DOI: 10.7641/CTA.2016.50713

通信时延下多智能体系统的安全一致性控制

伍益明[1], 丁佳骏[1], 何熊熊[1†], 欧县华[1,2]

(1. 浙江工业大学 信息工程学院, 浙江 杭州 310023; 2. 南洋理工大学 电子与电气工程学院, 新加坡 639798)

摘要: 研究了离散时间多智能体系统存在通信时延条件下的安全一致性问题. 本文的目标是设计一种一致性控制算法能够使得网络中各正常智能体抵御敌对智能体的攻击并实现最终状态一致. 该算法仅利用个体的自身状态和相邻个体的时延信息作为控制输入, 并根据控制器参数、拓扑属性和通信时延, 获得了所提算法实现收敛的充要条件. 最后, 通过仿真实例对理论结果进行了验证.

关键词: 多智能体系统; 一致性; 通信时延; 安全分布式控制

中图分类号: TP273 **文献标识码**: A

Secure consensus control for multi-agent systems under communication delay

WU Yi-ming[1], DING Jia-jun[1], HE Xiong-xiong[1†], OU Xian-hua[1,2]

(1. College of Information Engineering, Zhejiang University of Technology, Hangzhou Zhejiang 310023, China;
2. School of Electronic and Electrical Engineering, Nanyang Technological University, 639798, Singapore)

Abstract: This paper studies the secure consensus problem for discrete-time multi-agent systems under communication delay. The objective is to design a control protocol such that all normal agents can resist adversarial agents and asymptotically achieve an agreement as time goes to infinity. For the considered networked system, the control input of each normal agent can only use its own value and the delayed information of its neighbors. Sufficient and necessary conditions, which depend on the control parameters, the topological property, and the communication delay, are obtained to guarantee the final convergence of the consensus protocol. Finally, some numerical examples are given to demonstrate the theoretical results.

Key words: multi-agent systems; consensus; communication delay; secure distributed control

1 引言(Introduction)

近些年来, 多智能体系统协调控制问题受到了系统与控制领域专家学者的广泛关注. 在多智能体系统网络中, 一致性控制(consensus control)作为协调控制领域的代表性问题, 也是其他分布式控制和估计的研究基础, 是指通过设计适当的控制算法(协议), 使得多智能体系统中所有个体的状态值渐进地或者有限时间内趋于一致. 近年来, 伴随多智能体系统协调控制问题的深入研究以及其在工程领域的广泛应用, 一致性控制问题已成为当前的一个研究热点, 在理论研究与实际应用等方面都取得了丰硕的成果, 参见文献[1–12].

一致性控制的安全性问题作为多智能体系统研究中一个新兴且又十分重要的研究课题, 逐渐受到国内外研究人员的重视, 并且取得了一定的研究成果[13–16]. 多智能体系统安全一致性控制(secure consensus control)的基本思想, 是指通过对系统中正常智能体施加控制, 使得其在执行一致性协议中, 能够抵御敌对智能体的攻击行为, 确保其状态始终处于一个容许范围(安全域)内变化, 并最终趋于一致. 为了获取安全一致性算法, 已有许多学者做了相关的研究工作. 文献[17]最早在针对系统中存在部分敌对个体情况下, 研究了安全一致性算法, 结果表明在给定的网络通信条件下, 如果系统中敌对个体的数目占系统所有个体数三分之一以下, 则系统正常个体的状态值最终仍能相互达成一致. 文献[18]研究了多智能体系统分别在存有拜占庭(byzantine)和非共谋(non-colluding)两类敌对节点环境下的线性一致性问题, 得到了敌对个体数目与网络通信图连通度的对应关系. 而在文献[19]中则提出一种新的基于图论的r–健壮图(r-

收稿日期: 2015−08−30; 录用日期: 2016−04−22.

†通信作者. E-mail: hxx@zjut.edu.cn; Tel.: +86 571-85290587.

本文责任编委: 冯祖仁.

国家自然科学基金项目(61473262)资助.

Supported by National Natural Science Foundation of China (61473262).

robust)概念, 仅根据邻居的交互信息设计协议, 解决了网络中存有拜占庭敌对节点的一致性问题. 随后, 文献[20]将上述结果扩展到了二阶多智能体系统. 传统的安全一致性协议, 缺陷在于需要依附较高的网络连通度, 各节点需要较大的计算和通信能力. 为此, 如何有效减少通信链路而又能保证抵御敌对节点的干扰成为一批学者的研究重心. 文献[21]减弱了需要高复杂度通信拓扑的条件, 借助两跳邻居的信息, 提出了一种基于安全的平均一致算法 (secure average-consensus-based time synchronization, SATS), 成功解决了系统网络中的时钟同步问题. 而文献[22]则通过在网络中设立一类绝对可信节点, 提出了一种新的控制策略, 其研究结果表明, 如果设立的绝对可信节点能组成一个无向连通子图, 则即使面对任意数目的敌对个体, 系统仍可达成一致. 除上述工作外, 还有一批学者通过使用基于迭代的方法来设计安全一致性协议, 参见文献[23–25].

总的来说, 上述研究工作对多智能体系统安全一致性问题做了有益的理论和实践探索, 但仍存在一些需要考虑的问题: 一方面, 上述文献中均假设系统个体之间的通信是理想的状况, 即各节点能实时地交互信息. 然而对于实际的通信网络, 众所周知, 时延是普遍存在且不可避免的. 更有甚者, 存在一类敌对节点, 具有专门使通信链路产生特定时延的能力[26–27]; 另一方面, 目前大部分研究工作是针对静态的网络拓扑, 依据固定的邻居信息设计协议, 往往无法应对灵活可变的攻击节点, 因此具有一定的局限性.

