浙江工业大学

博士学位论文

论文题目：恶意攻击下的多智能体系统安全一致性问题研究

作者姓名 伍益明

指导教师 何熊熊 教授

学科专业 控制科学与工程

所在学院 信息工程学院

提交日期 2016 年 5 月 10 日

浙江工业大学博士学位论文

恶意攻击下的多智能体系统安全一致性问题研究

作者姓名: 伍益明

指导教师: 何熊熊 教授

浙江工业大学信息工程学院

2016 年 5 月

Dissertation Submitted to Zhejiang University of Technology
for the Degree of Doctor of Philosophy

Research on Secure Consensus for Multi-Agent Systems under Malicious Attacks

Candidate: Wu Yiming

Advisor: Prof. He Xiongxiong

College of Information Engineering
Zhejiang University of Technology
May, 2016

浙江工业大学

学位论文原创性声明

本人郑重声明：所提交的学位论文是本人在导师的指导下，独立进行研究工作所取得的研究成果。除文中已经加以标注引用的内容外，本论文不包含其他个人或集体已经发表或撰写过的研究成果，也不含为获得浙江工业大学或其它教育机构的学位证书而使用过的材料。对本文的研究作出重要贡献的个人和集体，均已在文中以明确方式标明。本人承担本声明的法律责任。

作者签名：　　日期：　　年　　月　　日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权浙江工业大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于

1、保密 □，在____ 年解密后适用本授权书。

2、不保密 □。

(请在以上相应方框内打”√”)

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

恶意攻击下的多智能体系统安全一致性问题研究

摘　要

近些年来，随着无线传感器网络、智能交通、机器人协作控制、无人机编队飞行等诸多技术在工程领域的广泛应用，使得人们的生活和工作方式得到了极大的改善。多智能体系统协同控制技术作为这些应用的关键技术之一，越来越受到国内外众多专家学者的关注并对其进行了大量的科学研究。

一致性控制作为多智能体系统协同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，其目标是通过系统中个体邻居间的信息交互，使得所有个体的状态值渐进地或者有限时间内趋于相同。由于实际的多智能体系统所处在一个复杂的网络环境中，智能体难免会遭遇一些外来的恶意攻击。安全性问题作为一致性控制一个新的研究领域逐渐被更多的研究者所重视。

本文在总结前人工作的基础上，运用控制理论、稳定性理论、矩阵分析和图论等工具，对多智能体系统一致性控制的安全性问题进行了系统、深入的研究。

本文的主要研究成果概括如下：

1. 概述了多智能体系统安全一致性控制问题，分析了目前研究中存在的一些不足。

2. 研究了通信时延条件下离散时间多智能体系统安全一致性问题。针对网络中存在的持有相反目的的正常节点和恶意节点两类节点，给出了一种新颖的描述节点间通信拓扑关系的框架：拓扑稳健性。然后，根据拓扑稳健性以及恶意节点的攻击部署特点，提出一种分布式自适应安全一致性控制算法。所提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。

3. 研究了恶意攻击与通信时延下连续时间非线性多智能体系统安全一致性问题。考虑一个由 n 个节点组成的有向多智能体系统网络，其中包含 n_s 个正常节点和 $n_a = n - n_s$ 个恶意节点。根据邻居间交互的时延信息，提出了一种同时具有抗攻击和时延能力的一致性算法。通过构造 Lyapunov-Krasovskii 函数以及运用 Barbalat-like 引理，给出了所提算法的收敛性分析。

4. 研究了在恶意攻击下多智能体系统有限时间一致性问题。根据邻居中最大恶意节点个数上限，以及相应的有向网络拓扑稳健性，设计了一种有效的节点信息删减法则。然后，结合迭代学习控制方法，提出一种有限时间安全一致性协议。理论结果表明：引入恰当的学习增益值和合理的通信链路权重，以及满足特定的网络连通度，那么就能确保正常节点在每一轮的迭代操作中，其状态值始终处于一个安全的容许范围内发生变化，并能够实现在有限时间内收敛。

5. 研究了在量化通信下多智能体系统的安全一致性问题。通过引入量化器，将网络中实时连续的状态信息转化成量化信息，降低系统的通信开销。然后结合一种邻居间节点的安全策略，设计给出了一种基于邻居量化信息的安全一致性算法。并且针对 f-局部有限恶意攻击模型的特点，给出了系统中所有正常智能体实现状态一致的充分性条件。

关键词：多智能体系统，一致性，安全性，时延系统，非线性系统，有限时间一致，迭代学习控制，量化一致性，离散时间系统，连续时间系统

RESEARCH ON SECURE CONSENSUS FOR MULTI-AGENT SYSTEMS UNDER MALICIOUS ATTACKS

ABSTRACT

In recent years, multi-agent systems have been widely applied in a large range of engineering fields such as wireless sensor networks (WSNs), intelligent transportation, robot cooperative control, unmanned aerial vehicles (UAVs) formation flight, etc. Multi-agent systems are penetrating into our daily lives, changing the way we work and live. The distributed coordinated control of multi-agent systems, as one of the key technologies of these applications, has attracted widespread concerns and has became one of the hottest research topics.

Consensus is a representative problem in the distributed coordinated control of multi-agent systems, and is also the basis of many other decentralized control and estimation problems, whose goal is to make the states of all agents asymptotically achieve an agreement as time goes to infinity according to exchange the local information with their neighboring agents. Note that in complex network environments, multi-agent systems may easily suffer from some malicious attacks. Therefore, as one of new research fields in multi-agent systems, the security issues of consensus problems has aroused many researchers' strong interest.

Based on the study of previous works, this dissertation systematically and deeply investigates the security issues of consensus control for multi-agent systems under malicious attacks, by applying control theory, stability theory, matrix theory as well as graph algebra theory.

The main contents of this dissertation are summarized as follows：

1. An overview of existing literature on secure consensus problem of multi-agent systems is provided, and some deficiencies of this research field have been analyzed.

2. The secure consensus problem for discrete-time multi-agent systems under communication delays is investigated. For both normal and malicious agents in the network, a novel graph-theoretic property referred to as topology robustness is introduced. Then, based on the topology robustness and malicious attack model, a distributed adaptive secure consensus protocol is given. 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 secure consensus protocol.

3. The secure consensus problem for nonlinear continuous-time multi-agent systems suffering from attacks and communication delays is investigated. Consider a directed multi-agent network composed of n agents with n_s normal agents and $n_a = n - n_s$ malicious agents. A novel delay robust secure consensus algorithm according to the neighboring nodes' delayed information is designed. Convergence analysis of the system under the protocol designed is provided by using Lyapunov-Krasovskii stability theory and Barbalat-like argument approach.

4. The finite-time secure consensus problem for multi-agent systems under attacks is investigated. Based on the maximum number of malicious agents in each normal agent's neighborhood and topology robustness, an effective method for choosing neighboring agent's information is designed. Then, by combining the iterative learning control approaches, a finite-time secure consensus protocol is proposed. The theorem result shows that the proposed protocol can guarantee all normal agents to resist the malicious attacks and achieve the finite-time consensus if the network topology has sufficient connectivity in terms of robustness.

5. The secure consensus problem for multi-agent systems with quantized communication is investigated. A novel quantized-data based secure control law with built-in security mechanism is proposed to achieve consensus in the presence of attack agents. Sufficient conditions for secure consensus protocol under f-locally bounded attack model have been provided.

Key Words: Multi-agent systems, consensus, security, time-delay systems, nonlinear systems, finite-time consensus, iterative learning control, quantized consensus, discrete-

time systems, continuous-time systems

目 录

主要符号对照表

$\mathbb{R}$	实数集
$\mathbb{R}^n$	n 维实 Euclidean 空间
$\mathbb{R}^{n\times m}$	n 行 m 列实矩阵集合
$\mathbb{Z}$	整数集
$\mathbb{Z}^+$	正整数集
$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G}\}$	图
$\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G},\mathcal{A}_\mathcal{G}\}$	加权图
$\mathcal{V},\ \mathcal{E}_\mathcal{G}$	顶点集, 边集
$\mathcal{N}$	邻居集
$\mathcal{A}_\mathcal{G}$	图对应的邻接矩阵
$\mathcal{D}$	图对应的度矩阵
$L_\mathcal{G}$	图对应的 Laplacian 矩阵
$\deg_{in}(\cdot),\deg_{out}(\cdot)$	入度, 出度
$\mathrm{diag}\{d_1,\cdots,d_n\}$	以 $d_j(j=1,2,\cdots,n)$ 为对角元素的对角矩阵
I	适当维数的单位矩阵
X^{T}	矩阵 X 的转置
X^{-1}	方阵 X 的逆
$\inf,\sup$	下确界, 上确界
M	正不变集
D^+V	函数 V 的 Dini 右上导数
$\|\cdot\|$	向量或矩阵范数
$\triangleq$	定义为
$\min(\cdot),\max(\cdot)$	最小值函数, 最大值函数
$\mathrm{sgn}(\cdot)$	符号函数

插图

第一章 绪 论

1.1 问题背景及研究意义

在自然界中，人们时常会发现一些非常有意思的动物群体行为，比如天空中飞过的整齐划一的迁徙的候鸟，夜间闪烁着同步频率光芒的萤火虫，又或者是沿着固定路线来回觅食的蚁群等。在这些动物界的例子中，单个个体往往只拥有有限的信息量，只能感知到周围邻居个体在做的事，并据此来规划自己的行为。尽管它们只拥有有限的感知能力，却能通过彼此间的协调合作，能够顺利完成一些十分复杂的任务。比如一个大到可以数以万计的蚁群，单独一只蚂蚁的能力是十分薄弱的，却能够通过彼此间合理的协调、分工与合作让整个蚁群完成筑巢、觅食、抵御外来侵略者等一系列原先单个个体无法完成的任务。正是受上述这些动物群体行为的启发，研究者们提出了多智能体系统（multi-agent systems）[1]的概念。

然而，似乎至今都没有人能够确切地解释“智能体”（agent）一词究竟首次是何时以及如何被引入到科学研究领域的。同时由于不同研究领域的专家学者们对智能体赋予的含义并不完全一致，因此至今我们都无法对多智能体系统给出一个明确统一的定义。而中科院的洪奕光研究员则给出了一种简单而贴切的解释：所谓多智能体系统，是指一群具备一定的感知、通信、计算和执行能力的智能体通过通信等方式关联而成的一个网络系统[1]。其中每个智能体可是指实体，例如一辆小车，一驾飞行器，一台机器人，一部手机，一个互联网路由等，也可以指虚拟的物体，例如一款计算机软件。它们兼具有结构简单、造价经济、功能可调、灵活可变等诸多优点。大量的事实已经证明，通过多智能体系统中许多个简单廉价的智能体彼此之间协调、配合工作，能够完成原先单个智能体无法胜任的复杂任务。

过去的十几年中，随着微型计算、网络通信以及传感技术的快速发展，多智能体系统分布式协同控制越来越受到控制领域专家学者的重视。分布式协同控制相较于集中式控制，在降低能耗，时延鲁棒性，容错性，可扩展性等方面，具有十分显著的优势。目前多智能体系统分布式协同控制技术已广泛应用于智能电网[2–6]，太空探测[7–12]，自主作战系统[13–15]，空中交通管制[16–18]，无线传感器网络[19–23]，等等。

[1]另有学者在文献中称其为多自主体系统，多个体系统或群系统

一致性问题是多智能体系统协同控制研究最为广泛的问题之一，也是根本性问题。究其原因，是因为基于一致性的思想可以为其他一些多智能体的问题提供解决思路，因而在工程技术领域有着广阔的应用前景。其中一些代表性的应用领域包括：

- **群集和集结（flocking and rendezvous）**
  集结是一致性问题应用中一种很常见的形式，该问题等同于一系列智能体通过交互包含位置信息的数据，最终出现在同一空间位置点上。群集相较于集结，则具有更大的挑战性，它在考虑聚集问题的同时，还需要考虑智能体间避免碰撞的问题。此时一致性问题在群集中的核心作用是能够让智能体与邻居智能体实现速度匹配。

- **编队控制（formation control）**
  编队控制在实际工程应用中具有诸多的优点，它可以使系统获得更好的稳定性、鲁棒性以及经济性。例如，对于一群地球轨道卫星，合理的队形能够帮助卫星减少能量消耗，拓宽它们彼此的感知能力，减少对目标的访问时间等。又比如对于一个智能交通系统，如果汽车保持一个指定的速度并以车辆间恰当的距离形成一排，那么整个交通网络的吞吐量可以大幅度提高。

- **耦合振荡器同步（synchronization of coupled oscillators）**
  归因于同步振荡器在耦合神经振荡器中的涌现现象，耦合振荡器同步问题目前吸引了物理学、生物学、神经学、以及数学等领域的众多专家学者的关注[24–26]。

- **分布式传感器融合（distributed sensor fusion）**
  传感器网络中分布式传感器融合是一致性问题一个较为新颖的应用。根据一致性协议设计卡尔曼滤波器、近似卡尔曼滤波器、低通以及高通一致滤波器、线性最小二乘估计器等，以此来求解网络分布式平均一致问题。

可见，无论是理论研究还是工程实践，对一致性问题的研究探讨都有着十分重要的意义。通常为了实现一致，系统中各智能体要求与其邻居之间进行局部的状态信息交互，该状态信息可以是位置信息、速度信息、或者单个智能体自身检测到的其他信息等。由于实际的多智能体系统经常处在各种复杂的网络环境当中，难免会遭遇一些怀有恶意的入侵与攻击，同时实际环境中一些无法避免的干扰，如通信时延、丢包、噪声、物理信道不稳定等因素，都可能破坏多智能体系统一致性的执

行。因此有必要从分析的角度研究多智能体系统一致性的安全性问题。在本文中，我们着重从综合的层面来研究如何应对系统中遭遇恶意攻击、并同时存在通信时延、信道不稳定导致的非线性干扰以及随机拓扑变换等因素对系统一致性的影响。

图 1.1　参与阅兵式的战斗机编队飞行

图 1.2　应用协同控制技术的智能交通系统

1.2　国内外研究现状分析

近些年来，多智能体系统协同控制技术逐渐得到研究人员的关注。获益于分布式传感器、计算、通信以及微处理器技术的飞速发展，分布于不同区域的智能体彼

此之间相互传递信息的能力限制得到了极大的改善，多智能体系统的研究经历了一个爆炸式的发展阶段。

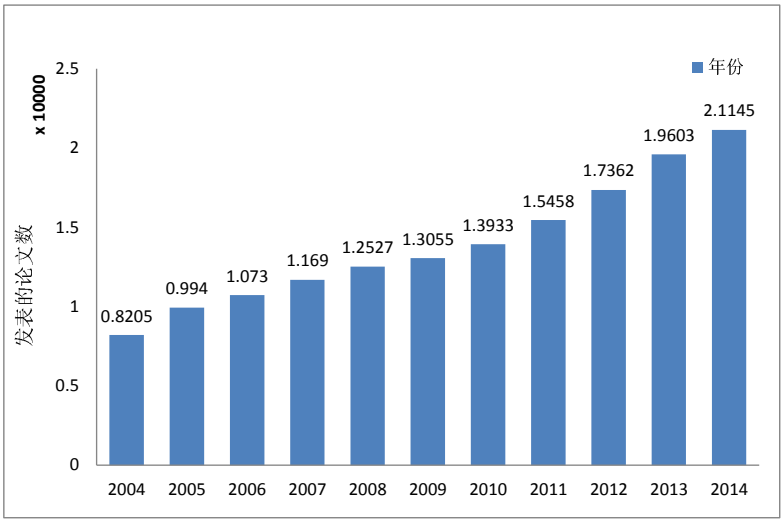


图 1.3　2004-2014 年 ScienceDirect 检索库包含主题词“multi-agent systems”的文章数

过去十年间，可以看作是多智能体系统研究发展的空前繁盛时期。我们仅从 ScienceDirect 的文献检索库中就可以看到，主题词为“multi-agent systems”的文献数量，从 2004 年的 8205 篇逐年增加至 2014 年的 21145 篇，并且这个数量仍在不断刷新。此外，国际、国内控制领域的知名期刊都刊载过大量关于多智能体系统的文章，国内期刊如自动化学报，控制理论与应用，控制与决策等，国际期刊如 IEEE Transactions on Automatic Control，Automatica，IET Systems & Control Letters，International Journal of Robust and Nonlinear Control 等。以上这些现象毫无疑问地表明了多智能体系统成为当今的研究热点。

1.2.1 多智能体系统一致性问题研究现状

一致性问题[2]作为多智能体系统分布式协调控制中的根本性问题，也是解决其他协调控制问题的基础，其研究具有十分重要的理论价值和现实意义。一致性控制属于分布式控制范畴，是指在没有中央协调控制或者全局通信的情况下，通过利用智能体相互之间的交互信息设计适当的控制协议（算法），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相同。

对一致性问题的研究最早可以追溯到 20 世纪 70 年代，由 DeGroot 在管理学与统计学领域首次提出了一致性问题[28]。在 DeGroot 提出的模型中，每个智能体将量

[2]另有学者在文献中称其为趋同问题

测获取的信息称作自身状态值。作者假定各智能体通过对上一轮收集的邻居信息取得加权平均值，并结合施以相应权重的上一轮自身状态，来更新获得本轮的状态。通过该模型研究发现，只要网络通信拓扑保持连通，所有个体的状态值最终会趋于一致。随后，控制理论与机器人学会的学者们展开了一系列的深入研究，先后涌现出大量类似的模型。这些研究的主要目标大体一致，即通过利用个体的局部交互信息设计分布式协议来实现全局目标。这其中包括由 Reynold 在 1987 年通过计算机仿真自然界中的鸟群、鱼群等行为之后提出的著名的 Boid 模型[29]。1995 年，另一个非常知名同时也被学术界大量引用的一个例子是最初出现在统计物理学文献中的 Vicsek 模型[30]。Vicsek 模型相较于 DeGroot 模型，最明显的不同是它的邻居对象不再固定，而是随着时间的变化而产生变化。尽管如此，它的仿真结果发现，在不考虑噪声的情况下，初始方向不同的粒子通过相互间信息交互最终会朝着同一方向前进。随后，2003 年，Jadbabaie 等人[31]给出了 Vicsek 模型中仿真现象的理论解释，运用图论与矩阵论方法，给出了此类型模型的收敛结果。之后的 2004 年，Olfati-Saber 和 Murray 在 Fax 和 Murray 研究工作的基础上，提出了研究多智能体系统一致性问题的基本理论框架，与此同时给出了最为一般的一致性协议。

自此以后，我们认为关于多智能体系统一致性问题的研究从探索研究阶段进入了日臻完善的阶段。这些年来，国内外众多的研究人员运用不同的数学工具和分析方法对一致性问题进行了丰富和扩展。在研究一致性问题上，研究人员陆续提出了许多有效的研究方法，主要可以归纳为以下最为常用的几类：随机矩阵法 [31–34, 64]，矩阵理论方法 [35–40]，Lyapunov 函数法 [41–45, 67, 153]，频域方法 [46–51, 63]，时延图法 [32, 52, 55–57, 61]。

在多智能体系统中，各智能体作为系统的核心组成部分，被分布在不同的地理位置当中，彼此间通过一个通信网络来交互信息。因此，在设计一个控制策略的时候，不仅需要考虑智能体个体的动态和协调方式，同时也需要考虑所依赖的通信网络条件。另外，一致性问题所研究的对象可以是一阶系统、二阶系统，甚至是高阶系统。一般地，对于一个由 n 个智能体组成的一阶连续多智能体系统，第 i 个个体的动态模型如下：

$$\dot{x}_i(t) = u_i(t), i \in \mathcal{V}$$

其中，x_i 为智能体 i 的状态值，u_i 为相应的控制协议。针对上述一阶线性系统，其

最基本的线性一致性协议如下：

$$u_i(t) = \sum_{j \in \mathcal{N}_i} a_{i,j}(x_j(t) - x_i(t)), i \in \mathcal{V}$$

其中 $\mathcal{N}_i$ 为智能体 i 的邻居智能体集合，$a_{i,j}$ 为智能体 j 到智能体 i 对应通信边的权值。从该协议中我们可以看到，每个智能体的控制输入 u_i 仅依赖于其自身和邻居智能体的状态值，具有这类特征的控制组 $U = \{u_1,\ u_2, ...,\ u_n\}$ 被称之为分布式协议。因此，一致性控制问题属于分布式控制问题的范畴。在控制协议 U 下，根据对系统最后所实现的共同状态值不同的目标需求，又可以将其分为弱一致性问题，强一致性问题，以及 χ-一致性问题。它们的具体的数学定义如下：

弱一致性：令 $\{x_i(t) \in \mathbb{R}, i = i,\ 2, ...,\ n\}$ 是系统中所有智能体状态的集合，如果系统满足：

$$\lim_{t \to \infty} |x_i(t) - x_j(t)| = 0,\ i, j = 1, 2, ..., n,$$

则称 $\{x_1,\ x_2, ...,\ x_n\}$ 为弱一致性。

强一致性：令 $\{x_i(t) \in \mathbb{R}, i = i,\ 2, ...,\ n\}$ 是系统中所有智能体状态的集合，如果存在 $x^* \in \mathbb{R}$，使得系统满足：

$$\lim_{t \to \infty} x_i(t) = x^*,\ i = 1, 2, ..., n,$$

则称 $\{x_1,\ x_2, ...,\ x_n\}$ 为强一致性。

χ-一致性： 令 $\chi : \mathbb{R}^n \to \mathbb{R}$ 是一个 n 元的函数，$\{x_i(t) \in \mathbb{R}, i = i,\ 2, ...,\ n\}$ 是系统中所有智能体状态的集合，如果对于任意 $x_i(0),\ i = 1, 2, ..., n$，都有

$$\lim_{t \to \infty} x_i(t) = \chi(x_1(0),\ x_2(0), ...,\ x_n(0)),\ i = 1, 2, ..., n,$$

则称 $\{x_1,\ x_2, ...,\ x_n\}$ 为 χ-一致性。

上述系统所对应的控制协议 U 分别被称为弱一致性协议，强一致性协议，以及 χ-一致性协议。通过它们各自的定义可知，对于弱一致性、强一致性和 χ-一致性这三类控制目标，后者总是前者的一个子集，在对控制目标设计的强度和难度上构成了递进的关系 [58]。

21 世纪以来，多智能体系统一致性问题得到了十分迅速的发展，研究成果层出

不穷，下面我们根据个体动力学、个体间通信网络、系统整体性能等特点，简单概述几个目前针对多智能体系统一致性问题的热点子课题。

1）带时延一致性问题

时延在多智能体系统实际应用中是普遍存在且不可避免的，如果疏于考虑就有可能导致系统振荡、发散甚至崩溃。为此，在设计多智能体系统一致性协议的时候，必须考虑时延对整个系统稳定性的影响。研究者们借助各种不同的分析方法，例如 Lyapunov 函数法[59]，时延图法[61]，最大值与最小值差值法[62] 和频域分析法[63, 163]等，对存在时延的多智能体系统进行了较为深入的研究。

Olfati-Saber 等[63]最先考虑了存在通信时延下的多智能体系统一致性问题，给出了针对无向固定的连通网络实现系统状态一致的最大时延上界。随后，文献 [49, 62, 68, 72] 对 Olfati-Saber 文章中得出的结论做了相应的扩展研究。对于离散系统，文献 [69] 研究表明：只要系统的通信网络拓扑固定，并且无向连通，那么通信时延对系统实现一致性没有影响。文献 [70] 则通过探索 Laplacian 矩阵的特点，将通信时延一致性问题转换为异步稳定性问题，并采用半离散化的方法，分析了异步系统的稳定性条件。对于连续系统，文献 [71] 提出一种基于截断预测反馈的控制律，实现了同时存在输入时延与通信时延下的系统状态一致。对于非线性系统在通信时延下的一致性问题，文献 [72] 根据压缩理论以及波形变量法，通过构造一个 Lyapunov-Krasovskii 函数，给出了实现系统渐近一致的充要条件，即对系统的拓扑要求为有向权值对称连通或者无向闭环连通。值得一提的是，Moreau 等[66]从另一方面研究发现，单纯增加更多的通信链路，并不一定能够加快时延系统的收敛速度，相反最终有可能会降低系统的收敛性能。此外，文献 [32, 60, 61] 采用时延图法分析研究了有向和无向网络拓扑结构下具有通信时延的离散系统实现渐进一致的条件。

2）切换拓扑一致性

受现实环境中诸多因素的影响，曝露在环境中多智能体系统无法避免随机通信失败、数据丢包、物理信道不稳定等情况，致使网络通信链路无法保证持续恒定的为之工作。于是，研究者们开始考虑切换拓扑结构下一致性问题，即系统的邻接矩阵由原先的固定转变为时变。

文献 [74] 最早对随机切换拓扑下一致性问题展开研究，作者假定系统中通信链路以某一概率值进行开启或闭合，运用随机稳定性理论，给出了系统实现渐进一致的充分条件。对于无向图，文献 [63] 指出只要切换拓扑联合连通，系统可实现一致。对于有向切换拓扑，文献 [64] 研究证明，只要出现联合生成树，且频率足够

大，那么系统可以实现一致。在文献 [75] 和 [76] 中，作者分别研究了无向网络多智能体系统在切换拓扑下基于系统状态增益反馈和基于观测器反馈的半全局动态一致性问题。文献 [77] 考虑了系统拓扑在界定范围内切换且存在通信时延的情况下分组一致性问题，通过引入双重树形态（double-tree-form）转换方法，将系统动态转换为一个降阶系统。文献 [79] 借助线性矩阵不等式（Linear Matrix Inequality，LMI）的方法，解决了在无向切换拓扑下，实现系统渐进平均一致问题。文献 [80] 研究了非线性系统在切换拓扑下的一致性问题，证明了在时间区间 $[t,+\infty]$ 中，系统的联合拓扑图满足特定的连通性条件，那么系统就能实现一致。文献 [73] 考虑了基于采样数据的一致性协议，通过调整控制器增益和采样周期，实现了系统在切换拓扑下状态一致。文献 [78] 对连续时间和离散时间的系统在随机切换拓扑下的一致性问题进行了研究，分别给出了在上述情况下实现一致的协议。此外，在文献 [32] 中，作者则考虑了切换拓扑下的异步一致性问题。

值得注意的是，对于切换拓扑，最终状态 x^* 是无法预测的，x^* 的值与初始状态和拓扑的切换规律有关。其他更进一步的有关切换拓扑下的一致性结果，可参见文献 [81–84]。

3）量化通信下一致性问题

在数字通信网络中，通信信道是有限的，某一智能体在某一时刻只能向该自己的邻居智能体发送有限位数的信息值。因此，系统与控制领域的研究人员开始对一致性协议在量化通信方面的研究引起了注意[86, 89–93]。

注意到，给系统引入量化器，等同于给系统引入了非线性特性，这样势必对原本一致性问题的探讨增加了更多的挑战性。在文献 [86, 132] 中，作者考虑在全连通网络下，引入整数量化器，提出一种简单的随机一致性协议，同时给出了实现系统状态一致的充分条件。文献 [85] 针对一阶多智能体系统，提出了一种量化一致性协议，证明了仅通过邻居间一个比特的信息交互就能使系统状态最终实现一致。文献 [88] 在研究连续时间一阶多智能体系统的平均一致性问题上，考虑将对数量化器引入到通信链路上，提出了分别基于连续时间和基于采样数据的两种控制协议。而文献 [87] 针对随机通信失联下的一致性问题，提出一种结合时变权值的随机量化器。对于时变切换拓扑，文献 [94] 考虑了均匀量化和随机量化对系统一致性的影响，给出了各自实现一致的充分条件。随后将上述结果应用于编队控制中[95]。此外，文献 [89] 则更加系统地研究了均匀量化对平均一致性的影响，比较分析了确定量化与概率量化，部分量化与全局量化各自的优缺点，并讨论了量化补偿的问题。

4）具有领导者的一致性问题

多智能体系统一致性控制中的另外一个问题是带有领导者的分布式跟踪控制问题，其控制目标是使得所有的跟随者智能体的状态渐近跟踪至领导者的状态。

文献 [99] 考虑了具有多个领导者网络的一致性跟踪控制问题，研究发现网络的通信拓扑结构决定了系统的可控性，并基于上述发现，作者勾勒出两种无法满足系统可控的拓扑属性。文献 [100, 101] 在假定领导者的控制输入为零和非零但能被网络中所有跟随者获取的前提下，分别考虑了有向网络中固定拓扑和切换拓扑情形下的跟踪控制问题。然而通常情况下领导者的控制信息可能是非零的且很难被所有跟随者获取。为此，文献 [102] 在领导者信息只能被部分跟随着获取的前提下设计了一个连续的分布式控制协议，结果证明了控制误差是有界的。而文献 [194] 考虑了在领导者状态不可测情况下的一致性跟踪问题。另外文献 [103, 104] 则在假设领导者控制输入未知且有界的前提下，设计了一个非连续控制器，证明了系统最终可以达到跟踪。文献 [193] 同时考虑了连续时间和离散时间线性多智能体系统，根据定向图中邻居间相对输出量测信息，提出一种基于降阶观测器一致性跟踪算法。此外，文献 [63, 180] 研究了在通信时延下的一致性跟踪问题。而文献 [119, 120] 研究了在切换拓扑下的一致性跟踪问题。

5）二阶和高阶的一致性问题

作为对一阶多智能体系统的补充扩展，一些学者开始对二阶和高阶系统的一致性问题展开了研究[154–158]。相较于一阶系统，二阶和高阶系统设计中需要考虑更多的参数，相应地对系统行为的分析也更为复杂。而作为实际应用，二阶和高阶一致性问题常常被应用于群集和聚集问题当中。

文献 [152] 分析研究了二阶系统下的一致性问题，发现网络中包含有向生成树只是二阶多智能体系统实现一致的必要而非充分条件。研究结果表明，不同于一阶系统，在二阶有向网络中，除了网络拓扑外，节点与邻居间相对速度的耦合强度也会对最终的收敛结果产生影响。文献 [110] 和 [111] 分别考虑了二阶和高阶非线性系统下一致性问题，均在假设非线性函数满足全局 Lipschitz 条件下，设计了输出反馈控制器。文献 [37] 在固定无向和有向网络下研究了二阶系统的收敛性能，提出两种分布式协调算法，其中第一种算法保证了小车最终速度为零，而第二种算法能够使得所有小车速度最终达成一个共同的常数值。与此同时，作者分别在采样周期、控制增益和通信拓扑上给出了实现上述两种算法收敛的充要条件。文献 [112, 113] 针对高阶线性时不变多智能体系统，利用状态反馈方法设计了系统一致性控制协议。此外，文献 [114] 研究了固定和切换拓扑情况下高阶多智能体系统的一致性问题，文献 [115, 116] 分别研究了带有切换拓扑和通信时延情况下高阶多智能体系统的一

致性算法。

6）有限时间一致性问题

有限时间一致性是指系统中的智能体状态在有限的时间内收敛并停留在一个相同的状态空间上。它是关心一致性算法收敛速度的问题。我们知道，收敛速度是衡量系统性能的一项重要指标之一。此外，有限时间收敛系统可以具备更好的抗干扰能力以及鲁棒性。因此，如何在有限时间内达到系统一致性越来越成为研究者人员的一个研究热点。

