

Distributed Resilient Coordination for Networked Multi-Agent Systems



FENG ZHI

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in fulfillment of the requirements for the degree of
Doctor of Philosophy

May 2017

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

Date

FENG ZHI

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor, Dr. Guoqiang Hu, for his patient guidance, generous help and encouragement which will benefit me a life time. As an advisor, he kept polishing my methodology and skills in doing research. As a mentor, he provided me with substantial research freedom and helped me prepare for future academic career with his professional skills and techniques. His specialty standard and rigorous attitude towards research will affect the rest of my life.

Thanks to the former and present members in Intelligent Robotics Lab for their friendship, discussions and kindly help during my PhD study. Thanks to all my friends at NTU. All the fun that we have had made my study and life in Singapore much more enjoyable.

Finally, I would like to greatly thank my parents and little sister for their encouragement, support and endless love.

Abstract

Critical infrastructures such as smart grid, wireless networks and multi-robot systems, are typical examples of networked multi-agent systems that consist of large-scale physical processes monitored and controlled over a set of communication networks and computers. The use of modern information and communication technologies typically adds efficiency, flexibility and scalability. However, it also increases the vulnerabilities to human operator mistakes, physical failures and cyber-attacks. Thus, an urgent need, for safety critical infrastructures, is to enhance resilience against physical failures as well as cyber-attacks. Control systems play a key role in critical infrastructure protection and performance recovery. It is of theoretical significance and practical relevance to develop resilient control algorithms for systems to provide high levels of robustness, reliability and security.

This dissertation investigates *distributed resilient coordination* in networked multi-agent systems. It aims to develop algorithms and techniques for networked agents to autonomously coordinate their actions/decisions and achieve a system-level group objective. The background, motivation and preliminaries for this topic are presented in the first two chapters. The problems studied in dissertation include: 1) distributed robust cooperative control; 2) distributed secure coordination.

Part I: distributed robust cooperative control. This dissertation starts with fundamental problems of consensus and consensus tracking. In the presence of uncertainties and disturbances, how to develop control algorithms for multiple unknown

Euler-Lagrange systems is studied to achieve robust coordination. In such a problem, the agents are not only influenced by interactions among neighboring agents, but also by their own dynamics with unknown uncertainties and disturbances. Identifier-based, continuous, distributed robust control algorithms are developed such that the states of all the agents reach consensus and track a desired time-varying trajectory under different communication topologies, respectively.

Next, we address a robust connectivity preserving rendezvous problem for mobile multi-robot systems under unknown dynamics and disturbances. By virtue of a potential field approach, a gradient-based distributed robust control scheme is proposed such that connectivity preserving rendezvous is achieved in the presence of unknown dynamics and disturbances. It is proven that although the multi-robot network has a time-varying network topology, the developed distributed controller is not only able to maintain the connectivity of an initially connected network, but also to guarantee that all the robots can track a desired time-varying trajectory.

Part II: distributed secure coordination. This part focuses on distributed control of networked multi-agent systems subject to different types of cyber-attacks. Works on resilience architecture, attack modeling and approaches for specific issues are studied. We firstly consider a distributed secure control problem for systems under two types of switching attacks. Attacks on edges of agents lead to loss of consensus performance. Two distributed secure control laws are developed for solving the issues from a switching perspective. Conditions on secure consensus are derived. Then, this work is extended to secure coordination in the presence of strategic attacks. We model these attacks with their dynamics captured by a random Markov process. A hybrid stochastic secure control scheme with a connectivity restoration mechanism is provided. It is shown that with the proposed design, secure consensus tracking is achieved in a mean-square sense. The effect of strategic attacks on discrete-time systems is also investigated.

In addition, we also consider an event-based resilient coordination for linear multi-agent systems under Denial-of-Service (DoS) attacks. The DoS attacks refer to interruptions of communications on the control channels carried out by an intelligent adversary. We model a time-sequence-based DoS attack allowed to occur aperiodically in an unknown attack strategy. An explicit analysis of frequency and duration of DoS attacks is investigated for secure leaderless and leader-following consensus issues. An event-based distributed control scheme is proposed and suitable scheduling of controller updating times is determined in the presence of DoS attacks. It is proven that under the proposed controller, the agent group can achieve secure consensus exponentially.

In summary, this dissertation investigates resilient coordination techniques for networked multi-agent systems in complex environments. On one hand, when the systems are subject to unknown uncertainties and disturbances, distributed robust cooperative control is studied. To solve this issue, an identifier-based, continuous distributed robust control approach is proposed. On the other hand, when the systems are subject to different types of cyber-attacks, distributed secure coordination is studied. A hybrid distributed secure control scheme is developed. To demonstrate the theoretical significance and practical relevance of our proposed algorithms in this dissertation, distributed multi-robot coordination and distributed voltage regulation of microgrid are investigated, respectively. Finally, brief conclusions and future work are presented in Chapter 8.

Contents

Acknowledgements	i
Abstract	iii
List of Contents	vii
List of Figures	xii
Symbols and Acronyms	xvi
1 Introduction	1
1.1 Background, Motivation and Objective	1
1.1.1 Threats Against Networked Multi-Agent Systems	2
1.1.2 Vulnerability Classification and Examples	4
1.1.3 Problem Formulation and A Potential Solution	11
1.2 Literature Review	13
1.2.1 Networked Multi-Agent Systems	13
1.2.2 Distributed Robust Cooperative Control	14
1.2.3 Distributed Secure Coordination	17
1.3 Contributions	20
1.4 Organization of the Thesis	23

2	Preliminaries	24
2.1	Graph Theory	24
2.2	Nonsmooth Analysis	26
2.3	Switched System Theory	27
I	Distributed Robust Cooperative Control	29
3	Robust Distributed Coordinated Control of Multiple Unknown Euler-Lagrange Systems	30
3.1	Introduction	30
3.2	Problem Formulation	32
3.2.1	Agent Model	32
3.2.2	Control Objective	33
3.3	Robust Distributed Coordination Under An Undirected Graph . . .	34
3.3.1	Robust Consensus Tracking Control Law Design	34
3.3.2	Filtered Error Dynamics	35
3.3.3	Closed-Loop System Development	36
3.3.4	Stability Analysis and Sufficient Conditions	38
3.4	Robust Distributed Coordination Under A Directed Graph	43
3.4.1	Distributed Leader Estimator Design	44
3.4.2	Robust Consensus Tracking Control Law Design	45
3.4.3	Closed-Loop System Development	46
3.4.4	Stability Analysis and Sufficient Conditions	47
3.5	Numerical Example	49
3.5.1	Robust consensus tracking under an undirected graph	50
3.5.2	Robust consensus tracking under a directed graph	52
3.6	Conclusion	55

4 Robust Connectivity Preserving Rendezvous of Multiple Mobile Robot Systems	56
4.1 Introduction	56
4.2 Problem Formulation	58
4.2.1 Multi-Robot Model	58
4.2.2 Connectivity Preservation Description	59
4.2.3 Control Objective	61
4.3 Robust Connectivity Preserving Rendezvous	62
4.3.1 Potential Function	62
4.3.2 Filtered Error Design	63
4.3.3 Distributed Control Law Design	63
4.3.4 Stability Analysis and Sufficient Condition	66
4.4 Numerical Example	73
4.5 Conclusion	75
 II Distributed Secure Coordination	 79
5 Distributed Consensus Tracking for Multi-Agent Systems under Two Types of Attacks	80
5.1 Introduction	80
5.2 Problem Formulation	82
5.2.1 Attack Model	83
5.2.2 Attacker and Defender Strategies	85
5.2.3 Control Objective	85
5.3 Exponential Consensus Tracking Under Only Connectivity-Maintained Attacks	86
5.4 Exponential Consensus Tracking Under Mixed Connectivity-Maintained /Broken Attacks	91

5.5	Numerical Example	97
5.6	Conclusion	101
6	Distributed Secure Coordinated Control for Multi-Agent Systems under Strategic Attacks	102
6.1	Introduction	102
6.2	Problem Formulation	104
6.2.1	Attack Model	105
6.2.2	Hybrid Stochastic Secure Control Framework	106
6.2.3	Control Objective	107
6.3	Mean-Square Consensus Under A Class of Strategic Attacks	107
6.3.1	Time-varying Markovian Graph	108
6.3.2	Connectivity Restoration Mechanism	108
6.3.3	Distributed Secure Control Law Design	109
6.3.4	Attack Frequency and Attack Length Rate	110
6.3.5	Stability Analysis	111
6.3.6	Extension to Discrete-time Case	117
6.4	Numerical Example	121
6.5	Conclusion	127
7	Distributed Event-Triggered Control of Linear Multi-Agent Sys- tems Subject to DoS Attacks	128
7.1	Introduction	128
7.2	Problem Formulation	130
7.2.1	Multi-Agent Network Model	130
7.2.2	DoS Attack Model	130
7.2.3	Control Objective	132
7.3	Event-Triggered Secure Leaderless Consensus	133

7.3.1	Distributed Event-triggered Controller Design	133
7.3.2	DoS Attack Frequency and Attack Duration	135
7.3.3	Stability Analysis of Secure Leaderless Consensus	136
7.4	Secure Leader-Following Consensus	145
7.4.1	Leader-Following Event-Triggered Controller Design	145
7.4.2	Stability Analysis of Secure Leader-Following Case	146
7.5	Numerical Example	150
7.5.1	Multi-Robot Simulation Setup & Conditions	150
7.5.2	Secure Leaderless Consensus	150
7.5.3	Secure Leader-Following Consensus	151
7.5.4	Microgrid Simulation Setup & Conditions	153
7.5.5	Secure Voltage Regulation	154
7.6	Conclusion	156
8	Conclusions and Future Work	157
8.1	Conclusions	157
8.2	Future Work	159
	Appendix A $\mathcal{P}(t)$ Is Nonnegative (Chapter 3)	161
	Appendix B System (3.40) Is Stable.	163
	Author's Publications	166
	Bibliography	166

List of Figures

1.1	Networked multi-agent systems.	2
1.2	Numbers of cyber security incidents reported to ICS-CERT. <i>Source:</i> ICS-CERT [35].	3
1.3	The percentages of cyber security incidents reported to ICS-CERT for different fields of systems in Fiscal Year 2014 [35].	4
1.4	Vulnerabilities in networked multi-agent systems.	5
1.5	A block diagram of malicious cyber-attacks on a communication net- work: (a) Data availability violation by a DoS attack; (b) Data in- tegrity violation by a false injection attack; (c) Data confidentiality violation by an eavesdropping attack.	8
1.6	A block diagram of smart grid and its variety of possible vulnerabil- ities in systems.	9
1.7	A block diagram of closed-loop Medical Device Systems (MDSs) and its variety of possible vulnerabilities in systems.	10
1.8	A multi-layer distributed resilient monitoring and control structure. .	12
1.9	Event-based mechanism under the condition (1.1): (a) in the absence of DoS attacks; (b) in the presence of DoS attacks. $\{t_{k_i}^i\}$ and $\{\tilde{t}_m\}$ represent the event time sequence and the DoS attack time sequence, respectively.	19

3.1	Diagram of the two-layer based distributed control law design.	46
3.2	An information-exchange undirected graph. Circles denote the labeled agents and the connecting lines denote weighted information edges among all agents. The desired time-varying trajectory is denoted as a virtual leader.	51
3.3	Trajectories of the states of the followers and the leader under (3.5)-(3.8).	51
3.4	Tracking errors between the followers and the leader under (3.5)-(3.8).	51
3.5	The control input τ_i in (3.5) and the convergence of β_{1i} in (3.8).	52
3.6	A directed graph. Circles denote the labeled agents and the connecting lines denote weighted information edges among all agents and a virtual leader.	53
3.7	Trajectories of the estimated states of the followers and the leader under the developed distributed leader estimator (3.37).	53
3.8	Estimated state tracking errors between the followers and the leader under the developed distributed leader estimator (3.37).	54
3.9	Trajectories of the states of the followers and the leader under (3.43).	54
3.10	Tracking errors between the followers and the leader under (3.43).	55
4.1	The model of mobile sensing robot networks. The robot 2 collects measurements from neighboring robots 1 and 3 in an R interactive range.	59
4.2	Distances among initially connected robots.	75
4.3	Position differences between the followers and the leader.	76
4.4	Velocity differences between the followers and the leader.	76
4.5	Rendezvous for one leader (black circle) and six follower robots (red circle): (A) initial configuration; (B) configuration at $t = 2.5s$; (C) configuration at $t = 5.6s$; (D) final configuration.	77

4.6	Plot of the potential function $\varphi(\ \xi_{ji}\ _\sigma)$ in (4.47).	77
4.7	Control input u_i in (4.10).	78
4.8	The convergence of the time-varying gain β_{1i} in (4.15).	78
5.1	Examples of the network topology under two types of attacks: (a) network topology under m connectivity-maintained attacks; (b) network topology under l connectivity-broken attacks.	84
5.2	Framework of attacker and defender strategies in multi-agent systems.	85
5.3	Switching topologies \mathcal{G}_1 and \mathcal{G}_2 in Example 5.1.	97
5.4	State trajectories $x_{ij}(t)$, $i = 0, 1, 2, \dots, 4$, $j = 1, 2, 3, 4$ under (5.5).	98
5.5	Switching topologies \mathcal{G}_3 , \mathcal{G}_4 , and \mathcal{G}_5 in Example 5.2.	99
5.6	State trajectories $x_{ij}(t)$, $i = 0, 1, 2, \dots, 4$, $j = 1, 2, 3, 4$ under (5.29).	99
5.7	IEEE 6-bus test system: (a) the single-line diagram, (b) the corresponding communication graph under attacks.	101
5.8	(a), (b) and (c) represent DG voltage magnitudes under different attack cases, respectively. (d) represents the signal $\tilde{\sigma}(t) \in \tilde{\Xi}$	101
6.1	Hybrid stochastic secure control framework in a multi-agent system.	107
6.2	Initial communication topologies \mathcal{G}_0 (a) and topologies under strategic attacks \mathcal{G}_1 , \mathcal{G}_2 , \mathcal{G}_3 (b-(d)) in Example 6.1.	122
6.3	Switching signal $\gamma(t)$ and $\sigma(t)$ in Example 6.1.	123
6.4	State trajectories $x_{ij}(t)$ under the distributed control law (6.11).	124
6.5	Consensus tracking errors $E_c(t)$	124
6.6	Switching signal $\gamma(k)$ and $\sigma(k)$ in Example 6.2.	126
6.7	State trajectories $x_{ij}(k)$ under the distributed control law (6.43).	126
6.8	Consensus tracking errors $E_d(k)$	127
7.1	Framework of the closed-loop multi-agent system under DoS attacks.	131
7.2	Sketch map of aperiodic time sequences: $\{\tilde{t}_m\}_{m \in \mathbb{N}}$ and $\{t_{k_i}^i\}_{k_i \in \mathbb{N}}$	132

7.3	Framework of event-based secure control setup with an estimator. . .	134
7.4	Communication topology of a multi-robot system: (a) in a leaderless consensus case; and (b) in a leader-follower consensus case.	151
7.5	Simulation results for secure consensus in the presence of DoS attack: (A) a sustained DoS attack with varying period and duty cycle, generated randomly. The vertical red stripes represent the time-intervals over which a DoS attack is active and it has an average duty cycle of 24%; (B) state trajectory $x_{ij}(t)$, $i = 1, 2, 3, 4, j = 1, 2$; (C) consensus error $Error_{\delta}(t)$; (D) occurrences of the events for all the robots. . . .	152
7.6	Simulation results for secure leader-following consensus in the presence of DoS attack: (A) a sustained DoS attack with an average duty cycle of 20%; (B) state trajectory $\eta_{ij}(t)$, $i = 2, \dots, 6, j = 1, 2$; (C) consensus tracking error $Error_{\eta}(t)$; (D) occurrences of the events for all the robots.	153
7.7	Distributed secondary control diagram of an islanded MG.	154
7.8	Simulation microgrid test system.	155
7.9	Simulation results for distributed voltage regulation of microgrid in the presence of DoS attack: (A) a sustained DoS attack with an average duty cycle of 20%; (B) state trajectory $V_{o, magi}(t)$, $i = 1, \dots, 4$; (C) voltage regulation error $Error_V(t)$; (D) occurrences of the events for all DGs.	155