针对上述问题, 本文在文献[28]的基础上, 进一步考虑了通信时延条件下多智能体系统的安全一致性问题. 考虑系统中存有两类相互对立的节点: 其中一类是安全可信的正常节点(safe agent), 该类节点将始终严格按照控制协议进行自身状态的信息更新; 而另一类则是持相反目的具有攻击行为的敌对节点(adversarial agent), 该类节点不受控制协议的约束, 恶意向周围正常节点发送虚假信息, 影响其状态更新, 试图使系统状态偏离安全域, 亦或使整个系统无法达成一致. 与文献[19, 23, 28]讨论的固定通信拓扑相比, 本文考虑的协议适用于时变通信拓扑.

将会用到的一些数学符号说明如下: $\mathbb{R}$(相应的, $\mathbb{R}^n$, $\mathbb{R}^{m\times n}$)表示实数集(相应的, 实n维向量, 实$m\times n$维度矩阵); $\mathbb{Z}$(相应的, $\mathbb{Z}^+$)表示整数集(相应的, 正整数集), $\bar{\mathbb{Z}}^+ \triangleq \mathbb{Z}^+\cup\{0\}$; $A^{i,j}$表示矩阵A第i行第j列的元素; I表示适当维数的单位矩阵. 给定一对集合$\mathcal{S}$和$\mathcal{T}$, $\mathcal{S}\setminus\mathcal{T}$表示元素属于$\mathcal{S}$而不属于$\mathcal{T}$. $|\mathcal{S}|$表示集合$\mathcal{S}$内的元素个数. $\mathcal{S}_1, \mathcal{S}_2, \cdots, \mathcal{S}_n$称为集合$\mathcal{S}$的划分子集, 若满足条件: i) $\mathop{\cup}\limits_{1\leqslant i\leqslant n}\mathcal{S}_i=\mathcal{S}$及ii) $\mathcal{S}_i\cap\mathcal{S}_j=\varnothing$, $\forall i\neq j$.

2 预备知识以及问题描述(Preliminaries and problem statement)

2.1 图论知识(Graph theory)

在多智能体系统的一致性问题研究中, 图论是重要的分析工具. 通常, 用记号$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G},A_\mathcal{G}\}$表示一个加权的有向图, 其中: $\mathcal{V}=\{v_1,v_2,\cdots,v_n\}$表示节点集, 有限集合$\mathcal{I}=\{1,2,\cdots,n\}$表示节点的序号集, $\mathcal{E}_\mathcal{G}\subseteq\mathcal{V}\times\mathcal{V}$表示边集; $A_\mathcal{G}=[a_{i,j}]\in\mathbb{R}^{n\times n}$表示图$\mathcal{G}$的非负邻接矩阵. $A_\mathcal{G}$中元素$a_{i,j}\geqslant 0$表示有向边的权重. 当有向边$(v_j,v_i)\in\mathcal{E}_\mathcal{G}$时, 即节点$v_i$能够获取节点$v_j$的信息时, $a_{i,j}>0$, 否则$a_{i,j}=0$. 如果$(v_i,v_i)\in\mathcal{E}_\mathcal{G}$, 则表示节点$v_i$存在自环. v_i的邻居序号集表示为$\mathcal{N}_i=\{j\in\mathcal{I}\,|(v_j,v_i)\in\mathcal{E}_\mathcal{G}\}$. 有序边$(v_i,v_{l_1}),(v_{l_1},v_{l_2}),\cdots,(v_{l_\mathrm{p}},v_j)$组成的有向序列称为节点$v_i$到$v_j$的路径, 其中$v_i, v_j, v_{l_1},\cdots,v_{l_\mathrm{p}}$分别为不同的节点. 对于一有向图, 如果至少存在一个节点, 可以沿着图中边的路径, 抵达其他任何一个节点的位置, 则称此图包含一生成树. 假设$\mathcal{G}_1,\mathcal{G}_2,\cdots,\mathcal{G}_k$为具有相同节点集的有向图, 令$\mathcal{G}$的节点集与$\mathcal{G}_1,\mathcal{G}_2,\cdots,\mathcal{G}_k$相同, 边集为$\mathcal{G}_1,\mathcal{G}_2,\cdots,\mathcal{G}_k$边集的并, 则称图$\mathcal{G}$为图$\mathcal{G}_1,\mathcal{G}_2,\cdots,\mathcal{G}_k$的联合图. 对于一具有相同节点集的无穷序列图$\mathcal{G}_1,\mathcal{G}_2,\cdots$如果存在一个正整数$q$, 使得每一子序列$\mathcal{G}_{qk+1},\mathcal{G}_{qk+2},\cdots,\mathcal{G}_{q(k+1)}$, $k\geqslant 0$的联合图均包含一生成树, 则称该无穷序列图包含频繁联合生成树.

基于上述图论的基本概念, 接下来需要引入一些通信拓扑连通性的定义, 下述定义采用自文献[19, 28], 并做了适当的修改, 具体如下:

定义 1 r–可及集. 对于一个有向图$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G}\}$以及其一非空节点子集$\mathcal{S}\subset\mathcal{V}$, 如果$\mathcal{S}$中存有至少一个节点$v_i$, 满足$|\mathcal{N}_i\backslash\mathcal{S}|\geqslant r$, $r\in\mathbb{Z}^+$. 称集合$\mathcal{S}$为r–可及集.

可以发现, 对于一个r–可及集$\mathcal{S}$, 它至少包含这样一个节点, 该节点保证至少有r个邻居信息来自集合$\mathcal{S}$外. 也就是说, $\mathcal{S}$当中至少存在一个节点, 可接收自身集合外一定数目的其他节点信息. 在r–可及集的定义上, 接下来给出r–健壮图的定义.