虽然有学者已经通过最大化系统 Laplacian 矩阵第二最小特征根的方法，证明可以加快一致性协议的收敛速度，但仍无法保证系统在有限时间内达成一致[98]。文献 [108] 通过应用有限时间稳定性理论，分别研究了双向交互和单向交互网络的有限时间一致性问题，其研究结果表明，只要网络拓扑联合连通，且保持连通的时间间隔足够大，那么系统就能够在有限时间内实现一致。文献 [109] 通过引入滑膜估计器，实现了智能体系统编队跟踪中的位置和速度在有限时间内达到一致。在文献 [53] 中，作者考虑了带有未知有界时变干扰的连续时间系统的有限时间一致性问题，提出一种基于局部交互作用的控制协议来实现有限时间一致性收敛问题。利用非光滑稳定性理论，文献 [138] 提出了一种基于非光滑梯度算法，实现系统在有限时间内达到一致。考虑到实际的系统，文献 [139] 使用有限时间控制技术研究了非完整移动机器人的跟踪一致性问题。此外，文献 [54, 96, 97] 研究了非线性系统下的有限时间一致性，文献 [105–107] 对二阶多智能体系统的有限时间一致性展开了研究。

除了上述所例举的几个典型研究子课题之外，仍还有许多其他关于一致性问题的子课题同样受到研究者的普遍关注，例如基于事件触发一致性[121–123]，带约束一致性[124, 125]、高速一致性[126, 127]、群一致性[77, 128, 129] 自适应一致性[130, 131] 等等，此处就不一一列举。

1.2.2 多智能体系统安全一致性问题研究现状

多智能体系统一致性问题经过十几年的研究，取得了一系列丰硕的研究成果，目前来说已步入成熟。然而，随着多智能体系统的在工业、军事以及商业领域的广泛普及，已融入到人们生活的方方面面，与之相关的安全性问题也越来越得到研究人员的重视。

尽管目前在计算机信息领域，我们已经取得了相当大一部分关于安全性问题的

研究文献，然而，相对于控制系统领域的安全性问题，这些文献中的研究思路与所提方法，并不尽然相同。

同样，现有的控制系统里面的鲁棒性和容错机制的目的是确保系统在遭受自身干扰和错误时具有一定的可恢复能力。但当攻击由外部侵入的时候，这些机制往往会失去效果。因此，对于一个安全控制系统来讲，单独的容错机制或鲁棒性设计是不能满足系统安全性要求的，额外还需要考虑系统在遭受恶意攻击下（外部源侵入攻击）仍然确保系统安全运转的能力。

一个没有安全机制的一致性网络，仅仅单个恶意节点的侵入，就可以对系统产生不可估量的破坏。例如对于这样的系统，只需单独一个恶意节点简单冒充领导者，就能够轻易将系统引入一个极端的状态（危险状态）。在实际应用中，如一个温控系统，又或是一个调速系统，极端的温度或者速度会超出系统的物理极限，就会对系统软硬件产生不可逆转的破坏，甚至造成重大的安全事故。同样，智能体不正确或不恰当的行为就有可能造成经济损失、数据丢失，更甚至对人体或者整个系统造成伤害。因此，对多智能体系统一致性的安全性问题的考虑是非常实际和必要的。例如，美国航空航天局（NASA）已率先采用多智能体系统来执行在外太空或者外星球上的任务，其中参与研发的科学家不仅需要考虑投入该系统执行任务的安全性，同时还需要考虑对自身机构的安全隐私性 [182]。

对于一个多智能体系统网络，在存有恶意节点攻击下，如果系统中所有的正常智能体在一个合理可容许的范围内更新自身状态值，且最终达到一个共同的状态，则称系统实现了安全一致。假定一个由正常智能体和恶意智能体两类智能体组成的系统，我们分别用集合 $\mathcal{N}$ 表示所有正常智能体的集合，用 $\mathcal{M}$ 表示所有恶意智能体的集合。通常意义上，安全一致性算法一般包括以下三方面的属性[117, 118, 144]：

- **一致性：** 随着时间的推移，系统中所有正常智能体的状态最终实现一致，即 $x_i(t) = x_j(t), \forall v_i, v_j \in \mathcal{N}$；
- **有效性：** 系统中所有正常智能体的状态变化至始至终局限于一个由初始状态决定的不变集内，即 $x_i(t) \in [a, b], \forall t \geq 0, v_i \in \mathcal{N}$，其中区间 $[a, b]$ 即所谓的安全区间；
- **限定性：** 系统中所有正常智能体在一个限定时间内完成任务。

从以上描述可以看出，安全一致性算法，在传统一致性算法的基础上提出了一些更高的控制要求，它规定被控智能体的状态只能在限定范围内发生变化，同时对

系统最终收敛的时间也给出了要求。

文献 [31] 针对多智能体系统提出了一种基于线性迭代方法的一致性协议。该协议实现了所有节点状态最终渐进一致。同时，作者证明了如果有单个节点停止状态更新，即自身状态维持一个常量，此时它将成为整个网络的领导者节点，在上述控制策略下，网络中所有其他节点的状态值最终会与该领导者节点的值趋于一致。而这一点同时也表明，攻击者仅需侵入单个节点，令其状态维持不变，就可顺利地操控整个网络最终一致状态值的走向。文献 [181] 同样对类似问题进行了探讨，指出不仅单个节点维持固定值就可以使得网络趋于该状态，对于一个可任意改变状态值的节点，同样可以操控整个网络最终的一致状态。上述工作都只考虑了将线性迭代方法简单应用于多智能体一致性网络，而未真正考虑如何解决各正常节点避免恶意节点攻击行为的应对机制。

在文献 [174]中，作者对线性迭代方法在多智能体系统恶意节点进行了一个全面的分析研究，给出了线性迭代方法能够有效获取保证节点信息可靠传播的最小界值，特别的，对于一个满足 $2f+1$ 连通度的网络，在以广播方式的通信前提下，该方法可保证使 f 个恶意节点无法对其系统内部任意初始值计算函数进行有效干预。面对同样的问题，采用类似研究方法的文献还有 [175, 176] 等。需要指出的是，上述研究方法有他们共同的局限之处，即一方面都需要依赖于网络最小连通度；另一方面，需要每个正常节点知晓整个网络的拓扑信息。这使得节点需要具有强劲的计算能力和较高能量储备来应付上述两方面的需求，而这在实际应用场景中，对一个规模庞大而资源有限的分布式控制系统来讲，突破上述局限，显得更为重要。

文献 [177] 较为深入地研究了在全局含有 f 个拜占庭（Bytanzine）恶意节点情形下的渐进一致性问题，作者致力于如何使系统中所有正常节点最终状态共同收敛于一个由初始状态组成的相对较小的凸包内。首先在一个全连通（图中节点两两互连）的网络中，每个正常节点先将接收到的邻居信息组成一个依次递减的序列，然后在该序列中首尾依次剔除掉 f 个最大和 f 个最小的值，再在剩余的值中精选出一个子集，并求取平均值，最后将该均值用作节点自身状态的更新。随后，以此为主要思想，该算法被不同领域的专家学者扩展成为一家族式系列算法，并统一将该系列算法命名为 MSR（Mean-Subsequence-Reduced）算法。尽管 MSR 算法随后得到了较为成熟的发展，但其仅适用全连通性质网络的条件过于苛刻，使得在对于较为一般连通性的网络研究上，缺少其施展的余地。

除了针对固定多智能体系统架构的安全问题，还有学者们对移动多智能体系统的安全性攻击展开了系统的研究。相对固定多智能体系统，对移动多智能体系统的

研究就显得更为复杂和具有挑战性。然而一旦拥有了解决移动多智能体系统安全性问题的方法，那么这些方法显然可以很容易地用于解决固定多智能体系统的安全问题 [186]。在文献 [187] 中，作者详细地将移动多智能体系统中常见的攻击方式分为：损毁、拒绝服务（DoS）、窃取、骚扰、事件促发攻击以及复合攻击等几类。而文献 [188] 通过分析移动多智能体系统在实际应用中引起安全性问题的因素，在传统绝对安全（absolute security）的概念之上，提出了足够安全（enough security）的概念。同时，作者探讨了如何评估移动多智能体系统安全性能的方法。

相对于上述同步网络，文献 [190] 对异步网络中含拜占庭攻击节点的一致性问题进行了研究，给出了实现一致的拓扑连通性条件，并同时证明了该条件同样适用于同步网络中。

以上只部分罗列了一些目前针对多智能体系统安全一致性问题展开的研究工作，若需要了解更加全面的关于多智能体系统安全性的内容，可参见综述性文献 [183–185, 191]。

总的来说，以上学者的研究工作，不仅为多智能体系统安全一致性控制的研究奠定了研究框架，也同时为安全一致性算法设计提供了方便有效的理论依据和仿真环境，具有一定的研究意义和参考价值。但是同时仍有许多还不够完善需要进一步研究的地方。

其中一个问题是，目前大多已有的工作基本建立在一个理想的网络状况下，即单纯地研究正常节点和恶意节点间的博弈关系，分析和设计安全一致性协议。但忽略了实际环境中一些干扰，如通信噪声、时延、丢包、信道不稳定等因素。而这些因素往往会对设计的协议有决定性影响。

而另一个问题是，现有的大多数关于安全一致性算法，对通信网络拓扑连通度以及信息储备量依附较高的要求，往往需要节点获知全局的信息，或者记录大量历史的信息。而结合多智能体系统的本身特点，它以分布式协同控制技术为特长，具有灵活、简单、廉价等优点，但也注定了相较于复杂单一系统来说，每个单独的智能体具有的存储容量和计算能力是有限的，所以即使它能够接收到全局的信息，为实现系统全局目标，它的计算负担也会过于沉重。因此，针对恶意攻击环境下的多智能体系统，设计轻便有效，同时考虑一些实际环境中常见的干扰，如通信噪声、时延、信道不稳定、通信受限等的安全一致性协议，具有很好的理论价值和现实意义，这些问题值得进一步的研究。

1.3 本文的主要研究工作

如之前所述，多智能体系统的一致性问题近年来受到国内外众多专家学者的广泛关注，并取得了丰硕的研究成果。然而，对于一致性算法安全性问题的研究，才处于刚刚起步阶段，相关的研究文献也并不多见，尤其随着多智能体系统在工业、军事以及商业领域的应用普及，已逐渐融入到人们生活的方方面面，因此对于多智能体系统的安全性问题也越来越受到重视和值得考虑。

本文在前人工作的基础上，较为深入地探索和研究了多智能体系统在遭遇恶意攻击情形下的安全一致性问题。

本文的结构安排如下：

第 1 章概述了多智能体系统一致性控制及其安全性问题的研究背景，研究现状和研究意义，介绍了一致性问题的主要应用、领域的研究热点以及目前已取得的研究成果，并指出了当前研究存在的不足和本文的研究方向。最后，概括了全文的研究内容和篇章层次结构安排。

第 2 章介绍了一些本文中常会用到的数学记号，介绍了一些和本文内容相关的代数图论，矩阵理论，稳定性理论等知识以及一些相关的定理。为本文后续研究安全一致性问题提供了较为完整的理论基础。

第 3 章研究了存有通信时延的多智能体系统在遭遇恶意节点攻击下的一致性问题。考虑一个由正常节点和恶意节点组成的有向的多智能体系统网络，假定网络中每个正常节点不知道任何关于通信拓扑的信息，仅知道自己邻居（或全网）中至多含有的恶意节点数目上限。正常节点在进行状态更新的时候，会以暂时切断邻居信号输入边的方式，有选择地摒弃一部分邻居节点给予的信息，从而导致原本固定的网络拓扑条件转化成一个基于状态值的随机切换拓扑图。针对上述情况，给出了一种新颖的描述节点间通信拓扑关系的框架：拓扑稳健性。另外，对于系统中存在的通信时延，采用时延图方法，将节点前一时刻的时延状态转换成一个和自身相连接的虚拟邻居节点。然后根据拓扑稳健性和时延图特点，提出了一种分布式自适应一致性控制算法。所提算法仅利用个体的自身状态值和相邻个体的时延状态值作为控制输入，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。研究结果表明，在所提控制协议下，系统中各正常节点尽管遭到恶意节点的攻击，但其自身的状态值始终维持在一个容许的安全区域内变化，并通过邻居间的信息交互，最终实现状态一致。最后，通过仿真实例对理论结果进行了验证。

第 4 章研究了在非线性连续时间设定下多智能体系统遭遇恶意节点攻击下的安全一致性问题。考虑一个由 n 个节点组成的有向多智能体系统网络，其中包含 n_l 个正常节点和 $n_a = n - n_l$ 恶意节点。其中每个正常节点遵循预先设定的控制律来更新自身的状态值。而相反地，恶意节点则无视系统控制律，可随意变更自身的状态信息，甚至能与其他恶意节点相互勾结，向周围邻居发送虚假信息，以干扰、破坏系统的一致性进程为目的。针对上述网络中目的上存有博弈关系的这两类节点，给出了必要的拓扑稳健性要求，从而保证正常节点在操作信息删减的过程中，网络拓扑保持联合连通。接着，仅利用个体的自身状态值和相邻个体的时延状态值作为控制输入，提出了适用于非线性动态一阶连续系统的安全一致性协议。然后通过构造 Lyapunov-Krasovskii 函数和 Barbalat-like 分析方法，获得了所提控制协议下系统实现收敛的充分条件。最后，通过一个实例仿真，对本章所提算法的正确性和有效性进行了验证。

第 5 章研究了在恶意攻击下一阶离散时间多智能体系统有限时间一致性问题。首先，根据邻居中最大恶意节点个数上限，以及相应的有向网络拓扑稳健性，设计了一种有效的节点信息删减法则。然后，结合迭代学习控制方法，提出了一种有限时间安全一致性协议。研究结果表明，只要选取恰当的学习增益和合理的通信链路权重，以及满足特定的网络连通度，那么就能确保正常节点在每一轮的迭代操作中，其状态值始终处于一个安全的容许范围内发生变化，并能够实现在有限时间内收敛。最后通过实例仿真验证了所提方法的有效性。

第 6 章研究了在量化通信下的多智能体系统的安全一致性问题。考虑一阶连续多智能体系统中个体间交互信息是量化的。结合一种邻居间节点的安全策略，提计了基于邻居量化信息的安全一致性协议。并且针对 f-局部有限恶意攻击模型的特点，给出了系统中所有正常智能体实现状态一致的充分性条件。最后进行了算法的仿真验证。

第 7 章对全文的研究工作进行了总结，并指出若干有待进一步研究的问题。

第二章　预备知识

本章简要回顾了一些本文中需要用到的基本概念以及结论，主要包括代数图论，矩阵理论，以及泛函微分方程稳定性等方面的知识。

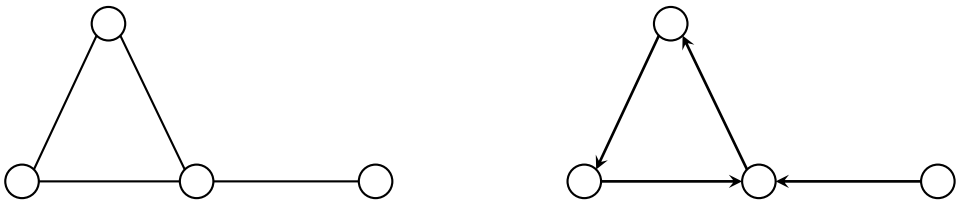
2.1　图论知识

在多智能体系统一致性问题的研究中，图论经常作为一种重要的分析工具而被用到，为此我们在这里提供一些代数图论的基本概念，详细的论述请参见文献[27, 151]。

通常，用记号 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}}\}$ 表示一个图，其中 $\mathcal{V}=\{v_1,v_2,\ldots,v_n\}$ 表示节点集（也称作顶点集），用有限非空集 $\mathcal{I}=\{1,2,\ldots,n\}$ 表示节点的序号集，$\mathcal{E}_{\mathcal{G}}=\mathcal{V}\times\mathcal{V}$ 表示边集。在图 $\mathcal{G}$ 中，一个节点代表一个智能体，每一条边代表一条通信链路。根据图中边的信息传递方向，可以将图分为无向图和有向图。我们可以根据节点之间信息传递的方向来区分有向图和无向图。在无向图中，边是没有方向指向的，也可以称是双向的，即这条边相连的两个节点之间可以相互传递信息。而与此相反，有向图中边的信息传递则是有方向指向的，一般通过一条带箭头的线表示，该边箭头指向的节点称为首节点，边的另一头的节点称为尾节点，信息只能够由尾节点传递给首节点，反之则不能。接下去的介绍主要针对有向图，无向图的相关结论可直接推广得到。我们用 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}},A_{\mathcal{G}}\}$ 表示一个需要考虑节点之间信道通信质量的有向图。其中节点集和边集与前面定义的一致。$A_{\mathcal{G}}=[a_{i,j}]\in\mathbb{R}^{n\times n}$ 表示图 $\mathcal{G}$ 的非负加权邻接矩阵。$A_{\mathcal{G}}$ 中元素 $a_{i,j}\geq 0$ 表示边的权重。当有向 $(v_j,v_i)\in\mathcal{E}_{\mathcal{G}}$ 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 $\mathcal{N}_i=\{j\in\mathcal{I}\,|(v_j,v_i)\in\mathcal{E}_{\mathcal{G}}\}$。一组有序边 $(v_i,v_{l_1}),(v_{l_1},v_{l_2}),\ldots,(v_{l_p},v_j)$ 组成的有向序列称为节点 v_i 到 v_j 的一条有向路径，其中 $v_i,\ v_j,\ v_{l_1},\ \ldots,\ v_{l_p}$ 为各不相同的节点。对于一个有向图，如果存在至少一个节点，可以沿着图中边的路径，抵达图中其他任何一个节点的位置，则称此图包含一棵生成树。

在有向图中，节点 v_i 的入度和出度分别定义为

$$\deg_{in}(v_i)=\sum_{j=1}^{n}a_{i,j},\quad \deg_{out}(v_i)=\sum_{j=1}^{n}a_{j,i},$$



(a) 无向图　　(b) 有向图

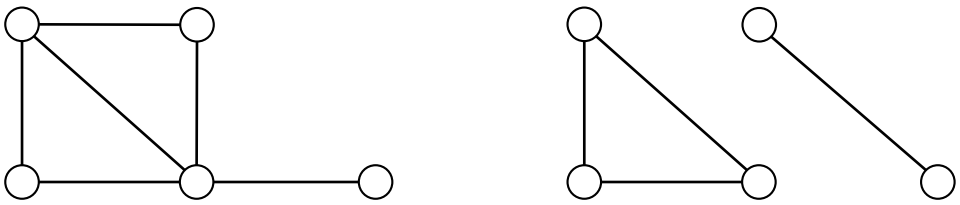
图 2.1　有向图和无向图示例

如果 v_i 的入度与出度相等，即

$$\deg_{in}(v_i) = \deg_{out}(v_i),$$

则称 v_i 为平衡节点。如果图中任意节点都为平衡节点时，此时称图为平衡图。显然地，无向图是平衡图。

对于图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}\}$，如果存在图 $\mathcal{G}' = \{\mathcal{V}', \mathcal{E}'_{\mathcal{G}}\}$，满足 $\mathcal{V}'$ 和 $\mathcal{E}'_{\mathcal{G}}$ 分别是 $\mathcal{V}$ 和 $\mathcal{E}_{\mathcal{G}}$ 的子集，那么称图 $\mathcal{G}'$ 为图 $\mathcal{G}$ 的子图。特别的，对于图 $\mathcal{G}'$，如果有 $\mathcal{V} = \mathcal{V}'$，则称 $\mathcal{G}'$ 为 $\mathcal{G}$ 的生成子图。



(a) 连通图　　(b) 非连通图

图 2.2　连通图和非连通图示例

下面是关于图的连通性以及一些其他需要用到的图的定义。

强连通 对于有向图 $\mathcal{G}$ 中任意两个不同的节点 v_i 和 v_j，总存在一条从 v_i 出发，终止于 v_j 路径，则称该图 $\mathcal{G}$ 是强连通的。

弱连通 如果将有向图 $\mathcal{G}$ 中的通信边转换成无相的，转换后的无向图是连通的，那么称图 $\mathcal{G}$ 是弱连通的。

全连通 如果有向图 $\mathcal{G}$ 中任意两个不同的节点都形成边，那么称该网络是全连通的，此时称图 $\mathcal{G}$ 是完全图。

注意到，对于无向图来说，强连通与弱连通的含义是一致的，我们可以统称为连通的。另外，从上述图的连通性定义来看，对于网络连通性要求的高低，从高到

底的排序依次为：全连通，强连通，弱连通，连通。

生成树 对于一个有向图 $\mathcal{G}$，如果存在至少一个节点，可以沿着图中边的路径，抵达图中其他任何一个节点的位置，则称此图包含一棵生成树。相应地，该节点称为根节点。

联合图 假设 $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_k$ 为具有相同节点集的有向图，令 $\mathcal{G}$ 的节点集与 $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_k$ 相同，边集为 $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_k$ 边集的并，则称图 $\mathcal{G}$ 为图 $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_k$ 的联合图。

联合连通 对于一组具有相同顶点集的拓扑图 $\mathcal{G}_1$，$\mathcal{G}_2$，$\cdots$，如果它们的联合图是连通的，那么称这一组图是联合连通的。

联合生成树 如果一组图的联合图包含一棵生成树，那么称其为联合生成树。

频繁联合生成树 对于一组具有相同节点集的无穷序列图 $\mathcal{G}_1$，$\mathcal{G}_2$，$\cdots$ 如果存在一正整数 q，使得每一组子序列 $\mathcal{G}_{qk+1}$，$\mathcal{G}_{qk+2}$，$\cdots$，$\mathcal{G}_{q(k+1)}$，$k \geq 0$ 的联合图均包含一棵生成树，则称该无穷序列图包含频繁联合生成树。

根图 对于有向图 $\mathcal{G}$ 中的节点 v_i，如果对于图中任一其他节点 v_j，都存在一条从 v_i 到 v_j 路径，那么称图 $\mathcal{G}$ 为根图。同时，v_i 被称为图 $\mathcal{G}$ 的根节点。

显然，对于每个根图，都含有一棵生成树。

强根图 我们称图 $\mathcal{G}$ 为一个强根图，当且仅当根节点 v_i 属于图中其他任意节点的邻居，即 v_i 与其他任意节点都存在一条长度为 1 的路径。

合成图 记 $\mathcal{G}(k_1) \circ \mathcal{G}(k_2)$ 为 $\mathcal{G}(k_1)$ 和 $\mathcal{G}(k_2)$ 两个图的合成图，两个图具有相同的顶点集 $\mathcal{V}$，当存在顶点 $v_l \in \mathcal{V}$ 满足 $(v_i, v_l) \in \mathcal{E}(\mathcal{G}(k_1))$ 及 $(v_l, v_j) \in \mathcal{E}(\mathcal{G}(k_2))$，则 $(v_i, v_j) \in \mathcal{E}(\mathcal{G}(k_1) \circ \mathcal{G}(k_2))$。

联合有根 称一有限序列图 $\mathcal{G}(k_1), \mathcal{G}(k_1), ..., \mathcal{G}(k_m)$ 是联合有根的，如果它们的合成图是一个根图。

频繁联合有根 称一无限序列图 $\mathcal{G}(k_1), \mathcal{G}(k_2), ...$ 是频繁联合有根的，如果存在一正整数 p，对于每一有限序列图 $\mathcal{G}(k_{t+1}), \mathcal{G}(k_{t+2}), ..., \mathcal{G}(k_{t+p})$ 是联合有根的。

2.1.1 矩阵理论

图论与矩阵分析有着十分密切的联系，通常一个有向或者无向图的节点和边的情况可以由一个相应的矩阵来表示，该图的性质相应地也可以通过分析这类矩阵反应出来。

一个由 N 个节点组成的有向图 $\mathcal{G}$ 的邻接矩阵 $A=\{a_{i,j}\}$，是一个 $N\times N$ 阶的矩阵，其定义为

$$a_{i,j}=\begin{cases}1, & \text{如果 } (v_j,v_i)\in\mathcal{E}\\ 0, & \text{其他}\end{cases}$$

很显然当 $\mathcal{G}$ 为无向图时，A 为对称矩阵。

入度矩阵记作 $D=diag\{d_1,d_2,\ldots,d_N\}$，其中 d_i 是顶点 v_i 的入度数，矩阵 D 中的每一个对角元素的值即为对应顶点的入度值。当 $\mathcal{G}$ 为无向图时, 各顶点的出度值与入度值相等，此时可以将 D 简称为度矩阵。

通常，我们将加权的邻接矩阵 A 定义如下

$$a_{i,j}=\begin{cases}w_{i,j}, & \text{如果 } (v_j,v_i)\in\mathcal{E}\\ 0, & \text{其他}\end{cases}$$

其中 $w_{i,j}>0$ 是对应边 (v_j,v_i) 的权值。这时，节点 v_i 的入度值为所有以 v_i 为边尾的边权值的总和，出度值为所有以 v_i 为边首的边权值的总和。这样前面的邻接矩阵可以看成特殊的权值全为 1 的加权邻接矩阵。

一个由 N 个节点组成的有向图 $\mathcal{G}$ 的 Laplacian 矩阵 L，是一个 $N\times N$ 阶的矩阵，其定义为 $L=D-A$，L 中的元素如下：

$$l_{i,j}=\begin{cases}\sum_{j\in\mathcal{N}_i}a_{i,j}, & i=j\\ -a_{i,j}, & i\neq j\end{cases}$$

定义 2.1: （Kronecker 积[135]）对于矩阵 $A=\{a_{i,j}\}_{m\times n}$，$B=\{b_{i,j}\}_{p\times q}$，那么 A 与 B 的 Kronecker 积计算如下：

$$A\otimes B=\begin{bmatrix}a_{11}B & a_{12}B & \cdots & a_{1n}B\\ a_{21}B & a_{21}B & \cdots & a_{2n}B\\ \vdots & \vdots & \ddots & \vdots\\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B\end{bmatrix}.$$

引理 2.1: （Schur 补定理[136]）对于一分块对称矩阵

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{12}^T & S_{22} \end{bmatrix},$$

其中 $S_{11} \in R^{n\times n}$。那么下列条件等价：

（i）$S < 0$;

（ii）$S_{11} < 0, S_{22} - S_{12}^T S_{11}^{-1} S_{12} < 0$;

（iii）$S_{22} < 0, S_{11} - S_{12} S_{22}^{-1} S_{12}^T < 0$.

根据上述对 Laplacian 矩阵的定义和关于矩阵引理，对于一个有向图 $\mathcal{G}$，设 $z = [z_1^T, \ldots, z_N^T]^T$， $L \in R^{N\times N}$，则下列条件相互等价[137]：

1. 0 是矩阵 L 的单一特征根，其他的特征根都有正的实部，且 0 特征根对应的特征向量为 1_N；
2. 有向图 $\mathcal{G}$ 包含一棵生成树；
3. 当 $(L \otimes I_N)z = 0$ 时，有 $z_1 = \cdots = z_N$；
4. 系统 $\dot{z} = -(L \otimes I_N)z$ 能够实现渐进一致；

另外，根据文献 [137]，如果有向图 $\mathcal{G}$ 满足强连通且对称或无向连通的，那么矩阵 L 是对称且半正定的，并且所有特征根均为非负实数，依次可以排列为

$$0 = \lambda_1(L) < \lambda_2(L) \leq \cdots \leq \lambda_n(L).$$

2.2 泛函微分方程的稳定性

考虑一个自主体的滞后型泛函微分方程：

$$\dot{x}(t) = f(x_t) \tag{2.1}$$

其中 $\Omega \in \mathcal{C}$， $f : \Omega \to \mathbb{R}^n$。给定$\varphi \in \mathcal{C}$， $\rho > 0$，如果对于 $x \in \mathcal{C}([-\tau\rho)$， $\mathbb{R}^n)x_t \in \Omega$，当 $t \in [0,\ \rho)$， $x(\varphi)(0) = \varphi$ 时， $x(t)$ 满足式（2.1），则称函数 $x(\varphi)$ 是式（2.1）在初始条件 φ 下的一个解。

定义 2.2: （ω-极限集[164]）设 $\varphi \in \Omega$，对于定义在 $[-\rho, \infty)$ 上的 $x(\varphi)(t)$，如果存在一个随着 $n \to \infty$，$t_n \to \infty$ 的非负实数序列，使其当 $n \to \infty$ 时，有 $\|x_{t_n}(\varphi) - \psi\| \to 0$，那么称 $\psi \in \Omega$ 是关于 φ 的 ω-极限集，用 $\omega(\varphi)$ 表示。

定义 2.3: （正不变集[164]）给定一个集合 $M \subset \Omega$，如果对于任意 $\varphi \in M$，在定义区间 $[-\tau, \infty)$ 上存在一个关于系统（2.1）的解 $x(\varphi)(t)$，当 $t \geq 0$，$x_0 = \varphi$ 时，有 $x_t \in M$，那么称集合 M 是关于系统（2.1）的正不变集。

对于上述存在的关于系统（2.1）的解 $x(\varphi)(t)$，它具有下列性质：
（i）轨迹经过 φ，即集合 $\{x_t(\varphi) : t \geq 0\}$ 为紧集；
（ii）$\omega(\varphi)$ 是非空连通不变紧集；
（iii）当 $t \to \infty$ 时，$x_t(\varphi)$ 趋于 $\omega(\varphi)$。

对于一给定 Lyapunov-Razumikhin 函数 $V = V(x)$，$V : D \to \mathbb{R}$，$D \subseteq \mathbb{R}^n$, 其关于系统（2.1）的右上 Dini 导数表示为

$$D^+V(\phi) = \lim_{h \to 0^+} \sup \frac{1}{h}(V(\phi(0) + hf(\phi)) - V(\phi(0))).$$

给定一个集合 $\Omega \subset \mathcal{C}$，定义:

$$E_V = \{\varphi \in \Omega : \max_{s \in [-\tau, 0]} V(x_t(\varphi)(s)) = \max_{s \in [-\tau, 0]} V(\varphi(s)), \forall t \geq 0\}, \tag{2.2}$$

$$M_V = \text{关于系统（2.1）在 } E_V \text{ 中存在的最大不变集.} \tag{2.3}$$

注意到，M_V 是函数 $\varphi \subset \Omega$ 的一个集合，如果令它的元素作为系统（2.1）的初始条件，则对 $t \in (-\infty, \infty)$，$x_t(\varphi)$，我们有

$$\max_{s \in [-\tau, 0]} V(\varphi(s)) = \max_{s \in [-\tau, 0]} V(x_t(\varphi)(s)).$$

此时，对于一个给定的 Lyapunov-Razumikhin 函数 $V = V(x)$，假定 $\varphi \in E_V$，当 $t > 0$ 满足 $\max_{-\tau \leq s \leq 0} V(x_t(\varphi)(s)) = V(x_t(\varphi)(0))$ 时，有 $D^+V(x_t(\phi)) = 0$。于是，可以得到下列结论：

引理 2.2: [164] 假设存在一个 Lyapunov-Razumikhin 函数 $V = V(x)$ 以及一个关于系统（2.1）的正不变闭集 Ω，该闭集满足:

$$D^+V(\varphi) \leq 0 \, \forall \varphi \in \Omega \; s.t. \; V(\varphi(0)) = \max_{-\tau \leq s \leq 0} V(\varphi(s)). \tag{2.4}$$

对任意 $\varphi \in \Omega$，其中 $x(\varphi)(\cdot)$ 定义在 $[-\tau, \infty)$ 上且有界，$\omega(\varphi) \subseteq M_V \subseteq E_V$，当 $t \to \infty$ 时，我们有 $x_t(\varphi) \to M_V$。

令 $h : (a, b) \to \mathbb{R}$ 在区间 (a, b) 为一个连续的函数，则 h 在 (a, b) 上是非增的当且仅当对于任意 $t \in (a, b)$，$D^+h(t) \leq 0$。

然后我们得到如下定理：

定理 2.1: [166] 令 $V_i(t, x) : \mathbb{R} \times \mathbb{R}^m \to \mathbb{R}(i = 1, 2, ..., n)$为一个$C^1$ 类函数，$V(t, x) = \max_{i=1,2,...,n} V_i(t, x)$，$\mathcal{I}(t) = \{i \in \{1, 2, ..., n\} : V_i(t, x(t)) = V(t, x(t))\}$ 为在时间 t 上获得最大值的指标集，于是有

$$D^+V(t, x(t)) = \max_{i \in \mathcal{I}(t)} \dot{V}_i(t, x(t)). \tag{2.5}$$

2.3 本章小结

本章作为后续章节的基础，详细介绍了一些文中所需的基本术语，定义以及性质等背景知识，为接下去研究多智能体系统安全一致性问题提供了必要的基础.