Symbols and Acronyms

Algebraic Operator

A^T	transpose of matrix A
A^{-1}	inverse of matrix A
$\rho(A)$	spectral radius of matrix A
$\sigma(A)$	singular value of matrix A
$\text{tr}(A)$	summation of all the diagonal elements of matrix A
A_{ij}	the element in the i -th row and j -th column of matrix A
$\ \cdot\ $	ℓ^2 norm for vector or the induced norm for matrix
$\ \cdot\ _\infty$	ℓ^∞ norm for vector or the induced norm for matrix
$ E $	the number of elements in the finite set E
$\text{col}(x_1, x_2, \dots, x_n)$	column vector formed by x_1, x_2, \dots, x_n
$\text{diag}\{x_1, x_2, \dots, x_n\}$	block diagonal matrix formed by x_1, x_2, \dots, x_n
$M > 0 (M \geq 0)$	M is positive definite(semi-definite)
$M_1 > M_2 (M_1 \geq M_2)$	$M_1 - M_2$ is positive definite(semi-definite)

diag $\{\lambda_{ij}\}$	For $i \in \{1, 2, \dots, N\}, j \in \{1, 2, \dots, n\}$, it denotes an $Nn \times Nn$ dimensional diagonal matrix defined as
$\text{diag}\{\lambda_{ij}\} =$	$\begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 \\ 0 & \lambda_{12} & & \\ & & \ddots & \vdots \\ \vdots & & & \lambda_{1n} \\ & & & & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_{Nn} \end{bmatrix}$
$\lambda_{\max}(\cdot), \lambda_{\min}(\cdot)$	maximum and smallest eigenvalues
I_n	$n \times n$ identity matrix
$\mathbf{1}_n$	an n -dimensional column vector with all elements of 1
$\mathbf{0}_n$	an n -dimensional column vector with all elements of 0
\otimes	Kronecher product
\odot	elementwise vector multiplication
\triangleq	equality by definition

Sets and Spaces

\mathbb{R}	set of real numbers.
$\mathbb{R}_{\geq 0}$	set of real numbers greater than or equal to 0
\mathbb{R}^n	set of n dimensional real vectors
$\mathbb{R}^{m \times n}$	set of $m \times n$ dimensional real matrices
\mathbb{Z}	set of integers

\mathbb{N}	set of positive natural numbers
\mathcal{N}_i	the neighboring set of agent i
$Y \setminus X$	the relative complement of X in Y , i.e., the set of elements belonging to Y , but not to X

Acronyms

a.e.	almost everywhere
ARE	Algebraic Riccati Equation
LQR	Linear Quadratic Regulation
LMI	Linear Matrix Inequality
MVT	Mean Value Theorem
UUB	Uniformly Ultimately Bounded
PID	Proportional Integral Derivative
CPS	Cyber Physical System
UAV	Unmanned Aerial Vehicle
ICT	Information and Communication Technology
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
SCADA	Supervisory Control and Data Acquisition

Chapter 1

Introduction

1.1 Background, Motivation and Objective

Modern infrastructure systems tightly integrate the physical systems operating in the real world with the cyberspace of increasing amount of computational resources, communication capabilities and sensing. Several classic examples can be given: 1) physiological sensors that monitor patient's health continuously and enable fast delivery of therapies [1,2]; 2) smart buildings that detect absence of occupants and shut down the cooling units for energy efficiency [3]; and 3) unmanned vehicles that utilize the environment vision information to perform search, exploration and surveillance [4–6]. In these systems a common characteristic is to utilize information from physical space over a communication network, and then impact the physical infrastructures in the operations as shown in Fig. 1.1. It can be seen that the rapid advancement and wide use of ICT have fostered the emergence of a new generation of large-scale networked systems, namely *networked multi-agent systems*. Such systems are defined as a class of systems with their operations being monitored, coordinated, and integrated by a computing and communication core. Additionally, such systems involve online social networking so that they can have significant interactions with human operators and participants. Hence they have much potential to enable tremendous changes in human's life and potentially bring great benefits

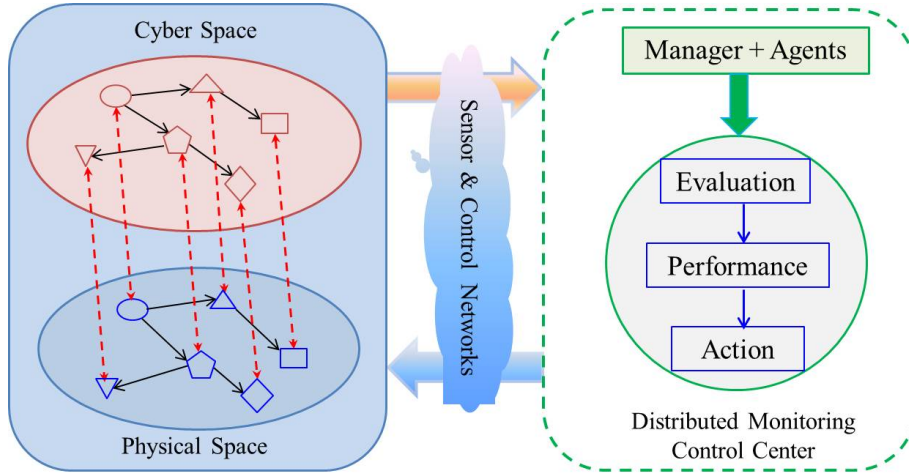


Figure 1.1: Networked multi-agent systems.

to our society. The widespread growth of network ICT has been creating a wide multitude of applications for networked multi-agent systems such as healthcare [2], autonomous vehicles [4,5], water network networks and smart critical infrastructures (e.g., smart building [1,3], smart transportation [5,6] and smart grid [7–9]).

In spite of the great importance and promise in engineering applications, there is a lack of scientific and systematic methodologies to understand and control networked multi-agent systems. Although their applications go across different domains, networked multi-agent systems share remarkable characteristics: they consist of large collections of networked agents who are capable of sensing, computation, communication and/or actuation that allows their interactions and abilities to solve issues beyond their individual capabilities. *The essential theme of controlling networked multi-agent systems is distributed decision-making; that is, developing algorithms and techniques for networked agents to coordinate their actions/decisions through local information exchanges and achieve a system-level group objective.*

1.1.1 Threats Against Networked Multi-Agent Systems

Networked multi-agent systems are prone to diverse threats in an unintentional or malicious way. In addition to failures on the physical infrastructures, systems are subject to malicious attacks on their communication networks as well as data

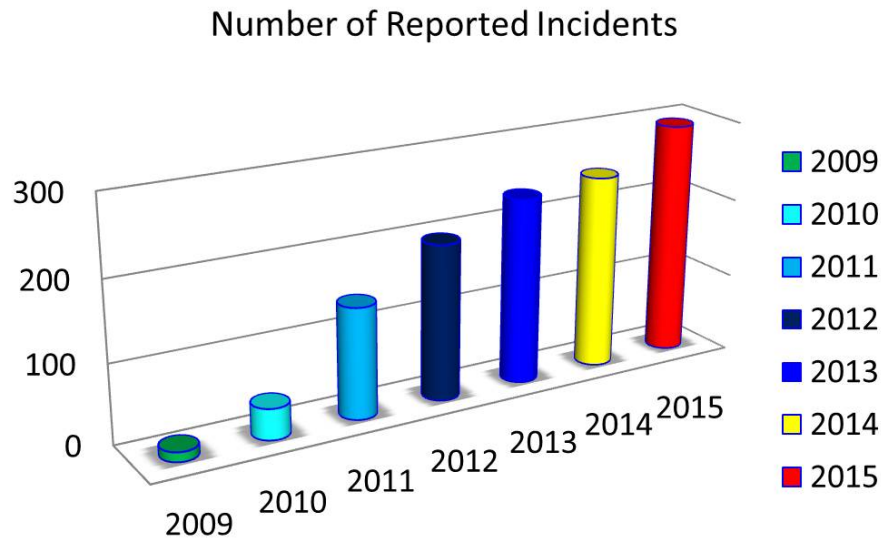


Figure 1.2: Numbers of cyber security incidents reported to ICS-CERT. *Source:* ICS-CERT [35].

management layers. While most networked multi-agent systems were safe in the past several decades, there were a few confirmed cases of malicious cyber-attacks [28]. The malwares “Stuxnet” and “Flame” [29] and “Maroochy Water Breach” incident [30] brought up discussions on how to make networked multi-agent systems safe from such cyber-attacks [31].

Take the incidents “Stuxnet” and “Maroochy Water Breach” for examples. The former [32] is a well-known case of an attack launched on the physical systems where StuxNet virus targeted Siemens’ SCADA systems. In the latter case, an attacker managed to successfully hack into the controllers in Maroochy Shire Council’s sewage control systems that activated and deactivated valves, causing inundation of grounds of a hotel, a park, and a river [30]. The readers can find more cases of malicious cyber-attacks in [33] and [34]. In fact, over the recent years, increasing cyber security incidents have been reported to ICS-CERT as shown in Fig. 1.2, while a classification of their percentages in variety of fields of practical systems is further presented in Fig. 1.3.

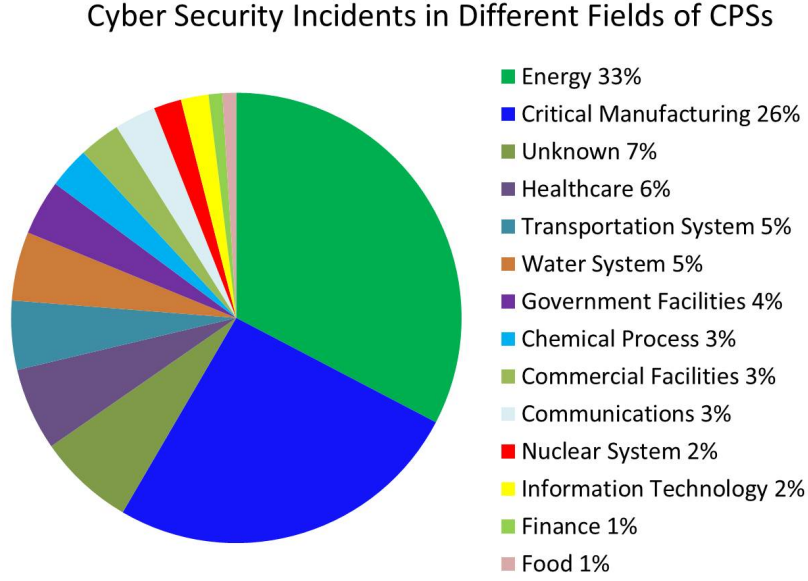


Figure 1.3: The percentages of cyber security incidents reported to ICS-CERT for different fields of systems in Fiscal Year 2014 [35].

Overall, the use of ICT improves efficiency and availability of systems. However, adding a layer of control and communication introduces increased vulnerabilities in systems to malicious cyber-attacks. Hence, it leads to new security challenges which are distinct from traditional information technology (IT) security as highlighted in [36]. The IT security solutions have shortcomings as they are implemented by a preventive device (e.g., a firewall, a reactive device, an anti-virus program or together). The recent security incidents demonstrate the inability of traditional information security approaches to achieving robust, reliable, and secure functionalities [7,8,33,37], which leads to severe social and economic consequences. Thus, there is an important need for resilient networked multi-agent systems.

1.1.2 Vulnerability Classification and Examples

Networked multi-agent systems are usually composed of multiple networked components, i.e., sensors, actuators, processing units and communication networks. Fig. 1.4 shows the closed-loop control model with interactions among physical systems, cyber systems and a distributed management control and monitoring center.

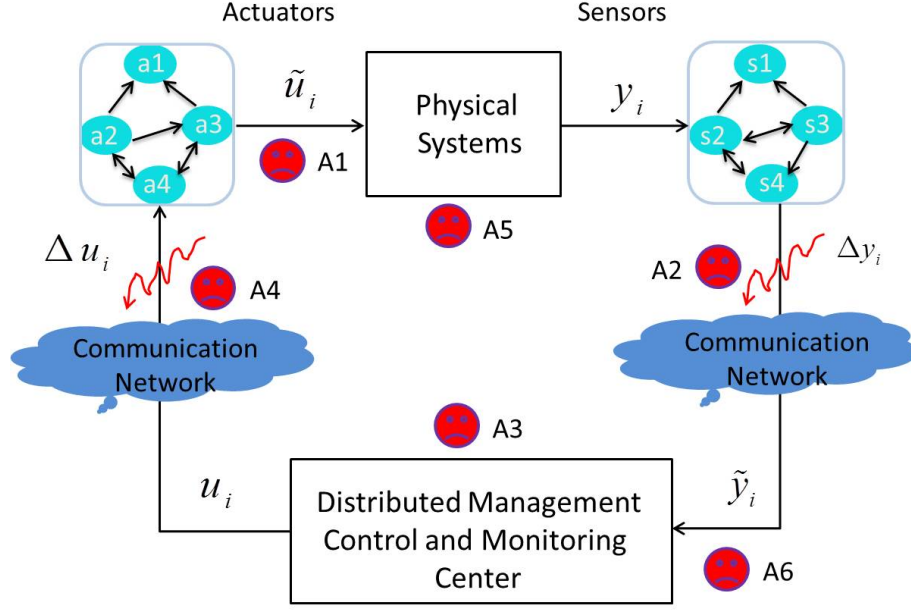


Figure 1.4: Vulnerabilities in networked multi-agent systems.

1. Sensors are the field devices measuring physical parameters (e.g., position, velocity, voltage and temperature).
2. Machine equipment is the component of physical systems being monitored.
3. Actuators are the mechanical devices which implement the changes on the machine equipment.
4. The distributed management control and monitoring center is the place where the measurement data from sensors is processed and analyzed such that the operational decisions can be made.
5. y_i is the measurement collected from the sensors.
6. u_i denotes the control messages carrying operational decisions sent to actuators.
7. Δu_i and Δy_i represents the false data injections in the control commands received by \tilde{u}_i , and in the measurements that are received by \tilde{y}_i , respectively.

Related to networked multi-agent system security goals: Availability, Integrity and Confidentiality, a variety of potential attacks A1-A6 in Fig. 1.4 can be summarized as follows.

- With respect to Availability, A1 and A6 represent a class of attacks (e.g., DoS). The adversary renders some or all the components in an inaccessible control system. Thus, Availability is violated. A DoS attack could be mounted by jamming the communication channels, compromising the devices, preventing them from sending data, and attacking the routing protocols, etc.
- With respect to Integrity, A2 and A4 represent a class of deception attacks (e.g., False data injection, Replay attacks). The adversary sends false information Δy_i and Δu_i via communication networks from sensors or controllers. Hence, Integrity is violated. The false information includes: incorrect measurement, its observed time and incorrect sender identity. These attacks can be performed by compromising sensors or controllers.
- With respect to Confidentiality, A3 represents a class of disclosure attacks (e.g. Eavesdropping attacks, Compromised-key attacks) in IT software and database. Attacks at the management level are similar to attacks in computer networks where the adversary can eavesdrop on communications to have access to the message contents. Confidentiality is thus violated.
- In addition to aforementioned malicious cyber-attacks, A5 represents a class of direct physical attacks on the plant. These attacks are modeled as the classic random and/or independent physical degradations and failures (e.g., disturbances, uncertainties and faults, etc).

Specifically, the specific malicious cyber-attacks are classified below.

1. DoS attacks compromise availability of data or resources by jamming the communication channels, compromising the devices, attacking the routing protocols, increasing the communication latency, etc.

a. Timing attacks, a variation of DoS attacks, introduce a delay in signal transmissions rather than completely denying communications between system and control.

b. Desynchronization attacks are a variation of timing attacks, targeting controls that require synchronizations.

2. Deception attacks refer to the possibility of compromising the integrity of control packets or measurements.

- a. False data injection attacks are a class of specific deception attacks by injecting new data in the network.
- b. Replay attacks are cast by hijacking sensors, recording readings for certain time and repeating while injecting an exogenous signal into system.
- c. Wormhole attacks receive packets at one point in network, “tunnels” them to a different point and then replays them, leading to dropping packets and time delays.
- d. Data integrity attacks can manipulate the signals to spurious values such that the control center makes wrong decisions or actuators incorrectly modify devices.

3. Disclosure attacks refer to the violation of confidentiality from keeping information secret from unauthorized users.

- a. Eavesdropping attacks refer to adversaries that can intercept any communication information in system.
- b. Compromised-key attacks refer to the possibility of compromising a key that is a secret code to interpret secure information. The attacker can decrypt or modify data by the compromising key, and further to compute additional keys to access other secured communications or resources.
- c. Virus-based attacks manipulate a legitimate user to bypass authentication and to have access to control mechanisms such that the malicious code injected by the attacker can be executed, e.g. (Trojan virus).