定义 2 r–健壮图. 对于一个有向图$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G}\}$, 若$\mathcal{V}$中任意一对划分子集, 记作$\mathcal{S}_1,\mathcal{S}_2$, 至少存在一个节点$v_i\in\mathcal{S}_\kappa$, $\kappa=1,2$, 满足$|\mathcal{N}_i\setminus\mathcal{S}_\kappa|\geqslant r, r\in\mathbb{Z}^+$. 称图$\mathcal{G}$是$r$–健壮图.

2.2 问题描述(Problem statement)

考虑用一有向图$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G},A_\mathcal{G}\}$表示一个由$n$个个体组成的多智能体系统, 图中每个节点代表一个智能体. 将节点集$\mathcal{V}$划分成两个子集, 分别用$\mathcal{V}_\mathrm{s}=\{v_1,v_2,\cdots,v_{n_\mathrm{s}}\}$表示包含$n_\mathrm{s}$个正常节点的集合, $\mathcal{V}_\mathrm{a}=\{v_{n_\mathrm{s}+1},v_{n_\mathrm{s}+2},\cdots,v_n\}$表示包含$n_\mathrm{a}=n-n_\mathrm{s}$个敌对

节点的集合. 显然有$\mathcal{V}=\mathcal{V}_{\rm s}\cup\mathcal{V}_{\rm a}$, $\varnothing=\mathcal{V}_{\rm s}\cap\mathcal{V}_{\rm a}$. 与之对应的序号集分别为$\mathcal{I}_{\rm s}=\{1,2,\cdots,n_{\rm s}\}$和$\mathcal{I}_{\rm a}=\{n_{\rm s}+1,n_{\rm s}+2,\cdots,n\}$.

考虑系统中各正常节点的动态方程如下:

$$x_i(k+1)=x_i(k)+u_i(k),\ i\in\mathcal{I}_{\rm s},\ k\in\bar{\mathbb{Z}}^+,\quad(1)$$

其中$x_i(k)\in\mathbb{R}^m$和$u_i(k)\in\mathbb{R}^m$分别表示节点v_i在k时刻的状态矢量和控制矢量. 为阐述方便, 不失一般性, 文中均假设$m=1$, 对于$m>1$的情况, 本文所得结论同样成立, 可通过引入Kronecker算子进行扩展.

2.3 攻击模型(Attack model)

通常, 网络中攻击模型由节点的攻击方式和部署范围两方面组成. 文献[13–14, 17, 24]介绍了几类多智能体网络中常见的攻击方式, 如碰撞(crash)攻击、共谋(colluding)攻击、拜占庭攻击等. 在各类型攻击方式中, 相关文献已经证明, 拜占庭攻击最具有破坏性. 这类拜占庭节点不受制控制协议u的约束, 可任意更换自身状态值, 它掌握网络的全局信息, 可与其他敌对节点共谋, 并能在同一时刻向周围不同邻居发送不同的虚假信息, 以此来干扰破坏系统的一致性进程. 鉴于拜占庭攻击特点涵盖了其他各类型的攻击. 所以但凡具备抵御拜占庭攻击的系统, 同样能抵御以上其他类型的攻击. 本文考虑的敌对节点假设具有上述拜占庭攻击能力外, 另具备可在任意时刻转换攻击对象或者暂停攻击的能力, 其具体定义为:

定义 3　敌对节点. 称节点$v_{\rm q}$, $q\in\mathcal{I}_{\rm a}$为敌对节点, 如果$v_{\rm q}$具有下列属性:

· 其状态更新方程满足下式:

$$x_{\rm p}^{\rm q}(k+1)=f_{\rm p}^{\rm q}(\{x_{\rm q}^{\rm p}(k)\}),\ q\in\mathcal{I}_{\rm a},\ p\in\mathcal{N}_{\rm q},\quad(2)$$

其中: $x_{\rm p}^{\rm q}(k)$表示k时刻节点$v_{\rm q}$向节点$v_{\rm p}$发送的状态值, $f_{\rm p}^{\rm q}(\cdot)$可以是任意函数;

· 同一时刻可向不同的邻居节点传递不同的信息值, 即$x_i^{\rm q}(k)\neq x_j^{\rm q}(k)$, $\forall i,j\in\mathcal{N}_{\rm q}$, 且$i\neq j$. 也就是说, 在同一时刻, 函数$f_i^{\rm q}(\cdot)\neq f_j^{\rm q}(\cdot)$;

· 在任意时刻可以随意改变攻击对象或者放弃攻击.

显然, 如果不对上述敌对节点数目进行限定, 则当系统中绝大多数个体为敌对节点时, 系统就很难实现一致. 为此, 本文对敌对节点的部署范围做如下假设.

假设 1　多智能体系统中任一正常节点的邻居中存有至多不超过f个数目的节点属于敌对节点, 即$|\mathcal{N}_i\cap\mathcal{V}_{\rm a}|\leqslant f$, $\forall i\in\mathcal{I}_{\rm s}$, $f\in\mathbb{Z}^+$.