第三章　通信延时下多智能体系统的安全一致性控制

3.1　引言

多智能体系统一致性问题已引起了广泛关注，并已取得极为丰硕的研究成果，然而对于一致性算法的安全性问题的研究，却处于一个刚刚起步的阶段，尤其随着多智能体系统技术渗入到人们生活的方方面面，并起着越发重要的作用，对于它的安全性问题势必会受到越来越多研究人员的重视。安全一致性（secure consensus）控制的基本思想，是通过对网络中正常节点施加控制，使得其在执行一致性协议中，能够抵御恶意节点的攻击行为，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。为了获取安全的一致性算法，已有许多学者做了相关的研究工作。例如，文献 [140] 研究了多智能体系统分别在存有拜占庭（Byzantine）和不合作（non-colluding）两类敌对节点环境下的一致性问题，得到了敌对个体数目与网络通信图连通度的对应关系。文献 [162] 提出了一种新的基于图论的 r-稳健图（r-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。文献 [141] 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 [142] 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(SATS)，成功解决了系统网络中的时钟同步问题。而文献 [143] 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。除以上工作，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 [144, 160, 174]。

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。更有甚至，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[145, 146, 148]；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。

如绪论中所述，时延是影响多智能体系统一致性算法十分重要的一个因素，也是研究人员极为关注的一个课题。严格来说，在一个控制系统的实际应用中，时延是普遍存在且不可避免的，如信号的量测、传输和处理以及物理、化学、生物等环境变化都会产生时延。时延的存在可能会使得系统动态性能变差甚至引起系统的不稳定。因此在设计一致性协议的时候，已有许多文献从理论角度分析和了解了时延对多智能体系统的影响。

一般按照类别，可以将时延分为输入时延、通信时延以及量测时延等。相应地带时延的一致性算法基本可以归为两类：其中一类算法只考虑获取邻居信息时存有时延，自身状态值是可以实时获取的，称为不对称性算法。另一类则是同时考虑智能体自身状态和邻居信息获取中都存有时延，这类算法称为对称性算法。以上两类算法典型的控制律形式表示如下：

$$u_i(t) = \sum_{j\in\mathcal{N}_i} a_{i,j}(t)\left((x_j(t-\tau_{i,j}) - x_i(t)\right); \tag{3.1}$$

$$u_i(t) = \sum_{j\in\mathcal{N}_i} a_{i,j}(t)\left((x_j(t-\tau_{i,j}) - x_i(t-\tau_i)\right). \tag{3.2}$$

针对以上问题，本章主要讨论在通信时延影响下，离散时间多智能体系统安全一致性控制律的设计问题。为了便于叙述，文中我们将智能体称为节点，通信链路称为边。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恶意节点（attack 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 [162, 174] 讨论的固定拓扑通信相比，本章考虑的协议适用于时变通信拓扑。

本章节中将会额外用到的一些数学符号及定义引理说明如下：

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。$\mathcal{S}_1$，$\mathcal{S}_2$，...，$\mathcal{S}_n$ 称为集合 $\mathcal{S}$ 的划分子集，若满足：（1）$\cup_{1\le i\le n}\mathcal{S}_i = \mathcal{S}$，以及（2）$\mathcal{S}_i\cap\mathcal{S}_j = \emptyset$，$\forall i\neq j$。

本章余下部分结构安排如下：第 3.2 节对一阶离散时间系统在恶意攻击下的安全性问题进行了分析，介绍了一些相关的恶意节点攻击模型，并针对攻击模型，详细设计了相应的安全一致性控制算法。第 3.3 节给出了本章节的主要结论，并且给出了具体的数学分析证明。第 3.4 节通过两个实例仿真实验，来对本章所提控制协

议进行有效性的验证。第 3.5 节对本章的内容进行了总结。

3.2 问题描述

考虑用有向图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}, A_{\mathcal{G}}\}$ 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 $\mathcal{V}_s = \{v_1, v_2, \cdots, v_{n_s}\}$ 表示包含 n_s 个正常节点的集合，$\mathcal{V}_a = \{v_{n_s+1}, v_{n_s+2}, \cdots, v_n\}$ 表示包含 $n_a = n - n_s$ 个恶意节点的集合。显然有，$\mathcal{V} = \mathcal{V}_s \bigcup \mathcal{V}_a$，$\emptyset = \mathcal{V}_s \bigcap \mathcal{V}_a$。与之对应的序号集我们分别用 $\mathcal{I}_s = \{1, 2, \cdots, n_s\}$ 和 $\mathcal{I}_a = \{n_s + 1, n_s + 2, \cdots, n\}$ 表示。

考虑系统中各正常节点的动态方程如下：

$$x_i(k+1) = x_i(k) + u_i(k), \quad i \in \mathcal{I}_s, k \in \bar{\mathbb{Z}}^+, \tag{3.3}$$

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，本章所得结论同样成立，可通过引入 Kronecker 算子进行扩展。

3.2.1 攻击模型

通常，多智能体系统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 [65, 159–161] 介绍了几类多智能体网络中常见的攻击方式，如击停（crash）攻击、共谋（colluding）攻击、拜占庭（Byzantine）攻击等。相应地，我们称持有这些特点攻击方式的节点分别为击停节点、共谋节点、拜占庭节点等。其中，击停节点在网络攻击中最为常见，其攻击方式相对简单，具体数学定义如下：

定义 3.1: （击停节点）[189] 称节点v_q，$q \in \mathcal{I}_a$ 为击停节点，如果 v_q 具有下列属性：

- 节点 v_q 在 t_k 时刻之前表现地和正常节点一致，严格按照给定的控制率执行自身状态更新，即

$$\dot{x}_q = f_{q,\sigma(t)}(t, x_j), \ j \in \mathcal{N}_q, \ t < t_k;$$

- 节点 v_q 从 t_k 时刻起，之后彻底停止状态更新，即

$$x_q(t) = x_q(t_k),\ t \geq t_k;$$

- v_q 向周围的邻居节点传送一致的信息值，即

$$x_{(q,i)} = x_{(q,j)},\ \forall i, j \in \mathcal{N}_q.$$

文献 [65] 中定义的攻击节点模型与上述击停节点的定义相类似。作者同样考虑节点在遭受攻击之后，状态值将维持固定不再变化，唯一的区别在于这个维持不变的值并非是受攻击那一刻停止的状态值，而是由攻击节点任意给定的。

此外，比较其他在各类型攻击节点，相关文献已经证明，拜占庭节点最具有破坏性。该类节点本身不受制控制协议 u 的约束，可任意变换自身状态值，它掌握网络的全局信息，可与网络中其他拜占庭节点共谋，并能在同一时刻向周围不同邻居发送不同的虚假信息，以此来干扰破坏多智能体网络的一致性。其具体的数学定义如下：

定义 3.2: （拜占庭节点）[189] 称节点v_q，$q \in \mathcal{I}_a$ 为拜占庭节点，如果 v_q 具有下列属性：

- 其状态更新方程满足下式：

$$x_p^q(k+1) = f_p^q(\{x_q^p(k)\}),\ q \in \mathcal{I}_a, p \in \mathcal{N}_q. \tag{3.4}$$

  其中：$x_p^q(k)$ 表示 k 时刻节点 v_q 向节点 v_p 发送的状态值，$f_p^q(\cdot)$ 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，$x_i^q(k) \neq x_j^q(k), \forall i, j \in \mathcal{N}_q$，且 $i \neq j$。也就是说，在同一时刻，函数 $f_i^q(\cdot) \neq f_j^q(\cdot)$；

- 在任意时刻可以随意改变攻击对象或者放弃攻击。

鉴于拜占庭攻击特点涵盖了其他各类型的攻击。所以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。本章考虑的恶意节点假设具有上述拜占庭攻击能力外，还具备可在任意时刻放弃攻击和转换攻击对象的能力。

显然，如果不对系统中的恶意节点数目进行限定，则当网络中的节点绝大多数为恶意节点时，系统就很难实现一致。同时也不便于科研人员对网络进行安全性分析研究工作。为此，我们有必要介绍以下常用的一些攻击节点部署模型。

定义 3.3: （f-全局攻击模型）多智能体系统全网中至多有 f 个节点为恶意节点的模型，称为 f-全局攻击模型，即 $|\mathcal{V}_a| \leq f$，$f \in \mathbb{Z}^+$。

定义 3.4: （f-局部攻击模型）多智能体系统网络中任意一个智能体的邻居当中存在至多有不超过 f 个数目的邻居节点为恶意节点，称为 f-局部攻击模型，即 $|\mathcal{N}_i \cap \mathcal{V}_a| \leq f$，$\forall i \in \mathcal{I}_s$，$f \in \mathbb{Z}^+$。

值得注意的是，f-局部攻击模型在针对时变拓扑系统的时候，仍要时刻保持局部恶意节点数目的限定，即正常节点的邻居数目在随着拓扑变化而发生增减的时候，恶意节点的最大上限数目仍需要保持不变。

定义 3.5: （f-局部占比攻击模型）多智能体系统网络中任意时刻任意一个智能体的邻居当中存在至多有不超过占比 f 个数目的邻居节点为恶意节点，称为 f-局部占比攻击模型，即 $|\mathcal{N}_i[t] \cap \mathcal{V}_a| \leq f|\mathcal{N}_i[t]|$，$\forall i \in \mathcal{I}_s$，$0 \leq f \leq 1$。

较于前两种攻击部署模型，f-局部占比攻击模型在目前的关于一致性安全性研究的文献中出现的频率相对较少，但该模型也具有相当的实际意义，逐渐被研究者们所重视。

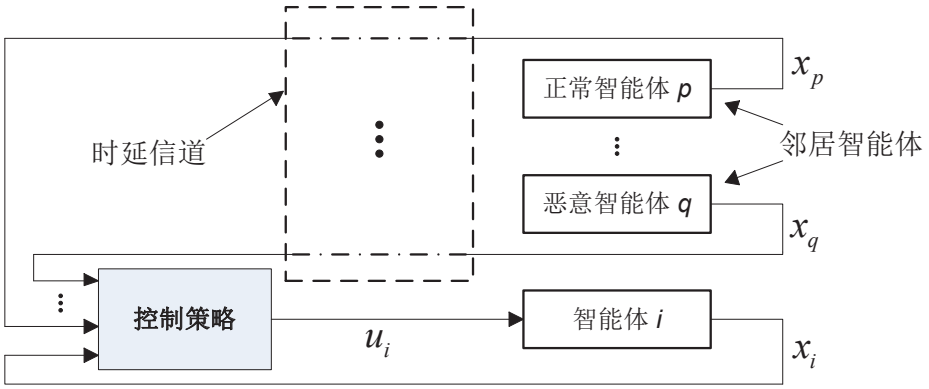


图 3.1　通信时延下安全一致性控制结构图

3.2.2 通信时延下的安全一致性算法

本章中我们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 个恶意节点或者在全网中至多拥有不超过 f 个恶意节点的前提下，即在相应的 f-局部攻击模型和 f-全局攻击模型下，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：

Step 1 对节点 v_i，$i \in \mathcal{I}_s$，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：

$$r_i(k) = \begin{cases} n_i(k) - f - 1, & n_i(k) < 2f + 1 \\ f, & n_i(k) \geq 2f + 1 \end{cases}. \tag{3.5}$$

Step 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。

Step 3 记 $\mathcal{R}_i(k)$ 表示 Step 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：

$$u_i(k) = \sum_{j \in \mathcal{N}_i(k) \setminus \mathcal{R}_i(k)} a_{i,j}(x_i^j(k - d_{i,j}(k)) - x_i(k)). \tag{3.6}$$

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 $\bar{d} = \sup_{k \geq 0} \max\{d_{i,j}(k), j \in \mathcal{N}_i, i \in \mathcal{I}_s\}$。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 $a_{i,j} \geq 0$，且 $\sum_{j=0}^{n} a_{i,j} = 1$。

注 3.1: 本文相比文献 [150], 在算法 Step 2 中，引入自适应参数项 $r_i(k)$，目的在于当恶意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 Step 2 中需移除信息的个数，确保各正常节点在 Step 3 中仍能获取有效个数的信息来更新状态。

注 3.2: 文献 [162] 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，且同时要求恶意节点必须具有固定的攻击目标，即一旦恶意节点放弃或者转移攻击目标，其算法也将随之失效。

注 3.3: 上述所提算法，基本思想是通过消减序列两头的极端值，来保证余下的值在参与节点自身更新的时候其状态不被极值过度影响，确保处于一个安全范围内。但是从根源上并没有能力完全排除恶意节点的信息，比如当一个恶意节点发送的状态信息处于序列中间段的时候，上述算法就没法保证将其摒除。

此时，联合式 (3.3) 和式 (3.6)，可以得到系统的闭环形式：

$$\begin{aligned} x_i(k+1) = \quad & x_i(k) + \frac{1}{\sum\limits_{j=1}^{n} a_{i,j}\delta_{i,j}(k)} \times \\ & \left(\sum_{j=1}^{n} a_{i,j}\delta_{i,j}(k)(x_j(k-d_{i,j}(k)) - x_i(k)) \right), \end{aligned} \tag{3.7}$$

其中，$\delta_{i,i}(k) \triangleq 1$，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

$$\begin{aligned} M(k) &= \max_{i\in\mathcal{I}_s,\theta=0,\ldots,\bar{d}} x_i(k-\theta), \\ m(k) &= \min_{i\in\mathcal{I}_s,\theta=0,\ldots,\bar{d}} x_i(k-\theta), \end{aligned}$$

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 $m(0)$ 即为正常节点在初始时刻的最大值和最小值。

定义 3.6: 对于多智能体系统 (3.3)，当且仅当满足下列两个条件时，即

$$m(0) \leq \inf_{k\geq 0} \min_{i\in\mathcal{I}_s} x_i(k) \leq \sup_{k\geq 0} \max_{i\in\mathcal{I}_s} x_i(k) \leq M(0), \tag{3.8a}$$

$$\lim_{k\to\infty} (x_i(k) - x_j(k)) = 0,\ \forall i,j \in \mathcal{I}_s. \tag{3.8b}$$

称系统 (3.3) 能实现安全一致。

定义 3.6 中可以看出，条件 (3.8a) 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 (3.8b) 保证了系统最终状态的一致性.

3.3 主要结果

为方便阐述系统中节点的时延状态，本文借鉴文献 [61] 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 前 j 步时刻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 3.7: （时延图[61]）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 $\{(v_{i,j-1}, v_{i,j}), j = 1, \cdots, \bar{d}\} \bigcup \{(v_{i,d_{j,i}}, v_{j,0}) : \forall (v_i, v_j) \in \mathcal{E}\}$。

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

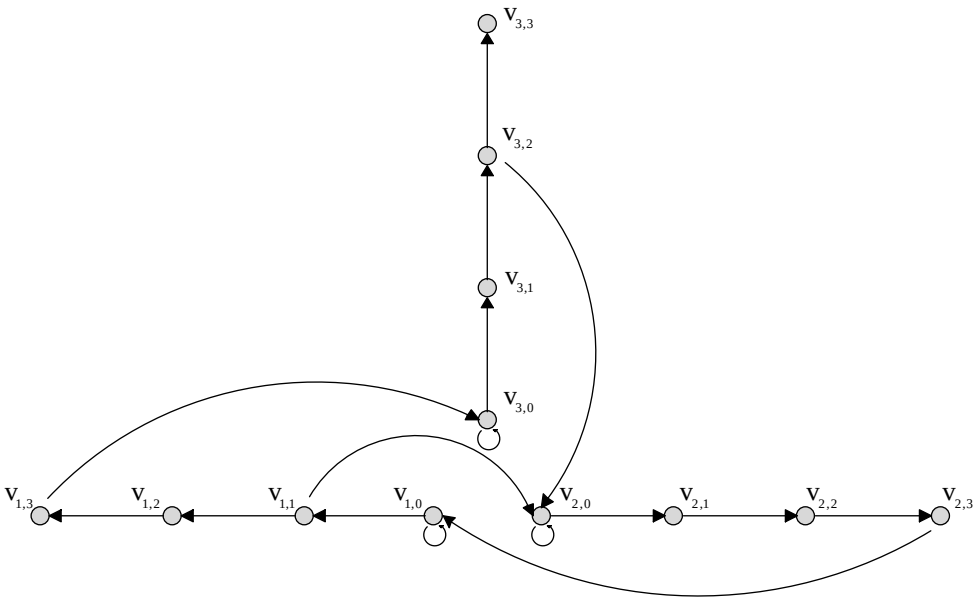


图 3.2　由 3 节点引出的时延图示例

定义 3.8: （商图[61]）令 $\mathbb{Q}(\bar{\mathcal{G}})$ 表示商图，是指顶点集为 $\mathcal{V}$，边集为（v_i, v_j）表示一条从集合 $\mathcal{V}_i$ 中某个节点到节点 v_j 的边。

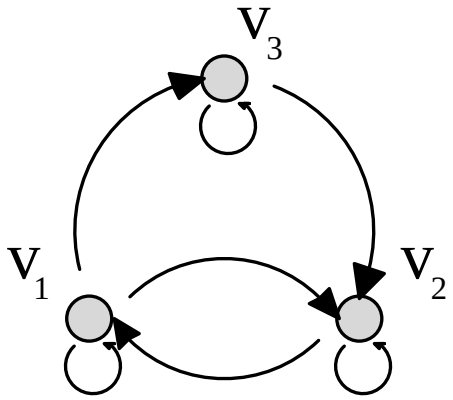


图 3.3　图 3.3 示例中的节点所对应的商图

值得注意的是，在商图中，节点之间传递的信息并没有具体说明是节点第几步的时延信息传递给了邻居。由此，容易验证，$\mathbb{Q}(\bar{\mathcal{G}}(k)) = \mathcal{G}(k)$。

在给出主要结论前，首先介绍以下一些需要用到的定义以及引理。

定义 3.9: （r-可得集[162]）对于一个有向图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}\}$ 以及其一非空节点集子集 $\mathcal{S} \subset \mathcal{V}$，如果 $\mathcal{S}$ 中至少存在一个节点 v_i，它的邻居集中至少有 r 个邻居来自集合 $\mathcal{S}$ 外部，即 $|\mathcal{N}_i \setminus \mathcal{S}| \geq r$，$r \in \mathbb{Z}^+$。我们称集合 $\mathcal{S}$ 为 r-可得集。

定义 3.10: （(r,s)-可得集[162]）对于一个有向图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}\}$ 以及其一非空节点集子集 $\mathcal{S} \subset \mathcal{V}$，如果 $\mathcal{S}$ 中存有不少于 s 个节点，这些节点各自的邻居集中至少有 r 个邻居来自集合 $\mathcal{S}$ 外部，即，令集合 $\mathcal{X}_{\mathcal{S}}^{r} = \{i \in \mathcal{S} : |\mathcal{N}_i \setminus \mathcal{S}| \geq r\}$，满足 $|\mathcal{X}_{\mathcal{S}}^{r}| \geq s$，$r$，$s \in \mathbb{Z}^+$。我们称集合 $\mathcal{S}$ 为 (r,s)-可得集。

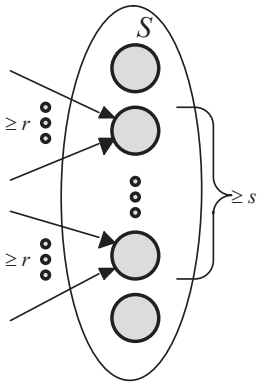


图 3.4　(r,s)-可得集示例图

我们不难发现，对于一个 r-可得集 $\mathcal{S}$，它至少包含这样一个节点，该节点保证有不少于 r 个邻居来自自身所在的集合 $\mathcal{S}$ 之外。也就是说，$\mathcal{S}$ 当中至少存在一个节

点，可获取自身集合外一定数目的其他节点信息。基于上述 r-可得集和 (r,s)-可得集的定义，接下来分别给出 r-稳健图和 (r,s)-稳健图的定义。

定义 3.11: （r-稳健图[162]）对于一个有向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}}\}$，如果 $\mathcal{V}$ 中任意一对划分子集，记作 $\mathcal{S}_1$，$\mathcal{S}_2\subset\mathcal{V}$，那么它们中至少有一个集合满足 r-可得集。我们称图 $\mathcal{G}$ 为 r-稳健图。

定义 3.12: （(r,s)-稳健图[162]）对于一个有向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}}\}$（节点个数 $n\geq 2$），我们称图 $\mathcal{G}$ 为 (r,s)-稳健图，如果 $\mathcal{V}$ 中任意一对划分子集，记作 $\mathcal{S}_1$，$\mathcal{S}_2\subset\mathcal{V}$，下列条件中至少有一个得到满足：

（1）$|\mathcal{X}_{\mathcal{S}_1}^r|=|\mathcal{S}_1|$;

（2）$|\mathcal{X}_{\mathcal{S}_2}^r|=|\mathcal{S}_2|$;

（3）$|\mathcal{X}_{\mathcal{S}_1}^r|+|\mathcal{X}_{\mathcal{S}_2}^r|\geq s$.

引理 3.1: [148] 令 $\mathcal{G}$ 是满足 r-稳健的有向图，$\mathcal{G}'$ 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 $(r-s)$-稳健的。

引理 3.2: 对于一个 (r,s)-可得集 $\mathcal{S}$，令 $s'\leq s$，则集合 $\mathcal{S}$ 同样是一个 (r,s')-可得集。

证明: 由可得集的定义 3.10 知，上述结论是显而易见的。 证明完毕。

引理 3.3: 令 $\mathcal{G}$ 是有向图，则 $\mathcal{G}$ 包含一棵生成树，当且仅当 $\mathcal{G}$ 是 1-稳健的。

证明: 必要性。用反证法证明。假设图 $\mathcal{G}$ 含有一生成树但不满足 1-稳健的拓扑性质。根据稳健图定义 3.11，易知存在一对非空互不相交的子集 $\mathcal{S}_1,\mathcal{S}_2\subseteq\mathcal{V}$，即 $\mathcal{S}_1$ 中的元素与 $\mathcal{S}_2$ 中的元素不存在任何信息交流，而这与拓扑中含有生成树的假设矛盾。

充分性。同样使用反证法证明。假设图 $\mathcal{G}$ 不含有生成树。令 A 表示 $\mathcal{G}$ 的邻接矩阵。则根据文献 [134, 149] 可知，可将 A 进行特殊分解，使得图中所有节点被分解成为两个互不存在信息交流的子集。这与 $\mathcal{G}$ 是 1-稳健图的性质矛盾。 证明完毕。

引理 3.4: 存在正整数 $\bar{k}\in\mathbb{Z}^+$，使得对于全部 $i=1,2,...,n$，由 $\mathcal{V}_i$ 引出的至少 $\bar{k}$ 步时延图 $\bar{\mathcal{G}}(k)$ 的合成图在顶点 $v_{i,0}$ 处是强有根的。

证明: 将证明分成以下两个步骤进行：

1. 寻找满足由 $\mathcal{V}_i$ 引出的至少 $\bar{k}$ 步时延图 $\bar{\mathcal{G}}(k)$ 的合成图在顶点 $v_{i,0}$ 处强有根的正整数 $\bar{k}$。

2. 证明 $\mathcal{V}_i$ 引出的子图的合成图包含于 $\mathcal{V}_i$ 引出的时延图 $\bar{\mathcal{G}}(k)$ 的合成图的子图。

第 1 步： 采用与文献 [178] 类似的证明思想。首先，令 $e_i \in \mathbb{R}^{m+1}$ 表示第 i 个元素为 1 其余全为 0 的列向量，$\mathbf{1}_{\mathrm{m+1}} \in \mathbb{R}^{\mathrm{m+1}}$ 表示元素全为 1 的列向量。由此定义

$$\Delta \triangleq [e_{r_{1,i}+1} + e_{r_{2,i}+1} e_1 e_2 \cdots e_m]^T \otimes I_{n_x}, \tag{3.9}$$

$$\Lambda \triangleq (1_{m+1} \cdot e_1^T) \otimes I_{n_x}, \tag{3.10}$$

根据文献 [178] 中引理 7 知，此时存在一个正整数 $\bar{k}$，满足对于 $\forall k \geq \bar{k}$，

$$\Delta^k \geq \Lambda. \tag{3.11}$$

令 $A_i(k)$ 表示时延图 $\bar{\mathcal{G}}(k)$ 子图的邻接矩阵，$\tilde{A}_i(k)$ 表示其相对应的关联矩阵，根据关联矩阵的定义形式，我们有 $\tilde{A}_i(k) \geq \Delta$。接着，由文献 [179] 知，对于 $\forall k \geq \bar{k}$，有

$$\prod_{j=k_0+1}^{k_0+k} \tilde{A}_i(j) \triangleq \tilde{A}_i(k_0+k)\tilde{A}_i(k_0+k-1)\cdots\tilde{A}_i(k_0+1) \geq \Delta^k \tag{3.12}$$

其中 k_0 为任意非负正数。由于前述定义知，存在一个正数 α 满足 $A_i(k) \geq \alpha\tilde{A}_i(k)$，再通过式 (3.11)和 (3.12) 推知 $\mathcal{V}_i$ 引出的不少于 $\bar{k}$ 步子图的合成图在顶点 $v_{i,0}$ 强有根。

第 2 步： 令图 $\bar{\mathcal{G}}_i(k)$ 为一以 $\bar{\mathcal{V}}$ 为顶点集，$\mathcal{E}(\bar{\mathcal{G}}(k)) \cap (\mathcal{V}_i \times \mathcal{V}_i)$ 为边集的子图。由于图 $\bar{\mathcal{G}}_i(k)$ 是由图 $\bar{\mathcal{G}}(k)$ 减去部分边得到，因此容易验证合成图 $\bar{\mathcal{G}}(k_p) \circ \ldots \circ \bar{\mathcal{G}}(k_1)$ 包含合成图 $\bar{\mathcal{G}}_i(k_p) \circ \ldots \circ \bar{\mathcal{G}}_i(k_1)$。$\mathcal{V}_i$ 引出的合成图 $\bar{\mathcal{G}}_i(k_p) \circ \ldots \circ \bar{\mathcal{G}}_i(k_1)$ 的子图，等同于 $\mathcal{V}_i$ 引出的相应子图的合成图。因此第 2 步得证。 证明完毕。

引理 3.5: 如果图 $\mathcal{G}(k)$ 是频繁联合连通的，那么存在一个正整数 $\bar{k}_1$，使得任意不少于 $\bar{k}_1$ 步时延图 $\bar{\mathcal{G}}(k)$ 的合成图是强有根的。

证明: 由于图 $\mathcal{G}(k)$ 是反复联合连通的，则存在一序列 $\{k_i, i = 1, ..., p\}$，满足

$$\tilde{\mathcal{G}}_0(p) \triangleq \mathcal{G}(k_p) \circ \mathcal{G}(k_{p-1}) \circ \cdots \circ \mathcal{G}(k_1) \tag{3.13}$$

有根，其中 $k_p > k_{p-1} > \cdots > k_1$。如果定义 $\tilde{\mathcal{G}}_1(\bar{k})$ 为 $\bar{\mathcal{G}}(k_p) \circ \bar{\mathcal{G}}(k_{p-1}) \circ \cdots \circ \bar{\mathcal{G}}(k_1)$ 的合成图，那么根据引理 3.4 可知，$\mathcal{V}_i$ 引出图 $\tilde{\mathcal{G}}_1(\bar{k})$ 的子图是强有根的。根据文献 [61] 推论 5，因为图 $\tilde{\mathcal{G}}_0(p)$ 有根，可知商图 $\mathbb{Q}(\tilde{\mathcal{G}}_1(p))$ 是有根的。再通过文献 [61] 引理 7，知合成图 $\tilde{\mathcal{G}}_1(p+\bar{k}) = \tilde{\mathcal{G}}_1(p) \circ \tilde{\mathcal{G}}_1(\bar{k})$ 的子图有根。由定义知合成图 $\tilde{\mathcal{G}}_1(p+\bar{k})$ 的子图中每个节点都带有自环，因此，根据文献 [60] 推论 2 知，具有不少于 $(n-1)^2$ 步长的合成图 $\tilde{\mathcal{G}}_1(p+\bar{k})$ 的子图是强有根的，即图 $\tilde{\mathcal{G}}_1((p+\bar{k})(n-1)^2)$ 含有一强有根子图。

令

$$\begin{aligned} \mathcal{G}^a &\triangleq \tilde{\mathcal{G}}_1((p+\bar{k})(n-1)^2), \\ \mathcal{G}^b &\triangleq \tilde{\mathcal{G}}_1(q), \end{aligned}$$

其中，$q \geq \bar{k}$。显然我们易知合成图 $\mathcal{G}^a \circ \mathcal{G}^b$ 是强有根的。那么，对于节点集 $\mathcal{V}(\mathcal{G})$ 中存在的一个节点，记作 v_i，由于 $\mathcal{G}^a$ 的子图是强有根的，则在图 $\mathcal{G}^a$ 中 v_i 可以到达任意其他在节点集 $\mathcal{V}(\mathcal{G})$ 中的节点。在另一方面，对于 $\forall v_j \in \mathcal{V}(\mathcal{G})$ 和 $\forall 0 \leq k \leq m$，从引理 3.4 知，由 $\mathcal{V}_i$ 引出的 $\mathcal{G}^b$ 的子图是强有根的，于是在图 $\mathcal{G}^b$ 存有一条从 v_j 到 $v_{j,k}$ 的边。因此，对于任意节点 $v_{j,k} \in \bar{\mathcal{V}}$，存在一条从 v_i 到 $v_{j,k}$ 的通信边。于是，令 $\bar{k}_1 = (p+\bar{k})(n-1)^2 + \bar{k}$，我们知不少于 $\bar{k}_1$ 步时延图 $\bar{\mathcal{G}}(k)$ 的合成图是强有根的。证明完毕。