The modeling of these vulnerabilities is neither fully disjoint nor exhaustive. However, this classification is somehow helpful for us to study the resilience issues for networked multi-agent systems. Due to the tight coupling of interdependent dynamics among physical, cyber and social realms, these interdependent and intertwined vulnerabilities will make resilient design and analysis become especially profound. Table. 1 summarizes attacks against different layers in systems.

Table 1. Attacks on Different Layers in Systems		
	Control layer	
	Regulatory control	Supervisory control
DoS attacks	Physical jamming	Network flooding
	Increase latency	Operational disruption
Deception Attacks	Relay, spoofing	Set-point change
	Measurement change	Controller change
Disclosure attacks	Management layer	
	Interpret and access secure information	
Physical attacks	Physical layer	
	Direct physical failures on the plants	

To facilitate the understanding of the above attacks classification, Fig. 1.5 is provided to show how cyber-attacks violate the system security goals.

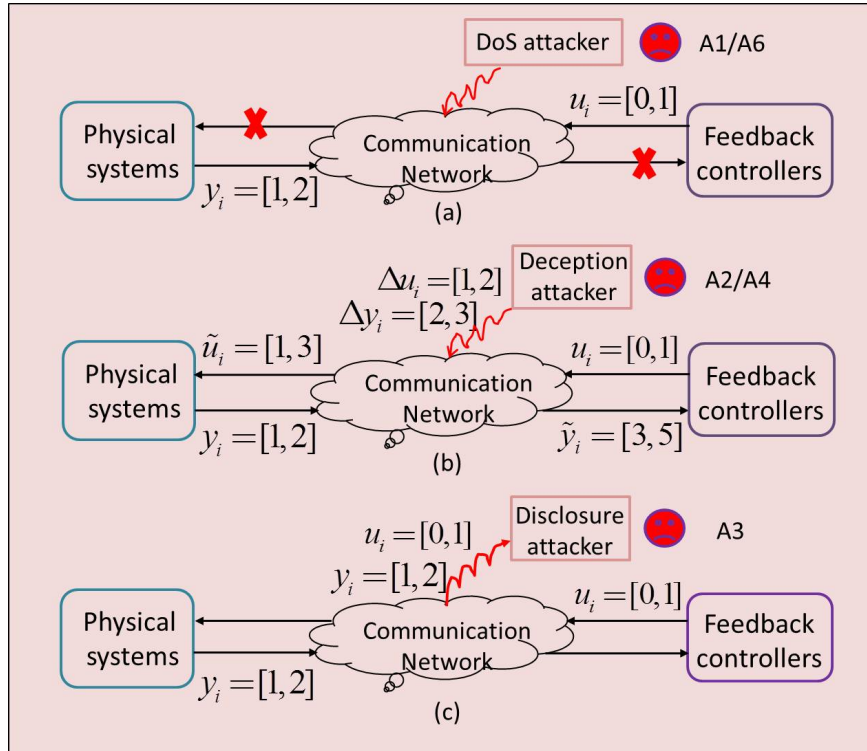


Figure 1.5: A block diagram of malicious cyber-attacks on a communication network: (a) Data availability violation by a DoS attack; (b) Data integrity violation by a false injection attack; (c) Data confidentiality violation by an eavesdropping attack.

To further illustrate the classification framework in Fig. 1.4, we consider the following two practical examples of networked multi-agent systems.

Example 1.1. Smart Grid

The power networks are supervised and controlled through SCADA systems. Taking remote terminal units (RTUs) as sensors/actuators, SCADA systems measure data and send them to the control center. These measurements are then processed and analyzed by a distributed energy management system (EMS), to send out the control commands. RTUs then receive data from the control center and connect to the power networks. Since SCADA systems are increasingly dependent on the Internet, more access points are exposed to potential malicious cyber-attacks.

- A DoS attack might be launched on the communications between the RTUs and distributed EMS (A1 and A6), limiting the device availability.
- A deception attack could be mounted on the communication network (A2 and A4), leading to the violation of data integrity.
- The system information inside the IT software and database in a distributed EMS (A3) can be the targets of a class of disclosure attacks having access to confidential data, resulting in the violation of confidentiality.

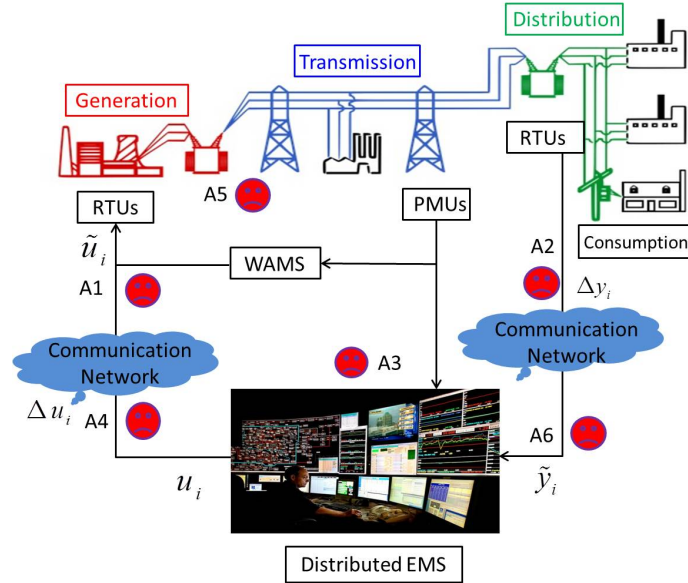


Figure 1.6: A block diagram of smart grid and its variety of possible vulnerabilities in systems.

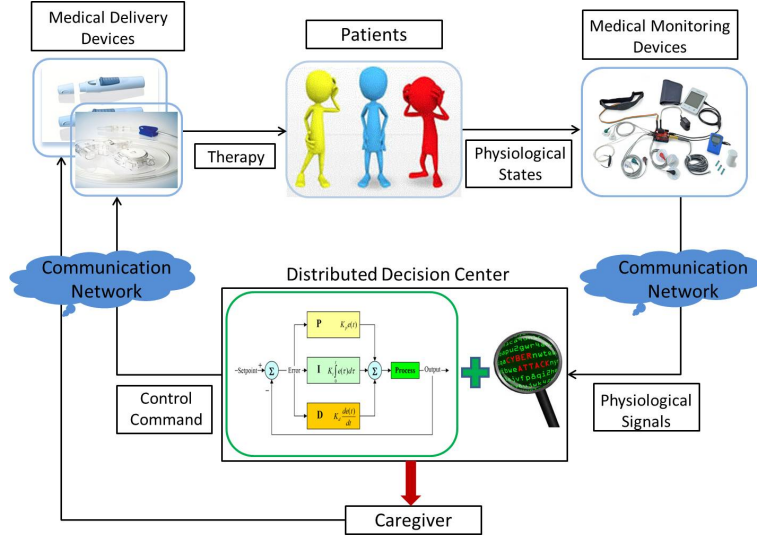


Figure 1.7: A block diagram of closed-loop Medical Device Systems (MDSs) and its variety of possible vulnerabilities in systems.

- A5 represents a class of direct physical attacks (e.g., physical failures and faults) on the power networks.

Example 1.2. Medical Device Systems

Next, we consider an example from a closed-loop control model of medical device systems (MDSs) as shown in Fig. 1.7. In general, adversaries can choose from the following targets when attacking the MDSs.

- Device: an attacker launches a DoS on MDSs in certain ways such that MDSs cannot perform tasks, which results in loss of the device availability.
- Institution: an attacker launches a class of deception attacks to compromise the interactions between MDSs and institution's internal network deployed to have access to the patient data, limiting the institution Integrity.
- Data: an attacker is able to obtain a patient's health data from MDSs in an unauthorized way and loss of patient privacy leads to potential discrimination and abuse. Thus, confidentiality is violated.
- Patient: an attacker targets the patient's health, e.g., an attacker programs an infusion pump to administer a larger than necessary dose of medicine.

1.1.3 Problem Formulation and A Potential Solution

This thesis addresses the problem of distributed resilient coordination for networked multi-agent systems. A reference architecture in the presence of diverse vulnerabilities in Fig. 1.4 is considered throughout the thesis.

Problem: Resilience of Networked Multi-Agent Systems

Resilience of networked multi-agent systems aims to maintain state awareness and an acceptable level of operational normalcy in response to physical failures from physical environments, malicious cyber-attacks from cyber environments, and strategic interactions of human decision makers in the design process.

This problem implies that a resilient agent system is able to defend against adversaries and recover from these attacks as well as strategic human decision makers in addition to being robust to unknown uncertainties and disturbances in physical infrastructures. Thus, resilience of an agent system can be classified at the following three interdependent levels and combining them can provide a trustworthy framework to build resilience into systems by maintaining synergistic integrations of human-centric elements with distributed monitoring and control processes.

Classification of Resilience Levels in Networked Multi-Agent Systems

1. Infrastructure resilience—how resilient is the physical infrastructure components (e.g., sensors, actuators, computing/storage elements, software environments) under physical failures that may lead to disruptions.
2. Information resilience—how resilient is the network information from the physical infrastructures given errors caused by malicious cyber-attacks on the communication networks and data analysis.
3. Social resilience—how resilient is the strategic interactions of human decision makers in the design process.

Designing such a resilient agent system requires a system-level perspective to propose a resilient control framework to maximize the survivability of critical infrastructures and systems under abnormal conditions. Control systems play a key role

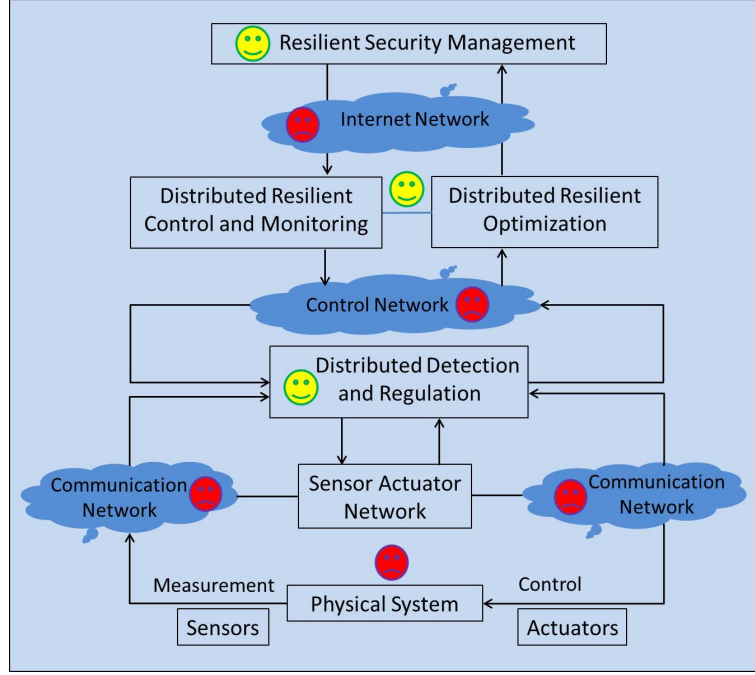


Figure 1.8: A multi-layer distributed resilient monitoring and control structure.

in critical infrastructure protection and performance recovery. It is important to increase the understanding of vulnerabilities in control systems and further develop resilient control algorithms to provide resilience. Novel theory and tools are lacking and need to be developed, requiring a systematic handling of complex couplings among the physical, cyber and social realms.

Fig. 1.8 shows a potential framework of multi-layer distributed resilient control and monitoring structure. In this hierarchical structure, the physical systems in the bottom layer are instrumented with distributed sensors and actuators, connected via a communication network, which implements the local control actions. The higher level is the supervisory control and regulation layer where the workstations are utilized for distributed monitoring and control. The top layer is risk security management involving the human decision makers who are in charge of economic and social control and optimization. Therefore, an overall resilience of networked multi-agent system can be built from a control perspective via this multi-layer distributed resilient monitoring and control design.

The thesis focuses on the following questions in networked multi-agent system.

Q1. Resilience Architecture: What core components should be addressed in a distributed resilient monitoring and control architecture?

Q2. Modeling Framework: How can physical failures and cyber-attacks be modeled from a control-theoretic perspective?

Q3. Resilience Issues: What kinds of main resilience issues are studied for building resilience of networked multi-agent systems?

Q4. Promising Approaches: What tools and methods can be devised to increase resilience of networked multi-agent systems?

1.2 Literature Review

In this section, relating works on networked multi-agent systems, distributed robust cooperative control and distributed secure coordination are presented.

1.2.1 Networked Multi-Agent Systems

In recent years, there has been an increasing interest in system and control community for studying distributed cooperative control of networked multi-agent systems [10–15]. The main objective is to develop distributed control algorithms and techniques for networked agents to autonomously coordinate their actions/decisions and achieve a system-level group objective. Some examples of group objectives include consensus, rendezvous, flocking and formation.

Over the past decade, leaderless consensus and leader-following consensus problems were first solved for single-integrator systems (e.g., [10,11]), and then double-integrator systems (e.g., [12,13]). Surveys of most recent advances on these problems can be found in [14,15]. The proposed different distributed algorithms have direct applications in attitude synchronization of spacecrafts [16], formation control [21], and rendezvous of mobile agents [22], etc. In [17], the authors studied the coordi-

nated tracking problem where the leader's acceleration should be accessible to all the followers, while an extension was given in [18] for discrete-time multi-agent systems. The leader-following formation of switching multi-robot systems was studied in [19] via an internal model method. The authors in [23] used passivity as a tool for constructing a distributed stabilizing feedback law to steer a group agents to a formation. A variable structure approach was employed to solve the consensus tracking problem for both first-order and second-order multi-agent systems in [13]. Based on a pinning control approach, the authors in [24] studied the consensus tracking problem by M -matrix theory. Different from the aforementioned results considering only single-integrator and double-integrator dynamics, the authors in [25–27] studied the consensus or consensus tracking problems for high-order linear systems.

1.2.2 Distributed Robust Cooperative Control

Networked multi-agent systems usually evolve in uncertain environments. Novel algorithms are needed to handle unknown uncertainties and disturbances.

Robust Consensus Tracking of Networked Euler-Lagrange Systems

Distributed coordination of multiple Euler-Lagrange systems has received increasing attention (e.g., [16], [40–49]). Due to the inherent nonlinearity of Euler-Lagrange systems, the results for linear multi-agent systems cannot be directly applied. [40] developed a model-based controller via nonlinear contraction analysis to analyze the coordinated tracking problem. Neural-network-based adaptive controllers were proposed in [42,43] to obtain UUB consensus tracking. In [44,45], the authors developed distributed algorithms for networked Euler-Lagrange systems in which a discontinuous sliding mode design was used. Based on the “linearity-in-parameters” assumption of systems, distributed adaptive controllers combined with discontinuous sliding mode estimators were proposed to solve the problem. Few results design continuous model-free distributed controller to deal with unstructured uncertainties of multiple Euler-Lagrange systems, especially under a directed graph.

Distributed coordinated tracking under unknown dynamics and disturbances is a practical and challenging problem. The agents are not only affected by the interaction among neighboring agents, but also by its own dynamics. A variety of approaches such as nonsmooth sliding mode control [13,44–51], pinning control [52], and neural-network-based control [53–55] have been used to solve this problem. A robust finite-time coordinated tracking problem for multiple Euler-Lagrange systems with input disturbances was examined in [50] using a discontinuous sliding mode controller. In practical implementations, discontinuous control methods may lead to chattering behavior and excite unmodelled high-frequency dynamics [51]. A pinning control scheme was introduced for synchronizing systems with identical dynamics in [52]. Practically, node dynamics are often non-identical or even unknown. Based on neural network methods, consensus problems for multi-agent systems with uncertainties and external disturbances were proven to yield UUB tracking in [53–55]. In contrast to the existing methods, an identifier-dependent distributed design was studied in [57] and [58] for first or second-order multi-agent systems.

Robust Connectivity Preserving Rendezvous of Multi-robot Systems

Network connectivity plays an important role in the distributed coordinated control of multi-robot systems. This work considers rendezvous, a coordinated control problem where network connectivity plays a crucial role. An artificial potential field approach (e.g, [75–77]) has been adopted to develop distributed gradient-based algorithms using the local artificial potential function to achieve rendezvous of multi-robot systems. These works assume that the robots are under a static network topology keeping its connectivity during the motion evolution. However, each mobile robot in practice has only limited sensing and communication capabilities. Therefore, connectivity preservation with robustness against the dynamic topology should be considered.