2.4 通信时延下的安全一致性算法(Secure consensus algorithm under communication delay)

本文考虑网络中所有节点均未知其他节点的识别序号, 在仅知道周围邻居中至多拥有不超过f个敌对节点的前提下, 根据自身状态和邻居的时延状态信息设计控制算法. 具体步骤如下:

步骤 1　对节点v_i, $i\in\mathcal{I}_{\rm s}$, 将k时刻收获的邻居时延信息进行整理后, 按数值的大小作降序排列. 记$n_i(k)$为k时刻v_i的邻居个数, $r_i(k)$为协议自适应参数, 其自适应律如下:

$$r_i(k)=\begin{cases}n_i(k)-f-1, & n_i(k)<2f+1,\\ f, & n_i(k)\geqslant 2f+1.\end{cases}\quad(3)$$

步骤 2　此时, 如果v_i整理的序列中有不少于$r_i(k)$个值严格大于自身状态值$x_i(k)$, 那么将序列中前$r_i(k)$个值移除, 如不足$r_i(k)$ 个, 则全部移除这些大于$x_i(k)$的值; 同样, 如果序列中有不少于$r_i(k)$个值严格小于自身状态值$x_i(k)$, 那么将序列中后$r_i(k)$个值移除, 如不足$r_i(k)$个, 则全部移除这些小于$x_i(k)$的值.

步骤 3　记$\mathcal{R}_i(k)$表示步骤2中被移除节点的序号集, 给节点v_i设计如下一致性协议:

$$u_i(k)=\sum_{j\in\mathcal{N}_i(k)\backslash\mathcal{R}_i(k)}a_{i,j}(x_i^j(k-d_{i,j}(k))-x_i(k)),\quad(4)$$

其中: $d_{i,j}(k)$表示节点v_j到节点v_i的通信时延, 满足$d_{i,j}(k)\in\{0,1,\cdots,\bar{d}\}$. 常数$\bar{d}\in\mathbb{Z}^+$为时延上界, 即$\bar{d}=\sup\limits_{k\geqslant 0}\max\{d_{i,j}(k),j\in\mathcal{N}_i,i\in\mathcal{I}_{\rm s}\}$. 假设节点$v_i$获取自身的状态信息时没有时延, 即$d_{i,i}(k)=0$. 权值$a_{i,j}\geqslant 0$, 且$\sum\limits_{j=0}^{n}a_{i,j}=1$.

注 1　本文相比文献[28], 在算法步骤2中, 引入自适应参数项$r_i(k)$, 目的在于当敌对节点在某轮突然停止或者改变攻击目标, 导致网络拓扑发生改变时, 该参数可适时调整步骤2中需移除信息的个数, 确保各正常节点在步骤3中仍能获取有效个数的信息来更新状态.

注 2　文献[19]在固定拓扑且不考虑时延的情况下提出类似的安全一致性算法, 该算法较本文算法需要依赖更高的网络连通度, 且同时要求敌对节点必须具有固定的攻击目标, 即一旦敌对节点放弃或者转移攻击目标, 其算法也将随之失效.

根据式(1)(4), 系统的闭环形式可表述为

$$\begin{aligned}&x_i(k+1)=\\&x_i(k)+\frac{1}{\sum\limits_{j=1}^{n}a_{i,j}\delta_{i,j}(k)}\times\\&(\sum_{j=1}^{n}a_{i,j}\delta_{i,j}(k)(x_i^j(k-d_{i,j}(k))-x_i(k))),\end{aligned}\quad(5)$$

其中: $\delta_{i,i}(k)\triangleq 1$, 满足当节点$v_i$在算法中采用节点$v_j$的信息时, $\delta_{i,j}(k)=1$, 否则$\delta_{i,j}(k)=0$, $\forall i\neq j$.

定义

$$M(k)=\max_{i\in\mathcal{I}_{\rm s},\ \theta=0,\cdots,\bar{d}} x_i(k-\theta),$$
$$m(k)=\min_{i\in\mathcal{I}_{\rm s},\ \theta=0,\cdots,\bar{d}} x_i(k-\theta),$$

分别为网络中正常节点k时刻状态(时延状态)的最大值和最小值. 显然$M(0)$和$m(0)$即为正常节点初始时刻的最大值和最小值.

定义 4 安全一致性. 对于多智能体系统(1), 当且仅当满足下列两个条件时, 即

$$m(0)\leqslant\inf_{k\geqslant 0}\min_{i\in\mathcal{I}_{\rm s}} x_i(k)\leqslant \sup_{k\geqslant 0}\max_{i\in\mathcal{I}_{\rm s}} x_i(k)\leqslant M(0), \tag{6a}$$

$$\lim_{k\to\infty}(x_i(k)-x_j(k))=0,\ \forall i,j\in\mathcal{I}_{\rm s}, \tag{6b}$$

称系统(1)能实现安全一致.

定义4中可以看出, 条件(6a)要求正常节点任意时刻的状态值处于安全域(初始状态区间)内, 即$x_i(k)\in[m(0),M(0)]$, 保证了安全性; 而条件(6b)保证了系统最终状态的一致性.

3 主要结果(Main results)

为方便阐述系统中节点的时延状态, 本文借鉴文献[29]的思想, 在此处引入虚拟节点的概念, 令$v_{i,j}$表示拥有节点v_i的j步时延状态信息的虚拟节点. 易知$v_{i,0}=v_i$. 令$\mathcal{V}_{(i)}=\{v_{i,0},\cdots,v_{i,\bar{d}}\}$表示所有拥有$v_i$时延状态信息的虚拟节点集.

定义 5 时延图[29]. 对于一个有向图$\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}}\}$, 令有向图$\bar{\mathcal{G}}$满足以下两个性质:

1) 节点集为$\bigcup\limits_{v_i\in\mathcal{V}}\mathcal{V}_{(i)}$;

2) 边集为$\{(v_{i,j-1},v_{i,j}),j=1,\cdots,\bar{d}\}\cup\{(v_{i,d_{j,i}},v_{j,0}):\forall(v_i,v_j)\in\mathcal{E}\}$.

则称$\bar{\mathcal{G}}$为$\mathcal{G}$相应的时延图.

在给出本文主要结论前, 介绍以下几个所要用到的引理.