引理 3.6: [61] 对于多智能体系统 (3.3)，在控制协议 (3.6) 下，若系统的频繁联合图均包含一棵生成树，那么系统将根据初始状态值，以指数速度收敛于一常数值 x^*，即

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

接下来给出本文的主要结论。

定理 3.1: 对于多智能体系统 (3.3)，在控制协议 (3.6) 下，假设系统攻击模型满足 f-局部攻击模型，且正常节点之间拓扑满足 $(f+1)$-稳健图，对于节点v_i，$i \in \mathcal{I}_s$，若 k 时刻接收到的信息 $x_p(k) \notin [m(k), M(k)]$，$p \in \mathcal{N}_i(k)$，则有 $p \in \mathcal{R}_i(k)$。

证明: 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 Step 2，移除相应数值后序列的第一个数的值为 $M'(k)$。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恶意邻居个数上限为 $r_i(k)$ 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，$M'(k) \leq M(k)$；

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$M'(k) \leq M(k)$。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 Step 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 $m'(k) \geq m(k)$。

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 $x_p(k) \notin [m(k), M(k)]$，可推得 $x_p(k) \notin [m'(k), M'(k)]$，由此可知，$v_p$ 的信息此刻被 v_i 移除，即 $p \in \mathcal{R}_i(k)$。 证明完毕。

定理 3.2: 对于多智能体系统（3.3），存在通信时延，且一致有界，系统攻击模型满足 f-局部攻击模型，则在控制协议（3.6）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 $(f+1)$-稳健图。

证明: 必要性。我们采用反证法证明。假如网络不满足 $(f+1)$-稳健的，则可将网络中所有节点划分为两个互不相交的子集，记 $S_1, S_2 \subseteq \mathcal{V}$，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 个恶意节点的值为 b，$b \neq a$，对系统中任意正常节点 v_i，$i \in \mathcal{I}_s$ 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 (3.3) 满足安全性；第 2 步，证明系统 (3.3) 收敛至一个相同值，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 3.1 及 $M(k)$、$m(k)$ 的定义，结合系统自身方程，对于任意 $i \in \mathcal{I}_s$，记 $\alpha = \sum_{j\in\mathcal{N}_i(k)\setminus\mathcal{R}_i(k)} a_{i,j}(k) \leq 1$。则有

$$\begin{aligned} x_i(k+1) &\leq x_i(k) + \sum_{j\in\mathcal{N}_i(k)\setminus\mathcal{R}_i(k)} a_{i,j}(k)(M(k)-x_i(k)) \\ &= \alpha M(k) + (1-\alpha)x_i(k) \\ &\leq M(k), \end{aligned} \tag{3.14}$$

因此，$M(k+1) \leq M(k)$。同理，可分析推得 $m(k+1) \geq m(k)$。以上结论保证了安全性条件 (3.8a)。

第 2 步 通过定理 3.1 可知，当恶意节点 v_q，$q \in \mathcal{I}_a$ 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_q 的信息用所有正常节点状态的凸组合表示，即

$$x_q(k) = \sum_{j\in\mathcal{I}_s} \beta_{i,j}(k)x_j(k),\ q\in\mathcal{I}_a\cap(\mathcal{N}_i(k)\setminus\mathcal{R}_i(k)),$$

其中 $\beta_{i,j}(k) \geq 0$，且 $\sum_{j\in\mathcal{I}_s} \beta_{i,j}(k) = 1$。值得注意的是，$x_q(k)$ 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恶意节点信息时，可令 $\beta_{i,j}(k) = 0$，$j \in \mathcal{I}_s$。

引入上述时延图定义 3.7，可将式 (3.7) 表述成如下矩阵形式：

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

其中:

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

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

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

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

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

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

根据定义 3.7，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 $\bar{\mathcal{G}}$ 表示 $\mathcal{G}$ 通过协议 (3.6) 消减去相应边数后的时延图，对应的邻接矩阵为 $\sum_{i=1,\ldots,\bar{d}} A_i(k)$。由于系统中正常节点组成的拓扑满足 $(f+1)$-稳健的，通过引理 3.1，引理 3.2，以及引理 3.3 可知，$\bar{\mathcal{G}}$ 满足 1-稳健，即相应拓扑中包含一棵生成树。另一方面，根据引理 3.5，与 Θ_1 对应的时延图，记 $\bar{\mathcal{G}}_1$，可知 $\bar{\mathcal{G}}_1$ 存在一个根节点若 $\bar{\mathcal{G}}$ 存在一个根节点，即图 $\bar{\mathcal{G}}_1$ 存在一棵生成树。与此同时，Θ 对应的时延图，记 $\bar{\mathcal{G}}_0$，$\bar{\mathcal{G}}_0$ 在 $\bar{\mathcal{G}}_1$ 的拓扑基础上，包含更多的有向边，从而保证 $\bar{\mathcal{G}}_0$ 同样包含一棵生成树，最后再由引理 3.6 可知，系统能够收敛到一平衡点。 证明完毕。

定理 3.3: 对于多智能体系统 (3.3)，存在通信时延且一致有界，则在控制协议 (3.6) 下，面对 f-全局攻击模型，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 $(f+1,f+1)$-稳健图。

证明: 我们采用与文献 [162] 相类似的证明思路。令 $N=|\mathcal{V}_s|$ 表示所有正常节点个数。令 $a_M[k]$ 和 $a_m[k]$ 分别表示 k 时刻所有正常节点中的最大最小状态值。根据定理 3.1，知 $a_M[k]$ 和 $a_m[k]$ 都为单调有界函数，因此存在极值，分别用 A_M 和 A_m 表示。注意到，如果 $A_M=A_m$，则所有正常节点实现状态一致。接下来，我们用反证法证明。

假设 $A_M \neq A_m$（根据定义知 $A_M > A_m$）。此时我们令一个大于零的常数 ϵ_0 满足下式

$$A_M - \epsilon_0 > A_m + \epsilon_0. \tag{3.15}$$

在任意时刻 k，对于一正实数 ϵ_i，令 $\mathcal{X}_M(k,\epsilon_i)$ 表示状态值在区间 $(A_M-\epsilon_i, A_M+\epsilon_i)$ 内所有正常节点的集合。$\mathcal{X}_m(k,\epsilon_i)$ 表示状态值在区间 $(A_m-\epsilon_i, A_m+\epsilon_i)$ 内所有正常节点的集合。根据 ϵ_0 定义可知，集合 $\mathcal{X}_M(k,\epsilon_0)$ 与 $\mathcal{X}_m(k,\epsilon_0)$ 无交集。

选取一正实数 ϵ, 使其满足 $\epsilon_0 > \epsilon > 0$，令 k_ϵ 表示满足 $a_M[k] < A_M + \epsilon$ 和 $a_m[k] > A_m - \epsilon, \forall t > t_\epsilon$ 的时间点 (根据收敛性定义可以知道时间点 k_ϵ 存在)。考虑不相交集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0), \mathcal{X}_m(k_\epsilon,\epsilon_0)$。在拓扑图假设 $(f+1, f+1)$-稳健下，至少它们其中一个不少于 $(f+1)$ 个节点满足 $(f+1)$-可得。如果 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 是 $(f+1)$-可得的，那么存在节点 $x_i \in \mathcal{X}_M(k_\epsilon,\epsilon_0)$，在集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 外有不少 $(f+1)$ 个正常邻居节点，根据定义，所有这些邻居节点的值都小于等于 $A_M - \epsilon_0$，而至少一个值会被节点 x_i 用来更新状态（算法中 v_i 至多移除 f 个比自己小的值）。注意到，在每一个时刻，每个正常节点的状态值是其自身状态值和接收到的邻居状态值的凸组合，组合中每项前的系数都小于 α。由于 k_ϵ 时刻节点 v_i 将会使用的最大值为 $a_M[k_\epsilon]$，将 $a_M[k_\epsilon]$ 赋予范围内最大权重后，可以推得如下不等式：

$$\begin{aligned} x_i(k_\epsilon+1) &\leq (1-\alpha)a_M[k_\epsilon] + \alpha(A_M - \epsilon_0) \\ &\leq (1-\alpha)(A_M+\epsilon) + \alpha(A_M-\epsilon_0) \\ &\leq A_M - \alpha\epsilon_0 + (1-\alpha)\epsilon. \end{aligned}$$

需要注意的是，上述上界值同样适用任意不属于集合 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 内的正常节点的状态更新过程中，因为该节点将采用自身的状态值来更新状态。同样地，如果当 $\mathcal{X}_m(k_\epsilon,\epsilon_0)$ 是 $(f+1, f+1)$-稳健的，那么存在节点 $x_j \in \mathcal{X}_m(k_\epsilon,\epsilon_0)$，满足

$$x_j[k_\epsilon+1] \geq A_m + \alpha\epsilon_0 - (1-\alpha)\epsilon. \tag{3.16}$$

再一次，任何状态值不在集合 $\mathcal{X}_m(k_\epsilon,\epsilon_0)$ 内的正常节点，将拥有相同的下界值。定义

$$\epsilon = \alpha\epsilon_0 - (1-\alpha)\epsilon, \tag{3.17}$$

并考虑集合 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 和 $\mathcal{X}_m(k_\epsilon+1,\epsilon_1)$。由于至少 $\mathcal{X}_M(k_\epsilon,\epsilon_0)$ 和 $\mathcal{X}_m(k_\epsilon,\epsilon_0)$中一个

是 $(f+1,f+1)$-可得的，则不等式 $|\mathcal{X}_M(k_\epsilon+1,\epsilon_1)|<|\mathcal{X}_M(k_\epsilon,\epsilon_0)|$ 和 $|\mathcal{X}_m(k_\epsilon+1,\epsilon_1)|<|\mathcal{X}_m(k_\epsilon,\epsilon_0)|$ 至少有一个成立，或两者都成立。另外，因为 $\epsilon_1<\epsilon_0$，所以集合 $\mathcal{X}_M(k_\epsilon+1,\epsilon_1)$ 和 $\mathcal{X}_m(k_\epsilon+1,\epsilon_1)$ 仍无交集。我们可以对时间 $k_\epsilon+j, j\geq 2$，进行上述同样的分析过程，定义集合 $\mathcal{X}_M(k_\epsilon+j,\epsilon_j)$ 和 $\mathcal{X}_m(k_\epsilon+j,\epsilon_j)$, 其中 ϵ_j 可通过递归定义式 $\epsilon_j=\alpha\epsilon_{j-1}-(1-\alpha)\epsilon$ 取得。更进一步, 在 $k_\epsilon+j$ 时刻，有不等式$|\mathcal{X}_M(k_\epsilon+j,\epsilon_j)|<|\mathcal{X}_M(k_\epsilon+j-1,\epsilon_{j-1})|$ 和 $|\mathcal{X}_m(k_\epsilon+j,\epsilon_j)|<|\mathcal{X}_m(k_\epsilon+j-1,\epsilon_{j-1})|$ 其中之一成立，或两者都成立。

由于 $|\mathcal{X}_M(k_\epsilon,\epsilon_0)|+|\mathcal{X}_m(k_\epsilon,\epsilon_0)|\leq N$，那么存在一些时刻 $k_\epsilon+T$ $(T\leq N)$，其中 $\mathcal{X}_M(k_\epsilon+T,\epsilon_T)$ 或 $\mathcal{X}_m(k_\epsilon+T,\epsilon_T)$ 为空集。当前者为空集时，在 $k_\epsilon+T$ 时刻的所有节点的值小于 $A_M-\epsilon_T$，当后者为空集时，在 $k_\epsilon+T$ 时刻的所有节点的值大于 $A_m+\epsilon_T$。接着我们将证明，$\epsilon_T>0$, 将会与实际的最大值单调收敛至 A_M 相矛盾（$\mathcal{X}_M(k_\epsilon+T,\epsilon_T)$ 为空集时），或者将会与实际的最小值单调收敛至 A_m 相矛盾（$\mathcal{X}_m(k_\epsilon+T,\epsilon_T)$ 为空集时）。为验证上述结论，注意到

$$\begin{aligned}
\epsilon_T &= \alpha\epsilon_{T-1}-(1-\alpha)\epsilon\\
&= \alpha^2\epsilon_{T-2}-\alpha(1-\alpha)\epsilon-(1-\alpha)\epsilon\\
&\vdots\\
&= \alpha^T\epsilon_0-(1-\alpha)(1+\alpha+\cdots+\alpha^{T-1})\epsilon\\
&= \alpha^T\epsilon_0-(1-\alpha^T)\epsilon\\
&\geq \alpha^N\epsilon_0-(1-\alpha^N)\epsilon.
\end{aligned}$$

选取 $\epsilon<\frac{\alpha^N}{1-\alpha^N}\epsilon_0$, 可以得 $\epsilon_T>0$，这与假设矛盾。因此一定有 $\epsilon_0=0$，即得出 $A_M=A_m$。 证明完毕。

如下推论是显而易见的。

推论 3.13: 考虑一阶多智能体系统 (3.3)，攻击节点满足 f-局部攻击模型，在协议 (3.6) 下更新状态，若网络中正常节点之间拓扑满足 $(f+1)$-稳健，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。

推论 3.14: 考虑一阶多智能体系统 (3.3)，攻击节点满足 f-全局攻击模型，在协议 (3.6) 下更新状态，若网络中正常节点之间拓扑满足 $(f+1,f+1)$-稳健，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。

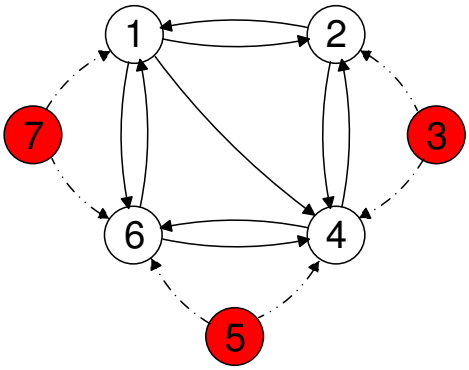


图 3.5　实例一：系统拓扑图

3.4　仿真实例

本节针对定理 3.2、定理 3.3，结合具体实例进行数值仿真实验，以此来验证所得结论的正确性和有效性。

3.4.1 实例一

考虑一个由 7 个节点组成的多智能体系统，通信拓扑如图 3.5 所示。其中节点 v_1，v_2，v_4，v_6 为正常节点，节点 v_3，v_5，v_7 为恶意节点，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 $x(0) = [1, 2, 3, 4, 5, 6, 7]^{\mathrm{T}}$，通信步长设为 $0.1s$，时延上界取 $0.5s$。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 3.11，容易验证图中正常节点 v_1，v_2，v_4，v_6 间拓扑满足 2-稳健图。简便起见，假设恶意节点 v_3，v_5，v_7 的动态方程分别为：

$$\begin{aligned} x_3(k+1) &= 0.8x_3(k) + 0.2u_a(k), \\ x_5(k+1) &= 1.5\sin(0.2\pi k) + 4, \\ x_7(k+1) &= 0.3x_7(k) + 0.7u_a(k). \end{aligned}$$

令 $u_a(k) = 8$。上述对通信拓扑的假定保证了各正常节点在任一时刻的恶意邻居数上限为 1。根据定理 3.2 可知，该网络在上述条件下能够实现安全一致。

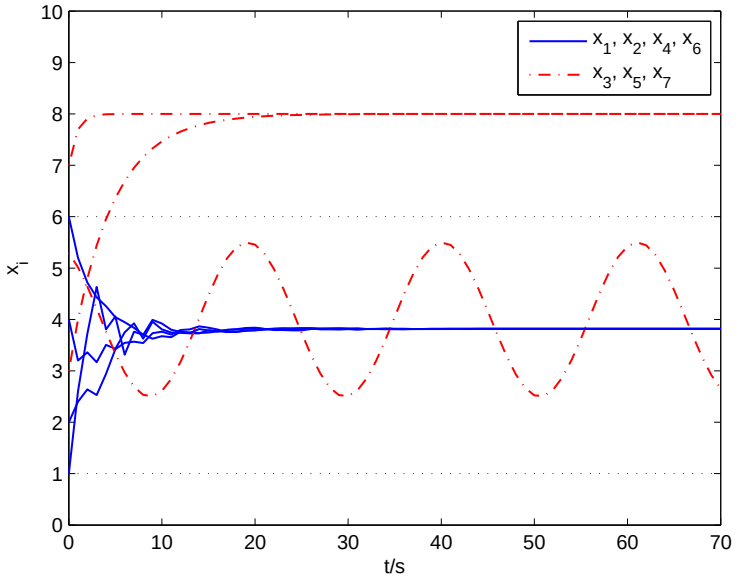


图 3.6　满足 2-稳健图系统在所提协议下各节点的状态轨迹

系统的状态轨迹如图 3.6 所示，尽管遭受 3 个恶意节点的攻击，各正常节点在

控制协议 (3.6) 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。

现在考虑将图 3.5 中节点 v_1 到节点 v_2 的输入边移除，致使正常节点间的拓扑图不再满足 2-稳健图。该情形下各节点状态轨迹如图 3.7 所示，此时恶意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 $[1, 6]$，本章所提的安全协议不再适用。

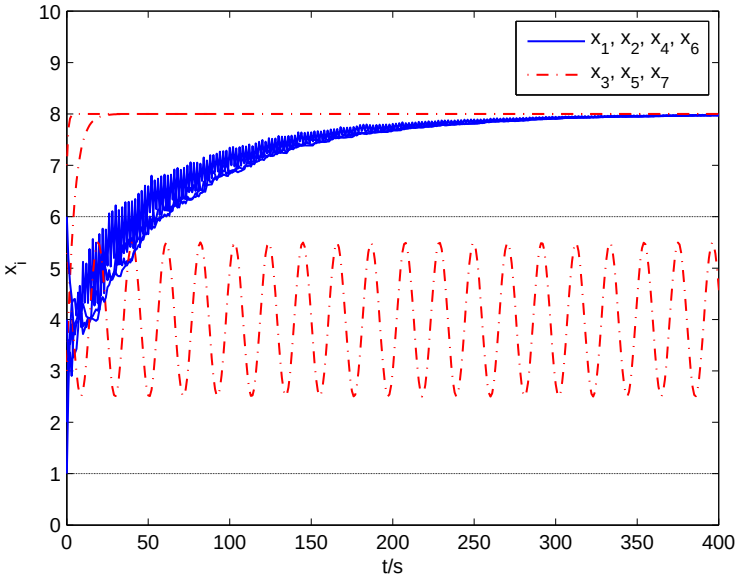


图 3.7　不满足 2-稳健图系统在所提协议下各节点的状态轨迹

此外，考虑图 3.5 中所有恶意节点放弃攻击的情况，即此刻将与恶意节点相连接的边全部移除。此时，文献 [150, 162] 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 3.8 所示.

3.4.2 实例二

考虑同样由 7 个智能体节点组成的有向网络，系统的拓扑结构如图 3.9 所示，其中 5 个为正常节点，另外 2 个为恶意节点（图中红色显示）。同样令初始值 $x(0) = [1, 2, 3, 4, 5, 6, 7]^{\mathrm{T}}$，通信步长设为 $0.1s$，时延上界取 $0.5s$。系统的安全域即为全部正常节点的初始值范围 $[1,\ 7]$。我们假定图中节点 v_3 和 v_5 为恶意节点，它们的状态方程式如下：

$$x_3(k+1) \quad = \quad -0.8x_3(k) + 0.2u_a(k),$$

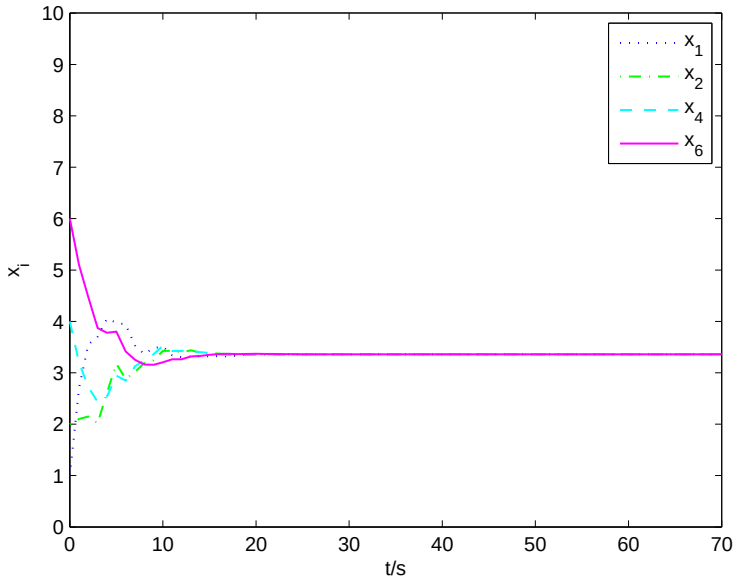


图 3.8　恶意节点暂停攻击情况下各正常节点状态轨迹

$$x_5(k+1) \quad = \quad -0.4x_5(k) + 0.4u_a(k).$$

本例中我们设定 u_a。系统的邻接矩阵如下：

$$A_{\mathcal{G}} = \frac{1}{3}\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

根据定义 3.12，我们逐一检测系统拓扑节点间的稳健性，验证图 3.9 满足 $(3,3)$-稳健。根据定理 根据定理 3.3 可知，该网络在上述稳健性能够抵御 2 个恶意节点的攻击。系统的状态轨迹如图 3.10 所图。从图中可以看到，在所提控制协议下，系统中 5 个正常节点状态始终在安全区域内 $[1,7]$ 变化，且最终实现了一致。

现在考虑将图 3.9 中节点 v_1 到节点 v_6 的输入边移除，可以检验，此时拓扑图不再满足 $(3,3)$-稳健。该情形下各节点状态轨迹如图 3.11 所示。可以看到，图中节点 v_6 的状态值被恶意节点引入至安全区域外的 10，且无法与其他正常节点保持一

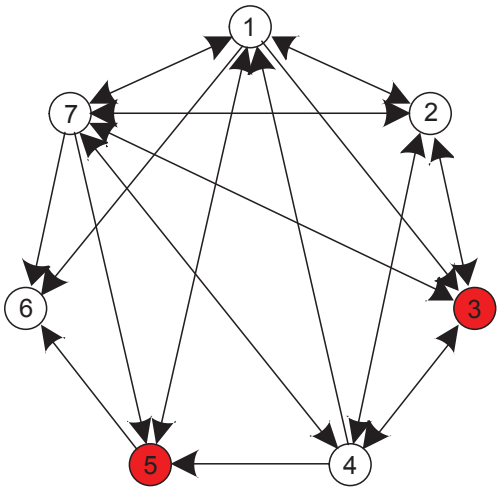


图 3.9　实例二：系统拓扑图

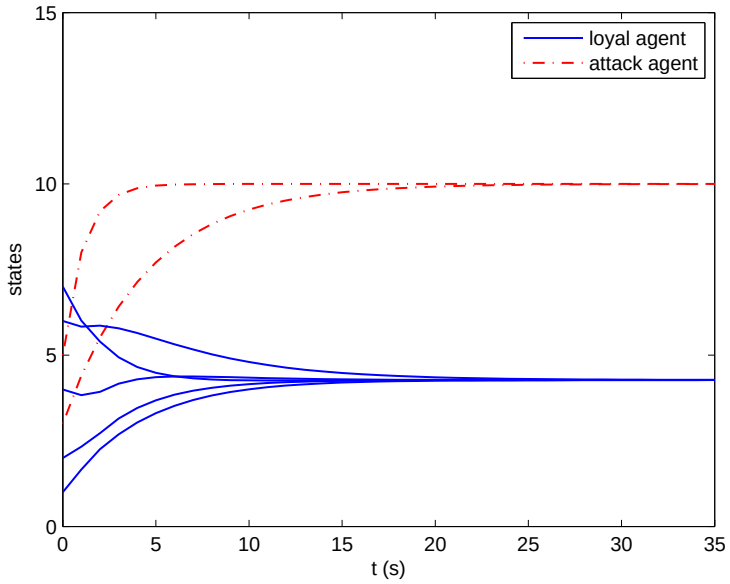


图 3.10　满足 $(3,3)$-稳健图系统在所提协议下各节点状态轨迹

致。表明在拓扑条件下本章的安全协议不再适用。

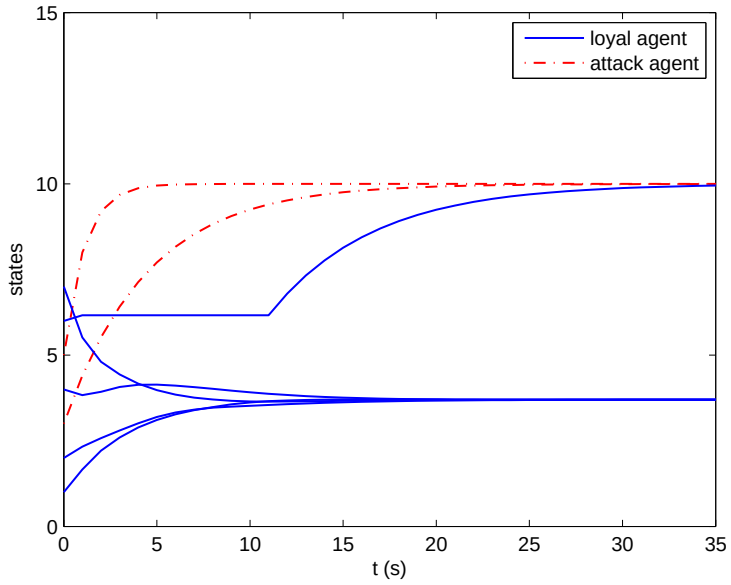


图 3.11　不满足 $(3,3)$-稳健图系统在所提协议下各节点状态轨迹

3.5 本章小结

本章节内容针对具有通信时延的一阶离散时间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分布式安全一致性算法，并基于稳健图概念，分别得到了系统拓扑结构为动态有向加权图且邻居中含有 f 个恶意节点上限的以及全局中含有 f 个恶意节点上限条件下，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有效性。

第四章　非线性动态系统的安全一致性控制

4.1　引言

我们知道，相比较线性多智能体系统的一致性协议设计，非线性多智能体系统的一致性协议设计的问题复杂和困难的多。不同的非线性对象动态特性相互间往往具有较大的差异，从而对于系统设计者而言，一般较难给出统一的设计方法。虽然研究者们已经在一致性方向开展了很多的研究工作，然而在非线性多智能体系统一致性控制领域的科研成果，还相对较少。一些很自然的问题，恶意节点的攻击行为是否会给非线性动态系统的智能体节点带来更多的不稳定因素？前面章节介绍的离散时间系统网络拓扑稳健性，是否仍然会对非线性系统适用？系统的收敛性能又会发生什么样的变化？对于一个非线性系统，要满足它的安全一致性收敛，需要对通信拓扑做哪些假设和要求？本章的主要内容将主要围绕以上几个问题针对恶意攻击下非线性动态系统的安全一致性问题进行理论分析并给出相关仿真算例来进行验证。

本章的结构安排如下：第 4.2 节对连续时间非线性动态系统在恶意攻击下的安全性问题进行了分析，建立了数学建模，并根据网络连通性条件，设计了相应的安全一致性控制协议。第 4.3 节给出了本章节的主要结论，并且给出了具体的数学分析证明。第 4.4 节通过仿真实例来验证非线性动态系统同时存在恶意节点攻击与通信时延条件下的一致性控制算法的有效性。本章的结论放在了第 4.5 节。

4.2　问题描述

同样考虑用一个有向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}},A_{\mathcal{G}}\}$ 表示一个由 n 个智能体组成的多智能体系统网络，图中每个节点代表一个智能体。不失一般性，我们将整个节点集 $\mathcal{V}$ 划分成两个子集，分别用 $\mathcal{V}_s=\{v_1,v_2,\ldots,v_{n_s}\}$ 表示包含 n_s 个正常节点的集合，$\mathcal{V}_a=\{v_{n_s+1},v_{n_s+2},\cdots,v_n\}$ 表示包含 $n_a=n-n_s$ 个恶意节点的集合。显然有，$\mathcal{V}=\mathcal{V}_s\bigcup\mathcal{V}_a$, $\emptyset=\mathcal{V}_s\bigcap\mathcal{V}_a$。对应的序号集分别为 $\mathcal{I}_s=\{1,2,\cdots,n_s\}$ 和 $\mathcal{I}_a=\{n_s+1,n_s+2,\cdots,n\}$。

考虑系统中所有正常节点采用如下一阶连续时间动态方程：

$$\dot{x}_i(t)=u_i(t),\ \ i\in\mathcal{I}_s, \tag{4.1}$$

其中 $x_i \in \mathbb{R}$ 为节点 i 的状态值，$u_i(t) \in \mathbb{R}$ 为系统控制输入，即待设计的控制协议。在网络中，我们假设邻居间相互发送的信息存在通信时延，令 $\tau_{i,j} \geq 0$ 为信息从节点 j 传递到节点 i 的通信时延，假定节点间传输的时延是不统一的，但存有一个上界值 $\bar{\tau} > 0$，即对任意 $i, j \in \mathcal{V}$，有$\tau_{i,j} \leq \bar{\tau}$。

本章我们的目的是在一个非线性连续时间的多智能体系统里，设计一个有效的控制协议 $u_i(t)$，能够使得所有的正常节点抵御网络中恶意节点的干扰，随着时间的推移，最终实现状态一致。

下面给出算法的具体步骤：

Step 1 对于一个正常节点 i，$i \in \mathcal{I}_s$，将时间 t 接收到的所有邻居传递给它的状态信息（时延信息）做一整理，使得这些信息按照数值从大到小进行排序。

Step 2 针对 Step 1 中排好的序列，从序列最大一端开始，如果有不足 k 个数严格大于自身状态值 $x_i(t)$，则节点 i 将这些大于自身状态值的数全部从该序列中移除（等同于切断该时刻相应信息的输入边）。否则，移除序列中从最大一端开始的前 k 个数。同样的，如果序列中不足 k 个数严格小于自身状态值 $x_i(t)$，节点 i 将这些小于自身状态值的数全部从序列中移除（等同于切断该时刻相应信息的输入边）。否则，移除序列中从最小一端开始的前 k 个数。

Step 3 由于 Step 2 中对邻居信息值的删减，即暂时切断输入边的操作，可能导致整个网络拓扑成为一个时变的拓扑，此时我们用 $\mathcal{G}_{\sigma(t)} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}, A_{\sigma(t)}\}$ 表示。这时，如果 $a_{i,j}(t) > 0$，则节点 j 称作节点 i 在时间 t 的邻居，用 $\mathcal{N}_i(\sigma(t))$ 表示节点 i 在时间 t 的邻居集。

结合上述操作，给节点 i 设计如下一致性协议：

$$u_i(t) = \sum_{j \in \mathcal{N}_i(\sigma(t))} a_{i,j}(t) f_{i,j}(x_j(t - \tau_{i,j}), x_i(t)),\ i \in \mathcal{I}_s. \tag{4.2}$$

其中，$a_{i,j}(t) \in \mathbb{R}$ 是相应边 (j, i) 的权重，$f_{i,j}(\cdot)$ 为非线性动态函数。

注 4.1: 注意到，上述所提算法具有较低的复杂度并且只需用局部节点信息即可完成系统安全控制要求。这样的优点是节点只需消耗较少的计算量和存储资源，这对于一个资源十分有限的大型分布式控制系统来说显得至关重要。同时我们也注意到，相对于传统的安全一致性算法，所提算法中不再需要知道网络的全局拓扑信