Recently, results in [78–87] studied network connectivity preservation when performing flocking and rendezvous for multi-robot systems. The works in [75–79,82] rely on maintaining a connected network among the agents, either for all the time or over sequences of bounded time intervals. The potential field based distributed approaches in [80–83] were developed to address the rendezvous problem while preserving network connectivity. In [81], the authors employed a hysteresis rule by adding new edges to maintain network connectivity for rendezvous of a first-order multi-robot system. The results based on this hysteresis rule were extended in [83] for a second-order multi-robot system under the assumption that agents have access to the acceleration information of the leader. A hybrid dynamic protocol was proposed in [22] to study a finite-time connectivity preservation rendezvous problem. The authors in [87] developed a decentralized controller by using a navigation function to achieve connectivity preserving formation with obstacle avoidance.

Distributed coordinated control of multi-robot systems with unknown dynamics and disturbances is a practical and challenging problem. Some results are reported (e.g., [54,55,58,88], just name a few) for solving robust consensus problem of multi-agent systems. However, few works consider connectivity preservation rendezvous for multi-robot systems under the unknown dynamics and disturbances. Recently, the authors in [72] studied this problem for a second-order multi-agent system under the external disturbances generated by an exosystem. The exosystem is considered as a leader for all the followers, which means the dynamics of the leader and all the followers are coupled with each other. Based on a cooperative output regulation method, a distributed rendezvous control law was proposed to solve this problem for multi-agent systems by using the hysteresis technique in [81,83]. An extension was made in [73] by developing a new controller via only position measurements. Recently, new coordinated rendezvous controllers are provided in [90–93]. To the best of our knowledge, few works deal with robust connectivity preserving rendezvous.

1.2.3 Distributed Secure Coordination

Distributed secure coordination of multi-agent systems is an interesting and important problem and few efforts have been made on achieving secure consensus against malicious cyber-attacks.

Distributed Secure Coordination under Switching Attacks

Multi-agent systems, like all large-scale spatially distributed systems, are vulnerable to cyber-attacks due to the development of network information and communication technologies. Typically, there are two different attack scenarios in a multi-agent system: attack on the dynamic behavior (or closed-loop dynamics) of the agents and attack on the communications among the agents. Both of these attacks can dramatically affect the consensus properties of the whole team of agents. Indeed, the collapse of the whole system can be caused by a single agent whose failure is broadcasting to its neighboring agents resulting in cascading damages. Some of the literature concerning this problem has been reported [101–104,106,107]. The authors in [101] and [102] studied the design of distributed fault (or attack) detection using unknown input observers (UIO) for networked multi-agent systems with double integrator dynamics. Based on the topological properties of the network, sufficient conditions for the feasibility of the UIO were derived. In [103], a consensus problem was considered for networked multi-agent systems with adversaries under the assumption that the network is complete. Recently, [102,127] considered distributed attack detection using unknown input observers for double integrator multi-agent systems. In [106], a distributed attack detection and identification algorithm via a distributed filter was investigated for cyber-physical systems. Note that [102,103,106,127] show that an attack on a specific node is identical to node removal on network graphs. In reality, it is more general to consider the second attack scenario that a number of edges are attacked [128–130].

In addition, the aforementioned detection techniques and control algorithms are always separated, which implies that there is no feedback to the control parameters when the attacks are detected or identified. Recently, [107] proposed a distributed receding-horizon control method for secure control of multi-agent systems by limiting the actions of the adversaries. [133] and [134] modeled attacker-defender interactions as a stochastic game and developed the game-theoretic resilient control schemes for cyber-physical systems. So far, how to design effective resilient algorithms is still challenging and of great significance to the distributed secure control problem of multi-agent systems. Few distributed effective control algorithms are proposed for this problem. In previous work [95], two types of attacks were studied and a hybrid secure control scheme was provided to achieve secure leader-follower consensus. However, on the one hand, the attacks on graphs are modeled by using a deterministic switching signal that determines the switching among various network topologies. That is, it is assumed that the system has complete access to the attacker moves. On the other hand, sufficient conditions for existence of consensus algorithms are established by solving two LMIs to get a common solution. The set of LMIs are dependent on the Laplacian matrix eigenvalues of all the communication topologies. Besides, the time-complexity of solving an LMI is $O(N^2s^4)$, where N and s denote the agents' number and the dimension of agent dynamics, respectively. Overall, it is conservative via LMI techniques.

Distributed Secure Coordination under DoS Attacks

As aforementioned, in reality it is more general to study attacks on communications, classified as either DoS or deception attacks. The former refers to interruptions of communication on control and/or measurement channels carried out by an intelligent adversary to violate availability. The latter refers to data trustworthiness where the adversary manipulates data transmitted over communication networks to violate integrity. Observe that [145–151, 154–156] studied secure control against DoS

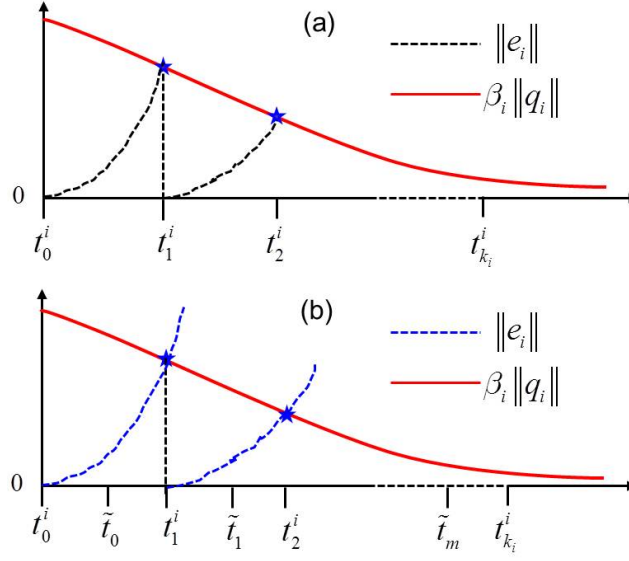


Figure 1.9: Event-based mechanism under the condition (1.1): (a) in the absence of DoS attacks; (b) in the presence of DoS attacks. $\{t_{k_i}^i\}$ and $\{\tilde{t}_m\}$ represent the event time sequence and the DoS attack time sequence, respectively.

attacks in a centralized setting. So far, there have been rare works addressing distributed resilient coordination of multi-agent systems under DoS attacks, although deception attacks were studied in [107,157–159].

In contrast to periodical sampling control that may waste much energy and shorten the lifespan of systems, an event-triggered control strategy is proposed in [160–166] to overcome the limitations of resource, computation and communication. The original idea of event-based control is to trigger an event and close the feedback loop whenever the state deviates from the equilibrium and crosses a threshold [160,161]. As proposed in [162–166], the following condition, as illustrated in Fig. 1.9(a), is given to guarantee average consensus.

$$\|e_i(t)\| = \|x_i(t_{k_i}^i) - x_i(t)\| \leq \beta_i \|q_i(t)\|, i = 1, \dots, N, \quad (1.1)$$

where $q_i(t) = \sum_{j=1}^N a_{ij}(x_j(t) - x_i(t))$ and β_i is a constant. However, it follows from Fig. 1.9(b) that the condition (1.1) may not be enforced in the presence of DoS attacks. Thus, a problem of interest is to study an event-based coordination from the perspective of resilience to achieve secure consensus.

The closet literature to this work are [94–96,149–151]. In previous works [94–96], two types of attacks were studied and a hybrid secure control scheme was designed to achieve secure consensus, provided that the attack frequency and duration satisfy certain conditions. However, [94–96] assume that the system has complete or part access to the attacker moves. Motivated by [94–96] this work concerns with DoS attacks of multi-agent systems where the attacker follows an unknown strategy. The authors in [149] proposed a centralized event-based controller to address energy-constrained DoS attacks by assuming that the known attacks occur periodically. [150,151] extended this centralized event-based design to deal with packet losses and unavailable measurements under DoS attacks, respectively. To the best of our knowledge, few works are on distributed event-based coordination from the perspective of resilience.

1.3 Contributions

This dissertation is on the development of distributed resilient control algorithms and techniques to deal with diverse vulnerabilities in networked multi-agent systems. The main contributions are achieved by deriving the following results:

- A distributed robust coordinated control problem is addressed for unknown networked Euler-Lagrange systems under both undirected and directed graphs. Challenging unstructured uncertainties including unknown nonlinear dynamics and disturbances are considered in the agent dynamics. An identifier-based, model-free, continuous distributed control approach is designed to solve this problem under undirected and directed graphs. Both the control inputs and coupling gains depend only on local information and the consensus tracking errors are proven to converge to zero asymptotically. Under an undirected graph, a distributed nonlinear identifier is developed for each agent to compensate for the unknown nonlinear dynamics and disturbances. Based on this identifier,

a continuous distributed control law is designed to enable asymptotic robust consensus tracking. Furthermore, the directed graph case is investigated via a distributed two-layer coordination scheme in which a model-independent continuous distributed controller is designed by using information obtained from a distributed leader estimator to enable the agent group to achieve robust consensus tracking asymptotically.

- As an application of the developed identifier-based consensus design, a robust connectivity preserving rendezvous problem is considered for a leader-following multi-robot system. Only a small group of mobile robots are informed to have access to the leader's information. A distributed robust dynamic control algorithm is proposed such that connectivity preserving rendezvous is achieved regardless of the unknown nonlinear dynamics and disturbances. Although the multi-robot network has a dynamic network topology, the developed controller is able to maintain the connectivity of an initially connected communication network. Using the tools from algebraic graph theory, Lyapunov method and nonsmooth analysis, sufficient conditions on the asymptotic convergence of the closed-loop multi-robot systems are derived.
- A distributed secure hybrid control approach is proposed to solve secure coordination problems for linear multi-agent systems subject to two types of attacks. Works on resilience architecture, attack modeling and approaches for specific issues are studied. We firstly consider a distributed secure control problem for systems under two types of switching attacks. Attacks on edges of agents lead to loss of consensus performance. Two distributed secure control laws are developed for solving the issues from a switching perspective. Sufficient conditions are derived to ensure secure consensus with a specified convergence rate by virtue of the idea of average dwell time (ADT) switch-

ing between some stable and unstable interconnected subsystems. Then, this work is further extended to secure coordination in the presence of strategic attacks. We model these attacks with their dynamics captured by a random Markov process. A hybrid stochastic secure control scheme with a connectivity restoration mechanism is provided to solve this problem. It is shown that under the proposed design, exponential secure consensus tracking is achieved in a mean-square sense. The influence of strategic attacks on discrete-time linear multi-agent systems is also investigated.

- A specific Denial-of-Service (DoS) attack is investigated to solve secure cooperative control problem for linear multi-agent systems via an event-based distributed control scheme. A time-sequence-based DoS attack is modeled in which the attack is allowed to occur aperiodically in an unknown attack strategy. An explicit analysis of the frequency and duration of DoS attacks is investigated for secure leaderless consensus problem. An event-based distributed control law is developed and suitable scheduling of controller updating times is determined in the presence of DoS attacks. The event condition is used to determine when the agent updates its control input and broadcasts the measurements to its neighbors. By specifying a positive inter-execution time interval for each agent, Zeno behavior can be avoided for controller implementations over a network. It is shown that with the proposed control scheme, the agent group can achieve secure consensus exponentially. Then, secure leader-following consensus is further achieved under a directed graph. Since the information-exchange matrix is asymmetric, it is challenging to develop a novel distributed secure controller to achieve secure leader-following consensus. The effectiveness of the proposed methods is illustrated through case studies on distributed multi-robot coordination and distributed voltage regulation of Microgrid, respectively.

1.4 Organization of the Thesis

The rest of the dissertation is structured as follows. In **Chapter 2**, some related preliminaries and definitions on graph theory, nonsmooth analysis and switched system theory are presented. **Chapters 3 and 4** consider distributed robust cooperative control for multi-agent systems from different perspectives. In **Chapter 3**, a distributed robust coordinated control problem for networked Euler-Lagrange systems is addressed under both undirected and directed topologies. An identifier-based, model-free, distributed control scheme is proposed to solve it. **Chapter 4** studies the application of identifier-based consensus design to robust connectivity preserving rendezvous in multi-robot systems. A distributed PID controller is thus leveraged to solve it via a gradient-based approach. This robust distributed control law not only maintains the connectivity of the multi-robot system, but also achieves asymptotic consensus tracking. The use of modern ICT technologies increases the vulnerabilities to malicious cyber-attacks. Therefore, **Chapters 5 and 6** propose a distributed secure hybrid control scheme to solve secure coordination problems under two types of deterministic and stochastic attacks, respectively, from a switching perspective. Noticing that in the aforementioned two types of switching attacks, the system has complete or part access to the attacker moves. Moreover, few works are on event-based distributed coordination from the perspective of resilience. Thus, in **Chapter 7** an event-based secure cooperative control problem is considered for linear multi-agent systems under Denial-of-Service (DoS) attacks. An explicit analysis of the frequency and duration of DoS attacks is investigated for secure leaderless and leader-following consensus problems. An event-based distributed control law is developed and suitable scheduling of controller updating times is determined in the presence of DoS attacks. It is shown that with the proposed control scheme, the agent group can achieve secure consensus exponentially. Conclusions on the thesis and future work are included in **Chapter 8**.

Chapter 2

Preliminaries

In this chapter, preliminaries on graph theory, nonsmooth analysis and switched system theory are presented.

2.1 Graph Theory

Fixed Graph: [64] Let $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ represent a graph and $\mathcal{V} = \{1, 2, \dots, N\}$ denote the set of vertices. Every agent is represented by a vertex. The set of edges is denoted as $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. An edge is an ordered pair $(i, j) \in \mathcal{E}$ if agent j can be directly supplied with information from agent i . In this dissertation, we assume that there is no self loop in the graph, that is, $(i, i) \notin \mathcal{E}$. Graph \mathcal{G} is said to be undirected if for any edge $(i, j) \in \mathcal{E}$, edge $(j, i) \in \mathcal{E}$. Hence, an undirected graph is a special case of a directed graph. A path is referred by the sequence of its vertices. Path \mathcal{P} between v_0 and v_k is the sequence $\{v_0, \dots, v_k\}$ where $(v_{i-1}, v_i) \in \mathcal{E}$ for $i = 1, \dots, k$ and the vertices are distinct. Graph \mathcal{G} contains a directed spanning tree if there is a vertex which can reach all the other vertices through a directed path. A matrix $A = [a_{ij}] \in \mathbb{R}^{N \times N}$ denotes the adjacency matrix of \mathcal{G} , where $a_{ij} > 0$ if and only if $(j, i) \in \mathcal{E}$, else $a_{ij} = 0$. A matrix $L \triangleq D - A \in \mathbb{R}^{N \times N}$ is called the Laplacian matrix of \mathcal{G} , where $D = [d_{ii}] \in \mathbb{R}^{N \times N}$ is a diagonal matrix with $d_{ii} = \sum_{j=1}^N a_{ij}$.

For a fixed directed graph \mathcal{G} , its Laplacian matrix L has the following property.

Lemma 2.1. [64] Denote the Laplacian matrix of graph \mathcal{G} as $L = [l_{ij}] \in \mathbb{R}^{N \times N}$, $l_{ij} = \sum_{k=1, k \neq i}^N a_{ik}$ if $i = j$, otherwise, $l_{ij} = -a_{ij}$, $i, j = 1, 2, \dots, N$. Then, the following statements are true:

(i) Zero is a simple eigenvalue of L , and $\mathbf{1}_N = [1, \dots, 1]^T \in \mathbb{R}^N$ is the corresponding eigenvector, that is $L\mathbf{1}_N = 0$.

(ii) If \mathcal{G} has a spanning tree, then the eigenvalue 0 is algebraically simple for its Laplacian matrix, and all the other eigenvalues have positive real parts.

Lemma 2.2. Suppose that matrix $L = [l_{ij}] \in \mathbb{R}^{N \times N}$ has $l_{ij} \leq 0$ for all $i \neq j$, $i, j = 1, 2, \dots, N$. Then, there exists a matrix $\Theta = \text{diag}\{\theta_1, \theta_2, \dots, \theta_N\} \in \mathbb{R}^{N \times N}$ such that the matrix $Q = L^T\Theta + \Theta L > 0$, where $\theta = [\theta_1, \theta_2, \dots, \theta_N]^T = L^{-T}\mathbf{1}_N$.