引理 1[28] 令$\mathcal{G}$是满足r–健壮的有向图, $\mathcal{G}'$表示将$\mathcal{G}(r>s)$中各节点去掉s条输入边后的图, 则图$\mathcal{G}'$是$(r$–$s)$–健壮的.

引理 2[28] 令$\mathcal{G}$是有向图, 则$\mathcal{G}$包含一生成树, 当且仅当$\mathcal{G}$是1–健壮的.

引理 3[29] 对于多智能体系统(1), 在控制协议(4)下, 若系统的频繁联合图均包含一生成树, 则系统将根据初始状态值, 以指数速度收敛于一常数x^*, 即

$$\lim_{k\to\infty}x_i(k)=x^*.$$

接下来给出本文的主要结论.

定理 1 对于多智能体系统(1), 在控制协议(4)下, 假设系统攻击模型满足假设1, 且正常节点之间拓扑满足$(f+1)$–健壮图, 对于节点v_i, $i\in\mathcal{I}_{\rm s}$, 若k时刻接收到的信息$x_i^{\rm p}(k)\notin[m(k),M(k)]$, $p\in\mathcal{N}_i(k)$, 则有$p\in\mathcal{R}_i(k)$.

证 由$M(k)$和$m(k)$的定义可知, v_i接收的正常邻居的状态信息均位于区间$[m(k),M(k)]$. 记k时刻经算法步骤2, 移除相应数值后序列的第1个数的值为$M'(k)$. 此时$M'(k)$的值分两种情况得出:

1) 若原序列中有不少于$r_i(k)$个值严格大于$x_i(k)$, 此时序列前$r_i(k)$数将被移除. 根据正常邻居发送信息的区间和敌对邻居个数上限为$r_i(k)$可知, 原序列中能够大于$M(k)$的值的个数至多为$r_i(k)$个, 故上述移除前$r_i(k)$个值的操作, 保证了大于$M(k)$ 的值必定被移除. 此时$M'(k)$取原序列第$r_i(k)+1$个数的值, 易知, $M'(k)\leqslant M(k)$;

2) 若原序列中严格大于$x_i(k)$的值不足$r_i(k)$个, 此时v_i将移除所有比自身大的值, $M'(k)$取v_i的状态值, 即$M'(k)=x_i(k)$, 又由$x_i(k)\in[m(k),M(k)]$, 得出$M'(k)\leqslant M(k)$. 可见, 上述两种情况, $M'(k)$的取值均小于等于$M(k)$.

记k时刻经算法中步骤2, 移除相应数值后序列的最后一个数的值为$m'(k)$. 同样可用上述对$M'(k)$的分析方法, 得出$m'(k)\geqslant m(k)$.

由此推出v_i经算法后保留节点集的值域满足$[m'(k),M'(k)]\subseteq[m(k),M(k)]$; 再根据已知的条件$x_{\rm p}(k)\notin[m(k),M(k)]$, 可以推得$x_i^{\rm p}(k)\notin[m'(k),M'(k)]$, $v_{\rm p}$的信息被v_i移除, 即$p\in\mathcal{R}_i(k)$. 证毕.

定理 2 对于多智能体系统(1), 存在通信时延, 且一致有界的情况下, 系统攻击模型满足假设1, 则在控制协议(4)下, 系统能够实现安全一致的充要条件是, 网络中正常节点之间拓扑满足$(f+1)$–健壮图.

证 必要性. 用反证法证明. 若网络不是$(f+1)$–健壮的, 则可将网络节点划分为两个互不相交的子集, 记S_1, S_2, 使得任一子集中任一元素的邻居信息当中含有至多不超过f个值来自对方集合. 不妨假定先前系统已收敛至一致状态a. 此时令f个敌对节点的值为b, $b\neq a$, 对系统中任意正常节点v_i, $i\in\mathcal{I}_{\rm s}$发送该值, 而此时网络下本文算法最多只能去除$f-1$个b值, 留存的b值将被v_i用于状态更新, 从而打破先前的平衡状态, 使网络无法保持一致.

充分性. 充分性的证明分为两步: 第1步, 证明系统(1)满足安全性; 第2步, 证明系统(1)收敛于一平衡点, 即网络中所有正常节点状态达成一致. 若以上两步得证, 则定理充分性得证.

第1步 根据定理1及$M(k)$, $m(k)$的定义, 结合系统自身方程, 对于任意$i\in\mathcal{I}_{\rm s}$, 记

$$\alpha=\sum_{j\in\mathcal{N}_i(k)\backslash\mathcal{R}_i(k)}a_{i,j}(k)\leqslant 1,$$

则有

$$\begin{aligned}&x_i(k+1)\leqslant\\&x_i(k)+\sum_{j\in\mathcal{N}_i(k)\backslash\mathcal{R}_i(k)}a_{i,j}(k)(M(k)-x_i(k))=\\&\alpha M(k)+(1-\alpha)x_i(k)\leqslant\\&\alpha M(k)+(1-\alpha)M(k)=M(k),\end{aligned}\tag{7}$$

得出$M(k+1)\leqslant M(k)$. 采用上述同样的分析过程, 可得$m(k+1)\geqslant m(k)$. 以上结论保证了安全性条件(6a).