息，仅需要知道每个正常节点邻居中恶意节点数目的上限即可。但鉴于所提算法的简易轻便，就无法期望算法能够彻底地去除所有恶意节点的信息。

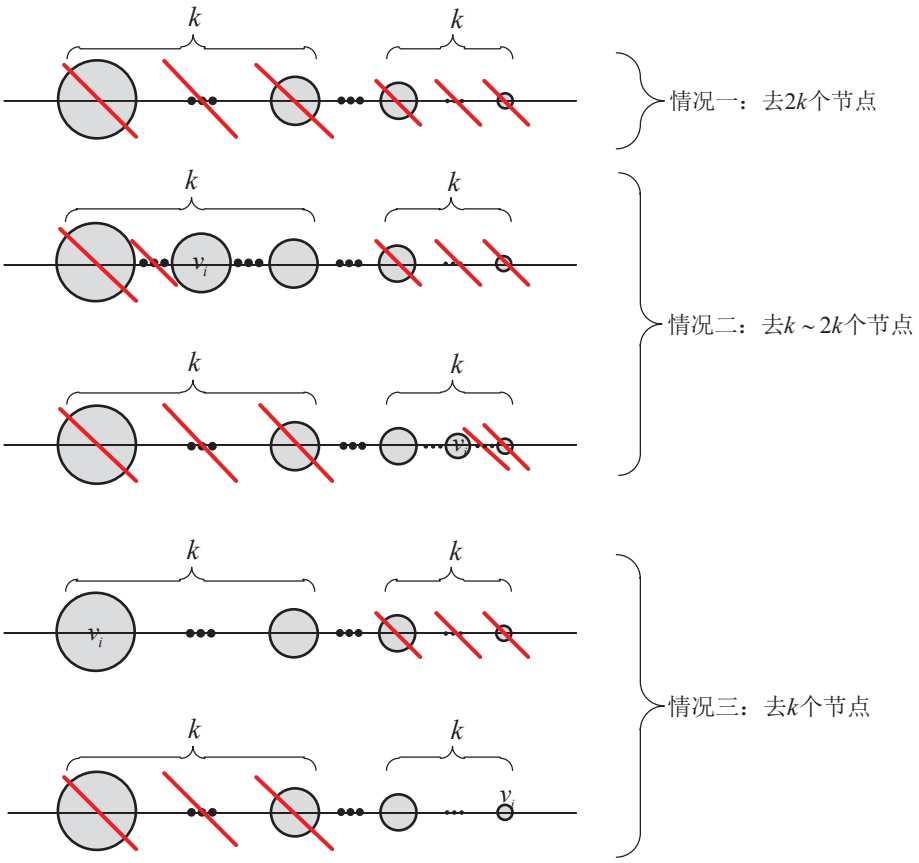


图 4.1　算法中节点删减信息个数的情况示意图

在本章节的讨论中，我们给出如下条件假设：

假设 4.1: 给出一非线性函数 $f_{i,j}(\mathbb{R}\times\mathbb{R})\to\mathbb{R}$，使其满足下列条件：

1. $f_{i,j}$ 具有连续映射且满足局部利普希茨条件；
2. $f_{i,j}(x,y)=0\Leftrightarrow x=y$；
3. 当 $x\neq y$ 时，$(x-y)f_{i,j}(x,y)>0$。

假设 4.2: 存在两个大于零的实数 $a^*>0$，$a_*>0$，满足$a_*\leq a_{i,j}(t)\leq a^*,(j,i)\in\mathcal{E}_{\sigma(t)}$，否则 $a_{i,j}(t)=0$。

假设 4.3: 在每两次转换时间中，存在一个间隔时间下限值 $\tau_D > 0$，令 $\{t_k\}_{k\in\mathbb{N}}$ 表示转换时间 $\sigma(t)$，满足 $t_{k+1} - t_k \geq \tau_D$。

在本章节中，我们假设条件 4.1、4.2 和 4.3 始终成立。结合控制协议（4.2），系统（4.1）的闭环形式可表述成

$$\begin{cases} \dot{x}_i(t) = \sum\limits_{j\in\mathcal{N}_i(\sigma(t))} a_{i,j}(t) f_{i,j}(x_j(t-\tau_{i,j}), x_i(t)),\ i \in \mathcal{I}_s,\ t > 0, \\ x_i(\varphi) = \varphi_i(t),\ t \in [-\bar{\tau}, 0]. \end{cases} \tag{4.3}$$

根据协议 (4.2) 中的算法描述，我们可以发现，每个正常节点能够在它接收到的信息中至多移除 $2k$ 个值。但是，当恶意节点发送的值处于正常节点初始值的最小值与最大值之间时，即本章节定义的安全区域内时，这可能会使得我们的算法无法移除该值，导致正常节点在更新自身值的时候采用该恶意节点的值。于是我们给出以下定义：

定义 4.1: 对于恶意节点 q，$q \in \mathcal{I}_a$，如果在时间 t 它发送的状态值没有被协议 (4.2) 移除，则称该恶意节点是临时温和的。此时，该值可以用所有正常节点的状态（时延状态）的线性组合表述，即

$$x_q(t) = \sum_{j\in\mathcal{I}_s} \varphi_{p,j}(t) x_j(t+\theta),\ q \in \mathcal{I}_a \cap \mathcal{N}_i(\sigma(t))\theta \in [-\bar{\tau}, 0], \tag{4.4}$$

其中 $0 \leq \varphi_{p,j}(t) \leq 1$，$\sum_{j\in\mathcal{I}_s} \varphi_{p,j}(t) = 1$。

值得注意的是，临时温和节点 q 的值对于协议中不同的正常节点 p，$p \in \mathcal{I}_s$，$x_q(t)$ 会有不同的组合形式，事实上可以有无穷多种，这时我们只需随意选取一种。

为了便于表述，对于在 t 时刻更新时不包含恶意节点信息的正常节点 p，设定 $\varphi_{p,j}(t) = 0,\ j \in \mathcal{I}_s$。

定义所有正常节点中在时间 t 时的最大值和最小值分别为

$$V_M(t) = \max_{i=1,2,\ldots,n_l} x_i(t),\ V_m(t) = \min_{i=1,2,\ldots,n_l} x_i(t). \tag{4.5}$$

令 $V_M(\varphi) = \sup_{0<\theta<\bar{\tau}} \max_{i\in\mathcal{I}_s} x_i(\theta) = \gamma^+$ 和 $V_m(\varphi) = \inf_{0<\theta<\bar{\tau}} \min_{i\in\mathcal{I}_s} x_i(\theta) = \gamma^-$ 分别为所有正常节点初始时刻的最大值和最小值，于是我们有如下定义。

定义 4.2: 在存在有界通信时延 $\{\tau_{i,j},\ i\in\mathcal{I}_s,\ j\in\mathcal{N}_i\}$ 情形下，如果系统 (4.1) 满足下列条件：

$$V_m(\varphi)\leq\inf_{t\geq0}\min_{i\in\mathcal{I}_s}x_i(t)\leq\sup_{t\geq0}\max_{i\in\mathcal{I}_s}x_i(t)\leq V_M(\varphi), \tag{4.6}$$

$$\lim_{t\to\infty}\left(x_i(t)-x_j(t)\right)=0,\ \forall i,j\in\mathcal{I}_s. \tag{4.7}$$

则称系统实现安全一致。

在定义 4.2 中，条件 (4.6) 称为安全性条件，它确保所有正常节点的状态值时刻处于给定的安全区域内，该条件等同于对任意 $t\geq0, V_m(t)\geq\gamma^-$，$V_M(t)\leq\gamma^+$。在另一方面，条件 (4.7) 称为一致性条件，它则保证了所有正常节点最终的状态值趋于相同，即 $x_i=x_j$，$\forall i,j\in\mathcal{I}_s$。

4.3 主要结果

在这一节中，我们首先介绍一些的需要用到的拓扑属性，然后通过构造 Lyapunov-Krasovskii 函数以及 Barbalat-like 分析方法来证明所设计算法的收敛性质。

下述定义与第三章节中介绍的定义相近，我们针对连续时间系统，稍做了适当的修改。

定义 4.3: （r-可得集）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 $|\mathcal{N}_i\setminus\mathcal{S}|\geq r$，$r\in\mathbb{Z}^+$。称集合 $\mathcal{S}$ 为 r-可得集。

同样地，我们给出在连续时间下 r-稳健图的定义。

定义 4.4: （r-稳健图）对于一个有向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_\mathcal{G}\}$，如果 $\mathcal{V}$ 在任意时刻取任意一对划分子集，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 $|\mathcal{N}_i\setminus\mathcal{S}_\kappa|\geq r$，$r\in\mathbb{Z}^+$，则称图 $\mathcal{G}$ 为 r-稳健图。

引理 4.1: 令 $\mathcal{G}$ 是满足 r-稳健的有向图，$\mathcal{G}'$ 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 $(r-s)$-稳健的。

引理 4.2: 令 $\mathcal{G}$ 是有向图，则 $\mathcal{G}$ 包含一棵生成树，当且仅当 $\mathcal{G}$ 是 1-稳健的。

引理 4.3: 假设在 k-局部攻击模型下，每个正常节点i，$i \in \mathcal{I}_s$，根据协议 (4.2) 更新自身状态值，那么对所有 $t \geq -\bar{\tau}$，都有$x_i(t) \in [\gamma^-, \gamma^+]$，且与网络通信时延和拓扑均无关。

证明: 首先我们证明 $x_i(t) \leq \gamma^+$。从给定的初始条件可知，对于 $\theta \in [-\bar{\tau}, 0]$，都有 $x_i(\theta) \leq \gamma^+$成立。接下去我们用反证法进行证明。假设在时间 t^* 时，上述条件不再成立。那么当发生这个情况时，我们有：对所有 $i \in \mathcal{I}_s$的节点，在$t \in [-\bar{\tau}, t^*]$时间段，有$x_i(t) \leq \gamma^+$; 在时间 t^* 时，存在一个节点 $i \in \mathcal{I}_s$，其满足 $x_i(t^*) = \gamma^+$，$\dot{x}_i(t^*) > 0$。假设这样的节点 i 存在，该时刻其动态方程为

$$\dot{x}_i(t^*) = \sum_{j \in \mathcal{N}_i(\sigma(t))} a_{i,j}(t) f_{i,j}(x_j(t^* - \tau_{i,j}), x_i(t^*)),\ i \in \mathcal{I}_s.$$

由于 $x_i(t^*) = \gamma^+ \geq x_j(t^* - \tau_{i,j})$，$a_{i,j}(t) > 0$，从上式可以观察到，等式右边累和的各项都是小于等于零的，因此，可推得$\dot{x}_i(t^*) \leq 0$，而这与上述假设 $\dot{x}_i(t^*) > 0$ 矛盾。同样地，可以用上述分析方法证明 $x_i(t) \geq \gamma^-$ 成立。即结论得证。

根据初始条件 $\varphi \in \mathcal{C}_{\mathbb{D}} = \mathcal{C}([-\bar{\tau}, 0], \mathbb{D})$，$\mathbb{D}$ 的吸引域为：

$$\mathbb{D} = \{x \in \mathbb{R}^{n_l} : \gamma^- \leq x_i \leq \gamma^+\} \tag{4.8}$$

由引理 4.3 可知，$\mathcal{C}_{\mathbb{D}}$ 是一个关于系统 （4.1） 的正不变集。

考虑如下 Lyapunov-Krasovskii 泛函方程：

$$\bar{V}(x_t) = \bar{V}_M(x_t) + \bar{V}_m(x_t), \tag{4.9}$$

其中

$$\bar{V}_M(x_t) = \max_{\theta_1 \in [0, \bar{\tau}]} V_M(x(t - \theta_1)), \tag{4.10}$$

以及

$$\bar{V}_m(x_t) = -\min_{\theta_2 \in [0, \bar{\tau}]} V_m(x(t - \theta_2)). \tag{4.11}$$

由于拓扑是时变的，$\bar{V}(x_t)$ 虽然连续，但不一定连续可导。然而，我们可以通过分析 $\bar{V}(x_t)$ 的狄尼导数来研究它的收敛性质。用特定的下标 I，J 表示满足方程

$x_I(t) = \max_{i\in\mathcal{I}_s} x_i(t)$，$x_J(t) = \min_{i\in\mathcal{I}_s} x_i(t)$ 的节点，如果满足条件的节点有多个，则考虑选取这些节点中导数值最大的一个，如果仍有多个满足条件的节点，则就任意选取一个。但我们用固定的 I 和 J 表示满足极值条件的这类节点。

现在我们给出主要结论。

定理 4.1: 考虑时延通信下的多智能体系统 (4.1)，令 $\bar{\tau} = \max_{i,j=1,\ldots,N}\tau_{i,j}$，通信拓扑满足 $(2k+1)$-稳健图，假设每个正常节点在 k-局部有界攻击模型下，采用协议（4.2）更新自身状态值，那么系统的状态值最终能够实现安全一致。

证明： 根据引理 4.3，可知包含所有正常节点状态值的集合为一个正不变集，从而可知对于任意 $i \in \mathcal{I}_s$，$x_i(\varphi)(t)$ 有界，这保证了安全性条件 (4.6) 成立。

接下去，我们证明一致性条件 (4.7) 同样成立。对任意 $p \in \mathcal{P}$，令 $t' = t - \theta_1$，$t'' = t - \theta_2$，根据引理 $\bar{V}_M(x_t)$，$\bar{V}_m(x_t)$ 关于系统（4.3）的右上狄尼导数为

$$D^+\bar{V}_M(x_t) = \dot{x}_I(t') = \sum_{j\in\mathcal{N}_I(\sigma(t'))} a_{I,j} f_{I,j}(x_j(t'-\tau_{I,j}), x_I(t')),\ I \in \mathcal{I}_s, \tag{4.12}$$

$$D^+\bar{V}_m(x_t) = -\dot{x}_J(t'') = -\sum_{j\in\mathcal{N}_J(\sigma(t''))} a_{J,j} f_{J,j}(x_j(t''-\tau_{J,j}), x_J(t'')),\ J \in \mathcal{I}_s. \tag{4.13}$$

合并式（4.12）和式（4.13），可得

$$\begin{aligned} D^+\bar{V}(x_t) &= D^+\bar{V}_M(x_t) + D^+\bar{V}_m(x_t) \\ &= \dot{x}_I(t') - \dot{x}_J(t'') \\ &= \sum_{j\in N_I(\sigma(t'))} a_{I,j} f_{i,j}(x_j(t'-\tau_{I,j}), x_I(t')) \\ &\quad - \sum_{j\in N_J(\sigma(t''))} a_{J,j} f_{i,j}(x_j(t''-\tau_{J,j}), x_J(t'')). \end{aligned} \tag{4.14}$$

显然，直接计算 $\bar{V}_M(x_t)$ 和 $\bar{V}_m(x_t)$ 右上狄尼导数是十分困难的。对此，我们可以通过分析这两个函数的各种可能情况来判定它们的右上狄尼导数都是小于等于零的。这里只讨论分析 $D^+\bar{V}_M(x_t)$ 的情况，对于 $D^+\bar{V}_m(x_t)$，可用同样的方法讨论分

析，此处不再赘述。令 $t^* \in [t-\bar{\tau}, t]$ 满足

$$x_I(t^*) = \max_{\theta\in[0,\bar{\tau}]} \max_{i\in\mathcal{I}_s} x_i(t-\theta). \tag{4.15}$$

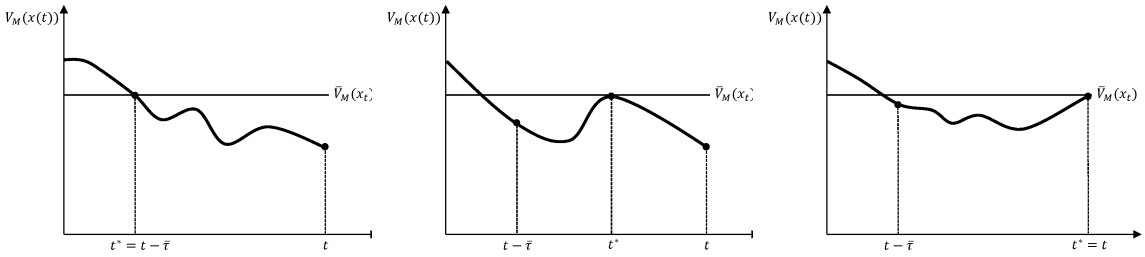


图 4.2　$D^+\bar{V}_M(x_t)$ 出现的 3 种情况

1）当 $t^* = t-\bar{\tau}$ 时：

$D^+\bar{V}_M(x_t) < 0$ 当且仅当，$t^* = t-\bar{\tau}$ 时，满足式（4.15），当 $t^* \in (t-\bar{\tau}, t)$ 时，不满足式（4.15），见图 4.2(a)。

2) 当 $t^* \in (t-\bar{\tau}, t)$ 时：

$D^+\bar{V}_M(x_t) = 0$ 当且仅当存在一个时间 $t^* \in (t-\bar{\tau}, t)$ 满足式（4.15），见图 4.2(b)。

3）当 $t^* = t$ 时：

在这种情况下，$D^+\bar{V}_M(x_t)$ 的值可能无法直接断定，见图 4.2(c)。然而在这个时间点上，我们知道 $x_I(t^*) = x_I(t) \geq x_j(t-\tau_{I,j})$。看到式 (4.12) 等号右边的每一项都是小于等于零的，因此可以得出 $D^+\bar{V}_M(x_t) \leq 0$。

对以上 $D^+\bar{V}_M(x_t)$ 所有可能出现的情况经过分析讨论，可以得出 $D^+\bar{V}_M(x_t) \leq 0$。

接下来，我们将通过运用 Barbalat-like 分析方法，证明当 t 趋于无穷时，$D^+\bar{V}(x_t) \to 0$。假设上述结论不成立，那么存在一个正标量 ε_0，满足对于任意 $T > 0$，存在一个时间 $t > T$，使得 $D^+\bar{V}(x_t) \leq -\varepsilon_0$（由之前的分析注意到 $D^+\bar{V}(x_t) \leq 0$）。因此，存在一个正标量 δ_0 和一个递增的时间序列 $\{t_i\}_{i\in\mathbb{N}}$，序列中随着 $i \to \infty$，$t_i \to \infty$，于是对于所有 i，有 $D^+\bar{V}(x_t) \leq -\varepsilon_0$，$|t_{i+1} - t_i| > \delta_0$。考虑任一时间区间 Δt，其中 $D^+\bar{V}(x_t)$ 在该区间是连续的，即对于所有 i，$t_k \notin \Delta t$。假设 4.1 和 4.2 保证了 $\dot{x}_i(t)$ 有界和 $D^+\bar{V}(x_t)$ 一致连续。于是，存在 $\delta_1 > 0$，使下列不

等式

$$\left|D^+\bar{V}(x_{t'}) - D^+\bar{V}(x_{t''})\right| < \frac{\varepsilon_0}{2}$$

对满足 $|t' - t''| < \delta_1$ 的任意 t'，t'' 成立。由此可知，对于任意在 t_i 的 δ_1-领域内的 t，即当 $t \in [t_i - \delta_1 t_i + \delta_1]$ 时，有

$$\begin{aligned} D^+\bar{V}(x_t) &= -\left|D^+\bar{V}(x_{t_i}) - (D^+\bar{V}(x_{t_i}) - D^+\bar{V}(x_t))\right| \\ &\leq -(\left|D^+\bar{V}(x_{t_i})\right| - \left|D^+\bar{V}(x_{t_i}) - D^+\bar{V}(x_t)\right|) \\ &\leq -\varepsilon_0 + \frac{\varepsilon_0}{2} \\ &= -\frac{\varepsilon_0}{2}. \end{aligned}$$

接下来，讨论 t_i 处于不连续的时间点 t_k 的右侧情况。此时，$D^+\bar{V}(x_t)$ 可能在 t_k 时刻出现递增的情况，因此在当 $t_k \in [t_i - \delta_1, t_i + \delta_1]$ 时，结论 $D^+\bar{V}(x_t) \leq -\varepsilon_0/2$ 无法再保证成立。然而，通过假设 4.3 可知，在下一个不连续点出现之前，存在一个驻留时间 τ_D。于是，存在一个 $\delta_2 \in (0, \tau_D)$，对于所有 $t \in [t_k, t_k + \delta_2]$，满足 $D^+\bar{V}(x_t) \leq -\varepsilon_0/2$。通过两边积分，可得到

$$\begin{aligned} \int_0^\infty D^+\bar{V}(x_t)\mathrm{d}t &\leq \lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} D^+\bar{V}(x_t)\mathrm{d}t \\ &\leq -\lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} \frac{\varepsilon_0}{2}\mathrm{d}t \\ &= -\lim_{N\to\infty} N\varepsilon_0\delta \\ &= -\infty, \ \delta \in \min\{\delta_1, \delta_2\}. \end{aligned}$$

这明显与上述 $\bar{V}(x_t) \geq 0$，$\forall t$ 相矛盾。于是，当 $t \to \infty$ 时，我们有

$$D^+\bar{V}(x_t) \to 0. \tag{4.16}$$

从而推得 $\lim_{t\to\infty}\bar{V}(x_t)$ 为一个固定的常数，即在所有正常节点中，含最大值的节点和最小值的节点的状态保持固定值，不再发生变化。这时我们可定义一个常数 α，令当 $t \to \infty$ 时，$\bar{V}_M(x_t) = x_I(t') = \alpha$。由于网络拓扑满足 $(2k+1)$-稳健图，通过引理 4.1 和引理 4.2 可知，此时图中包含一棵有向生成树。因此，从生成树的根节点出发达到节点 I 的路径中的所有节点具有相同的状态 α，凡是不在该路径的其他节

点拥有小于等于 α 的状态值。同样的方法，可知从该根节点出发达到节点 J 的路径中的所有节点具有相同的最小状态值 β，凡是不在该路径的其他节点拥有大于等于 β 的状态值。这样，该根节点必需保证同时具有最大值和最小值，显然只能有 $\alpha=\beta$ 成立。 证明完毕。

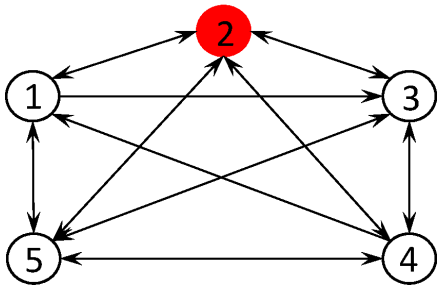


图 4.3 5 个节点组成的有向图

4.4 仿真实例

本节中，我们通过一个实例，借此来验证上述理论的有效性。考虑一个有 5 个多智能体组成的有向多智能体系统网络，其中包含 1 个恶意智能体（红色），其他 4 个为正常智能体。在 $\varphi\in[-\bar{\tau},0]$ 时，令它们的初始值分别为 $x_1(\varphi)=5$，$x_2(\varphi)=4$，$x_3(\varphi)=3$，$x_4(\varphi)=2$，$x_5(\varphi)=1$，假设时延上界 $\bar{\tau}$ 为 1 秒。为描述理论 4.1，令系统的通信网络满足 3-稳健图，参见图 4.3。令 $\tau_{1,2}=\tau_{1,4}=\tau_{1,5}=0.4s$，$\tau_{3,2}=\tau_{3,4}=\tau_{3,5}=0.5s$，$\tau_{4,1}=\tau_{4,2}=\tau_{4,3}=\tau_{4,5}=0.6s$，$\tau_{5,1}=\tau_{5,2}=\tau_{5,3}=\tau_{5,4}=0.7s$。为验证拓扑满足 3-稳健图，我们通过逐一检查每一对非空的划分子集，保证每对子集中至少一个子集中的 1 个元素在另一个子集中有不少于 3 个邻居数。本例中令非线性函数 $f_{i,j}(x,y)=\arctan(x-y)$，即该函数 $f_{i,j}(\cdot)$ 满足局部 Lipschitz 条件。假设标号为 2 的智能体（红色）是恶意智能体，它的状态更新方程设计为

$$\dot{x}_2(t)=-0.7x_2(t)+0.7u,$$

其中令控制输入 $u=8$。当 $j\in\mathcal{N}_i(\sigma(t))$，令加权邻接矩阵 $A(t)=[a_{i,j}(t)]\in\mathbb{R}^{n\times n}$ 如

下

$$A(t)=\begin{bmatrix} 0 & 2 & 0 & 1 & 3 \\ 1 & 0 & 2 & 2 & 1 \\ 1 & 3 & 0 & 2 & 3 \\ 0 & 1 & 3 & 0 & 1 \\ 2 & 2 & 3 & 1 & 0 \end{bmatrix},$$

否则，$a_{i,j}(t)=0$。

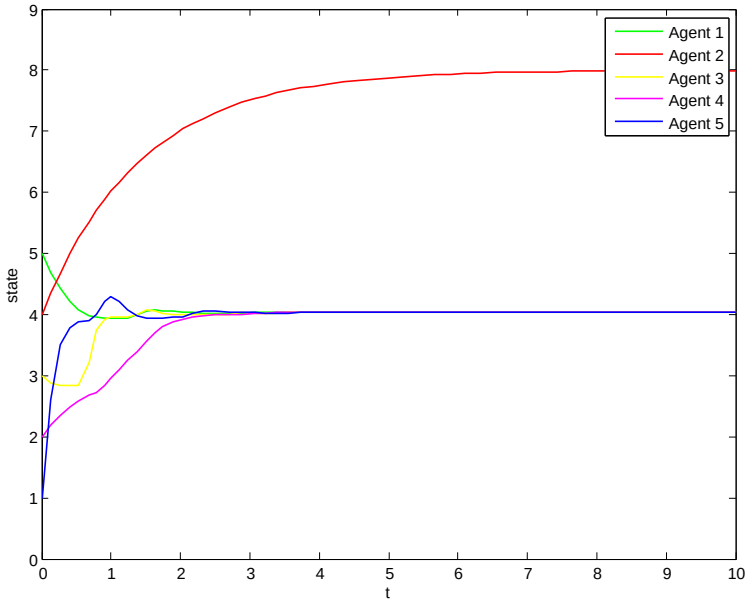


图 4.4　所提协议下系统各节点的状态轨迹图

由于网络拓扑满足 3-稳健图，所以由定理 4.1 可知，在周围邻居数不超过 1 个恶意智能体情况下，系统中所有正常智能体最终能够实现安全一致。系统的状态轨迹见图 4.4，从中可以看到，4 个正常智能体渐进地取得了一致状态值。尽管恶意智能体 2 试图诱导其他智能体到达一个安全区域 $[1,5]$ 外的状态值 8，不过在本章设计的协议 (4.2) 下，恶意智能体的目标没能实现。除此之外，图 4.5 是本章设计的算法在含恶意节点和不含恶意节点两种情况下的状态轨迹图。可以看出，在不包含恶意智能体的网络中，系统的一致性收敛速度更快一些。

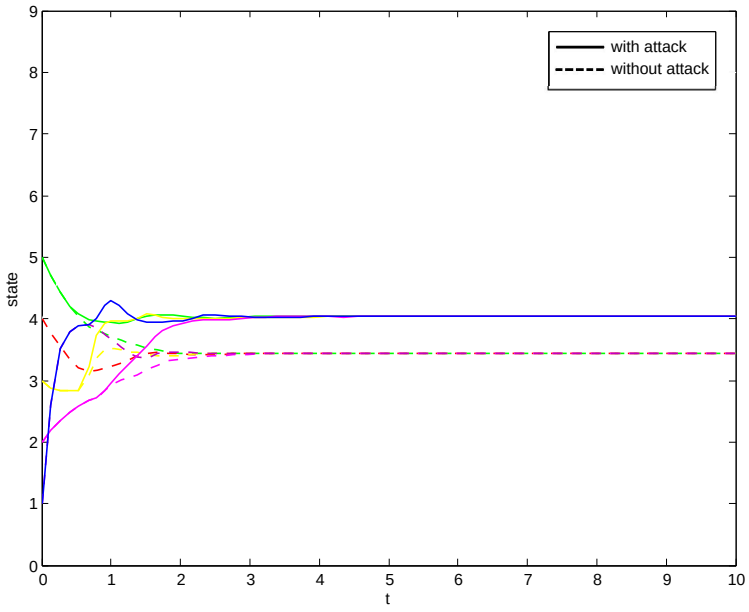


图 4.5　在有攻击和无攻击下的系统状态轨迹

4.5 本章小结

本章节我们考虑了非线性连续时间多智能体系统在恶意攻击下的安全一致性问题。传统的方法，如 Lyapunov 分析法以及 Barbalat 引理，无法直接应用于遭遇攻击下的非线性动态系统的收敛性分析。结果表明，如果网络拓扑满足 $(2k+1)$-稳健图，那么对于通信时延一致有界的多智能体系统，在本章所设计的控制协议下，能够在遭受邻居中至多含有 k 个恶意节点攻击的情况下实现安全一致。

第五章　有限时间安全一致性控制

5.1　引言

前面的章节，我们分别研究了线性离散系统和非线性连续系统下的多智能体系统一致性控制的安全性问题，分别设计给出了相应的安全一致性协议。本章研究在恶意攻击下多智能体系统的有限时间安全一致性控制问题。

有限时间一致性是指系统中的智能体状态在有限的时间内收敛并停留在一个相同的状态空间上。它是关心一致性算法收敛速度的问题。我们知道，收敛速度是衡量系统性能的一项重要指标之一。此外，有限时间收敛系统，在处理系统干扰和对不确定性的鲁棒能力上具有更优良的表现[108]。因此，如何在有限时间内达到系统一致性越来越成为研究者人员的一个研究热点。

迭代学习控制（Iterative Learning Control，ILC）作为处理有限区间 $[0,T]$ 内重复运行系统控制问题的最有效控制方法之一，其核心思想是通过利用上次或者上几次运行的误差、控制输入的特点，修正本次的控制器参数，逐渐提高受控系统的控制精度，以求达到完美的控制效果。

将迭代学习控制技术引入多智能体系统作为一个新的研究领域，目前相关的研究文献还比较少。文献 [168] 首次将迭代学习控制方法引入到非线性多智能体系统编队控制问题当中，通过设立智能体之间相对位置的状态轨迹为参考轨迹，提出了一种新的控制策略。而文献 [169] 的作者通过构造 PD-型学习律，解决了在初始误差条件下的多智能体系统领导者-跟随者跟踪问题。文献 [170] 研究了高阶多智能体系统一致性跟踪问题，在网络中仅有部分智能体能获知参考轨迹的前提下，提出一种新的分布式自适应迭代学习控制方法。文献 [171] 从二维系统（即时间维度和迭代维度）的视角分析了多智能体系统有限时间一致性问题，研究结果表明，只要选取适当的学习增益，则有向网络中所有智能体在作者提出的迭代学习协议作用下，能够有限时间内实现状态一致。此外，作者通过进一步改进该控制协议，证明了只要通过对部分节点事先给定期望的输出值，那么系统在该协议下所有节点则在有限时间内一致收敛到上述期望输出值。随后，根据最近邻居原则，作者将上述研究成果扩展到了符号有向网络[173]。