Proof. The first assertion is well-known (see Theorem 4.25 in [112]). Since L is a nonsingular M -matrix, L^{-1} is nonnegative. Then, it is easy to verify $\theta > 0$ and hence $\Theta L\mathbf{1}_N \geq 0$. By noting that $L^T\Theta\mathbf{1}_N = L^T\theta = L^TL^{-T}\mathbf{1}_N = \mathbf{1}_N$, we can conclude that $(L^T\Theta + \Theta L)\mathbf{1}_N > 0$ which implies that $L^T\Theta + \Theta L$ is strictly diagonally dominant. Then, it follows from Gershgorin's disc theorem that every eigenvalue of $L^T\Theta + \Theta L$ is positive. Thus, there exist positive definite diagonal matrix $\Theta = \text{diag}\{\theta_1, \theta_2, \dots, \theta_N\}$ with $[\theta_1, \theta_2, \dots, \theta_N]^T = L^{-T}\mathbf{1}_N$ such that $Q = L^T\Theta + \Theta L > 0$. \square

A distributed coordinated tracking case where the access of agents to a desired time-varying trajectory is represented by a diagonal matrix $B = \text{diag}\{b_1, b_2, \dots, b_N\} \in \mathbb{R}^{N \times N}$. If b_i is equal to 1, then the i -th agent has access to the desired trajectory; otherwise, $b_i = 0$. For further analysis, an information exchange matrix $H \in \mathbb{R}^{N \times N}$ is defined as $H = L + B$. To facilitate the subsequent design, a virtual leader \mathcal{V}_0 is defined for all the agents of \mathcal{G} . The following lemmas present several properties of matrices L and H for undirected and directed graphs.

Lemma 2.3. [18] *If \mathcal{G} is an undirected graph and the virtual leader \mathcal{V}_0 has directed paths to all the agents of \mathcal{G} , then $H = L + B$ is symmetric and positive definite.*

Lemma 2.4. [89] *If \mathcal{G} is a directed graph containing a directed spanning tree with the leader being the root, then H is a non-singular and positive definite matrix. Define $v = [v_1, v_2, \dots, v_N]^T = H^{-T}\mathbf{1}$, $P = \text{diag}\{\frac{1}{v_1}, \frac{1}{v_2}, \dots, \frac{1}{v_N}\}$ and $Q = PH + H^T P$, then $P = \text{diag}(p_1, p_2, \dots, p_N)$ ensures that Q is symmetric and positive definite.*

Proof. The proof is easy to obtain from Lemma 2.2, and it is thus omitted here. \square

2.2 Nonsmooth Analysis

A LaSalle-Yoshizawa Theorem [65] providing boundedness and convergence of solutions for systems with a discontinuous right-hand side will be recalled below.

Consider the following differential equation

$$\dot{x} = f(x, t), \quad (2.1)$$

where $x(t) \in \mathbb{R}^n$ denotes the state vector, $f : \mathbb{R}^n \times \mathbb{R} \rightarrow \mathbb{R}^n$ is Lebesgue measurable and essentially locally bounded¹. Existence and uniqueness of the continuous solution $x(t)$ are provided if the function f is Lipschitz continuous [74].

A vector function $x(t)$ is called a Filippov solution of (2.1) on $[t_0, t_1]$ if $x(t)$ is absolutely continuous on $[t_0, t_1]$ and for almost all $t \in [t_0, t_1]$, $\dot{x} \in \mathbb{K}[f](x, t)$. Here, $\mathbb{K}[f](x, t) \triangleq \bigcap_{\delta > 0} \bigcap_{\mu N = 0} \overline{\text{co}} f(B(x, \delta) \setminus N, t)$, where $\bigcap_{\mu N = 0}$ denotes the intersection over sets N of Lebesgue measure zero, $\overline{\text{co}}$ denotes convex closure, and $B(x(t), \delta) = \{\nu \in \mathbb{R}^n \mid \|x(t) - \nu\| < \delta\}$. For a locally Lipschitz function $V : \mathbb{R}^n \times \mathbb{R} \rightarrow \mathbb{R}$, the generalized gradient of V at (x, t) is defined by $\partial V(x, t) = \overline{\text{co}}\{\lim \nabla V(x, t) \mid (x_i, t_i) \rightarrow (x, t), (x_i, t_i) \notin \Omega_V\}$, where Ω_V is the set of measure zero where the gradient of V is not defined. The generalized time derivative of this Lipschitz function V with

¹A function $f(x)$ defined on a space X is called essentially locally bounded, if for any $x \in X$, there exists a neighborhood $U \subseteq X$ of x such that $f(U)$ is a bounded set for almost all $u \subseteq U$ [65].

respect to the nonlinear system (2.1) with a discontinuous right-hand side is further defined as $\dot{\tilde{V}} \triangleq \cap_{\xi \in \partial V} \xi^T \begin{pmatrix} \mathbb{K}[f](x, t) \\ 1 \end{pmatrix}$.

Lemma 2.5. [65] *For the system given in (2.1), let $\mathcal{D} \subset \mathbb{R}^n$ be an open and connected set containing $x = 0$ and suppose $f(x, t)$ is Lebesgue measurable and $x \rightarrow f(x, t)$ is essentially locally bounded, uniformly in t . Let $V : \mathcal{D} \times [0, \infty) \rightarrow \mathbb{R}$ be locally Lipschitz and regular such that*

$$\begin{aligned} W_1(x) &\leq V(x, t) \leq W_2(x), \forall t \geq 0, \forall x \in \mathcal{D}, \\ \dot{\tilde{V}}(x, t) &= \frac{\partial V}{\partial t} + \frac{\partial V}{\partial x} f(x, t) \leq -W(x), \end{aligned} \quad (2.2)$$

where $W_1(x)$ and $W_2(x)$ are continuous positive definite functions, and $W(x)$ is a continuous positive semi-definite function on \mathcal{D} . Choose $r > 0$ and $c > 0$ such that $B_r \subset \mathcal{D}$ and let $c < \min_{\|x\|=r} W_1(x)$. Then, all Filippov solutions of (2.1) such that $x(t_0) \in \{x \in B_r | W_2(x) \leq c\}$ are bounded and satisfy: $W(x(t)) \rightarrow 0$ as $t \rightarrow \infty$.

2.3 Switched System Theory

Switched systems theory consists of tools developed for systems containing a combination of continuous and discrete dynamics. Consider a switched system described by the following differential equation:

$$\dot{x} = f_\sigma(x), \quad (2.3)$$

where $\sigma : [0, \infty) \rightarrow \mathcal{P} = \{1, 2, \dots, p\}$, called a switching signal, is a piecewise constant function dependent on state or time, and $\{f_p : p \in \mathcal{P}\}$ is a family of sufficiently regular functions from \mathbb{R}^n to \mathbb{R}^n .

In the three classic stability problems for the switched system (2.3), the following reviews a class of stability problem under a slowly switching using multiple Lyapunov function techniques.

Definition 2.1. [117] (*Average Dwell Time*)

For a switching signal $\sigma(t)$ and $T > t \geq 0$, let $N_\alpha(t, T)$ denote the number of discontinuities of $\sigma(t)$ over $[t, T)$. If there exist $N_0 \geq 0$ and $\tau_a \geq 0$ such that

$$N_\alpha(t, T) \leq N_0 + \frac{T - t}{\tau_a}. \quad (2.4)$$

Then, τ_a and N_0 are called the average dwell time and chattering bound, respectively.

Lemma 2.6. [117] Consider the family of system (2.3). Suppose that there exist \mathcal{C}^1 functions $V_p : \mathbb{R}^n \rightarrow \mathbb{R}$, $p \in \mathcal{P}$, two classes \mathcal{K}_∞ functions α_1 and α_2 , and positive constants λ_a and μ , such that we have

$$\alpha_1(|x|) \leq V_p(x) \leq \alpha_2(|x|), \quad V_p(x) \leq \mu V_q(x), \quad \forall x, \forall p, q \in \mathcal{P}, \quad (2.5)$$

$$\frac{\partial V_p(x)}{\partial x} f_p(x) \leq -\lambda_a V_p(x), \quad \forall x, \forall p \in \mathcal{P}. \quad (2.6)$$

Then the switched system (2.3) is globally asymptotically stable for every switching signal σ and arbitrary N_0 with average dwell time satisfying

$$\tau_a > \frac{\log(\mu)}{\lambda_a}. \quad (2.7)$$

Part I

Distributed Robust Cooperative Control

Chapter 3

Robust Distributed Coordinated Control of Multiple Unknown Euler-Lagrange Systems

3.1 Introduction

As stated in Chapter 1, due to the inherent nonlinearity of Euler-Lagrange systems and unstructured uncertainties, the results for linear multi-agent systems cannot be directly applied. The existing results using a variety of approaches such as nonlinear contraction analysis [40], sliding mode control [44–51], pinning control [52] and neural-network-based control [42,43,53–55] have certain limitations with conservative results. The nonlinear contraction analysis requires some kind of model information to be implemented. In practical implementations, discontinuous sliding mode control may lead to chattering behavior and excite unmodelled high-frequency dynamics [51]. Moreover, the neural-network-based controllers yield only UUB results. Few results design model-free, continuous, distributed controller to deal with uncertainties of multiple Euler-Lagrange systems, especially under a directed graph.

In this chapter, we address a robust consensus tracking problem for heterogeneous multiple Euler-Lagrange systems. Challenging unstructured uncertainties including unknown nonlinear dynamics and disturbances are considered in the agent dynamics. The objective is that a team of agents can track a desired time-varying trajectory. A key challenge is to design an identifier to compensate for the unknown dynamics and disturbances. We leverage a blend of Lyapunov methods and graph theory to resolve this challenge. In comparison to previous works on distributed cooperative control of multiple Euler-Lagrange systems, the main contributions of this chapter can be summarized as follows.

- The networked agents are modelled by the nonlinear Euler-Lagrange dynamics. The unstructured uncertainties present a challenge that inhibits direct application of results developed for linear systems (cf. [16,18,23,38,39], [13,52–61]).
- Compared with the results in [13,40–61], the developed continuous distributed controller is model-independent and the model that used for stability analysis does not include the typical linear in the uncertain parameters assumption.
- Compared with centralized approaches (cf., [13,16,18,23,38–61]), the developed controller does not require global graph information. Asymptotic consensus tracking is achieved under derived distributed stability conditions.
- Directed information topology is considered compared with results in [13,40–61] that only consider undirected graphs assuming that the upper bounds of the disturbances are exactly known constants. The developed distributed control scheme in this work does not require this prior knowledge. This directed graph case is nontrivial and brings significant theoretical challenges. In this chapter, by a distributed two-layer coordination design and by using information obtained from a distributed leader estimator, a novel model-free, continuous, distributed robust control law is developed to solve this problem.

The rest of this chapter is organized as follows. In Section 3.2, a distributed robust coordinated tracking problem is formulated. First, the distributed controller design and stability analysis are presented for asymptotic robust consensus tracking under an undirected graph in Section 3.3. Then, a novel control scheme via a distributed two-layer design is further presented for a directed graph case in Section 3.4. Numerical examples are given in Section 3.5 to verify the effectiveness of the proposed methods. Brief conclusions of this chapter are presented in Section 3.6.

3.2 Problem Formulation

3.2.1 Agent Model

Consider a team of N agents governed by the unknown Euler-Lagrange dynamics

$$M_i(q_i)\ddot{q}_i + C_i(q_i, \dot{q}_i)\dot{q}_i + G_i(q_i) + f_i(\dot{q}_i) + \delta_i = \tau_i, \quad (3.1)$$

where $q_i \in \mathbb{R}^l$ denote the vector of generalized configuration coordinates, $M_i(q_i) \in \mathbb{R}^{l \times l}$ is the inertia matrix, $C_i(q_i, \dot{q}_i)\dot{q}_i \in \mathbb{R}^l$ is the vector of Coriolis and centrifugal torques, $G_i(q_i) \in \mathbb{R}^l$ is the vector of gravitational torque, $\tau_i \in \mathbb{R}^l$ is the vector of control inputs, $f_i(\dot{q}_i) \in \mathbb{R}^l$ represents the unknown unmodelled dynamics (or frictions), and $\delta_i \in \mathbb{R}^l$ is the time-varying input disturbances. The inertia, Coriolis, gravity, and friction terms are all assumed unknown. To facilitate the subsequent analysis, the results are based on the assumption that $q_i(t)$ and $\dot{q}_i(t)$ are available. Moreover, the following properties in [68,69] are exploited in the subsequent development.

Property 3.1. *The inertia matrix $M_i(q_i)$ is symmetric, positive definite, and satisfies $\underline{m}_i \|y\|^2 \leq y^T M_i(q_i) y \leq \overline{m}_i(q_i) \|y\|^2$, $\forall y \in \mathbb{R}^l$, where $\underline{m}_i \in \mathbb{R}$ is a known positive constant, $\overline{m}_i(q_i) \in \mathbb{R}$ is a known positive function.*

Property 3.2. *$M_i(q_i)$, $C_i(q_i, \dot{q}_i)$, $G_i(q_i)$, and $f_i(\dot{q}_i)$ are second-order differentiable such that their first-order and second-order partial derivatives exist and are bounded, if $q_i, \dot{q}_i, \ddot{q}_i, \ddot{\ddot{q}}_i \in \mathcal{L}_\infty$.*

Denote the virtual leader \mathcal{V}_0 as the desired time-varying trajectory for all the followers. The following assumptions are made on δ_i and \mathcal{V}_0 , respectively.

Assumption 3.1. *The disturbance term $\delta_i(t)$ and its first two time derivatives are bounded by some unknown constants (i.e., $\delta_i(t), \dot{\delta}_i(t), \ddot{\delta}_i(t) \in \mathcal{L}_\infty, i \in \{1, \dots, N\}$).*

Assumption 3.2. *The desired trajectory $q_d(t)$ and its m -order ($m = 1, 2, 3, 4$) time derivatives are assumed to be bounded by some unknown constants.*

Remark 3.1. *Assumptions 3.1 and 3.2 are mild as widely used in [54,55,58,88,89]. Many practical disturbance terms are continuous and differentiable including frictions, wind disturbances, wave/ocean disturbances, unmodeled sufficiently smooth disturbances, etc. In addition, many guidance and navigation applications utilize smooth, high-order differentiable desired trajectories. Curve fitting methods can also be used to generate sufficiently smooth time-varying trajectories.*

3.2.2 Control Objective

The control objective is to ensure that the states of all the agents modeled by (3.1) reach robust consensus asymptotically and track a desired time-varying trajectory. The model-independent continuous distributed control law for each agent will be synthesized based on local information exchanged from neighboring agents despite the unknown nonlinear dynamics $f_i(\dot{q}_i)$ and disturbances δ_i .

Definition 3.1. (*Robust Consensus Tracking*)

Design a distributed control law $\tau_i(t)$, $i \in \{1, \dots, N\}$ such that the states $q_i(t)$ and $\dot{q}_i(t)$ of N networked Euler–Lagrange systems governed by (3.1) can reach asymptotic robust consensus, respectively, and track the corresponding desired time-varying signals $q_d(t)$ and $\dot{q}_d(t)$ in the sense that

$$q_i(t) - q_d(t) \rightarrow \mathbf{0}_l \text{ and } \dot{q}_i(t) - \dot{q}_d(t) \rightarrow \mathbf{0}_l \text{ as } t \rightarrow \infty,$$

for all the agents under the unknown nonlinear dynamics $f_i(\dot{q}_i)$ and disturbances δ_i .

3.3 Robust Distributed Coordination Under An Undirected Graph

For further analysis, an information exchange matrix $H \in \mathbb{R}^{N \times N}$ is defined as $H = L + B$, where L is the Laplacian matrix of the graph \mathcal{G} and $B = \text{diag}\{b_1, b_2, \dots, b_N\}$. If $b_i = 1$, then the i -th agent has access to the desired trajectory; otherwise, $b_i = 0$.