第2步　通过定理1可知, 当敌对节点$v_{\rm q}$, $q\in\mathcal{I}_{\rm a}$发送的信息位于$[m(k), M(k)]$内时, 该信息将可能与其他正常节点发送的信息一样, 被节点v_i所采用. 此时可通过状态分解思想, 将该时刻$v_{\rm q}$的信息用一所有正常节点状态的凸组合表示, 即

$$x_i^{\rm q}(k)=\sum_{j\in\mathcal{I}_{\rm s}}\beta_{i,j}(k)x_j(k),\ q\in\mathcal{I}_{\rm a}\cap(\mathcal{N}_i(k)\backslash\mathcal{R}_i(k)),$$

其中: $\beta_{i,j}(k)\geqslant 0$, 且$\sum\limits_{j\in\mathcal{I}_{\rm s}}\beta_{i,j}(k)=1$. 值得注意的是, $x_i^{\rm q}(k)$对于不同的v_i存在多组不同的表达式, 事实上可有任意多组, 此时可任意选取一组. 如果k时刻v_i获取的周围信息中不包含敌对节点信息时, 可令$\beta_{i,j}(k)=0$, $j\in\mathcal{I}_{\rm s}$.

引入上述时延图定义5, 可将式(5)表述成如下矩阵形式:

$$\bar{X}(k+1)=\Theta(k)\bar{X}(k),$$

其中:

$$\bar{X}(k)=\begin{bmatrix}X(k)\\X(k-1)\\\vdots\\X(k-\bar{d})\end{bmatrix},\ X(k)=\begin{bmatrix}x_1(k)\\x_2(k)\\\vdots\\x_{n_{\rm s}}(k)\end{bmatrix},$$

$$\Theta(k)=\Theta_1(k)+\Theta_2(k),$$

$$\Theta_1(k)=\begin{bmatrix}A_0&A_1&\cdots&A_{\bar{d}}\\I&&&\\&\ddots&&\\&&I&\end{bmatrix},\ \Theta_2(k)=\begin{bmatrix}B&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{bmatrix},$$

$$B^{i,j}(k)=\beta_{i,j}(k),$$

$$A_0^{j,q}(k)=\begin{cases}1-\sum\limits_{q\in\mathcal{N}_j(k)\backslash\mathcal{R}_j(k)}a_{j,q}(k), & j=q,\\a_{j,q}(k)\delta_{0,d_{j,q}}, & j\neq q,\end{cases}$$

$$A_i^{j,q}(k)=a_{j,q}(k)\delta_{i,d_{j,q}},\ i=1,\cdots,p.$$

根据定义3, 容易验证, 矩阵Θ, Θ_1, Θ_2分别是对应时延图的有效邻接矩阵. 用$\tilde{\mathcal{G}}$表示$\mathcal{G}$通过协议(4)消减去相应边数后的时延图, 对应的邻接矩阵为$\sum\limits_{i=1,\cdots,\bar{d}}A_i(k)$. 通过引理1和引理2可知, $\tilde{\mathcal{G}}$满足1–健壮, 即相应拓扑中包含一生成树. 另一方面, 根据文献[30], 与Θ_1对应的时延图, 记$\mathcal{G}_1$, 可知$\mathcal{G}_1$包含一生成树若$\tilde{\mathcal{G}}$包含一生成树. 与此同时, Θ对应的时延图, 记$\mathcal{G}_0$, $\mathcal{G}_0$在$\mathcal{G}_1$的拓扑基础上, 包含更多的有向边, 从而保证$\mathcal{G}_0$同样包含一生成树, 最后通过引理3可知, 系统能够收敛到一平衡点.　　证毕.

推论 1　考虑一阶多智能体系统(1), 攻击模型满足假设1, 在协议(4)下更新状态, 若网络中正常节点之间拓扑满足$(f+1)$–健壮, 则该系统的一致平衡点是正常节点初始状态构成的凸组合.

4　数值仿真(Numerical simulation)

考虑一个由7个节点组成的多智能体系统, 通信拓扑如图1所示.

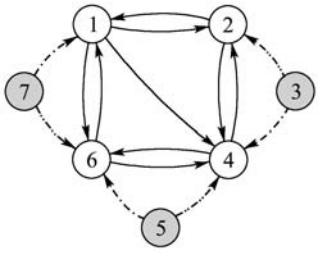

图 1　7个节点组成的有向图

Fig. 1　Directed graph with 7 agents

图中节点v_1, v_2, v_4, v_6为正常节点, 节点v_3, v_5, v_7为敌对节点, 图中单点划线箭头表示在时间序列k为奇数时连通信道, 双点划线箭头表示k为偶数时连通信道, 实线箭头表示恒定连通信道, 其初始值$x(0)=[1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7]^{\rm T}$, 通信步长设为0.1 s, 时延上界取0.5 s. 系统的安全域即为正常节点的初始值范围$[1,\ 6]$, 在时间序列为奇数和偶数时加权图的邻接矩阵分别为

$$A'_{\mathcal{G}}=\begin{bmatrix}0&0.2&0&0&0&0.3&0.3\\0.3&0&0&0.2&0&0&0\\0&0&0&0&0&0&0\\0.2&0.2&0.1&0&0.3&0&0\\0&0&0&0&0&0&0\\0.1&0&0&0.2&0.2&0&0\\0&0&0&0&0&0&0\end{bmatrix},$$

$$A''_{\mathcal{G}}=\begin{bmatrix}0&0.2&0&0&0&0.3&0\\0.3&0&0.3&0.2&0&0&0\\0&0&0&0&0&0&0\\0.2&0.2&0&0&0.3&0.1&0\\0&0&0&0&0&0&0\\0.1&0&0&0.2&0&0&0.3\\0&0&0&0&0&0&0\end{bmatrix}.$$

根据定义3, 容易验证图中正常节点v_1, v_2, v_4, v_6间拓扑满足2–健壮图. 简便起见, 假设敌对节点v_3, v_5, v_7的动态方程分别为

$$x_3(k+1)=0.8x_3(k)+0.2u_{\rm a}(k),$$

$$x_5(k+1)=1.5\sin(0.2\pi k)+4,$$
$$x_7(k+1)=0.3x_7(k)+0.7u_{\rm a}(k).$$

令$u_{\rm a}(k)=8$. 上述对通信拓扑的假定保证了各正常节点在任一时刻的敌对邻居数上限为1. 根据定理2可知, 该网络在上述条件下能够实现安全一致.