在文献 [172] 中，作者针对现有文献大多单独设计连续和非连续有限时间一致性协议，提出一种可同时处理连续和非连续两种情况的集中式可切换一致性协议，

且能够实现较快的收敛速度。

本章考虑了在恶意攻击条件下多智能体系统的有限时间一致性问题。同样，我们将网络中节点分为两类，即正常节点和恶意节点，然后，设计了一种与安全机制相结合的迭代学习一致性控制协议，我们通过分析网络拓扑连通性和迭代学习控制参数，得到了实现有限时间一致性收敛的条件。

本章后续内容主要安排如下：第 5.2 节对多智能系统在恶意攻击下的一致性问题进行建模，并根据迭代学习控制方法，设计了相应的有限时间安全一致性协议。第 5.3 节给出了本章节的主要结论，并且给出了具体的数学分析证明。第 5.4 节通过仿真实例来验证所提算法遭遇恶意节点攻击下实现有限时间安全一致的有效性。第 5.5 节总结本章的内容。

5.2 问题描述

考虑包含有 N 个智能体组成的系统，其中含有 n 个正常节点和 $m = N - n$ 个恶意节点。系统中每个智能体由定向图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}, A\}$ 中的相应的一个节点表示。我们用 $\mathcal{V}_n$ 和 $\mathcal{V}_m$ 分别表示正常节点和恶意节点的集合。显然地，$\mathcal{V}_n \cup \mathcal{V}_m = \mathcal{V}$ 以及 $\mathcal{V}_n \cap \mathcal{V}_m = \emptyset$。

令 $k \in \mathbb{Z}^+$ 表示迭代次数。对于每个正常节点。在第 k 次迭代中，我们考虑正常节点 i 遵循如下动力学方程：

$$\dot{x}_{k,i}(t) = u_{k,i}, \ \ i \in \mathcal{V}_n \tag{5.1}$$

其中，$t \in [0, T]$，$T > 0$ 表示每一轮迭代的执行时间，$x_{k,i}(t) \in \mathbb{R}$ 表示节点 i 的状态值，$u_{k,i} \in \mathbb{R}$ 表示待设计的控制输入。

本章中恶意节点的目的与前述章节一致，其主要目标是破坏系统中正常节点实现状态一致的进程。同时我们假定恶意节点知晓整个网络的拓扑结构，并且不遵循控制规律 u_k 来更新自身状态值，相反地，它能随意改变自身状态，并将这些虚假状态信息传递给周围邻居节点。

对于网络中每个正常节点，我们假设每个正常节点的邻居集中至多存在 f 个恶意节点邻居。并将此攻击模型称作“f-局部攻击模型”。

结合上述给出的攻击模型，我们给出有限时间安全一致性的定义。定义第 k 轮

中所有正常节点中最大和最小的状态值值如下：

$$M_k(t) = \max_{i\in\mathcal{V}_n} x_{k,i}(t),\ \ m_k(t) = \min_{i\in\mathcal{V}_n} x_{k,i}(t). \tag{5.2}$$

令 $M_0 = \max_{i\in\mathcal{V}_n} x_{i0}$ 和 $m_0 = \min_{i\in\mathcal{V}_n} x_{i0}$ 分别为初始条件下正常节点中最大和最小状态值。

接下去，我们给出如下有限时间安全一致性定义：

定义 5.1: （有限时间安全一致性）对于多智能体系统 (5.1)，如果系统同时满足以下两个条件：

$$x_{k,i}(t) \in [m_0, M_0], t \in [0, T], \forall i \in \mathcal{V}_n, \tag{5.3}$$

$$\lim_{k\to\infty} [x_{k,i}(T) - x_{k,j}(T)] = 0,\ \forall i, j \in \mathcal{V}_n. \tag{5.4}$$

则称系统实现有限时间安全一致。

在定义 5.1 中，条件（5.3）保证了所有正常节点的状态值在任意时刻都处于一个安全区域（本章给定为初始状态值凸集中）内变化；另一方面，条件（5.4）则保证了所有正常节点随着迭代次数的增加，最终在给定时间 T 内趋于一致，即 $x_{k,i}(t) = x_{k,j}(t)$，$\forall i, j \in \mathcal{V}_n$，当 $t > T, k \to \infty$。

本章中，我们的目标是设计控制器 $u_{k,i}$，使得系统中所有的正常节点，根据自身和邻居的状态信息作为输入，并通过不断地迭代学习更新控制律，能够抵御恶意节点的攻击并在给定的有限时间内实现状态一致。

现在我们对本章所提控制算法给出其具体描述：在第 k 轮迭代时，正常节点获取 t 时刻周围邻居节点发送给它的状态信息，用集合 $\Theta_k(t) = \{x_{k,j}(t)|j \in \mathcal{N}_i\}$ 表示，然后将这些得到的信息值按照数值从大到小进行排列，记为列表 $\mathcal{L}_i$。如果有不少于 f 个值严格大于节点 i 的自身状态值 $x_{k,i}(t)$，那么节点 i 将列表 $\mathcal{L}_i$ 前数 f 个值去除；否则，去除 $\mathcal{L}_i$ 中所有比 $x_{k,i}(t)$ 大的数值；同样地，如果有不少于 f 个值严格小于节点 i 的自身状态值 $x_{k,i}(t)$，那么节点 i 将列表 $\mathcal{L}_i$ 后数 f 个值去除；否则，去除 $\mathcal{L}_i$中所有比 $x_{k,i}(t)$ 小的数值。被上述操作去除的状态值，我们用集合 $\mathcal{R}_{k,i}(t)$ 表示。

对正常节点 i 给出如下迭代学习协议：

$$u_{k+1,i} = u_{k,i} + \gamma_i \sum_{j=0}^{n} a_{i,j}\phi_{i,j}(T)[x_{k,j}(T) - x_{k,i}(T)], i \in \mathcal{V}_n \tag{5.5}$$

其中，$a_{i,j} \in \mathbb{R}$ 表示边 (j,i) 的权重，$\gamma_i > 0$ 表示待定的学习增益，$\phi_{i,j}$ 是过滤函数，满足当邻居节点 j 的发送的数值被 i 接受并保留时，取值为 1, 否者，取零值。

通过式（5.1），可推得 $x_{k,i}(t) = x_{k,i}(0) + tu_{k,i}$。再由初始设定条件，即 $x_{k,i}(0) = x_{i0}$，$\forall k \in \mathbb{Z}^+$可知，正常节点 i 在限定时刻 T 时满足

$$\begin{aligned} x_{k+1,i}(T) &= x_{k,i}(T) + [x_{k+1,i}(T) - x_{k,i}(T)] \\ &= x_{k,i}(T) + [x_{k+1,i}(0) - x_{k+1,i}(0)] \\ &\quad + T(u_{k+1,i} - u_{k,i}) \\ &= x_{k,i}(T) + T(u_{k+1,i} - u_{k,i}). \end{aligned} \tag{5.6}$$

通过观测式 (5.5)，由式 (5.6) 可直接推得

$$x_{k+1,i}(T) = x_{k,i}(T) + T\gamma_i \sum_{j=0}^{n} \phi_{i,j}(T) \times a_{i,j}[x_{k,j}(T) - x_{k,i}(T)], \tag{5.7}$$

将上式写成紧凑形式如下：

$$x_{k+1}(T) = (I - T\Gamma L_k)x_k(T), \tag{5.8}$$

其中，$\Gamma = \mathrm{diag}\{\gamma_1, \gamma_2, ..., \gamma_n\}$。

由控制协议（5.5），易知每一时刻正常节点 i 在列表 $\mathcal{L}_i$ 中至多将移除 $2f$ 个状态值。然而值得注意的是，当攻击节点传递的信息值未处于列表 $\mathcal{L}_i$ 的前后 f 个数的位置时，上述算法并不能有效地将其此时的状态值除去。此种情况下，正常节点 i 将采用这个状态值更新自身的状态信息。我们可以将这类攻击节点的状态值做如下定义：

定义 5.2: 称攻击节点 q 为瞬时温和节点，若该节点在 t 时刻发送的状态信息并未被节点 $i \in \mathcal{V}_n$ 通过控制算法（5.5）移除。此种情况下，瞬时温和节点 q 的状态

值可由节点 i 邻居集中的所有正常节点的状态值的线性组合的方式来表示，即

$$x_q(t) = \sum_{j\in\mathcal{N}_i} \varphi_{q,j}(t)x_j(t),\ q \in \mathcal{V}_m \cap \mathcal{N}_i, \tag{5.9}$$

其中，$0 \leq \varphi_{q,j}(t) \leq 1$，以及 $\sum_{j\in\mathcal{N}_i} \varphi_{q,j}(t) = 1$。

注 5.1: 定义 5.2 中，瞬时温和节点 q 的状态值 $x_q(t)$，依照控制协议以及周围正常邻居的状态值存在不同种（只需调整各个系数，事实上可有任意多种）表现形式，我们在每一时刻可随意选取一种。

5.3 主要结果

在上一节中，我们对有限时间安全一致性问题进行了建模，本节中我们将给出本章的主要结论。在这之前，我们先回顾一些证明需要用到的定义、引理以及结论。

引理 5.1: [137] 对于有向图 $\mathcal{G}$ 的 Laplacian 矩阵 L，如果 0 是矩阵 L 的单一特征根，那么 0 特征根对应的特征向量为 1_N，此时有向图 $\mathcal{G}$ 包含一棵生成树。

引理 5.2: [149] 如果一系列有向图的联合图 $\{\mathcal{G}_{i_1}, \mathcal{G}_{i_2}, ..., \mathcal{G}_{i_m}\} \subset \bar{\mathcal{G}}$ 包含有一棵生成树，那么矩阵直积 $D_{i_m}...D_{i_2}D_{i_1}$ 满足 SIA，其中，D_{i_j} 是有向图 $\mathcal{G}_{i_j}$ 相应的随机矩阵。

引理 5.3: [149] 考虑一个 SIA 矩阵有限集 $L_1, L_2, ..., L_k$，满足其每一个子序列 $L_{i_j}, L_{i_{j-1}}, ..., L_{i_1}$ 为 SIA 矩阵。那么，对于一无穷序列 $L_{i_1}, L_{i_2}, ...$ 存在一列向量 y 满足

$$\lim_{j\to\infty} L_{i_j}L_{i_{j-1}}\cdots L_{i_1} = 1y^{\mathrm{T}}.$$

定义 5.3: （r-可得集[162]）对于一个有向图 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$ 以及其一非空节点集子集 $\mathcal{S} \subset \mathcal{V}$，如果 $\mathcal{S}$ 中至少存在一个节点 v_i，它的邻居集中至少有 r 个邻居来自集合 $\mathcal{S}$ 外部，即 $|\mathcal{N}_i \setminus \mathcal{S}| \geq r$，$r \in \mathbb{Z}^+$。我们称集合 $\mathcal{S}$ 为 r-可得集。

定义 5.4: （r-稳健图[162]）对于一个有向图$\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$，如果 $\mathcal{V}$ 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 $|\mathcal{N}_i \setminus \mathcal{S}_\kappa| \geq r$，$r \in \mathbb{Z}^+$，则称图 $\mathcal{G}$ 为 r-稳健图。

定理 5.1: 如果图 $\mathcal{G}$ 是 r-稳健的有向图，其中，$r \geq 1$，那么 $\mathcal{G}$ 含有一棵生成树。

证明： 此定理可以直接由第三章引理 3.3 推得。 证明完毕。

接下来，我们给出本章的主要结论。

定理 5.2: 考虑控制协议（5.5）下的多智能体系统（5.1），令系统的学习增益 γ_i 满足

$$T\gamma_i < 1,\ i \in \mathcal{V}_n. \tag{5.10}$$

如果系统的拓扑图 $\mathcal{G}$ 为一个 $(2k+1)$-稳健图，那么系统随着 $k \to \infty$，所有正常节点可实现有限时间安全一致。

证明： 我们将此证明分成 2 步，首先第 1 步：证明条件（5.3）成立，接着第 2 步：证明一致性条件（5.4）成立。如果上述两个条件得证，即定理得证。

第 1 步： 根据 （5.2）中 $M_k(t)$ 和 $m_k(t)$ 的定义，由式（5.7）可推得，对于 $\forall i \in \mathcal{V}_n$，我们有：

$$\begin{aligned} x_{k+1,i}(t) &= x_{k,i}(t) + t\gamma_i \sum_{j=0}^{n} \phi_{i,j}(t) a_{i,j}[x_{k,j}(t) - x_{k,i}(t)] \\ &\leq x_{k,i}(t) + t\gamma_i \sum_{j=0}^{n} \phi_{i,j}(t) a_{i,j}[M_k(t) - x_{k,i}(t)] \\ &= \alpha M_k(t) + (1-\alpha) x_{k,i}(t) \\ &\leq M_k(t), \end{aligned} \tag{5.11}$$

由上述结果可推得 $M_{k+1}(t) \leq M_k(t)$。其中 $\alpha = t\gamma_i \sum_{j=0}^{n} \phi_{i,j}(t) a_{i,j} < 1$。同样的分析方法，我们不难推得 $m_{k+1}(t) \geq m_k(t)$，上述结果保证了安全性条件（5.3）的成立。

第 2 步： 注意到系统的初始网络是一个满足 $(2f+1)$-稳健的拓扑图，根据引理 5.3 可知，当网络中所每个节点移除 $2f$ 条输入边后，拓扑仍然满足 1-稳健。再根据定理 5.1 可知，系统的有向网络 $\mathcal{G}$ 包含一棵生成树。记 A_k 和 L_k 分别为系统在 k 轮时的邻接矩阵和 Laplacian 矩阵。由 $L_k = \Delta - A_k$，我们有 $I - T\Gamma L_k = (I - T\Gamma\Delta) + T\Gamma A_k$。显然，$I - T\Gamma\Delta$ 是一个对角矩阵，它的对角元素值为$1 - T\gamma_i d_i = 1 - T\gamma_i \sum_{j=1}^{n} \phi_{i,j}(T) a_{i,j}$，在条件（5.10）下，上述元素值皆为正。由此可知 $I - T\Gamma\Delta \geq 0$ 为一个非负矩阵。根据文献 [179]，由于

$T>0$，$\Gamma\geq 0$，以及 $A\geq 0$，可知 $T\Gamma A_k\geq 0$ 是一个非负矩阵。因此，可以得出 $I-T\Gamma L_k=(I-T\Gamma\Delta)+T\Gamma A_k\geq 0$ 是一个非负矩阵。再从引理 5.1 可知，Laplacian 矩阵 L_k 满足性质 $L_k 1_{\mathrm{n}}=0$。由此可以推得 $(I-T\Gamma L_k)1_{\mathrm{n}}=1_{\mathrm{n}}$。从而知 $I-T\Gamma L_k$ 在有向图 $\mathcal{G}$ 下是一个随机矩阵。

根据文献 [64]，我们知道当有向图 $\mathcal{G}$ 包含一棵生成树时，随机矩阵 $I-T\Gamma L_k$ 的特征值 $\lambda=1$ 为一个单根。由 $T\gamma_i a_{i,i}=0,\forall i\in\mathcal{V}_n$，可以推得对角元素值 $I-T\Gamma L_k$ 等同于 $I-T\Gamma\Delta$ 的值，从而在条件（5.10）下保证了该值为正。再根据文献 [64] 可知，如果随机矩阵 $I-T\Gamma L_k$ 的特征值 λ 不等于 1，则它的模小于 1，即，$|\lambda|<1$。根据引理 5.2 和引理 5.3，可知 $\{I-T\Gamma L_k\}$ 是一个 SIA 矩阵集合，满足

$$\lim_{k\to\infty}(I-T\Gamma L_k)\cdots(I-T\Gamma L_2)(I-T\Gamma L_1)=1y^{\mathrm{T}}. \tag{5.12}$$

将式（5.12）代入式（5.8），系统一致性状态值 x_C 可以表述为 $x_C=y^{\mathrm{T}}x_0(T)$。这即表明，系统的一致性条件（5.4）得到满足。 证明完毕。

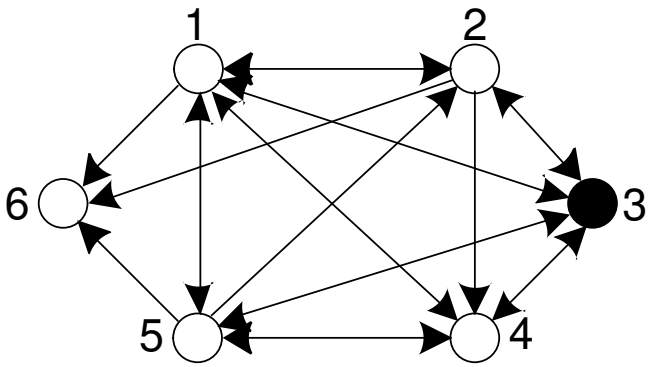


图 5.1　6 个节点组成的有向图

5.4　仿真实例

本节我们通过结合具体实例来进行仿真实验，以此来验证本章所提出理论结果的正确性和所设计协议的有效性。

考虑由 5 个正常节点和 1 个恶意节点组成的有向多智能体系统网络图，其通信拓扑连接情况如图 5.1 所示。各节点初始状态值为 $x_1(0)=15$，$x_2(0)=9$，$x_3(0)=10$，$x_4(0)=7$，$x_5(0)=5$，$x_6(0)=10$。我们假定一轮的迭代时间取 $T=20s$，学习增益取 $\Gamma=\mathrm{diag}\{0.02,0.03,0.02,0.01,0.02,0.01\}$。为简便起见，我们可选取初始控

制输入为零，即 $u_{0,i}=0$。假定节点 3 为恶意节点（黑色节点），其动力学方程为

$$\dot{x}_{k,3}(t)=10sin(0.01\pi t)+10. \tag{5.13}$$

为了验证所提理论，令图 5.1 中的通信拓扑连接满足一个 3-稳健的有向图，相应的邻接矩阵为

$$A=\frac{1}{10}\begin{bmatrix} 0 & 2 & 3 & 2 & 3 & 0 \\ 3 & 0 & 2 & 0 & 5 & 0 \\ 2 & 2 & 0 & 4 & 2 & 0 \\ 5 & 1 & 2 & 0 & 2 & 0 \\ 1 & 0 & 4 & 5 & 0 & 0 \\ 3 & 5 & 0 & 0 & 2 & 0 \end{bmatrix}. \tag{5.14}$$

根据上述 T 和 Γ 的取值，易知能够使得定理 5.2 中的条件 $T\gamma_i<1$ 成立，这样即可从定理上推知系统中所有正常节点将在规定的有限时间内实现安全一致。6 个节点在迭代学习进程中的状态变化在图 5.2 中所示。从图中可以看出，5 个正常节点的状态值在规定时间内最终趋于一致。尽管恶意节点 3 不断干预其他节点的状态更新，企图使正常节点的状态值带入到初始状态区间 $[5,15]$ 之外的状态值 18，然而在我们所设计的控制协议（5.5）的作用下，攻击节点的目的最终无法得逞。

在运行迭代过程中，系统的状态轨迹如图 5.3 所示。对比图 5.2 与图 5.3 可以看到，其他条件不变的情况下，降低系统的收敛时间 T，系统需要运行的迭代次数则会上升，即收敛时间与迭代运行次数成反比。

另外根据上述设定，由定理 5.2 中的条件 $T\gamma_i<1$ 可知，对于本例中取值为 $\Gamma=\mathrm{diag}\{0.02,0.03,0.02,0.01,0.02,0.01\}$ 的学习增益，系统的收敛时间取值范围应该满足：$T<1/\gamma_i$，即 $T\in[0,33.33]$。我们令 $T=40s$，特意使得上述条件不成立。此时，系统的状态轨迹如图 5.4 所示。从图中的实验结果可以看出，系统中正常节点的状态出现了振荡，并有部分节点的值被恶意节点带入了不安全的状态位置 18。

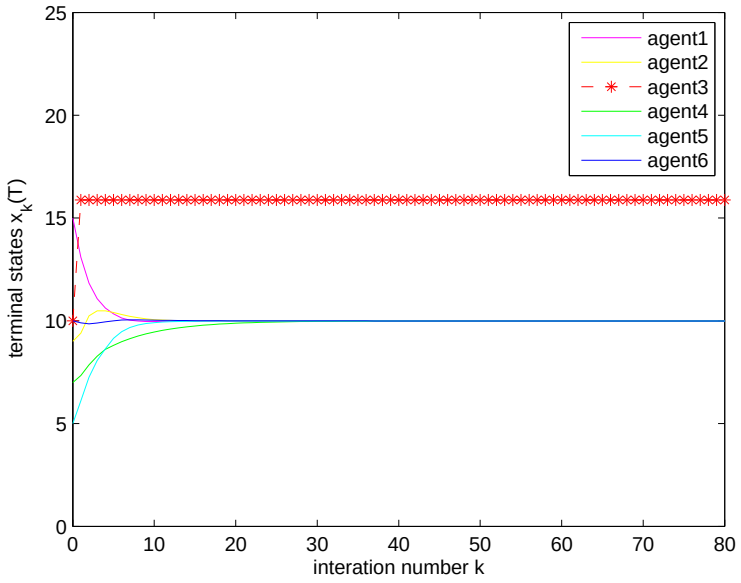


图 5.2　$T = 20s$ 时，所提协议下智能体的状态轨迹图

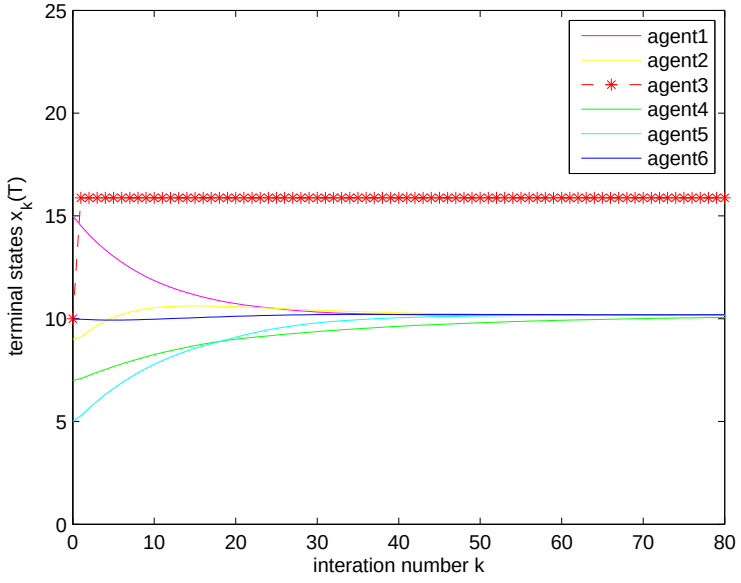


图 5.3　$T = 10s$ 时，所提协议下智能体的状态轨迹图

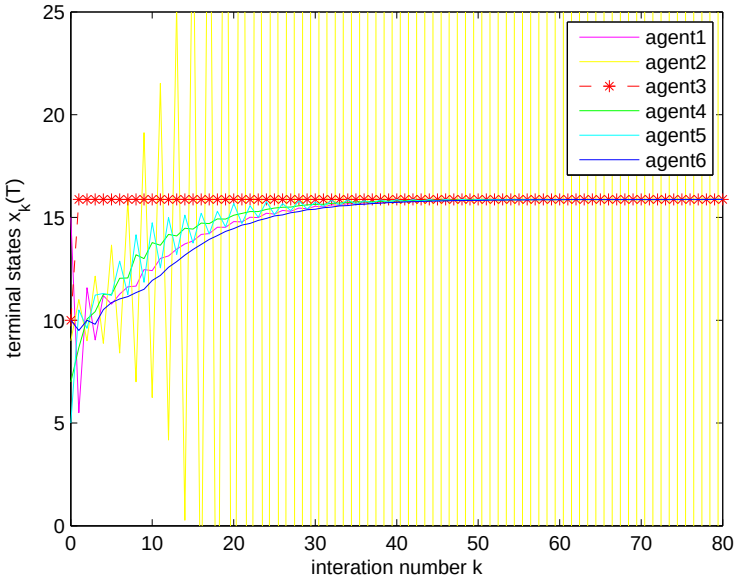


图 5.4　$T = 40s$ 时，所提协议下智能体的状态轨迹图

5.5 本章小结

本章研究了在恶意环境下多智能体网络的有限时间安全一致性问题。借助终端迭代学习方法，提出了一种全新的确保所有正常节点在有限时间内状态达成一致的分布式一致性控制算法。在最多存有 f 个恶意邻居节点的前提下，根据网络连通度，学习增益值和有限时间 T，给出了系统实现收敛的条件。

第六章　量化通信下多智能体系统安全一致性控制

6.1　引言

现有的关于安全一致性问题的工作中，我们发现绝大多数结果都建立在一个理想的通信环境下，即多智能体网络中个体能够实时连续地接收到邻居的状态信息。然而，对于一个在实际环境中的分布式多智能体系统，每个个体的计算能力和能量储备往往是有限制的，以及个体与个体之间的通信带宽也是有限的。因此，基于量化通信的安全一致性控制问题具有重要的理论研究意义和实用价值。

本章我们主要研究在量化通信下的多智能体系统的安全一致性问题。考虑一个由正常节点和拜占庭恶意攻击节点组成的有向网络，通过引入量化器，将网络中实时连续的状态信息转化成量化信息，降低系统的通信开销。然后结合一种邻居间节点的安全策略，设计给出了一种基于邻居量化信息的安全一致性算法。并且针对f-局部有限恶意攻击模型的特点，给出了系统中所有正常智能体实现状态一致的充分条件。

本章的结构安排如下：第 6.2 节对通信有限连续时间系统在恶意攻击下的安全性问题进行了分析，建立了数学建模，并根据有限邻居智能体的量化信息和拓扑稳健性条件，设计了相应的安全一致性控制协议。第 6.3 节给出了本章节的主要结论，并且给出了具体的数学分析证明。第 6.4 节通过仿真实例来验证量化通信下系统的安全一致性控制算法的有效性。第 6.5 节对本章内容进行总结。

6.2　问题描述

考虑一个由 N 个个体组成的多智能体系统，其中含有 n 个正常智能体和 m 个恶意智能体，其中，$n+m=N$。用一个定向图 $\mathcal{G}=\{\mathcal{V},\mathcal{E}_{\mathcal{G}},A\}$ 表示上述多智能体系统。分别用 $\mathcal{V}_n$ 和 $\mathcal{V}_m$ 表示图中正常节点和恶意节点的集合。显然地，我们有 $\mathcal{V}_n\cup\mathcal{V}_m=\mathcal{V}$ 以及 $\mathcal{V}_n\cap\mathcal{V}_m=\emptyset$。

考虑系统中每个正常智能体采用如下动态方程：

$$\dot{x}_i(t)=u_i(t),\ \ i\in\mathcal{V}_s, \tag{6.1}$$

其中 $x_i\in\mathbb{R}$ 为节点 i 的状态值，$u_i(t)\in\mathbb{R}$ 为待设计的控制协议。

6.2.1 攻击模型

本章中我们继续考虑恶意节点采用拜占庭攻击方式，拜占庭攻击方式的特点读者可回顾第 3 章定义 3.1。同时，对于网络中每个正常节点，我们假设它的邻居集中至多存在 f 个恶意节点邻居。并将此攻击模型称作“f-局部攻击模型”。其数学定义如下：

定义 6.1: （f-局部攻击模型）多智能体系统网络中任意一个智能体的邻居当中存在至多有不超过 f 个数目的邻居节点为恶意节点，称为 f-局部攻击模型，即 $|\mathcal{N}_i \cap \mathcal{V}_a| \leq f$，$\forall i \in \mathcal{I}_s$，$f \in \mathbb{Z}^+$。

6.2.2 均匀量化器

该小节中，我们引入量化器的概念。量化器 $q_t(\cdot) : \mathbb{R} \to \Gamma$ 是一种将状态值从 $\mathbb{R}$ 映射（量化）到集合 Γ 的装置。其中 Γ 是一个有限集合。如果集合 $\Gamma = \{0, \pm i, i = 1, 2, ..., M(t)\}$，则量化器 $q_t(\cdot)$ 被称之位均匀量化器。相对应的定义如下：

$$q_t(x) = \begin{cases} 0, & -\frac{1}{2} < x < \frac{1}{2}; \\ i, & \frac{2i-1}{2} \leq x < \frac{2i+1}{2}, i = 1, ..., M(t); \\ M(t), & x \geq \frac{2M(t)-1}{2}; \\ -q_t(-x), & x \leq -\frac{1}{2}, \end{cases} \tag{6.2}$$

其中 $M(t) \in \mathbb{Z}^+$ 是量化器 $q_t(\cdot)$ 的量化级别数。显然，从定义式 (6.2) 中可以看出量化器总的量化级别数目是 $2M(t) + 1$。本章中，我们假定 $q_t(\cdot)$ 量化级别数足够表示系统中所有节点的状态值。

6.2.3 量化通信下的安全一致性算法

假设系统中任意正常节点 i 接收到的信息为其邻居的量化状态信息：

$$y_{i,j}(t) = q_t(x_j(t)),\ j \in \mathcal{N}_i,\ i \in \mathcal{V}_n, \tag{6.3}$$

其中，$q_t(\cdot)$ 是上述小节给出的量化器 (6.2)。

定义在时间 t 时所有正常节点状态值中最大值和最小值如下：

$$M(t)=\max_{i\in\mathcal{V}_n} x_i(t),\ \ m(t)=\min_{i\in\mathcal{V}_n} x_i(t). \tag{6.4}$$

然后，我们给出量化通信下的安全一致性定义。

定义 6.2: 在量化通信条件下，针对 f-局部攻击模型，多智能体系统 (6.1) 能够实现安全一致如果下列条件成立：

$$m(0)\le \inf_{t\ge 0}\min_{i\in\mathcal{V}_n} x_i(t)\le \sup_{t\ge 0}\max_{i\in\mathcal{V}_n} x_i(t)\le M(0), \tag{6.5}$$

$$\lim_{t\to\infty}\left(q_t(x_i(t))-q_t(x_j(t))\right)=0,\ \forall i,j\in\mathcal{V}_n. \tag{6.6}$$

定义 6.2 中，条件式 (6.5) 保证了所有正常节点的状态值任意时刻处在一个由最大和最小初始状态值确定的安全区域 ϱ 内。上述条件式等同表述为，对于任意 $t\ge 0$ 和 $i\in\mathcal{V}_n$，有 $x_i(t)\in\varrho=[m(0),M(0)]$。另外条件式 (6.6) 则保证了所有正常节点的状态值最终处于一个相同的量化区间内。

注 6.1: 值得注意的是，在上述定义中我们采用量化后的状态值是否最终一致来判定系统实现一致性进程的依据。量化器的引入必然会产生一致性误差，即真实状态值与量化后的状态值之间的差值。而研究对于产生一致性误差的关键因素，比如量化器密度、系统初始条件、网络连通度等，将会成为我们今后的一项工作内容。

针对恶意节点的攻击部署范围以及网络的量化通信信息，我们设计如下系统中邻居智能体间的安全机制：

Step 1 对于一个正常节点 i，$i\in\mathcal{V}_n$，将时间 t 接收到的所有邻居传递给它的经过量化器量化的状态信息做一整理，使得这些量化值按照数值从大到小进行排序。