Assumption 3.3. *The communication graph \mathcal{G} is undirected and \mathcal{V}_0 has directed paths to all the agents of \mathcal{G} .*

Lemma 3.1. *[16] Suppose that Assumption 3.3 holds, then the information-exchange matrix H is positive definite and symmetric.*

Since not all the agents have access to the desired trajectory, the relative position and velocity consensus tracking errors $e_{\xi_i}(t), e_{x_i}(t) \in \mathbb{R}^l$, and tracking errors $e_{f_i}(t) \in \mathbb{R}^l, i=1, 2, \dots, N$, are defined using only local information exchanged from neighboring agents as

$$e_{\xi_i} = \sum_{j=1}^N a_{ij} (q_j - q_i) + b_i (q_d - q_i), \quad (3.2)$$

$$e_{x_i} = \sum_{j=1}^N a_{ij} (\dot{q}_j - \dot{q}_i) + b_i (\dot{q}_d - \dot{q}_i), \quad (3.3)$$

$$e_{f_i} = e_{x_i} + \alpha_{1i} e_{\xi_i}, \quad i = 1, 2, \dots, N, \quad (3.4)$$

where $\alpha_{1i} \in \mathbb{R}$ is a positive constant gain to be designed.

3.3.1 Robust Consensus Tracking Control Law Design

The distributed control protocol is designed as

$$\tau_i(t) = b_i \dot{q}_d(t) - \alpha_{1i} \dot{q}_i(t) + \alpha_{2i} e_{f_i}(t) + \hat{f}_i(t), \quad (3.5)$$

where $\alpha_{1i}, \alpha_{2i} \in \mathbb{R}$ are two control gains and $\hat{f}_i(t) \in \mathbb{R}^l$ denotes a subsequently designed term to compensate for the unknown dynamics and disturbances.

The distributed estimation law for $\hat{f}_i(t)$ is given by

$$\begin{aligned}\dot{\hat{f}}_i(t) &= (k_{si} + 1)(\dot{e}_{fi}(t) + \alpha_{2i}e_{fi}(t)) + b_i\beta_i(t) \odot \eta_i(t) + \theta_i(t), \\ \theta_i(t) &= \sum_{j=1}^N a_{ij}(\beta_i(t) \odot \eta_i(t) - \beta_j(t) \odot \eta_j(t)), \\ \eta_i(t) &= \text{vsgn}(e_{fi}(t)), \hat{f}_i(0) = \hat{f}_{iO},\end{aligned}\tag{3.6}$$

where \hat{f}_{iO} is an initial condition, k_{si} and α_{2i} are two positive constant control gains, $\beta_i(t) \in \mathbb{R}^l$ is a time-varying control term to be determined later, the symbol \odot denotes the elementwise vector multiplication, and $\text{vsgn}(e_{fi}) \triangleq [\text{sgn}(e_{fi1}), \text{sgn}(e_{fi2}), \dots, \text{sgn}(e_{fil})]^T \in \mathbb{R}^l$. Since $\dot{e}_{fi}(t)$ in (3.6) is not available, the following form is utilized to generate the estimation signal $\hat{f}_i(t)$ ¹:

$$\begin{aligned}\hat{f}_i(t) &= (k_{si} + 1)(e_{fi}(t) - e_{fi}(0)) + v_i(t), \\ \dot{v}_i(t) &= (k_{si} + 1)\alpha_{2i}e_{fi}(t) + b_i\beta_i(t) \odot \eta_i(t) + \theta_i(t),\end{aligned}\tag{3.7}$$

where $\beta_i(t)$ introduced in (3.6) and (3.7) is defined as

$$\begin{aligned}\beta_i(t) &= \beta_{1i}(t) + \beta_{2i}\mathbf{1}_l, \beta_{1i}(0) = \mathbf{0}_l, \\ \beta_{1i}(t) &= |e_{fi}(t)| - |e_{fi}(0)| + \alpha_{2i} \int_0^t |e_{fi}(\tau)| d\tau,\end{aligned}\tag{3.8}$$

where $|e_{fi}(t)| = [|e_{fi1}(t)|, |e_{fi2}(t)|, \dots, |e_{fil}(t)|]^T \in \mathbb{R}^l$, $\beta_{1i}(t) \in \mathbb{R}^l$, and $\beta_{2i}\mathbf{1}_l \in \mathbb{R}^l$ is a positive constant part.

3.3.2 Filtered Error Dynamics

To facilitate the subsequent stability analysis, define an auxiliary error $r_i(t) \in \mathbb{R}^l$

$$r_i = \kappa_i^{-1}(\dot{e}_{fi} + \alpha_{2i}e_{fi} + \sum_{j=1, j \neq i}^N a_{ij}r_j),\tag{3.9}$$

¹Note that $\hat{f}_i(t)$ is the Filippov solution to the differential equation in (3.6) that is discontinuous due to the presence of the sign function. Using Filippov's theory of differential inclusions, the existence of solutions can be established for a system with a discontinuous right-hand side: $\dot{\varphi} \in \mathbb{K}[h](\sigma, t)$, where h is defined as the right-hand side of $\dot{\varphi}$ and $\mathbb{K}[h](\sigma, t) \triangleq \cap_{\delta > 0} \cap_{\mu N = 0} \overline{\text{co}}h(B_\delta(\sigma) \setminus N, t)$ as shown in [65] for more details.

where $\kappa_i = \sum_{j=1, j \neq i}^N a_{ij} + b_i$. Defining vectors $r \triangleq \text{col}(r_1, \dots, r_N)$ and $E_f \triangleq \text{col}(e_{f1}, \dots, e_{fN}) \in \mathbb{R}^{Nl}$ yields $((D + B) \otimes I_l)r = \dot{E}_f + \Lambda_2 E_f + (A \otimes I_l)r$, where $\Lambda_2 \triangleq \text{diag}(\alpha_{21}, \dots, \alpha_{2N}) \otimes I_l \in \mathbb{R}^{Nl \times Nl}$ denotes a diagonal matrix, and I_l is a $l \times l$ identity matrix. Thus, $\tilde{H}r = \dot{E}_f + \Lambda_2 E_f$, $\tilde{H} = (\mathcal{L} + B) \otimes I_l$. By Lemma 3.1, \tilde{H} is positive definite and symmetric. Thus, it follows from (3.9) that

$$r = \tilde{H}^{-1}(\dot{E}_f + \Lambda_2 E_f). \quad (3.10)$$

3.3.3 Closed-Loop System Development

The expressions in (3.2)-(3.5) can be rewritten as

$$\begin{aligned} E_\xi &= -\tilde{H}(Q - Q_d), \dot{E}_\xi = -\tilde{H}(\dot{Q} - \dot{Q}_d), \\ E_f &= \dot{E}_\xi + \Lambda_1 E_\xi, \Gamma = \tilde{B}\dot{Q}_d - \Lambda_1 \dot{Q} + \Lambda_2 E_f + \hat{F}, \end{aligned} \quad (3.11)$$

which yields that the time derivative of E_f is given by

$$\begin{aligned} \dot{E}_f &= \tilde{H}M^{-1}(F + C\dot{Q} + G + \delta - \tilde{B}\dot{Q}_d + \Lambda_1 \dot{Q} - \hat{F} - \Lambda_2 E_f) \\ &\quad - \Lambda_1 \tilde{H}\dot{Q} + \Lambda_1 \tilde{B}\dot{Q}_d + \tilde{B}\ddot{Q}_d, \end{aligned} \quad (3.12)$$

where $Q \triangleq \text{col}(q_1, \dots, q_N)$, $E_\xi \triangleq \text{col}(e_{\xi 1}, \dots, e_{\xi N})$, $F \triangleq \text{col}(f_1, \dots, f_N)$, $\hat{F} \triangleq \text{col}(\hat{f}_1, \dots, \hat{f}_N)$, $G \triangleq \text{col}(G_1, \dots, G_N)$, $\delta \triangleq (\delta_1, \dots, \delta_N)$, $Q_d \triangleq (\mathbf{1}_N \otimes q_d)$; and $\tilde{B} \triangleq \text{diag}(b_1, b_2, \dots, b_N) \otimes I_l$, $\Lambda_1 \triangleq \text{diag}(\alpha_{11}, \dots, \alpha_{1N}) \otimes I_l$, $M \triangleq \text{diag}(M_1, \dots, M_N)$ and $C \triangleq \text{diag}(C_1, \dots, C_N)$. After premultiplying (4.9) by M , the following expression is obtained using (4.9) and (3.12) as

$$\begin{aligned} Mr &= F - \hat{F} + G + \delta - (I_{Nl} - M\tilde{H}^{-1}\Lambda_1)\tilde{B}\dot{Q}_d + M\tilde{H}^{-1}\tilde{B}\ddot{Q}_d \\ &\quad - (I_{Nl} - M\tilde{H}^{-1})\Lambda_2 E_f + (C + \Lambda_1 - M\tilde{H}^{-1}\Lambda_1\tilde{H})\dot{Q} \\ &\triangleq \Omega - \hat{F} - (I_{Nl} - M\tilde{H}^{-1})\Lambda_2 E_f + \delta - \tilde{B}\dot{Q}_d, \end{aligned} \quad (3.13)$$

where $\Omega \triangleq F + G + (C + \Lambda_1 - M\tilde{H}^{-1}\Lambda_1\tilde{H})\dot{Q} + M\tilde{H}^{-1}(\tilde{B}\ddot{Q}_d + \Lambda_1\tilde{B}\dot{Q}_d) \in \mathbb{R}^{Nl}$ and I_{Nl} is an identity block matrix.

According to (3.6)-(3.8), the time derivative of \hat{F} is given by

$$\dot{\hat{F}} = (K_s + I_{Nl})(\dot{E}_f + \Lambda_2 E_f) + \tilde{H} \text{sgn}(E_f) \Pi_1 + \tilde{H} \text{sgn}(E_f) \Pi_2 \mathbf{1}_{Nl}, \quad (3.14)$$

$$\dot{\Pi}_1 = \text{sgn}(E_f)(\dot{E}_f + \Lambda_2 E_f), \quad (3.15)$$

where $\text{sgn}(E_f) \triangleq \text{diag}(\text{dsgn}(e_{f1}), \dots, \text{dsgn}(e_{fN}))$, $\text{dsgn}(e_{fi}) \triangleq \text{diag}(\text{sgn}(e_{fi1}), \dots, \text{sgn}(e_{fil}))$, $K_s \triangleq \text{diag}(k_{s1}, \dots, k_{sN}) \otimes I_l$, $\Pi_2 \triangleq \text{diag}(\beta_{21}, \dots, \beta_{2N}) \otimes I_l \in \mathbb{R}^{Nl \times Nl}$, and $\Pi_1(t) \triangleq \text{col}(\beta_{11}(t), \dots, \beta_{1N}(t)) \in \mathbb{R}^{Nl}$.

To obtain the closed-loop error system, differentiating (4.17) gives

$$\begin{aligned} M\dot{r} = & -\frac{1}{2}\dot{M}r - (K_s + I_{Nl})\tilde{H}r - \tilde{H}E_f + \dot{\delta} - \tilde{B}\ddot{Q}_d \\ & - \tilde{H}\text{sgn}(E_f)(\Pi_1 + \Pi_2 \mathbf{1}_{Nl}) + N(t), \end{aligned} \quad (3.16)$$

where $N(t) \in \mathbb{R}^{Nl}$ denotes an auxiliary term defined as

$$\begin{aligned} N(t) \triangleq & \dot{\Omega} - [\frac{1}{2}\dot{M} + (I_{Nl} - M\tilde{H}^{-1})\Lambda_2\tilde{H}]r + (\tilde{H} + \dot{M}\tilde{H}^{-1}\Lambda_2)E_f \\ & + (I_{Nl} - M\tilde{H}^{-1})\Lambda_2^2 E_f. \end{aligned} \quad (3.17)$$

To facilitate the subsequent analysis, an auxiliary term $N_d(t) \in \mathbb{R}^{Nl}$ is defined as

$$\begin{aligned} N_d(t) \triangleq & N_d(Q_d, \dot{Q}_d, \ddot{Q}_d, \ddot{\ddot{Q}}_d, \mathbf{0}_{Nl}, \mathbf{0}_{Nl}, \mathbf{0}_{Nl}) \\ = & \frac{\partial F(\dot{Q}_d)}{\partial \dot{Q}_d} \ddot{Q}_d + \frac{\partial G(Q_d)}{\partial Q_d} \dot{Q}_d + C(Q_d, \dot{Q}_d) \ddot{Q}_d + \dot{C}(Q_d, \dot{Q}_d) \dot{Q}_d \\ - & \dot{M}(Q_d) \tilde{H}^{-1} \Lambda_1 \tilde{H} \dot{Q}_d + M(Q_d) \tilde{H}^{-1} \Lambda_1 \tilde{B} \ddot{Q}_d \\ + & [\dot{M}(Q_d) \tilde{H}^{-1} \tilde{B} + (\Lambda_1 - M(Q_d) \tilde{H}^{-1} \Lambda_1 \tilde{H})] \ddot{Q}_d \\ + & M(Q_d) \tilde{H}^{-1} \tilde{B} \ddot{\ddot{Q}}_d + \dot{M}(Q_d) \tilde{H}^{-1} \Lambda_1 \tilde{B} \dot{Q}_d. \end{aligned} \quad (3.18)$$

After adding and subtracting $N_d(t)$ in (3.18), the closed-loop error system is

$$\begin{aligned} M\dot{r} = & -\frac{1}{2}\dot{M}r - (K_s + I_{Nl})\tilde{H}r + \tilde{\Delta}(t) + \tilde{H}\Delta_d(t) \\ & - \tilde{H}E_f - \tilde{H}\text{sgn}(E_f)(\Pi_1 + \Pi_2 \mathbf{1}_{Nl}), \end{aligned} \quad (3.19)$$

where the unmeasurable auxiliary term $\tilde{\Delta}(t) \in \mathbb{R}^{Nl}$ is given by

$$\tilde{\Delta}(t) \triangleq N(t) - N_d(t), \quad \Delta_d(t) \triangleq \tilde{H}^{-1}(N_d(t) + \dot{\delta} - \tilde{B}\ddot{Q}_d).$$

Based on Properties. 3.1 and 3.2, Assumptions 3.1 and 3.2, the auxiliary term $\Delta_d(t)$ and its time derivative satisfy:

$$\sup_{t \in [0, \infty)} |\Delta_{d_m}(t)| < c_{1m}, \quad \sup_{t \in [0, \infty)} \left| \dot{\Delta}_{d_m}(t) \right| < c_{2m}, \quad (3.20)$$

where $m = 1, 2, \dots, Nl$, $\Delta_{d_m}(t)$ and $\dot{\Delta}_{d_m}(t)$ denote the m^{th} element of $\Delta_d(t)$ and $\dot{\Delta}_d(t)$, respectively. Let $c_1 = \text{col}(c_{11}, c_{12}, \dots, c_{1N})$, $c_2 = \text{col}(c_{21}, c_{22}, \dots, c_{2N}) \in \mathbb{R}^{Nl}$, where $c_{1i}, c_{2i} \in \mathbb{R}^l$, $i \in \mathcal{V}$. Then in (3.20), c_1 and c_2 can be used to denote some unknown upper bounds on the corresponding element of $\Delta_d(t)$ and $\dot{\Delta}_d(t)$, respectively. Furthermore, the Mean Value Theorem can be utilized to show that the auxiliary error $\tilde{\Delta}(t)$ is upper bounded as [59,60,67–70]

$$\| \tilde{\Delta}(t) \| \leq \rho(\| z(t) \|) \| z(t) \|, \quad (3.21)$$

where $\rho(\cdot)$ is a positive, globally invertible, nondecreasing function and $z(t) \triangleq [E_\xi^T(t), E_f^T(t), r^T(t)]^T \in \mathbb{R}^{3Nl}$.