系统的状态轨迹如图2所示, 尽管遭受3个敌对节点的攻击, 各正常节点在控制协议(4)作用下, 其状态值始终保持在安全域内变化, 且最终达成一致.

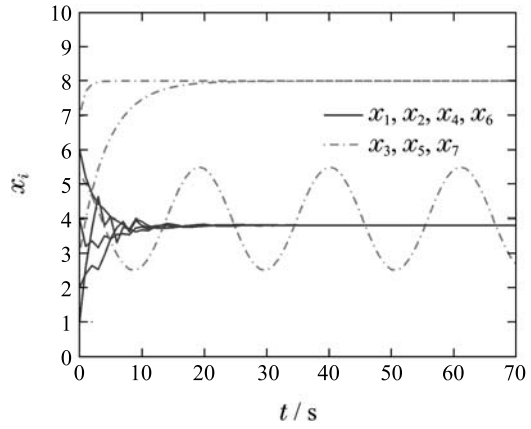

图 2 2–健壮图下各节点的状态轨迹

Fig. 2 State trajectories of the agents under digraph satisfying 2–robust

考虑图1中移除节点v_1到节点v_2的输入边, 使得正常节点间的拓扑图不再满足2–健壮. 该情况下各节点状态轨迹如图3所示, 此时敌对节点成功将所有正常节点的状态值引领至8. 虽然系统最终仍可以达到一致平衡状态, 却已偏离出安全域$[1,6]$, 本文的安全协议不再适用.

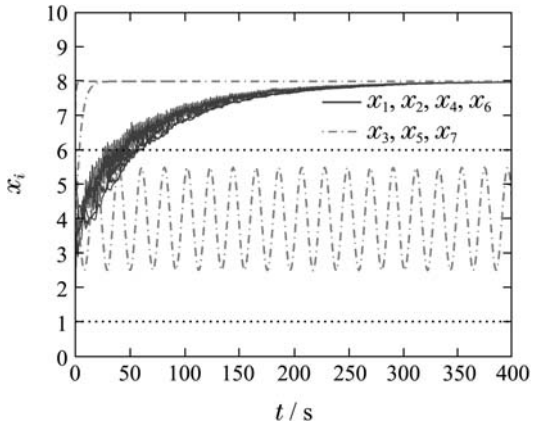

图 3 非2–健壮图下各节点状态轨迹

Fig. 3 State trajectories of the agents under digraph not satisfying 2–robust

此外, 考虑图1中所有敌对节点放弃攻击的情况, 即此刻将与敌对节点相连接的边全部移除. 此时, 文献[19, 28] 提出的算法由于此时拓扑的连通性条件无法满足其算法执行的需求, 故不再适用. 而本文提出的自适应控制算法仍能很好的解决该拓扑条件下的一致性问题, 各正常节点的轨迹如图4所示.

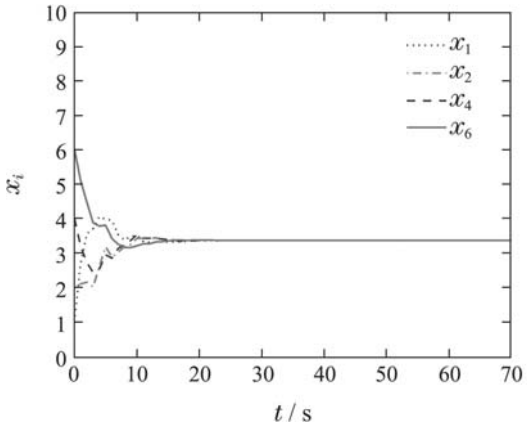

图 4 放弃攻击情况下各正常节点状态轨迹

Fig. 4 State trajectories of the safe agents under no attacks

5 结论(Conclusions)

本文针对具有通信时延的多智能体系统的安全一致性问题进行了研究, 提出了一种具有自适应能力的安全一致性算法, 并基于r–健壮图概念, 得到了系统拓扑结构为动态有向加权图且邻居中含有f个敌对节点上限的条件下, 实现安全一致的充要条件. 最后通过仿真实例验证了所设计控制算法的正确性.

参考文献(References):

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

[2] REN W, BEARD R W. Consensus seeking in multiagent systems under dynamically changing interaction topologies [J]. *IEEE Transactions on Automatic Control*, 2005, 50(5): 655 – 661.

[3] HUANG M, MANTON, J H. Coordination and consensus of networked agents with noisy measurements: stochastic algorithms and asymptotic behavior [J]. *SIAM Journal on Control and Optimization*, 2009, 48(1): 134 – 161.

[4] CHENG L, HOU Z G, TAN M. A mean square consensus protocol for linear multi-agent systems with communication noises and fixed topologies [J]. *IEEE Transactions on Automatic Control*, 2014, 59(1): 261 – 267.

[5] LI T, ZHANG J F. Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises [J]. *IEEE Transactions on Automatic Control*, 2010, 55(9): 2043 – 2057.

[6] LI Z K, LIU X D, REN W, et al. Distributed tracking control for linear multiagent systems with a leader of bounded unknown input [J]. *IEEE Transactions on Automatic Control*, 2013, 58(2): 518 – 523.

[7] DONG X W, XI J X, SHI Z Y, et al. Practical consensus for high-order linear time-invariant swarm systems with interaction uncertainties, time-varying delays and external disturbances [J]. *International Journal of Systems Science*, 2013, 44(10): 1843 – 1856.