Step 2 针对 Step 1 中排好的序列，从排在序列最前头的值开始逐一与自身值 $q_t(x_i(t))$ 对比，如果有不足 f 个值严格大于自身状态值 $q_t(x_i(t))$，则节点 i 将这些大于自身状态值的数全部从该序列中移除（等同于切断该时刻相应信息的输入边）。否则，移除序列中从最前头开始的前 f 个值。同样的，如果

序列中不足 f 个值严格小于自身值 $q_t(x_i(t))$，节点 i 将这些小于自身值的值全部从序列中移除。否则，移除序列中从最后头开始的后 f 个值。

Step 3 由于 Step 2 中对部分邻居信息值的移除，即等同于暂时切断输入边的操作，可能导致整个网络拓扑成为一个时变的拓扑，此时我们用 $\mathcal{G}_{\sigma(t)} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}, A_{\sigma(t)}\}$ 表示。用 $\mathcal{N}(\mathcal{G}_{\sigma(t)}, i)$ 表示量化信息在 Step 2 中被节点 i 接收并且保留的邻居节点集。然后给予节点 i 如下控制协议：

$$u_i(t) = \sum_{j \in \mathcal{N}_i(\sigma(t))} a_{i,j}[y_{i,j}(t) - y_{i,i}(t)], \tag{6.7}$$

其中，$a_{i,j} \in \mathbb{R}$ 是相应边 (j, i) 的权重。

将协议 (6.7) 代入系统 (6.1) - (6.3)，我们有

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i(\sigma(t))} a_{i,j}[q_t(x_j(t)) - q_t(x_i(t))]. \tag{6.8}$$

值得注意的是，上述所提算法并不能保证完全去除掉恶意节点发送的状态信息。事实上，恶意节点极有可能混入到正常节点的更新过程中。比如，当恶意节点发送的信息值没有排在序列前头 f 个数和后头 f 个数的时候，上述算法就无法去除该时刻这个恶意节点的信息。这时候会导致正常节点在更新自身值的时候采用该恶意节点的值。但根据网络稳健性以及算法的删减原则，我们发现，经算法操作后，即使恶意节点的值被正常节点接受并参与其状态更新，该恶意信息值不会对系统状态产生破坏，保留下来恶意信息值已经没有破坏系统实现安全一致的能力，该值可以用一组所有正常节点状态值的凸组合来表示。因此我们给出“温和攻击信息”的定义：

定义 6.3: （温和攻击信息）

称某时间 t 时恶意节点 q，$q \in \mathcal{V}_n$ 的信息值为温和攻击信息，如果该时刻此节点的信息值被正常节点 p，$p \in \mathcal{V}_m$ 接收并参与其状态更新过程。此时 $x_q(t)$ 可以用一组所有正常节点的量化信息值的凸组合来表示，即

$$x_q(t) = \sum_{j \in \mathcal{V}_n} \varphi_{p,j}(t) q_t(x_j(t)), \ \ q \in \mathcal{V}_m \cap \mathcal{N}_i(\sigma(t)), \tag{6.9}$$

其中 $0 \leq \varphi_{p,j}(t) \leq 1$，$\sum_{j\in\mathcal{V}_n} \varphi_{p,j}(t) = 1$。

显然地，根据上述定义可知，温和攻击信息 $x_q(t) \in \varrho$，$\forall q \in \mathcal{N}_i(\sigma(t))$。

另外在本章的讨论中，我们还需要建立以下假设：

假设 6.1: 在网络拓扑每两次转换过程中，存在一个间隔时间下限值 $\tau_D > 0$，令 $\{t_k\}_{k\in\mathbb{N}}$ 表示转换时间 $\sigma(t)$，满足 $t_{k+1} - t_k \geq \tau_D$。

6.3 主要结果

在给出本章主要结论前，先介绍一些需要用到的引理。

引理 6.1: [148] 令 $\mathcal{G}$ 是满足 r-稳健的有向图，$\mathcal{G}'$ 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 $(r-s)$-稳健的。

引理 6.2: 令 $\mathcal{G}$ 是有向图，则 $\mathcal{G}$ 包含一棵生成树，当且仅当 $\mathcal{G}$ 是 1-稳健的。

下面给出主要结论。

定理 6.1: 考虑采用控制协议 (6.7) 下的多智能体系统 (6.1)。系统中所有正常节点能够最终实现状态安全一致如果网络中个体间的通信链路满足 $(2f+1)$-稳健图。

证明： 首先，我们来证明系统 (6.1) 满足安全性条件 (6.5)，即，在任意时间 t，$x_i(t) \in \varrho$，$i \in \mathcal{V}_n$。根据定义 (6.4)，我们有 $x_i(0) \leq M(0)$。假如上述条件在时间 t^* 时不再成立了，则当该情况发生时，对于任意 $t \in [0, t^*]$，我们有 $x_i(t) \leq M(0)$，$i \in \mathcal{V}_n$；在 t^* 时，存在一个节点 $i \in \mathcal{V}_n$，满足 $x_i(t^*) = M(0)$ 以及 $\dot{x}_i(t^*) > 0$。根据式 (6.8)，此时我们有

$$\dot{x}_i(t^*) = \sum_{j\in\mathcal{N}_i(\sigma(t))} a_{i,j}[q_t(x_j(t^*)) - q_t(x_i(t^*))],\ i \in \mathcal{V}_n. \tag{6.10}$$

通过观察等式右边，由于 $a_{i,j} > 0$ 以及 $q_t(x_i(t^*)) = q_t(M(0)) \geq q_t(x_j(t^*))$，可推知等式右边是非正的，因此有 $\dot{x}_i(t^*) \leq 0$，而这与之前的假设相矛盾，于是在任意时间 t，有 $x_i(t) \leq M(0)$。用相同的逻辑，我们可以分析推得 $x_i(t) \geq m(0)$。因而推知系统 (6.1) 满足安全性条件 (6.5)。

接下来我们进行系统 (6.1) 满足一致性条件 (6.6) 的证明。选取 $W = \max_{i\in\mathcal{V}_n}\{x_1, ..., x_n\} - \min_{i\in\mathcal{V}_n}\{x_1, ..., x_n\}$ 作为李雅普诺夫函数。由于在执行邻居信息值

删减时对通信拓扑产生了变化，W 虽然连续，但不一定连续可导。该情况下我们可以通过分析 W 的狄尼导数来研究它的收敛性质。

定义 $x_{\max} = x_I$，$x_{\min} = x_J$，其中 $I \triangleq \max_i\{i : x_i = \max_{k\in\mathcal{V}_l}\{x_k\}\}$，$J \triangleq \min_i\{i : x_i = \min_{k\in\mathcal{V}_l}\{x_k\}\}$。根据量化器 (6.2) 的结构特点，知 $sign(q_t(x)) = sign(x)$，$\max_{i\in\mathcal{V}_n} q_t(x_i) = q_t(x_{\max})$，$\min_{i\in\mathcal{V}_n} q_t(x_i) = q_t(x_{\min})$。由于 $q_t(x_{\max}) \geq q_t(x_i) \geq q_t(x_{\min})$ 对任意 $i \in \mathcal{V}_n$ 成立，根据文献 [133] 中的引理 2，有 $\dot{x}_{\max} = \sum_{j\in\mathcal{N}_{\max}} a_{I,j}[q_t(x_j) - q_t(x_{\max})] \leq 0$，和 $\dot{x}_{\min} = \sum_{j\in\mathcal{N}_{\min}} a_{J,j}[q_t(x_j) - q_t(x_{\min})] \geq 0$，因此知 W 在系统一致性进程中是非增的。

接下来我们证明当 $t \to \infty$ 时，$D^+W(t) \to 0$。假如随着 $t \to \infty$，$D^+W(t)$ 没有收敛到零。那么该情形下必然存在一个常数 $\varepsilon_0 > 0$，以至于对于 $\bar{T} > 0$，存在 $t > \bar{T}$ 满足 $D^+W(t) \leq -\varepsilon_0$（注意到$D^+W \leq 0$）。

我们知道此时必然存在一个常数 $\delta_0 > 0$ 和一组时间序列 $\{t_i\}_{i\in\mathbb{N}}$，随着 $t_i \to \infty$，$i \to \infty$，满足 $D^+W(t) \leq -\varepsilon_0$ 以及 $|t_{i+1} - t_i| > \delta_0$ 对任意 i。

对于 Δt，当 $D^+W(t)$ 处于连续段时，即，$t_k \notin \Delta t$ 对任意 i，由于安全性条件 (6.5) 保证了 $x_i(t)$ 和 $\dot{x}_i(t)$ 的有界，我们可得知此时 $D^+W(t)$ 是一致连续的。因此，存在一个常数 $\delta_1 > 0$，对于任意时间 t' 和 t''（满足 $|t' - t''| < \delta_1$），我们有：

$$\left|D^+W(t') - D^+W(t'')\right| < \frac{\varepsilon_0}{2}. \tag{6.11}$$

从而对任意 $t \in [t_i - \delta_1, t_i + \delta_1]$，推知

$$\begin{aligned} D^+W(t) &= -\left|D^+W(t_i) - (D^+W(t_i) - D^+\bar{V}(t))\right| \\ &\leq -(|D^+W(t_i)| - |D^+W(t_i) - D^+W(t)|) \\ &\leq -\varepsilon_0 + \tfrac{\varepsilon_0}{2} \\ &= -\tfrac{\varepsilon_0}{2}. \end{aligned} \tag{6.12}$$

接着假设另外一种可能情况，即当 t_i 处于不连续点 t_k 右边的情况。在该情形下，$D^+W(t) \leq -\varepsilon_0/2$ 则可能无法满足，因为 $D^+W(t)$ 可能在 t_k 时刻增大。然而，通过假设 6.1 可知，系统在下一个不连续时刻到来前存在一个驻留时间 τ_D。这确保了存在一个时间 $\delta_2 \in (0, \tau_D)$ 满足 $D^+W(t) \leq -\varepsilon_0/2$ 对任意 $t \in [t_k, t_k + \delta_2]$。接着，

在 $(0,\infty)$ 上对 $D^+W(t)$ 进行积分，我们有

$$\begin{aligned}\int_0^{\infty} D^+W(t)\mathrm{d}t &\leq \lim_{N\to\infty}\sum_{i=1}^{N}\int_{t_i-\delta}^{t_i+\delta} D^+W(t)\mathrm{d}t \\ &\leq -\lim_{N\to\infty}\sum_{i=1}^{N}\int_{t_i-\delta}^{t_i+\delta}\frac{\varepsilon_0}{2}\mathrm{d}t \\ &= -\lim_{N\to\infty} N\varepsilon_0\delta \\ &= -\infty,\ \delta\in\min\{\delta_1,\delta_2\}.\end{aligned} \tag{6.13}$$

而这与对任意 $t>0$，$W(t)\geq 0$ 的条件相矛盾。因此可知，$D^+W(t)\to 0$ 随着时间趋于无穷，从而推知 $\lim_{t\to\infty}W(t)=constant$，即，分别持最大值状态和最小值状态的正常节点最终保持固定状态。对于节点 I 来说，这等同于 $\sum_{j\in\mathcal{N}_I}a_{I,j}[q_t(x_j)-q_t(x_{\max})]=0$，由于 $q_t(x_{\max})\geq q_t(x_j)$ 对任意 $j\in\mathcal{N}_I$ 成立，后者推出 $q_t(x_j)=q_t(x_{\max})$ 对任意 $j\in\mathcal{N}_I$ 成立。选取任意 $k\in\mathcal{N}_I$，其中 k 不为最大值节点。于是 $q_t(x_k)\geq q_t(x_j)$ 对任意 $j\in\mathcal{N}_k$ 成立，因而 $\dot{x}_k=\sum_{j\in\mathcal{N}_k}a_{k,j}[q_t(x_j)-q_t(x_k)]\leq 0$。若 $\dot{x}_k<0$，则必须 $\dot{x}_I<0$ 因为 $q_t(x_k)=q_t(x_{\max})$。若 $\dot{x}_k=0$，我们有 $q_t(x_j)=q_t(x_k)=q_t(x_{\max})$ 对任意 $j\in\mathcal{N}_k$ 成立。接着我们可随机选取一个数 $l\in\mathcal{N}_k$ 对上述操作进行重复。由于初始网络是一个 $(2f+1)$-稳健图，即使对每个正常节点移除 $2f$ 条通信边，根据引理 6.1 知，网络仍然是一个 1-稳健图。再通过引理 6.2 知，此时的网络包含有一棵生成树。将上述过程经过有限次操作后，可扩散至网络中的全部节点。并由此可知，所有从根节点到节点 I 路径中的节点拥有与 $q_t(x_{\max})$ 相同的值。类似地，我们可以推知所有从根节点到节点 J 路径中的其他节点拥有与 $q_t(x_{\min})$ 相同的值。在生成树中所有正常节点同时保持着最大值和最小值，即，$q_t(x_{\max})=q_t(x_{\min})$。于是知系统的一致性条件 (6.6) 是满足的。　证明完毕。

6.4　仿真实例

在这一章节中，我们通过设计一个仿真实例来验证本章所提算法的有效性。考虑一个由 7 个节点组成的网络，其中包含 5 个正常节点和 2 个恶意节点。网络的拓扑连接如图 6.1 所示，根据稳健性的定义检验，网络拓扑满足 3-稳健图。7 个节点的初始状态值分别为 $x_1(0)=17$，$x_2(0)=2$，$x_3(0)=5$，$x_4(0)=18$，$x_5(0)=10$，$x_6(0)=8$，$x_7(0)=25$。假定节点 3 和节点 5 为恶意节点（图中黑色表示），

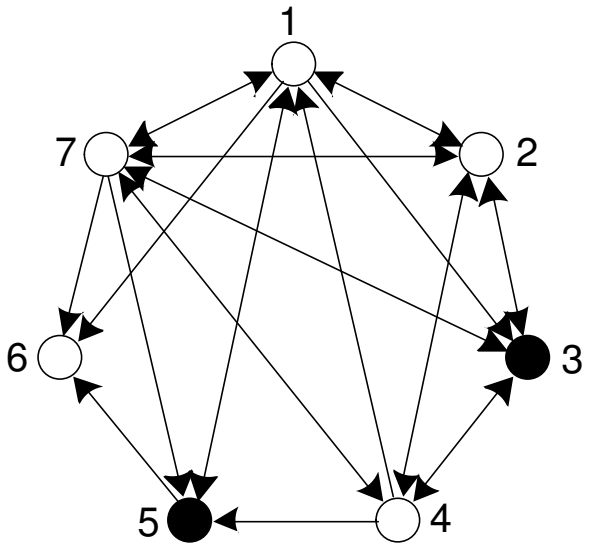


图 6.1　7 个节点组成的有向图

它们的系统动态设计如下：

$$\begin{aligned}\dot{x}_3(t) &= -0.8x_3(t) + 0.8u_a,\\ \dot{x}_5(t) &= -0.4x_5(t) + 0.4u_a,\end{aligned} \tag{6.14}$$

其中参考输入 $u_a = 30$。恶意节点的目标是将正常节点的状态领导至一个安全区域 $\varrho = [2, 25]$ 外的数值 30。令邻接矩阵为：

$$A = \frac{1}{3}\begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1 & 0 & 0 & 1\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 1 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 1 & 0 & 1\\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}. \tag{6.15}$$

从网络拓扑图中可以发现，每一个正常节点至少拥有一个恶意节点的邻居。因此，通过定理 6.1，可以推知，对于一个 3-稳健的网络图，可以抵御邻居中至多一个恶意节点的攻击。系统的仿真结果如图 6.2 所示。

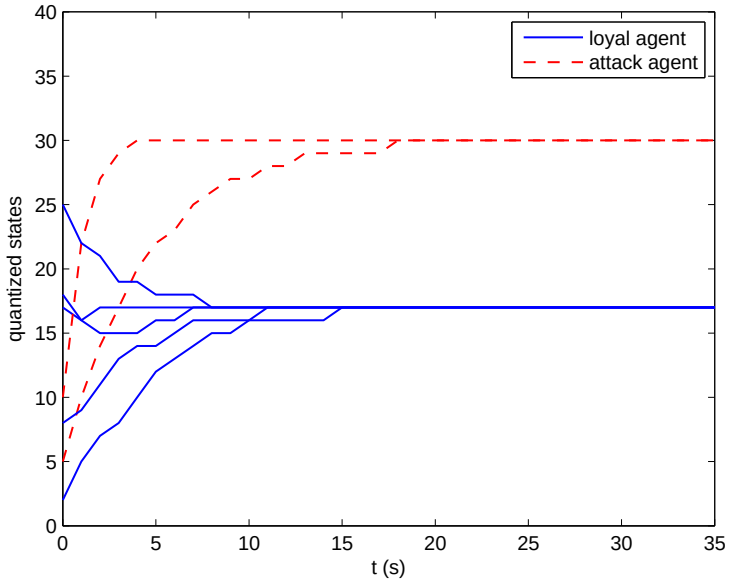


图 6.2　量化通信下系统各节点的状态轨迹图

6.5 本章小结

本章节中，我们集中研究了在量化通信网络下的多智能体系统抵御恶意节点攻击的安全一致性算法。结合一种邻居间节点的安全策略，设计给出了一种基于邻居量化信息的安全一致性算法。并且针对 f-局部有限恶意攻击模型的特点，给出了系统中所有正常智能体实现状态一致的充分条件。最后，通过实例仿真，验证了所提结论的正确性。

第七章　总结与展望

7.1　总结

近十年来，多智能体系统一致性控制因具备很强的发展潜力以及广阔的工程应用背景，引起了系统与控制领域专家学者的普遍关注。随着多智能体系统控制技术逐渐完备成熟，以及其在工业、军事和民用等领域的普及推广，系统的安全性问题，也越来越被更多的研究人员所重视。近五年内开始涌现出一批科研人员，专门针对多智能体系统一致性算法的安全性问题展开研究，并取得了一些喜人的成果。然而，目前多数的文献均假设在一个理想的条件下考虑两类智能体的博弈关系，即只针对一个不考虑通信时延、丢包、噪声、拥塞等问题的理想网络进行安全性的分析与设计工作。本文着重研究了存在部分恶意智能体攻击情形下的多智能体系统安全一致性问题。通过矩阵论、时延图法、Lyapunov 函数法、Babalat-like 引理法、迭代学习控制理论等分析方法，分别研究了如何实现通信时延下安全一致性，非线性动态系统安全一致性，量化通信条件下安全一致性，以及有限时间安全一致性。

本文的主要工作归纳如下：

（1）分析总结了已有的关于多智能体系统一致性问题的研究成果，并分门别类对部分代表性工作进行了评述，提出一些仍需解决的难题；另外，简要回顾了一些需要用到的基本数学概念以及结论，主要包括代数图论，矩阵理论，以及泛函微分方程稳定性等方面的知识。

（2）介绍了目前多智能体系统网络中常见的几类恶意攻击模型，并对其中部分攻击模型的结构特点进行了分析。针对存在通信时延和恶意节点攻击的有向网络，提出了一种分布式自适应安全一致性协议。系统中正常节点不需要知道任何关于网络拓扑的信息，也不需要知道邻居节点的信标。在不同的攻击模型下，分别给出了系统正常节点实现状态安全一致的充分必要条件。最后，通过仿真实例对理论结果进行了验证。

（3）研究了非线性连续时间多智能体系统在遭遇恶意节点攻击下的安全一致性问题。正常节点在进行邻居信息删减操作的时候，以暂时切断邻居信号输入边的方式，会有选择地摒弃一部分邻居节点给予的信息，从而导致原本固定的网络拓扑环境转化成一个基于状态值的随机切换拓扑网络。针对上述情况，给出了一种新颖的描述节点间通信拓扑关系的框架：拓扑稳健性。并根据攻击节点的部署范围情

况，给出了设计安全一致性协议所需要的拓扑稳健性条件，保证正常节点在操作信息删减的过程中，系统通信拓扑仍旧联合连通。通过构造一种 Lyapunov-Krasovskii 函数和 Barbalat-like 引理方法，获得了所提控制协议下系统实现收敛的条件。最后，通过一个实例仿真，对所提算法的正确性和有效性进行了验证。

（4）研究了在恶意节点攻击下的多智能体系统有限时间安全一致性问题。结合迭代学习控制方法，提出一种有限时间安全一致性协议，为处理有限时间一致性问题提供了新的途径。理论结果表明：引入恰当的学习增益值和合理的通信链路权重，以及满足特定的网络连通度，那么就能确保正常节点在每一轮的迭代操作中，其状态值始终处于一个安全的容许范围内发生变化，并能够实现在有限时间内收敛。同时通过理论研究发现，在允许范围内，系统的收敛时间 T 与控制协议迭代的操作次数成反比。最后通过实例仿真验证了所提方法的有效性。

（5）研究了在量化通信下的多智能体系统的安全一致性问题。考虑一阶连续多智能体系统中个体间交互信息是量化的。结合一种邻居间节点的安全策略，提计了基于邻居量化信息的安全一致性协议。并且针对 f-局部有限恶意攻击模型的特点，给出了系统中所有正常智能体实现状态一致的充分性条件。最后进行了算法的仿真验证。

7.2 展望

以下是作者基于本文的研究内容以及对相关文献的阅读总结，提出的几个有待进一步研究的问题：

（1）在考虑时延对多智能体系统安全一致性的影响时，本文只考虑了通信时延，即不对称时延对安全控制协议的影响。而实际应用中，节点往往自身也会产生一定的输入时延，这时候同时考虑通信时延和输入时延，即对称时延，是非常有必要的。

（2）本中文仅仅利用邻居智能体的信息来设计一致性协议。相对来说，系统中节点获取的信息资源还是比较贫瘠的，尤其对一个安全系统来说，接下去可以考虑利用系统中节点的二跳或者多跳信息，或者利用节点自身上一轮或者前几轮的历史信息来设计控制律，使得正常节点在处理恶意节点的攻击时具有更多的参考信息，以此获得更好的抗击能力和鲁棒性。

（3）在本文中只讨论了一阶多智能体系统的安全一致性问题，对于二阶和高阶系统的一致性问题并未展开研究，二阶和高阶系统对通信拓扑的连通性相比于一

阶系统有更加苛刻的要求，同时在抵御恶意节点攻击下的表现也不尽相同，因此如何将本文所得的结果拓展到二阶以及高阶系统的一致性问题当中需要在接下去的工作中作更为深入的研究。

（4）在文中已经证明，网络拓扑的稳健性越高，系统的抗恶意攻击能力越强，但是文中并没有研究如何设计和提高系统通信拓扑稳健性的方法。显然，单纯地增加通信链路不一定能够有效提高拓扑稳健性，相反有可能增多恶意节点攻击的路径，降低系统的安全性能。因此如何设计和提高拓扑稳健性是一个非常实际且需要解决的问题。

（5）有限时间收敛是一个非常有意义的工作，尤其对于一个多智能体系统的安全性来讲，设计者往往会对收敛时间有着较高的要求。尽管迭代学习控制方法给我们解决有限时间收敛问题提供了一个新的思路，但仍有一些不够完善的地方，比如在对于每一轮初始时刻的状态值设定上，仍有许多比较强的假设。如何突破这些假设和限制，更好地服务于安全一致性算法也是值得一个深入研究的问题。

参考文献

[1] 洪奕光, 翟超. 多智能体系统动态协调与分布式控制设计[J]. *控制理论与应用*, 2011, 28(10): 1506-1512.

[2] Eddy F, Gooi H B, Chen S X. Multi-agent system for distributed management of microgrids [J]. *IEEE Transactions on Power Systems*, 2015, 30(1): 24-34.

[3] Kahrobaee S, Rajabzadeh R A, Soh L K, *et al*. A multiagent modeling and investigation of smart homes with power generation, storage, and trading features [J]. *IEEE Transactions on Smart Grid*, 2013, 4(2): 659-668.

[4] Kahrobaee S, Rajabzadeh R A, Soh L K, *et al*. Multiagent study of smart grid customers with neighborhood electricity trading [J]. *Electric Power Systems Research*, 2014, 111: 123-132.

[5] Dimeas A L, Hatziargyriou N D. Operation of a multiagent system for microgrid control [J]. *IEEE Transactions on Power Systems*, 2005, 20(3): 1447-1455.

[6] Manickavasagam K. Intelligent energy control center for distributed generators using multi-agent system [J]. *IEEE Transactions on Power Systems*, 2015, 30(5): 2442-2449.

[7] Zhao Y, Duan Z S, Wen G H, *et al*. Fully distributed tracking control for non-identical multi-agent systems with matching uncertainty [J]. *International Journal of Adaptive Control and Signal Processing*, 2015, 29(8): 1024-1037.

[8] Chichka D F. Satellite clusters with constant apparent distribution [J]. *Journal of Guidance, Control, and Dynamics*, 2001, 24(1): 117-122.

[9] Sabol C, Burns R, McLaughlin C A. Satellite formation flying design and evolution [J]. *Journal of Spacecraft and Rockets*, 2001, 38(2): 270-278.

[10] Beard R W, Lawton J, Hadaegh F Y. A coordination architecture for spacecraft formation control [J]. *IEEE Transactions on control systems technology*, 2001, 9(6): 777-790.

[11] Schaub H, Vadali S R, Junkins J L, *et al*. Spacecraft formation flying control using mean orbit elements [J]. *Journal of the Astronautical Sciences*, 2000, 48(1): 69-87.

[12] Yang H, Jiang B, Cocquempot V, *et al*. Spacecraft formation stabilization and fault tolerance: a state-varying switched system approach [J]. *Systems & Control Letters*, 2013, 62(9): 715-722.

[13] Giulietti F, Pollini L, Innocenti M. Autonomous formation flight [J]. *IEEE Control Systems Magazine*, 2000, 20(6): 34-44.

[14] Gruszka A, Malisoff M, Mazenc F. Bounded tracking controllers and robustness analysis for UAVs [J]. *IEEE Transactions on Automatic Control*, 2013, 1(58): 180-187.

[15] Wang Y, Yan W, Li J. Passivity-based formation control of autonomous underwater vehicles [J]. *Control Theory & Applications*, 2012, 6(4): 518-525.

[16] Agogino A K, Tumer K. A multiagent approach to managing air traffic flow [J]. *Autonomous Agents and Multi-Agent Systems*, 2012, 24(1): 1-25.

[17] Bazzan A L C, Klügl F. A review on agent-based technology for traffic and transportation [J]. *The Knowledge Engineering Review*, 2014, 29(03): 375-403.

[18] Leitão P, Marik V, Vrba P. Past, present, and future of industrial agent applications [J]. *IEEE Transactions Industrial Informatics*, 2013, 9(4): 2360-2372.

[19] Olfati-Saber R. Distributed Kalman filtering for sensor networks [C]. *Proceedings of the 46th IEEE Conference on Decision and Control*, New Orleans, LA, USA, 2007: 5492-5498.

[20] Kar S, Moura J M F. Distributed consensus algorithms in sensor networks with imperfect communication: Link failures and channel noise [J]. *IEEE Transactions on Signal Processing*, 2009, 57(1): 355-369.

[21] Yu W, Chen G, Wang Z, Yang W. Distributed consensus filtering in sensor networks [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2009, 39(6): 1568-1577.

[22] Shen B, Wang Z, Hung Y S. Distributed H_∞-consensus filtering in sensor networks with multiple missing measurements: the finite-horizon case [J]. *Automatica*, 2010, 46(10): 1682-1688.

[23] He J, Cheng P, Shi L H, *et al*. Sats: Secure average-consensus-based time synchronization in wireless sensor networks [J]. *IEEE Transactions on Signal Processing*, 2013, 61(24): 6387-6400.

[24] Olfati-Saber R. Swarms on sphere: A programmable swarm with synchronous behaviors like oscillator networks [C]. *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, 2006: 5060-5066.

[25] Menon P P, Edwards C. Decentralised static output feedback stabilisation and synchronisation of networks [J]. *Automatica*, 2009, 45(12): 2910-2916.

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

[27] West D B. *Introduction to graph theory* [M]. Upper Saddle River, NJ, USA: Prentice hall, 2001.

[28] DeGroot M H. Reaching a consensus [J]. *Journal of the American Statistical Association*, 1974, 69(345): 118-121.

[29] Reynolds C. Flocks, herds and schools: a distributed behavioral model [C]. *In Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques*, 1987, 21(4): 25-34.

[30] Vicsek T, Czirók A, Ben-Jacob E, Cohen I, Shochet O. Novel type of phase transition in a system of self-driven particles [J]. *Physical review letters*, 1995, 75(6): 1226.

[31] 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.

[32] Xiao F, Wang L. Asynchronous consensus in continuous-time multi-agent systems with switching topology and time-varying delays [J]. *IEEE Transactions on Automatic Control*, 2008, 53(8): 1804-1816.

[33] Chen Y, Lu J, Yu X, *et al*. Multi-agent systems with dynamical topologies: Consensus and applications [J]. *IEEE Circuits and Systems Magazine*, 2013, 13(3): 21-34.

[34] Qin J, Gao H, Yu C. On discrete-time convergence for general linear multi-agent systems under dynamic topology [J]. *IEEE Transactions on Automatic Control*, 2014, 59(4): 1054-1059.

[35] Xie G, Liu H, Wang L, *et al*. Consensus in networked multi-agent systems via sampled control: fixed topology case [C]. *Proceedings of the American Control Conference*, St. Louis, Missouri, USA, 2009: 3902-3907.

[36] Wang S, Xie D. Consensus of second-order multi-agent systems via sampled control: undirected fixed topology case [J]. *IET Control Theory & Applications*, 2012, 6(7): 893-899.

[37] Cao Y, Ren W. Multi-vehicle coordination for double-integrator dynamics under fixed undirected/directed interaction in a sampled-data setting[J]. *International Journal of Robust and Nonlinear Control*, 2010, 20(9): 987-1000.

[38] Liu H, Xie G, Wang L. Necessary and sufficient conditions for solving consensus problems of double-integrator dynamics via sampled control [J]. *International Journal of Robust and Nonlinear Control*, 2010, 20(15): 1706-1722.

[39] Tan C, Liu G P, Duan G R. Group consensus of networked multi-agent systems with directed topology [C]. *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 2011: 8878-8893.

[40] Gao Y, Ma J, Zuo M, *et al*. Consensusability of continuous-time multi-agent systems with general linear dynamics and intermittent measurements [J]. *IET Control Theory & Applications*, 2013, 7(6): 842-847.

[41] Zhang Z, Hao F, Zhang L, *et al*. Consensus of linear multi-agent systems via event-triggered control [J]. *International Journal of Control*, 2014, 87(6): 1243-1251.

[42] Dimarogonas D V, Frazzoli E, Johansson K H. Distributed event-triggered control for multi-agent systems [J]. *IEEE Transactions on Automatic Control*, 2012, 57(5): 1291-1297.

[43] Chen X, Hao F. Event-triggered average consensus control for discrete-time multi-agent systems [J]. *IET Control Theory & Applications*, 2012, 6(16): 2493-2498.

[44] Garcia E, Cao Y, Yu H, *et al*. Decentralised event-triggered cooperative control with limited communication [J]. *International Journal of Control*, 2013, 86(9): 1479-1488.