3.3.4 Stability Analysis and Sufficient Conditions

Theorem 3.1. *Suppose that Assumptions 3.1-3.3 hold. Then, the proposed distributed control law in (3.5)-(3.8) ensures that the semi-global asymptotic robust consensus tracking objective for N agents with dynamics in (3.1) can be achieved as*

$$[q_1^T, \dots, q_N^T]^T - \mathbf{1}_N \otimes q_d(t) \rightarrow \mathbf{0}_{Nl}, \quad (3.22)$$

$$[\dot{q}_1^T, \dots, \dot{q}_N^T]^T - \mathbf{1}_N \otimes \dot{q}_d(t) \rightarrow \mathbf{0}_{Nl}, \quad \text{as } t \rightarrow \infty,$$

provided that the control gain k_{si} is selected sufficiently large² based on the stabilizing initial conditions (see the subsequent stability analysis) and α_{1i} , α_{2i} and β_{2i} in (3.5)-(3.8) are selected according to the following sufficient conditions:

$$\alpha_{1i} > 0.5, \alpha_{2i} > 1, \beta_{2i} > 0, \beta_{1i}(0) = \mathbf{0}_l. \quad (3.23)$$

²A lower bound on the control gain k_{si} can be selected as $k_0 = \rho^2(c_0) / (4\lambda_0 \lambda_{\min}(\tilde{H}))$ where $c_0 \geq \sqrt{\lambda_2/\lambda_1} \sum_{i \in \mathcal{V}} \|y_i(0)\|$ with $y_i(0)$ related to the initial values of states. Note that this lower bound requires global information. A large enough k_{si} is thus selected before the controller is implemented so that $k_{si} = k_s > k_0$ to yield a semi-global stability result [67–70].

Proof. From Lemma 2.5, let $\mathcal{D} \subset \mathbb{R}^{4Nl+2}$ be a domain containing $y(t) \triangleq [z^T(t), \tilde{\Pi}_1^T(t), \sqrt{\mathcal{P}(t)}, \sqrt{\Phi(t)}]^T$, where $z(t)$ is given in (4.22) and $\mathcal{P}(t)$ is an auxiliary function, defined as

$$\mathcal{P}(t) = E_f^T(0)\hat{\Pi}_1 \text{sgn}(E_f(0))\mathbf{1}_{Nl} - E_f^T(0)\Delta_d(0) - \mathcal{S}(t), \quad (3.24)$$

where $\mathcal{S}(t)$ is the Filippov generalized solution to the following differential equation

$$\dot{\mathcal{S}}(t) = r^T(t)\tilde{H}(\Delta_d(t) - \hat{\Pi}_1 \text{sgn}(E_f(t))\mathbf{1}_{Nl}), \mathcal{S}(0) = 0,$$

where $\hat{\Pi}_1 \triangleq \text{diag}(\hat{\beta}_{11}, \dots, \hat{\beta}_{1N}) \otimes I_l \in \mathbb{R}^{Nl \times Nl}$ is a subsequently designed matrix introduced in (3.26) and $\hat{\beta}_{1i} > \|c_{1i}\|_\infty + \frac{1}{\alpha_{2i}} \|c_{2i}\|_\infty$ such that $\mathcal{P}(t) \geq 0$ ³.

Similarly, another auxiliary function $\Phi(t)$ is the Filippov generalized solution to the following defined differential equation

$$\dot{\Phi} = \dot{E}_f^T \Pi_2 \text{sgn}(E_f)\mathbf{1}_{Nl}, \quad \Phi(0) = E_f^T(0)\Pi_2 \text{sgn}(E_f(0))\mathbf{1}_{Nl}. \quad (3.25)$$

Let $V_L: \mathcal{D} \times [0, \infty) \rightarrow \mathbb{R}$ be a continuously differentiable, non-negative function (i.e., a Lyapunov candidate), defined as

$$V_L(y, t) \triangleq E_\xi^T E_\xi + \frac{1}{2} E_f^T E_f + \frac{1}{2} r^T M r + \frac{1}{2} \tilde{\Pi}_1^T \tilde{\Pi}_1 + \mathcal{P}(t) + \Phi(t), \quad (3.26)$$

where $\tilde{\Pi}_1(t) = \Pi_1(t) - \hat{\Pi}_1 \mathbf{1}_{Nl}$ and the positive constant time-varying term $\hat{\Pi}_1$ is an estimate of $\Pi_1(t)$. Under Assumption 1, the Lyapunov function in (3.26) is non-negative and satisfies: $\lambda_1 \|y\|^2 \leq V_L(y, t) \leq \lambda_2(Q) \|y\|^2$, where $\lambda_1 \triangleq \frac{1}{2} \min\{1, \min_{j \in \mathcal{V}}(\underline{m}_j)\}$ and $\lambda_2 \triangleq \max\{\frac{1}{2} \sum_{j \in \mathcal{V}} \bar{m}_j, 1\}$.

Under Filippov's framework, the time derivative of $V(y, t)$ exists almost everywhere (a.e.), i.e., for almost all $t \in [0, \infty)$ and $\dot{V}_L \stackrel{\text{a.e.}}{\in} \dot{\tilde{V}}_L$ by Lemma 2.5, where

$$\dot{\tilde{V}}_L = \bigcap_{s \in \partial V_L} s^T \mathbb{K}[\dot{E}_\xi^T, \dot{E}_f^T, \dot{r}^T, \dot{\tilde{\Pi}}_1^T, \frac{1}{2} \dot{\mathcal{P}}^{-\frac{1}{2}}, \frac{1}{2} \dot{\Phi}^{-\frac{1}{2}}, 1]^T, \quad (3.27)$$

³The proof is provided in Lemma A.1 in Appendix A.

where ∂V_L is the generalized gradient of V_L [65]. Since V_L is continuously differentiable in y , then it gives

$$\dot{\tilde{V}}_L \subset \nabla V_L^T \mathbb{k}[\dot{E}_\xi^T, \dot{E}_f^T, \dot{r}^T, \dot{\tilde{\Pi}}_1^T, \frac{1}{2}\mathcal{P}^{-\frac{1}{2}}\dot{\mathcal{P}}, \frac{1}{2}\Phi^{-\frac{1}{2}}\dot{\Phi}, 1]^T, \quad (3.28)$$

where $\nabla V_L \triangleq [2E_\xi^T, E_f^T, r^T M, \tilde{\Pi}_1^T, 2\mathcal{P}^{\frac{1}{2}}, 2\Phi^{\frac{1}{2}}, \frac{1}{2}r^T \dot{M}r]^T$.

By using (4.9)-(3.14) and (3.19), the expression in (4.29) becomes

$$\begin{aligned} \dot{\tilde{V}}_L \subset & r^T \left\{ -\frac{1}{2}\dot{M}r - (K_s + I_{Nl})\tilde{H}r - \tilde{H}E_f + \tilde{\Delta}(t) + (\tilde{H}\Delta_d(t) - \tilde{H}\mathbb{k}[\text{sgn}(E_f)]) \right. \\ & \times (\Pi_1 + \Pi_2 \mathbf{1}_{Nl}) \left. \right\} + 2E_\xi^T (E_f - \Lambda_1 E_\xi) + E_f^T (\tilde{H}r - \Lambda_2 E_f) + \frac{1}{2}r^T \dot{M}r \\ & + (\Pi_1 - \hat{\Pi}_1 \mathbf{1}_{Nl})^T \mathbb{k}[\text{sgn}(E_f)]\tilde{H}r + (\tilde{H}r - \Lambda_2 E_f)^T \Pi_2 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl} \\ & - r^T (\tilde{H}\Delta_d(t) - \tilde{H}\hat{\Pi}_1 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl}), \end{aligned} \quad (3.29)$$

where $\mathbb{k}[\text{sgn}(E_f)] = \text{SGN}(E_f)$ such that $\text{SGN}(E_{fik}) = 1$ if $E_{fik} > 0$, $[-1, 1]$ if $E_{fik} = 0$, and -1 if $E_{fik} < 0$, $i = 1, 2, \dots, N$, $k = 1, 2, \dots, l$ [65].

After canceling the corresponding common terms and exploiting (4.22), the expression in (3.29) is rewritten as

$$\begin{aligned} \dot{\tilde{V}}_L \stackrel{a.e.}{\leq} & \|r\| \rho(\|z(t)\|) \|z(t)\| + 2\|E_\xi\| \|E_f\| - \lambda_{\min}(\Theta) \|r\|^2 \\ & - \lambda_{\min}(\tilde{H}) \|r\|^2 - 2\lambda_{\min}(\Lambda_1) \|E_\xi\|^2 - \lambda_{\min}(\Lambda_2) \|E_f\|^2, \end{aligned} \quad (3.30)$$

where $\Theta = \frac{1}{2}(K_s \tilde{H} + \tilde{H} K_s)$ and (3.29) reduces to the scalar inequality in (3.30) since the RHS is continuous a.e., i.e., the RHS is continuous except for the Lebesgue negligible set of time when $r^T \tilde{H} \mathbb{k}[\text{sgn}(E_f)](\Pi_1 + \Pi_2 \mathbf{1}_{Nl}) - r^T \tilde{H} \mathbb{k}[\text{sgn}(E_f)](\Pi_1 + \Pi_2 \mathbf{1}_{Nl}) \neq \{0\}$ and $r^T \tilde{H} \hat{\Pi}_1 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl} - r^T \tilde{H} \hat{\Pi}_1 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl} \neq \{0\}$ [65].

Based on Young's Inequality and by completing the squares for r , the expression in (3.30) can be rewritten as

$$\begin{aligned} \dot{\tilde{V}}_L \stackrel{a.e.}{\leq} & -\lambda_0 \|z(t)\|^2 - \lambda_{\min}(\Theta) \|r\|^2 + \|r\| \rho(\|z(t)\|) \|z(t)\| \\ \stackrel{a.e.}{\leq} & -\left(\lambda_0 - \frac{\rho^2(\|z(t)\|)}{4\lambda_{\min}(\Theta)} \right) \|z(t)\|^2, \end{aligned} \quad (3.31)$$

where $\lambda_0 \triangleq \min\{2(\lambda_{\min}(\Lambda_1) - \frac{1}{2}), \lambda_{\min}(\Lambda_2) - 1, \lambda_{\min}(\tilde{H})\}$, and the bounding function $\rho(\|z(t)\|)$ is a positive globally invertible nondecreasing function. By selecting α_{1i} and α_{2i} , according to (3.23) and using the fact that H is of full rank, λ_0 is positive. Let $U_1(y) = -\left(\lambda_0 - \frac{\rho^2(\|z(t)\|)}{4\lambda_{\min}(\Theta)}\right) \|z\|^2 = -u_1 \|z\|^2$ be a continuous negative semi-definite function, which is defined on the following domain:

$$\mathcal{D} \triangleq \{y/\|y\| < \rho^{-1}[2\sqrt{\lambda_0\lambda_{\min}(\Theta)}]\}. \quad (3.32)$$

Let the set of stabilizing initial conditions be defined as

$$y(0) \in \Upsilon \triangleq \{y \in \mathcal{D} \mid \|y\| < \sqrt{\frac{\lambda_1}{\lambda_2}} \rho^{-1}[2\sqrt{\lambda_0\lambda_{\min}(\Theta)}]\}. \quad (3.33)$$

Under the condition (3.23) and the control gain k_{si} is selected sufficiently large such that $y(0) \in \Upsilon$, it gives $\dot{V}_L \stackrel{a.e.}{\leq} -u_1 \|z\|^2$ for all $y \in \mathcal{D}$ and a positive constant $u_1 \in \mathbb{R}$. Thus, \dot{V}_L is negative semi-definite and $V_L \leq V_L(0) \in \mathcal{L}_\infty$ holds in \mathcal{D} . The details are given as below. Based on (3.2), (3.4) and (3.7), the initial errors $e_{\xi i}(0)$, $e_{fi}(0)$ and $r_i(0)$ are not related to k_{si} . Thus, k_{si} can be selected sufficiently large such that $y(0) \in \Upsilon$. That is, the ratio of the function $\rho^2(\|z(0)\|)$ to k_{si} in (3.31) can be made sufficiently small such that $\dot{V}_L(0) \leq 0$. For $t > 0$, a proof by contradiction is provided as follows to show that V_L is monotonically decreasing.

Proof by contradiction: Let $4\lambda_{\min}(\Theta) = c$. Assume that there exists a time instant $t^* > 0$ such that $\lambda_0 < \rho^2(\|z(t^*)\|)/c$ and $\lambda_0 \geq \rho^2(\|z(t)\|)/c$ for $t \in [0, t^*)$. Thus, $\dot{V}_L(t) \leq 0$ for $t \in [0, t^*)$. That is, $\|z(t)\| \leq \|z(0)\|$ for $t \in [0, t^*)$.

Case i. $\|z(t)\| < \|z(0)\|$ for $t \in [0, t^*)$. From the assumption, $\rho^2(\|z(t^*)\|) > \lambda_0 c$. In addition, by $y(0) \in \Upsilon$, $\lambda_0 c > \rho^2(\|z(0)\|)$. Thus, $\rho^2(\|z(t^*)\|) > \rho^2(\|z(0)\|)$. Since $\rho(\|z(t)\|)$ is a positive nondecreasing function, $\|z(t^*)\| > \|z(0)\|$ holds, which contradicts with $\|z(t)\| < \|z(0)\|$ for $t \in [0, t^*)$ by the state continuity.

Case ii. $\|z(t)\| \equiv \|z(0)\|$ for $t \in [0, t^*)$. Since $\lambda_0 c > \rho^2(\|z(0)\|)$ by $y(0) \in \Upsilon$, $\lambda_0 c > \rho^2(\|z(t)\|)$ for $t \in [0, t^*)$, which contradicts with $\rho^2(\|z(t^*)\|) > \lambda_0 c$.

Hence, $V_L \leq V_L(0) \in \mathcal{L}_\infty$ holds in \mathcal{D} for $\forall t \geq 0$.

Since $V_L \in \mathcal{L}_\infty$ and the fact that H is positive definite by Lemma 3.1, it follows from (3.11) and (3.26) that $E_\xi(t), \dot{E}_\xi(t), E_f(t), r(t) \in \mathcal{L}_\infty$ in \mathcal{D} . From Properties 1 and 2, we have $\dot{F} \in \mathcal{L}_\infty$ in \mathcal{D} . From (3.16), $\dot{r}(t) \in \mathcal{L}_\infty$ in \mathcal{D} . From (3.9) and (3.12), $\ddot{E}_\xi(t), \ddot{E}_\xi(t), \ddot{E}_f(t) \in \mathcal{L}_\infty$ in \mathcal{D} , then $\ddot{F} \in \mathcal{L}_\infty$ in \mathcal{D} . Thus, Lemma 2.5 can be used to show that $u_1 \|z\|^2 \rightarrow 0$, as $t \rightarrow \infty$, $\forall y(0) \in \Upsilon$. That is $E_\xi(t) \rightarrow \mathbf{0}_{Nl}$, $E_f(t) \rightarrow \mathbf{0}_{Nl}$ and $r(t) \rightarrow \mathbf{0}_{Nl}$, as $t \rightarrow \infty$, $\forall y(0) \in \Upsilon$. Based on (3.11), $Q = Q_d$. Similarly, based on $E_\xi(t) = \mathbf{0}_{Nl}$ and $E_f(t) = \mathbf{0}_{Nl}$, it follows from (3.11) that $\dot{Q} = \dot{Q}_d$. Thus, $q_i(t) \rightarrow q_d(t)$ and $\dot{q}_i(t) \rightarrow \dot{q}_d(t)$ as $t \rightarrow \infty$, $\forall y(0) \in \Upsilon$. \square

Remark 3.2. According to Theorem 3.1, a large enough control parameter k_{si} in (3.7) can be selected to enlarge the domain of convergence to enclose any a priori given arbitrarily large bounded set as its subset.

Remark 3.3. Several consensus algorithms are developed for Euler-Lagrange systems (e.g., [16], [40–49]). However, most of these works only deal with structured uncertainties based on a model-based parametric linearization. Challenging unstructured uncertainties including unknown nonlinear dynamics and disturbances is an important and challenging problem. The algorithms in [16], [40] and [41] are based on the exact knowledge of the dynamics and the leader's acceleration information was available to all the followers. Robust UUB coordinated tracking result was obtained in [43] by using the neural-network-based control. In [44] and [45], the proposed discontinuous distributed sliding mode estimators required the parametric uncertainties to satisfy the linearity-in-parameters assumption. However, the proposed algorithm in this work removes these constraints.