[8] JADBABAIE A, LIN J, MORSE A S. Coordination of groups of mobile autonomous agents using nearest neighbor rules [J]. *IEEE Transactions on Automatic Control*, 2003, 48(6): 988 – 1001.

[9] FAX J A, MURRAY R M. Information flow and cooperative control of vehicle formations [J]. *IEEE Transactions on Automatic Control*, 2004, 49(9): 1465 – 1476.

[10] XIAO L, BOYD S, LALL S. A scheme for robust distributed sensor fusion based on average consensus [C] //*Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*. Los Angeles, California, USA: IEEE, 2005, 4: 63 – 70.

[11] YOU K Y, LI Z K, XIE L H. Consensus condition for linear multi-agent systems over randomly switching topologies [J]. *Automatica*, 2013, 49(10): 3125 – 3132.

[12] DONG X W, YU B C, SHI Z Y, et al. Time-varying formation control for unmanned aerial vehicles: Theories and applications [J]. *IEEE Transactions on Control Systems Technology*, 2015, 23(1): 340 – 348.

[13] ZENG W T, CHOW M Y, NING P. Secure distributed control in unreliable D–NCS [C] //*Proceedings of the 21st International Symposium on Industrial Electronics*. Hangzhou, China: IEEE, 2012, 5: 1858 – 1863.

[14] AGMON N, PELEG D. Fault-tolerant gathering algorithms for autonomous mobile robots [J]. *SIAM Journal on Computing*, 2006, 36(1): 56 – 82.

[15] HE J P, CHENG P, SHI L, et al. Sats: Secure average-consensus-based time synchronization in wireless sensor networks [J]. *IEEE Transactions on Signal Processing*, 2013, 61(24): 6387 – 6400.

[16] MENG D Y, MOORE K L. Studies on resilient control through multiagent consensus networks subject to disturbances [J]. *IEEE Transactions on Cybernetics*, 2014, 44(11): 2050 – 2064.

[17] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem [J]. *ACM Transactions on Programming Languages and Systems*, 1982, 4(3): 382 – 401.

[18] PASQUALETTI F, BICCHI A, BULLO F. On the security of linear consensus networks [C] //*Proceedings of the 48th IEEE Conference on Decision and Control*. Shanghai, China: IEEE, 2009, 12: 4894 – 4901.

[19] LEBLANC H J, ZHANG H T, KOUTSOUKOS X, et al. Resilient asymptotic consensus in robust networks [J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(4): 766 – 781.

[20] DIBAJI S M, ISHII H. Resilient consensus of double-integrator multi-agent systems [C] //*Proceedings of the 2014 American Control Conference*. Portland, Oregon, USA: IEEE, 2014, 6: 5139 – 5144.

[21] ZHAO C C, HE J P, CHENG P, et al. Secure consensus against message manipulation attacks in synchronous networks [C] //*Proceedings of the 19th IFAC World Congress*. Cape Town, South Africa: IFAC, 2014, 8: 1182 – 1187.

[22] ABBAS W, VOROBEYCHIK Y, KOUTSOUKOS X. Resilient consensus protocol in the presence of trusted nodes [C] //*Proceedings of the 7th International Symposium on Resilient Control Systems*. Denver, Colorado, USA: IEEE, 2014, 8: 1 – 7.

[23] SUNDARAM S, HADJICOSTIS C N. Distributed function calculation via linear iterative strategies in the presence of malicious agents [J]. *IEEE Transactions on Automatic Control*, 2011, 56(7): 1495 – 1508.

[24] PASQUALETTI F, BICCHI A, BULLO F. Consensus computation in unreliable networks: a system theoretic approach [J]. *IEEE Transactions on Automatic Control*, 2012, 57(1): 90 – 104.

[25] VAIDYA N H, TSENG L, LIANG G. Iterative approximate Byzantine consensus in arbitrary directed graphs [C] //*Proceedings of the 2012 ACM Symposium on Principles of Distributed Computing*. Madeira, Portugal: ACM, 2012, 7: 365 – 374.

[26] SONG H, ZHU S, CAO G. Attack-resilient time synchronization for wireless sensor networks [J]. *Ad Hoc Networks*, 2007, 5(1): 112 – 125.

[27] KIM E J, IN J, YOUM S, et al. Delay attack-resilient clock synchronization for wireless sensor networks [J]. *IEICE Transactions on Information and Systems*, 2012, 95(1): 188 – 191.

[28] WU Y M, HE X X, LIU S, et al. Consensus of discrete-time multi-agent systems with adversaries and time delays [J]. *International Journal of General Systems*, 2014, 43(3/4): 402 – 411.

[29] CAO M, MORSE A S, ANDERSON B D. Reaching a consensus in a dynamically changing environment: Convergence rates, measurement delays, and asynchronous events [J]. *SIAM Journal on Control and Optimization*, 2008, 47(2): 601 – 623.

[30] XIAO F, WANG L. State consensus for multi-agent systems with switching topologies and time-varying delays [J]. *International Journal of Control*, 2006, 79(10): 1277 – 1284.

作者简介:

伍益明　(1987–), 男, 博士研究生, 主要研究方向为多智能体系统、安全网络控制, E-mail: yimgwu@126.com;

丁佳骏　(1990–), 男, 博士研究生, 主要研究方向为多智能体系统、最优控制与优化, E-mail: djiajun@126.com;

何熊熊　(1965–), 男, 教授, 博士生导师, 主要研究方向为学习控制、多智能体系统、信号处理等, E-mail: hxx@zjut.edu.cn;

欧县华　(1990–), 男, 博士研究生, 主要研究方向为空气温湿度控制, E-mail: oxhzjut@163.com.