[45] Meng X, Chen T. Event based agreement protocols for multi-agent networks [J]. *Automatica*, 2013, 49(7): 2125-2132.

[46] Yang W, Bertozzi A L, Wang X. Stability of a second order consensus algorithm with time delay [C]. *Proceedings of the 47th IEEE Conference on Decision and Control*, Cancun, Mexico, 2008: 2926-2931.

[47] Wang J, Elia N. Consensus over networks with dynamic channels [J]. *International Journal of Systems, Control and Communications*, 2010, 2(1-3): 275-297.

[48] Tian Y P, Liu C L. Consensus of multi-agent systems with diverse input and communication delays [J]. *IEEE Transactions on Automatic Control*, 2008, 53(9): 2122-2128.

[49] Lee D, Spong M W. Agreement with non-uniform information delays [C]. *Proceedings of the American Control Conference*, Minneapolis, MN, USA, 2006: 756-761.

[50] Dong W, Farrell J A. Cooperative control of multiple nonholonomic mobile agents [J]. *IEEE Transactions on Automatic Control*, 2008, 53(6): 1434-1448.

[51] Wang X, Saberi A, Stoorvogel A A, *et al*. Consensus in the network with uniform constant communication delay[J]. *Automatica*, 2013, 49(8): 2461-2467.

[52] Xiao F, Wang L. Consensus problems of multiagent systems under discrete communication structure [C]. *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, 2006: 4289-4294.

[53] Franceschelli M, Giua A, Pisano A, *et al*. Finite-time consensus for switching network topologies with disturbances [J]. *Nonlinear Analysis: Hybrid Systems*, 2013, 10: 83-93.

[54] 沈艳军, 刘万海, 张勇. 一类非线性系统全局有限时间观测器设计[J]. *控制理论与应用*, 2010, 27(5): 668-674.

[55] Cao M, Morse A, Anderson B. Reaching an agreement using delayed information [C]. *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, 2006: 3375-3380.

[56] Xiao F, Wang L. Dynamic behavior of discrete-time multiagent systems with general communication structures [J]. *Physica A: Statistical Mechanics and its Applications*, 2006, 370(2): 364-380.

[57] Gazi V. Stability of an asynchronous swarm with time-dependent communication links [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2008, 38(1): 267-274.

[58] 李韬, 孟扬, 张纪峰. 多自主体量化趋同与有限数据率趋同综述[J]. *自动化学报*, 2013, 39(11): 1805-1811.

[59] Wang W, Slotine J J. Contraction analysis of time-delayed communications and group cooperation [J]. *IEEE Transactions on Automatic Control*, 2006, 51(4): 712-717.

[60] Cao M, Morse A S, Anderson B D. Reaching a consensus in a dynamically changing environment: a graphical approach [J]. *SIAM Journal on Control and Optimization*, 2008, 47(2): 575-600.

[61] 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.

[62] Moreau L. Stability of continuous-time distributed consensus algorithms [C]. *Proceedings of the 43rd IEEE Conference on Decision and Control*, Nassau, Bahamas, 2004: 3998-4003.

[63] 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.

[64] 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.

[65] Zeng W, Chow M Y, Ning P. Secure distributed control in unreliable d-ncs [C]. *Proceedings of the 21st IEEE International Symposium on in Industrial Electronics*, Hangzhou, China, 2012: 1858-1863.

[66] Moreau L. Stability of multiagent systems with time-dependent communication links [J]. *IEEE Transactions on Automatic Control*, 2005, 50(2): 169-182.

[67] Guo G, Ding L, Han Q L. A distributed event-triggered transmission strategy for sampled-data consensus of multi-agent systems [J]. *Automatica*, 2014, 50(5): 1489-1496.

[68] Bliman P A, Ferrari-Trecate G. Average consensus problems in networks of agents with delayed communications [J]. *Automatica*, 2008, 44(8): 1985-1995.

[69] Tanner H G, Christodoulakis D K. State synchronization in localinteraction networks is robust with respect to time delays [C]. *Proceedings of the IEEE Conference on Decision Control*, Seville, Spain, 2005: 4945-4950.

[70] Sheng J, Ding Z. Optimal consensus control of linear multi-agent systems with communication time delay [J]. *IET Control Theory & Applications*, 2013, 7(15): 1899-1905.

[71] Zhou B, Lin Z. Consensus of high-order multi-agent systems with large input and communication delays [J]. *Automatica*, 2014, 50(2): 452-464.

[72] Wang W, Slotine J J E. Contraction analysis of time-delayed communications and group cooperation [J]. *IEEE Transactions on Automatic Control*, 2006, 51(4): 712-717.

[73] Gao Y, Wang L. Sampled-data based consensus of continuous-time multi-agent systems with time-varying topology [J]. *IEEE Transactions on Automatic Control*, 2011, 56(5): 1226-1231.

[74] Hatano Y, Mesbahi M. Agreement over random networks [J]. *IEEE Transactions on Automatic Control*, 2005, 50(11): 1867-1872.

[75] Su H, Chen M Z Q, Lam J, et al. Semi-global leader-following consensus of linear multi-agent systems with input saturation via low gain feedback [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2013, 60(7): 1881-1889.

[76] Su H, Chen M Z Q, Wang X, et al. Semiglobal observer-based leader-following consensus with input saturation [J]. *IEEE Transactions on Industrial Electronics*, 2014, 61(6): 2842-2850.

[77] Yu J, Wang L. Group consensus in multi-agent systems with switching topologies and communication delays. *Systems & Control Letters*, 2010, 59(6): 340-348.

[78] 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.

[79] Sun Y G, Wang L, Xie G. Average consensus in networks of dynamic agents with switching topologies and multiple time-varying delays [J]. *Systems & Control Letters*, 2008, 57(2): 175-183.

[80] Shi G, Hong Y. Global target aggregation and state agreement of nonlinear multi-agent systems with switching topologies [J]. *Automatica*, 2009, 45(5): 1165-1175.

[81] Wen G, Hu G, Yu W, *et al*. Distributed H_∞ consensus of higher order multiagent systems with switching topologies [J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2014, 61(5): 359-363.

[82] Wen G, Hu G, Yu W, *et al*. Consensus tracking for higher-order multi-agent systems with switching directed topologies and occasionally missing control inputs [J]. *Systems & Control Letters*, 2013, 62(12): 1151-1158.

[83] Wen G, Duan Z, Chen G, *et al*. Consensus tracking of multi-agent systems with Lipschitz-type node dynamics and switching topologies [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2014, 61(2): 499-511.

[84] Meng D, Jia Y, Du J. Robust consensus tracking control for multiagent systems with initial state shifts, disturbances, and switching topologies[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2015, 26(4): 809-824.

[85] Li T, Fu M, Xie L, Zhang J F. Distributed consensus with limited communication data rate [J]. *IEEE Transactions on Automatic Control*, 2011, 56(2): 279-92.

[86] Kashyap A, Başar T, Srikant R. Quantized consensus [J]. *Automatica*, 2007, 43(7): 1192-1203.

[87] Kar S, Moura J M F. Distributed consensus algorithms in sensor networks: Quantized data and random link failures [J]. *IEEE Transactions on Signal Processing*, 2010, 58(3): 1383-1400.

[88] Liu S, Li T, Xie L H, Fu M Y, Zhang J F. Continuous-time and sampled-data-based average consensus with logarithmic quantizers [J]. *Automatica*, 2013, 49(11): 3329-3336.

[89] Carli R, Fagnani F, Frasca P, Zampieri S. Gossip consensus algorithms via quantized communication [J]. *Automatica*, 2010, 46(1): 70-80.

[90] Cai K, Ishii H. Quantized consensus and averaging on gossip digraphs [J]. *IEEE Transactions on Automatic Control*, 2011, 56(9): 2087-2100.

[91] Zhang Q, Zhang J F. Quantized data-based distributed consensus under directed time-varying communication topology [J]. *SIAM Journal on Control and Optimization*, 2013, 51(1): 332-352.

[92] Yuan D M, Xu S Y, Zhao H Y, Rong L N. Distributed dual averaging method for multi-agent optimization with quantized communication [J]. *Systems & Control Letters*, 2012, 61(11): 1053-1061.

[93] Nedić A, Olshevsky A, Ozdaglar A, Tsitsiklis J N. On distributed averaging algorithms and quantization effects [J]. *IEEE Transactions on Automatic Control*, 2009, 54(11): 2506-2517.

[94] Dimarogonas D V, Johansson K H. Quantized agreement under time-varying communication topology [C]. *Proceedings of the American Control Conference*, Seattle, WA, USA, 2008: 4376-4381.

[95] Dimarogonas D V, Johansson K H. Stability analysis for multi-agent systems using the incidence matrix: quantized communication and formation control [J]. *Automatica*, 2010, 46(4): 695-700.

[96] Jiang F, Wang L. Finite-time information consensus for multi-agent systems with fixed and switching topologies [J]. *Physica D: Nonlinear Phenomena*, 2009, 238(16): 1550-1560.

[97] Jiang F, Wang L. Finite-time weighted average consensus with respect to a monotonic function and its application [J]. *Systems & Control Letters*, 2011, 60(9): 718-725.

[98] Kim Y, Mesbahi M. On maximizing the second smallest eigenvalue of a state-dependent graph Laplacian [J]. *IEEE Transactions on Automatic Control*, 2006, 51(1): 116-120.

[99] Ji Z, Wang Z, Lin H, Wang Z. Interconnection topologies for multi-agent coordination under leader - follower framework [J]. *Automatica*, 2009, 45(12): 2857-2863.

[100] Ren W. Multi-vehicle consensus with a time-varying reference state [J]. *Systems & Control Letters*, 2007, 56(7): 474-483.

[101] Ren W. Consensus tracking under directed interaction topologies: Algorithms and experiments [J]. *IEEE Transactions on Control Systems Technology*, 2010, 18(1): 230-237.

[102] Hong Y, Hu J, Gao L. Tracking control for multi-agent consensus with an active leader and variable topology [J]. *Automatica*, 2006, 42(7): 1177-1182.

[103] Chen F, Cao Y, Ren W. Distributed average tracking of multiple time-varying reference signals with bounded derivatives [J]. *IEEE Transactions on Automatic Control*, 2012, 57(12): 3169-3174.

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

[105] Khoo S, Xie L, Man Z. Robust finite-time consensus tracking algorithm for multirobot systems [J]. *IEEE/ASME Transactions on Mechatronics*, 2009, 14(2): 219-228.

[106] Li S, Du H, Lin X. Finite-time consensus algorithm for multi-agent systems with double-integrator dynamics [J]. *Automatica*, 2011, 47(8): 1706-1712.

[107] Chen G, Lewis F L, Xie L. Finite-time distributed consensus via binary control protocols [J]. *Automatica*, 2011, 47(9): 1962-1968.

[108] Wang L, Xiao F. Finite-time consensus problems for networks of dynamic agents [J]. *IEEE Transactions on Automatic Control*, 2010, 55(4): 950-955.

[109] Cao Y, Ren W, Meng Z. Decentralized finite-time sliding mode estimators and their applications in decentralized finite-time formation tracking [J]. *Systems & Control Letters*, 2010, 59(9): 522-529.

[110] Mei J, Ren W, Ma G. Distributed coordination for second-order multi-agent systems with nonlinear dynamics using only relative position measurements [J]. *Automatica*, 2013, 49(5): 1419-1427.

[111] Wang X H, Ji H B. Leader-follower consensus for a class of nonlinear multi-agent systems [J]. *International Journal of Control, Automation and Systems*, 2012, 10(1): 27-35.

[112] Xiao F, Wang L. Consensus problems for high-dimensional multi-agent systems [J]. *IET Control Theory & Applications*, 2007, 1(3): 830-837.

[113] Wang J, Cheng D, Hu X. Consensus of multi-agent linear dynamic systems [J]. *Asian Journal of Control*, 2008, 10(2): 144-155.

[114] Jiang F, Wang L, Xie G. Consensus of high-order dynamic multi-agent systems with switching topology and time-varying delays [J]. *Journal of Control Theory and Applications*, 2010, 8(1): 52-60.

[115] Lin P, Li Z, Jia Y, *et al*. High-order multi-agent consensus with dynamically changing topologies and time-delays [J]. *IET Control Theory & Applications*, 2011, 5(8): 976-981.

[116] Liu Y, Jia Y. Consensus problem of high-order multi-agent systems with external disturbances: An H_∞ analysis approach [J]. *International Journal of Robust and Nonlinear Control*, 2010, 20(14): 1579-1593.

[117] Amitanand S, Sanketh I, Srinathant K, *et al*. Distributed consensus in the presence of sectional faults [C]. *Proceedings of the 2003 ACM Symposium on Principles of Distributed Computing*. Boston, MA, USA, 2003: 202-210.

[118] Vaidya N H, Garg V K. Byzantine vector consensus in complete graphs [C]. *Proceedings of the 2013 ACM Symposium on Principles of Distributed Computing*. Montreal, Quebec, Canada, 2013: 65-73.

[119] Qin J, Zheng W X, Gao H. Consensus of multiple second-order vehicles with a time-varying reference signal under directed topology [J]. *Automatica*, 2011, 47(9): 1983-1991.

[120] Ren W. On consensus algorithms for double-integrator dynamics [J]. *IEEE Transactions on Automatic Control*, 2008, 53(6): 1503-1509.

[121] Dimarogonas D V, Frazzoli E, Johansson K H. Distributed event-triggered control for multi-agent systems [J]. *IEEE Transactions on Automatic Control*, 2012, 57(5): 1291-1297.

[122] Fan Y, Feng G, Wang Y, *et al*. Distributed event-triggered control of multi-agent systems with combinational measurements [J]. *Automatica*, 2013, 49(2): 671-675.

[123] Seyboth G S, Dimarogonas D V, Johansson K H. Event-based broadcasting for multi-agent average consensus [J]. *Automatica*, 2013, 49(1): 245-252.

[124] Bauso D, Giarré L, Pesenti R. Non-linear protocols for optimal distributed consensus in networks of dynamic agents [J]. *Systems & Control Letters*, 2006, 55(11): 918-928.

[125] Hu J, Prandini M, Tomlin C. Interesting conjugate points in formation constrained optimal multi-agent coordination [C]. *Proceedings of the American Control Conference*, Portland, OR, USA, 2005: 1871-1876.

[126] Olfati-Saber R. Ultrafast consensus in small-world networks [C]. *Proceedings of the American Control Conference*, Portland, OR, USA, 2005: 2371-2378.

[127] Xiao L, Boyd S. Fast linear iterations for distributed averaging [J]. *Systems & Control Letters*, 2004, 53(1): 65-78.

[128] Hu H, Yu L, Zhang W A, *et al*. Group consensus in multi-agent systems with hybrid protocol [J]. *Journal of the Franklin Institute*, 2013, 350(3): 575-597.

[129] Feng Y, Xu S, Zhang B. Group consensus control for double-integrator dynamic multi-agent systems with fixed communication topology [J]. *International Journal of Robust and Nonlinear Control*, 2014, 24(3): 532-547.

[130] Li X F, Leung A C S, Liu X J, *et al*. Adaptive synchronization of identical chaotic and hyper-chaotic systems with uncertain parameters [J]. *Nonlinear Analysis: Real World Applications*, 2010, 11(4): 2215-2223.

[131] Su H, Chen G, Wang X, *et al*. Adaptive second-order consensus of networked mobile agents with nonlinear dynamics [J]. *Automatica*, 2011, 47(2): 368-375.

[132] Kashyap A, Başar T, Srikant R. Consensus with quantized information updates [C]. *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, 2006: 2728-2733.

[133] Danskin J M. The theory of max-min, with applications [J]. *SIAM Journal on Applied Mathematics*, 1966, 14(4): 641-664.

[134] Seneta E. *Non-negative matrices and Markov chains* [M]. New York Heidelberg Berlin: Springer Science & Business Media, 2006.

[135] 郑大钟. *线性系统理论(第二版)* [M]. 北京: 清华大学出版社, 2002.

[136] El Ghaoui L, Feron E, Balakrishnan V. *Linear matrix inequalities in system and control theory* [M]. Philadelphia: Society for Industrial and Applied Mathematics, 1994.

[137] Ren W, Beard R W. *Distributed consensus in multi-vehicle cooperative control* [M]. London: Springer-Verlag, 2008.

[138] Cortés J. Finite-time convergent gradient flows with applications to network consensus [J]. *Automatica*, 2006, 42(11): 1993-2000.

[139] Chen H, Wang C, Zhang B, *et al*. Saturated tracking control for nonholonomic mobile robots with dynamic feedback [J]. *Transactions of the Institute of Measurement and Control*, 2013, 35(2): 105.

[140] 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, 2009: 4894-4901.

[141] Dibaji S M, Ishii H. Resilient consensus of double-integrator multi-agent systems [C]. *Proceedings of the American Control Conference*, Portland, Oregon, USA, 2014: 5139-5144.

[142] Zhao C, He J, 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, 2014: 1182-1187.

[143] 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, 2014: 1-7.

[144] 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, 2012: 365-374.

[145] Song H, Zhu S, Cao G. Attack-resilient time synchronization for wireless sensor networks [J]. *Ad Hoc Networks*, 2007, 5(1): 112-125.

[146] Hu X, Park T, Shin K G. Attack-tolerant time-synchronization in wireless sensor networks [C]. *Proceedings of the 27th Conference on Computer Communications*. Phoenix, AZ, USA, 2008: 448-456.

[147] Eui-Jik K I M, Jeongsik I N, Sungkwan Y, *et al*. Delay attack-resilient clock synchronization for wireless sensor networks [J]. *IEICE Transactions on Information and Systems*, 2012, 95(1): 188-191.

[148] Zhang H, Sundaram S. Robustness of information diffusion algorithms to locally bounded adversaries [C]. *Proceedings of the American Control Conference*, Fairmont Queen Elizabeth, Montréal, Canada, 2012: 5855-5861.

[149] Wolfowitz J. Products of indecomposable, aperiodic, stochastic matrices [J]. *Proceedings of the American Mathematical Society*, 1963, 14(5): 733-737.

[150] Wu Y, He X, Liu S, Xie L. Consensus of discrete-time multi-agent systems with adversaries and time delays [J]. *International Journal of General Systems*, 2014, 43(3-4): 402-411.

[151] Godsil C, Royle G F. *Algebraic graph theory* [M]. New York, USA: Springer-Verlag, 2001.

[152] Ren W, Atkins E. Distributed multi-vehicle coordinated control via local information exchange [J]. *International Journal of Robust and Nonlinear Control*, 2007, 17(10-11): 1002-1033.

[153] Zhang H, Feng G, Yan H, *et al*. Observer-based output feedback event-triggered control for consensus of multi-agent systems [J]. *IEEE Transactions on Industrial Electronics*, 2014, 61(9): 4885-4894.

[154] Li J, Li J. Adaptive iterative learning control for coordination of second-order multi-agent systems [J]. *International Journal of Robust and Nonlinear Control*, 2014, 24(18): 3282-99.

[155] Su H, Chen G, Wang X, Lin Z. Adaptive second-order consensus of networked mobile agents with nonlinear dynamics [J]. *Automatica*, 2011, 47(2): 368-75.

[156] Hu G. Robust consensus tracking of a class of second-order multi-agent dynamic systems [J]. *Systems & Control Letters*, 2012, 61(1): 134-42.

[157] Song Q, Cao J, Yu W. Second-order leader-following consensus of nonlinear multi-agent systems via pinning control [J]. *Systems & Control Letters*, 2010, 59(9): 553-62.

[158] Yanping G, Long W. Sampled-data based consensus of continuous-time multi-agent systems with time-varying topology [J]. *IEEE Transactions on Automatic Control*, 2011, 56(5): 1226-31.

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

[160] 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.

[161] Lamport L, Shostak R, Pease M. The Byzantine generals problem [J]. *ACM Transactions on Programming Languages and Systems*, 1982, 4(3): 382-401.

[162] LeBlanc H J, Zhang H, Koutsoukos X, Sundaram S. Resilient asymptotic consensus in robust networks [J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(4): 766-781.

[163] Lee D, Spong M W. Agreement with non-uniform information delays [C]. *Proceedings of the 2006 American Control Conference*, Minneapolis, Minnesota, USA, 2006: 756-761.

[164] Haddock J R, Terjéki J. Liapunov-Razumikhin functions and an invariance principle for functional differential equations [J]. *Journal of Differential equations*, 1983, 48(1): 95-122.

[165] Danskin J M. The theory of max-min, with applications [J]. *SIAM Journal on Applied Mathematics*, 1966, 14(4): 641-664.

[166] Shi G D, Johansson K H, Hong Y G. Reaching an optimal consensus: dynamical systems that compute intersections of convex sets [J]. *IEEE Transactions on Automatic Control*, 2013, 58(3): 610-622.

[167] 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.

[168] Ahn H S, Chen Y Q. Iterative learning control for multi-agent formation [C]. *Proceedings of the ICROS-SICE International Joint Conference*, Fukuoka, Japan, 2009: 3111-3116.

[169] Yang S, Xu J X, Ren Q. Multi-agent consensus tracking with initial state error by iterative learning control [C]. *Proceedings of the 11th IEEE International Conference on Control & Automation*, Taichung, Taiwan, 2014: 625-630.

[170] Xu J. Adaptive iterative learning control for high-order nonlinear multi-agent systems consensus tracking [J]. *Systems & Control Letters*, 2016, 89(2016): 16-23.

[171] Meng D, Jia Y. Iterative learning approaches to design finite-time consensus protocols for multi-agent systems [J]. *Systems & Control Letters*, 2012, 61(2012): 187-194.

[172] Liu X, XLam J, Yu W, Chen G. Finite-Time Consensus of Multiagent Systems With a Switching Protocol [J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2016, 27(4): 853-862.

[173] Meng D, Jia Y, Du J. Finite-Time Consensus for Multiagent Systems With Cooperative and Antagonistic Interactions [J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2016, 27(4): 762-770.

[174] 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.

[175] 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.

[176] Kieckhafer R M, Azadmanesh M H. Reaching approximate agreement with mixed-mode faults [J]. *IEEE Transactions on Parallel and Distributed Systems*, 1994, 5(1): 53-63.

[177] Dolev D, Lynch N A, Pinter S S, et al. Reaching approximate agreement in the presence of faults [J]. *Journal of the ACM*, 1986, 33(3): 499-516.

[178] Xiao F, Wang L. Consensus protocols for discrete-time multi-agent systems with time-varying delays [J]. *Automatica*, 2008, 44(10): 2577-2582.

[179] Hom R A, Johnson C R. *Matrix analysis* [M]. Cambridge, UK: Cambridge University Express, 1985.

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

[181] Gupta V, Langbort C, Murray R M. On the robustness of distributed algorithms [C]. *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, 2006: 3473-3478.

[182] Spears D, Kerr W, Spears W. *Safety and security multi-agent systems* [M]. Berlin Heidelberg: Springer-Verlag, 2009.

[183] Jung Y, Kim M, Masoumzadeh A, Joshi J B. A survey of security issue in multi-agent systems [J]. *Artificial Intelligence Review*, 2012, 37(3): 239-260.

[184] Cavalcante R C, Bittencourt I I, da Silva A P, *et al*. A survey of security in multi-agent systems [J]. *Expert Systems with Applications*, 2012, 39(5): 4835-4846.

[185] Bijani S, Robertson D. A review of attacks and security approaches in open multi-agent systems [J]. *Artificial Intelligence Review*, 2014, 42(4): 607-636.

[186] Ghanea-Hercock R, Gifford I. Top-secret multi-agent systems [J]. *Electronic Notes in Theoretical Computer Science*, 2002, 63: 77-90.

[187] Greenberg M S, Byington J C, Harper D G. Mobile agents and security [J]. *IEEE Communications Magazine*, 1998, 36(7): 76-85.

[188] Wang S, Hu J, Liu A, Wang J. Security frame and evaluation in mobile agent system [C]. *Proceedings of the 2nd International Conference on Mobile Technology, Applications and Systems*, Guangzhou, China, 2005: 1-6.

[189] LeBlanc H J, Zhang H, Sundaram S, Koutsoukos X. Resilient continuous-time consensus in fractional robust networks [C]. *Proceedings of the American Control Conference*, Washington, DC, USA, 2013: 1237-1242.

[190] Haseltalab A, Akar M. Approximate byzantine consensus in faulty asynchronous networks [C]. *Proceedings of the American Control Conference*, Chicago, IL, USA, 2015: 1591-1596.

[191] Zhu Q, Bushnell L, Başar T. *Resilient distributed control of multi-agent cyber-physical systems* [M]. Switzerland: Springer International Publishing, 2013.

[192] Li Z, Duan Z, Chen G, Huang L. Consensus of multiagent systems and synchronization of complex networks: a unified viewpoint [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2010, 57(1): 213-224.

[193] Li Z, Liu X, Lin P, Ren W. Consensus of linear multi-agent systems with reduced-order observer-based protocols [J]. *Systems & Control Letters*, 2011, 60(7): 510-516.

[194] Hong Y, Hu J, Gao L. Tracking control for multi-agent consensus with an active leader and variable topology [J]. *Automatica*, 2006, 42(7): 1177-1182.

致　　谢

时光荏苒，在博士生涯进入尾声之际，我谨以最诚挚的声音向所有在我求学时光里给予我帮助的师长、同窗和亲友们表示衷心的感谢。

在此，我要深深感谢我的导师何熊熊教授。何老师尽自己所能为我创造了良好的学习和科研环境，同时在生活中给予我无微不至的亲切关怀，使我的论文得以顺利完成。可以说，我今天取得的成绩和进步，得益于导师的大力培养，这里面倾注了他大量的心血。他不止教授我如何做学问，更教给我许多为人处世的基本道理。他曾试想扮演一个严师的角色，却又总是不忍心带给我压力。导师渊博的学识、幽默风趣的人格魅力、积极乐观的生活态度，为我树立了一辈子学习的典范，有幸师从何老师，实为我平生一大幸事！我们一起学习讨论，一起参会郊游，甚至一同在田间劳作，在滩涂捉蛏子，点点滴滴，渗透了我的整个研究生学习阶段。所有的一切，学生都将铭记于心。在今后的日子里，唯使自己更加努力地学习和工作，以不辜负恩师对我的栽培和期望！

诚挚感谢新加坡南洋理工大学谢立华教授在我两年的交流学习期间给予的悉心指导。谢老师渊博的专业知识、严谨的治学态度、精益求精的工作作风，深深感染了我，并不断激励我努力前行。每周一次的学术报告会让我感受到国际知名学者做学问的认真态度和精神。在南洋理工大学交流学习是一段愉快而又宝贵的经历，令我终身受益。

感谢在我求学期间，智能系统与机器人研究所的庄华亮老师、李胜老师、汤健彬老师、张霓老师对我学习及研究工作给予的帮助与支持！还要感谢实验室的同门博士生沈林武、秦贞华、武宪青、欧县华、陈中天、丁佳骏，以及硕士生师弟师妹们，感谢你们给予我学习和生活中的支持和帮助！这个团结、友爱、互助的大家庭，给了我太多的美好回忆。

感谢我的师娘胡朝阳女士给予我学习、工作和生活等各个方面的悉心关怀和热心帮助！

感谢在我新加坡留学期间，传感器网络实验室（Sensor Network Lab）的同窗好友们。他（她）们是：刘帅、黄宝琦、李武全、李韬、郭宇骞、赵东亚、屈小媚、李建祯、徐俊、游科友、孟伟、肖楠、胡劲文、高婷婷、俞成浦、杨在、江灏、张奎泽、朱善迎、李海涛、王力立、张生凤、焦强、刘正凡、忻克菲、刘梦晨、朱翠、王雪鹤、徐梁、邹焓、邱智荣、卢晓轩、郭克信。与你们相处的日子纯粹而又

快乐，与你们的珍贵友谊是我一生的财富。

感谢我的父母，感谢你们在我求学过程中的每一次选择所给予的充分尊重和全力支持。

谨以此文献给所有帮助我、关心我、支持我的亲人和朋友。

伍益明

二〇一六年五月于屏峰校区

攻读博士学位期间的研究成果及发表的论文

发表/录用的期刊论文

[1] **Wu Yiming**, He Xiongxiong, Liu Shuai, Xie Lihua. Consensus of discrete-time multi-agent systems with adversaries and time delays. *International Journal of General Systems*, 2014, 43(3-4): 402-411.

[2] **Wu Yiming**, He Xiongxiong. Secure consensus control for multi-agent systems with attacks and communication delays. *IEEE/CAA Journal of Automatica Sinica*, accepted.

[3] **伍益明**, 丁佳骏, 何熊熊, 欧县华. 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*, 录用.

发表/录用的会议论文

[1] **Wu Yiming**, Zheng Jingyi, He Xiongxiong. A quantized-data based resilient consensus algorithm. *Proceedings of the 4th International Conference on Computer Science and Network Technology*, 2015.

[2] **Wu Yiming**, He Xiongxiong, Ou Xianhua. Distribute consensus for multi-agent systems with attacks and delays. *Proceedings of the 34th Chinese Control Conference*, 2015.

[3] **Wu Yiming**, He Xiongxiong, Liu Shuai, Qin Zhenhua. A secure finite-time consensus scheme for multi-agent systems via terminal iterative learning. *Proceedings of the 35th Chinese Control Conference*, 2016.

[4] **Wu Yiming**, He Xiongxiong, Liu Shuai. Resilient consensus for multi-agent systems with quantized communication. *Proceedings of the 2016 American Control Conference*, 2016.

[5] Zheng Jingyi, He Xiongxiong, **Wu Yiming**, Qin Zhenhua. Iterative Learning Control with a Forgetting Factor for Consensus Tracking in Multi-agent Systems. *Proceed-*

ings of the 28th Chinese Control and Decision Conference, 2016.

[6] Ou Xianhua, He Xiongxiong, Cai Wenjian, **Wu Yiming**. A Simple Dynamic Model of Dehumidifier for Control and Optimization in LDDS. *Proceedings of the 11th IEEE Conference on Industrial Electronics and Applications*, 2016.

在投期刊论文

[1] **Wu Yiming**, He Xiongxiong, Wu Xianqing. Secure consensus for non-linear multi-agent systems under malicious attacks. *IEEE Transactions on Automatic Control*, under review.

[2] **Wu Yiming**, He Xiongxiong. Finite-time secure consensus protocols for multi-agent systems under attacks. *International Journal of Systems Science*, under review.

[3] Wu Xianqing, He Xiongxiong, **Wu Yiming**, Li Sheng. A regulation control method for overhead cranes. *IEEE Transactions on Industrial Electronics*, minor revision.

发明专利

[1] 一种恶意环境下的多智能体系统安全趋同控制方法. 第一发明人,
专利号: 201510788018.7

[2] 基于改进型粒子滤波的多智能体网络目标跟踪方法. 第一发明人,
专利号: 201510786472.9

[3] 基于无线传感技术的楼宇能耗监测分析系统. 第一发明人,
专利号: 201120128468.0

作为主要人员参加的科研项目

[1] 国家自然科学基金: 迭代学习控制有限精度下优化设计与实现及其应用研究 (61473262).

[2] 国家自然科学基金: 基于多收缩系数的参数估计自适应算法在无线传感器系统中的应用 (61503339).

[3] 国家科技支撑计划课题: 安全高效自动桥式吊车关键技术与系统集成 (2013BAF07B03).