655–661

9 Huang M Y, Manton J H. Coordination and consensus of networked agents with noisy measurements: stochastic algorithms and asymptotic behavior. SIAM J Control Opt, 2009, 48: 134–161

10 Li T, Zhang J F. Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises. IEEE Trans Automat Contr, 2010, 55: 2043–2057

11 Cheng L, Hou Z G, Tan M. A mean square consensus protocol for linear multi-agent systems with communication noises and fixed topologies. IEEE Trans Automat Contr, 2014, 59: 261–267

12 Ge X H, Han Q L. Consensus of multiagent systems subject to partially accessible and overlapping markovian network topologies. IEEE Trans Cybern, 2017, 47: 1807–1819

13 Cao Y, Zhang L Y, Li C Y, et al. Observer-based consensus tracking of nonlinear agents in hybrid varying directed topology. IEEE Trans Cybern, 2017, 47: 2212–2222

14 Pasqualetti F, Bicchi A, Bullo F. Consensus computation in unreliable networks: a system theoretic approach. IEEE Trans Automat Contr, 2012, 57: 90–104

15 Wu Y M, He X X. Secure consensus control for multiagent systems with attacks and communication delays. IEEE/CAA J Autom Sin, 2017, 4: 136–142

16 Zhang W B, Wang Z D, Liu Y R, et al. Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks. Int J Robust Nonlin Control, 2018, 28: 53–67

17 LeBlanc H J, Koutsoukos X. Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multiagent systems. IEEE Trans Control Netw Syst, 2018, 5: 1219–1231

18 Zhao C C, He J P, Chen J M. Resilient consensus with mobile detectors against malicious attacks. IEEE Trans Signal Inf Process Over Netw, 2018, 4: 60–69

19 LeBlanc H J, Zhang H T, Koutsoukos X, et al. Resilient asymptotic consensus in robust networks. IEEE J Sel Areas Commun, 2013, 31: 766–781

20 de Azevedo M M, Blough D M. Multistep interactive convergence: an efficient approach to the fault-tolerant clock synchronization of large multicomputers. IEEE Trans Parallel Distrib Syst, 1998, 9: 1195–1212

21 Wu Y M, Ding J J, He X X, et al. Secure consensus control for multi-agent systems under communication delay. Contr Theor Appl, 2016, 33: 1039–1045 [伍益明, 丁佳骏, 何熊熊, 等. 通信时延下多智能体系统的安全一致性控制. 控制理论与应用, 2016, 33: 1039–1045]

22 Zhang N, Du W, He X X, et al. Secure consensus control of multi-agent systems based on median state strategy. Contr Decis, 34: 567–571 [张霓, 杜伟, 何熊熊, 等. 基于中间状态值的多智能体系统安全一致性控制. 控制与决策, 2019, 34: 567–571]

23 Wu Y M, He X X, Liu S. Resilient consensus for multi-agent systems with quantized communication. In: Proceedings of 2016 American Control Conference (ACC), Boston, 2016. 5136–5140
24 Dibaji S M, Ishii H, Tempo R. Resilient randomized quantized consensus. IEEE Trans Automat Contr, 2018, 63: 2508–2522
25 Dibaji S M, Ishii H. Resilient consensus of double-integrator multi-agent systems. In: Proceedings of 2014 American Control Conference, Portland, 2014. 5139–5144
26 Dibaji S M, Ishii H. Consensus of second-order multi-agent systems in the presence of locally bounded faults. Syst Control Lett, 2015, 79: 23–29
27 Dibaji S M, Ishii H. Resilient consensus of second-order agent networks: Asynchronous update rules with delays. Automatica, 2017, 81: 123–132
28 Abbas W, Laszka A, Koutsoukos X. Improving network connectivity and robustness using trusted nodes with application to resilient consensus. IEEE Trans Control Netw Syst, 2018, 5: 2036–2048
29 Cao Y C, Ren W. Sampled-data discrete-time coordination algorithms for double-integrator dynamics under dynamic directed interaction. Int J Control, 2010, 83: 506–515

Secure consensus control for heterogeneous multi-agent systems with trusted nodes

Jinbo HUANG[1], Yiming WU[2*], Liping CHANG[1] & Xiongxiong HE[1]

1. *College of Information Engineering, Zhejiang University of Technology, Hangzhou* 310023*, China*;
2. *School of Cyberspace, Hangzhou Dianzi University, Hangzhou* 310018*, China*
* Corresponding author. E-mail: ymwu@hdu.edu.cn

Abstract This study focuses on the secure consensus problem for heterogeneous multi-agent systems composed of first- and second-order agents. First, we show that the network robustness can be significantly improved by setting a subset of nodes as trusted nodes. Then, we propose a secure consensus algorithm for heterogeneous systems with trusted nodes. The sufficient conditions for the convergence of the normal agents' states to a common value under adversarial nodes are presented. Finally, certain numerical examples are provided to illustrate the effectiveness of the theoretical results.

Keywords heterogeneous systems, multi-agent systems, secure consensus, secure control, trusted node

Jinbo HUANG was born in 1994. He received his B.E. degree in communication engineering from Zhejiang University of Technology, Hangzhou, China. Currently, he is now working toward his Master's degree at College of Information Engineering, Zhejiang University of Technology, Hangzhou, China. His research interests include multi-agent systems, consensus, and resilient control.

Liping CHANG was born in 1980. She received her B.S. degree in measure-control technology and instruments from Zhengzhou University, Zhengzhou, in 2003, and her Ph.D. degree in optical engineering from Institute of Optical and Fine Mechanics, Shanghai, in 2008. She is currently serving as an Associate Professor in College of Information Engineering, Zhejiang University of Technology. Her major interests are signal processing, distributed network control system, and compressed sensing, as well as their applications to speeches, images, and optics.

Yiming WU was born in 1987. He received his B.E. degree in automation and Ph.D. degree in control science and engineering from Zhejiang University of Technology, Zhejiang, China, in 2010 and 2016, respectively. From April 2012 to April 2014, he was a research assistant at Nanyang Technological University, Singapore. Since July 2016, he has been with School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. His current research interests include multi-agent systems, resilient consensus, and secure control systems.

Xiongxiong HE was born in 1965. He received his M.S. degree from Qufu Normal University, Qufu, China, in 1994, and Ph.D. degree from Zhejiang University, Hangzhou, China, in 1997. He held a post-doctoral position with Harbin Institute of Technology from 1998 to 2000. He joined Zhejiang University of Technology, Hangzhou, China, in 2001, where he has been a Professor at College of Information Engineering. His research areas include nonlinear control and signal processing.