Remark 3.4. Several control gains α_{1i} , α_{2i} , k_{si} and a time-varying control term $\beta_i(t) = \beta_{1i}(t) + \beta_{2i}\mathbf{1}_l$ are used in (3.5)–(3.8). According to (3.23), sufficient conditions are derived to achieve robust consensus tracking. An agent based Lyapunov approach is used, where $\hat{\beta}_{1i}(t)$ is an estimate of the time-varying gain $\beta_{1i}(t)$ satisfying: $\hat{\beta}_{1i}(t) > \|c_{1i}\|_\infty + \alpha_{2i}^{-1} \|c_{2i}\|_\infty$. However, this gain $\hat{\beta}_{1i}(t)$ is only introduced to

facilitate the Lyapunov analysis and not used in the controller. Thus, the designed distributed control law does not need the unknown upper bounds of c_1 and c_2 . The proposed distributed controller shown in (3.5)-(3.8) is decentralized in the sense that only local feedback is required to compute the controller. However, by (3.32) the control gain k_{si} is related to \tilde{H} containing global information. This k_{si} can thus be selected large enough before the control law is implemented to yield a semi-global tracking result as described in Theorem 3.1.

3.4 Robust Distributed Coordination Under A Directed Graph

For a digraph, the information-exchange matrix H is asymmetric. In such a case, if we choose a Lyapunov function $r^T M r$, then the term $-r^T \tilde{H} r$ will appear in its derivative. Thus, it is unclear how (3.5) can be applied, especially when considering to compensate for $r^T \tilde{H}(\Delta_d - \hat{\Pi}_1 \text{sgn}(E_f) \mathbf{1}_{Nl})$ via the defined errors in (3.2)-(3.4) and the filter error: $\tilde{H} r = \dot{E}_f + \Lambda_2 E_f$. Hence, new distributed schemes are needed to achieve asymptotic robust consensus tracking for a directed graph. In this section, a distributed two-layer coordination scheme will be proposed, where in the top layer, a distributed leader estimator is presented to estimate the leader's states. Then, by this distributed estimator, a novel distributed controller is developed.

Assumption 3.4. *The communication graph \mathcal{G} is directed and \mathcal{V}_0 has directed paths to all the agents of \mathcal{G} .*

Lemma 3.2. *[64] Suppose that Assumption 3.4 holds, then H is nonsingular and all the eigenvalues of H have positive real parts.*

To facilitate the distributed leader estimator design, we assume that \mathcal{V}_0 is generated by the following leader system [72,73]:

$$\ddot{q}_d(t) = S_1 \dot{q}_d(t) + S_2 \dot{q}_d(t), \quad (3.34)$$

where $S_1, S_2 \in \mathbb{R}^{l \times l}$ are arbitrary constant matrices.

Define $S = \begin{bmatrix} 0_{l \times l} & I_l \\ S_1 & S_2 \end{bmatrix}$, (3.34) can be rewritten as

$$\begin{bmatrix} \dot{q}_d \\ \ddot{q}_d \end{bmatrix} = S \begin{bmatrix} q_d \\ \dot{q}_d \end{bmatrix}. \quad (3.35)$$

Assumption 3.5. [38] *The system in (3.35) is marginally stable.*

Remark 3.5. *Note that when $S_1 = S_2 = 0_{l \times l}$, (3.35) is a double integrator system. However, in this subsection, we do not require (3.35) to be a double integrator system. The system in (3.35) can generate a large class of reference signals.*

3.4.1 Distributed Leader Estimator Design

For $i = 1, 2, \dots, N$, the following leader estimation errors are defined by using only relative information as

$$\begin{aligned} \varrho_{di1}(t) &= \sum_{j=1}^N a_{ij} (\varrho_{j1} - \varrho_{i1}) + b_i (q_d - \varrho_{i1}), \\ \varrho_{di2}(t) &= \sum_{j=1}^N a_{ij} (\varrho_{j2} - \varrho_{i2}) + b_i (\dot{q}_d - \varrho_{i2}), \end{aligned} \quad (3.36)$$

where $\varrho_{i1}(t), \varrho_{i2}(t) \in \mathbb{R}^l$ are designed for a gain $\kappa_i > 0$,

$$\begin{aligned} \dot{\varrho}_{i1}(t) &= \varrho_{i2}(t) + \kappa_i \varrho_{di1}(t), \\ \dot{\varrho}_{i2}(t) &= S_1 \varrho_{i1}(t) + S_2 \varrho_{i2}(t) + \kappa_i \varrho_{di2}(t), \end{aligned} \quad (3.37)$$

Define new variables: $\varrho_i(t) \triangleq \text{col}(\varrho_{i1}, \varrho_{i2})$, $\varrho_{di}(t) \triangleq \text{col}(\varrho_{di1}, \varrho_{di2})$ and $\varrho_d(t) \triangleq \text{col}(q_d, \dot{q}_d)$. Then, the system composed of (3.36) and (3.37) can be expressed as

$$\begin{aligned} \dot{\varrho}_i(t) &= S \varrho_i(t) + \kappa_i \varrho_{di}(t), \\ \varrho_{di}(t) &= \sum_{j=1}^N a_{ij} (\varrho_j - \varrho_i) + b_i (\varrho_d - \varrho_i). \end{aligned} \quad (3.38)$$

Lemma 3.3. *Suppose that Assumptions 3.4 and 3.5 hold. Then, under the proposed distributed leader estimator in (3.37), it follows that for all $\kappa_i > 0$, $i = 1, 2, \dots, N$,*

$$\varrho_{i1}(t) - q_d(t) \rightarrow \mathbf{0}_l \text{ and } \varrho_{i2}(t) - \dot{q}_d(t) \rightarrow \mathbf{0}_l, \text{ as } t \rightarrow \infty. \quad (3.39)$$

Proof. Define a new variable $\tilde{\varrho}_i(t) = \varrho_i(t) - \varrho_d(t)$. Then it follows from (3.35) and (3.38) that the closed-loop estimate error system can be given by

$$\begin{aligned}\dot{\tilde{\varrho}}_i(t) &= \dot{\varrho}_i(t) - \dot{\varrho}_d(t) = S\varrho_i(t) - S\varrho_d(t) + \kappa_i\varrho_{di}(t) \\ &= S\tilde{\varrho}_i(t) - \kappa_i\left(\sum_{j=1}^N a_{ij}(\tilde{\varrho}_i(t) - \tilde{\varrho}_j(t)) + b_i\tilde{\varrho}_i(t)\right),\end{aligned}$$

which can be rewritten in the following compact form for $\tilde{\varrho} \triangleq \text{col}(\tilde{\varrho}_1, \tilde{\varrho}_2, \dots, \tilde{\varrho}_N)$ and $\kappa \triangleq \text{diag}(\kappa_1, \kappa_2, \dots, \kappa_N) \otimes I_{2l}$.

$$\dot{\tilde{\varrho}}(t) = [(I_N \otimes S) - \kappa(H \otimes I_{2l})]\tilde{\varrho}(t), \quad (3.40)$$

Based on Lemma B.1 in Appendix B, if all the eigenvalues of S have nonpositive real parts, then for any $\kappa > 0$, the origin of the closed-loop estimate error system (3.40) is exponentially stable. That is, for all $i = 1, 2, \dots, N$, $\lim_{t \rightarrow \infty} \tilde{\varrho}_i(t) = \mathbf{0}_l$. Thus, $\lim_{t \rightarrow \infty} \varrho_{i1}(t) - q_d(t) = \mathbf{0}_l$ and $\lim_{t \rightarrow \infty} \varrho_{i2}(t) - \dot{q}_d(t) = \mathbf{0}_l$ hold. \square

3.4.2 Robust Consensus Tracking Control Law Design

To introduce the distributed controller design for the directed communication graph, similar to (3.2)-(3.4) and (3.9), we define the following error signals based on information from the distributed leader estimator.

$$\begin{aligned}\dot{q}_{ri} &= \varrho_{i2}(t) + \kappa_i\varrho_{di1}(t) - \alpha_{\varrho i}(q_i - \varrho_{i1}), \\ s_i &= \dot{q}_i - \dot{q}_{ri} = \dot{q}_i - \dot{\varrho}_{i1} + \alpha_{\varrho i}(q_i - \varrho_{i1}),\end{aligned} \quad (3.41)$$

where κ_i and $\alpha_{\varrho i}$ are two positive controller gains, s_i is the sliding surface, q_{ri} is the virtual reference. Similar to (3.9), for a positive constant $\alpha_{ri} \in \mathbb{R}$, a filter error signal $r_{si}(t) \in \mathbb{R}^l$ is defined as

$$r_{si} = \dot{s}_i + \alpha_{ri}s_i. \quad (3.42)$$

The two-layer based distributed control law shown in Fig. 3.1 is given by

$$\tau_i(t) = -\alpha_{qi}\dot{v}_i - \alpha_{si}s_i - \hat{f}_{\varrho i}(t), \quad (3.43)$$

where $v_i = q_i - \varrho_{i1}$, α_{qi} and α_{si} are two control gains, and similar to (3.7) and (3.8),

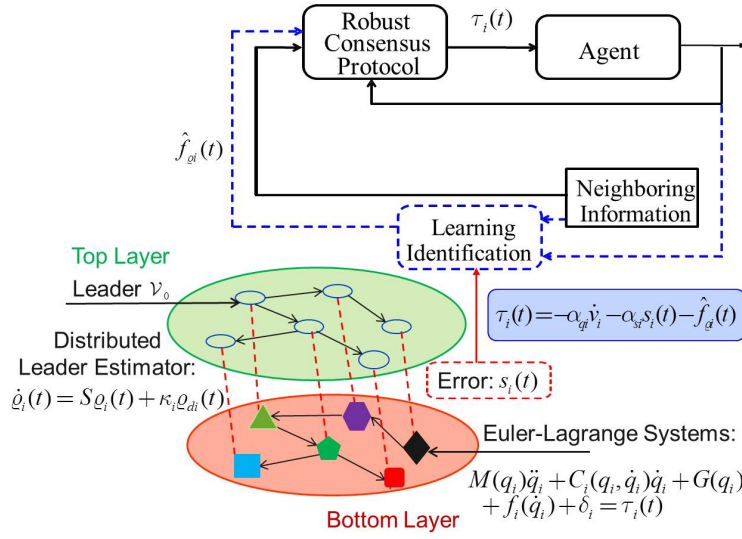


Figure 3.1: Diagram of the two-layer based distributed control law design.

the distributed estimation law $\hat{f}_{\varrho i}(t)$ is given by

$$\begin{aligned}
 \hat{f}_{\varrho i}(t) &= (k_{\varrho si} + 1)(s_i(t) - s_i(0)) + v_{\varrho i}(t), \\
 \dot{v}_{\varrho i}(t) &= (k_{\varrho si} + 1)\alpha_{ri}s_i(t) + \beta_{\varrho i}(t) \odot \text{vsgn}(s_i(t)), \\
 \beta_{\varrho i}(t) &= \beta_{\varrho 1i}(t) + \beta_{\varrho 2i}\mathbf{1}_l, \quad \beta_{\varrho 1i}(0) = \mathbf{0}_l, \\
 \beta_{\varrho 1i}(t) &= |s_i(t)| - |s_i(0)| + \alpha_{ri} \int_0^t |s_i(\tau)| d\tau.
 \end{aligned} \tag{3.44}$$

3.4.3 Closed-Loop System Development

The filter error signal (3.42) and the control law (3.41) together with (3.44) can be expressed in the following compact form

$$r_s = \dot{s} + \Lambda_r s, \quad s = \dot{v} + \Lambda_\varrho v, \quad \Gamma = -\Lambda_q \dot{v} - \Lambda_s s - \hat{F}_\varrho, \tag{3.45}$$

where given (3.1), the time derivative of s is written as

$$\dot{s} = M^{-1}[\Gamma - (F + C\dot{Q} + G + \delta)] - \ddot{\varrho}_1 + \Lambda_\varrho \dot{v}, \tag{3.46}$$

where $s \triangleq \text{col}(s_1, \dots, s_N)$, $r_s \triangleq \text{col}(r_{s1}, \dots, r_{sN})$, $v \triangleq \text{col}(v_1, \dots, v_N)$, $\hat{F}_\varrho \triangleq \text{col}(\hat{f}_{\varrho 1}, \dots, \hat{f}_{\varrho N})$, $\varrho_1 \triangleq \text{col}(\varrho_{11}, \dots, \varrho_{N1})$; and $\Lambda_q \triangleq \text{diag}(\alpha_{q1}, \dots, \alpha_{qN}) \otimes I_l$, $\Lambda_\varrho \triangleq \text{diag}(\alpha_{\varrho 1}, \dots, \alpha_{\varrho N}) \otimes I_l$, $\Lambda_r \triangleq \text{diag}(\alpha_{r1}, \dots, \alpha_{rN}) \otimes I_l$, $\Lambda_s \triangleq \text{diag}(\alpha_{s1}, \dots, \alpha_{sN}) \otimes I_l$.

After premultiplying (3.46) by M , it follows from (3.45) that

$$\begin{aligned} Mr_s &= -\Lambda_q \dot{v} - \Lambda_s s - \hat{F}_\varrho - (F + C\dot{Q} + G + \delta) - M\ddot{\varrho}_1 + M\Lambda_\varrho \dot{v} + M\Lambda_r s \\ &\triangleq N_\varrho(t) + N_{d\varrho}(t) - \hat{F}_\varrho, \end{aligned} \quad (3.47)$$

where $N_\varrho(t) \triangleq F_d - F + C_d\dot{Q}_d - C\dot{Q} + G_d - G + (M\Lambda_\varrho - \Lambda_q)\dot{v} + (M\Lambda_r - \Lambda_s)s + (M_d - M)\ddot{\varrho}_1$, $N_{d\varrho}(t) \triangleq -F_d - C_d\dot{Q}_d - G_d - M_d\ddot{\varrho}_1 - \delta$, and $F_d \triangleq F(\dot{Q}_d)$, $G_d \triangleq G(Q_d) \in \mathbb{R}^{Nl}$, and $C_d \triangleq C(Q_d, \dot{Q}_d)$, $M_d \triangleq M(Q_d) \in \mathbb{R}^{Nl \times Nl}$.

Similar to (3.14)-(3.16), differentiating (3.47) by using (3.44) yields

$$M\dot{r}_s = -\frac{1}{2}\dot{M}r_s - (K_{\varrho s} + I_{Nl})r_s + \tilde{\Delta}_\varrho(t) + \Delta_{d\varrho}(t) - s - \text{sgn}(s)(\Pi_{\varrho 1}(t) + \Pi_{\varrho 2}\mathbf{1}_{Nl}),$$

where the unmeasurable auxiliary terms $\tilde{\Delta}_\varrho(t)$ and $\Delta_{d\varrho}(t)$ are defined as $\tilde{\Delta}_\varrho(t) \triangleq \dot{N}_\varrho(t) - \frac{1}{2}\dot{M}r_s + s$, $\Delta_{d\varrho}(t) \triangleq \dot{N}_{d\varrho}(t)$; and $K_{\varrho s} \triangleq \text{diag}(k_{\varrho s1}, \dots, k_{\varrho sN}) \otimes I_l$, $\Pi_{\varrho 2} \triangleq \text{diag}(\beta_{\varrho 21}, \dots, \beta_{\varrho 2N}) \otimes I_l$, $\Pi_{\varrho 1}(t) \triangleq \text{col}(\beta_{\varrho 11}(t), \dots, \beta_{\varrho 1N}(t))$.

Under Assumption 3.5, q_d and \dot{q}_d are bounded and so are ϱ_{i1} and ϱ_{i2} by (3.37) and (3.39). In addition, based on Properties 1 and 2, Assumptions 4 and 5, similar to that in (3.20), the auxiliary term $\Delta_{d\varrho}(t)$ and its time derivative satisfy:

$$\sup_{t \in [0, \infty)} |\Delta_{d\varrho_m}(t)| < c_{3m}, \quad \sup_{t \in [0, \infty)} \left| \dot{\Delta}_{d\varrho_m}(t) \right| < c_{4m}, \quad (3.48)$$

where $m = 1, 2, \dots, Nl$, $c_3 \triangleq \text{col}(c_{31}, c_{32}, \dots, c_{3N})$, $c_4 \triangleq \text{col}(c_{41}, c_{42}, \dots, c_{4N})$ with $c_{3i}, c_{4i} \in \mathbb{R}^l$, $i \in \mathcal{V}$.

Furthermore, similar to (3.21), the auxiliary error $\tilde{\Delta}_\varrho(t)$ is upper bounded as

$$\|\tilde{\Delta}_\varrho(t)\| \leq \rho_\varrho(\|z_\varrho(t)\|) \|z_\varrho(t)\|, \quad z_\varrho(t) = [v^T(t), s^T(t), r_s^T(t)]^T. \quad (3.49)$$

3.4.4 Stability Analysis and Sufficient Conditions

Theorem 3.2. *Suppose that Lemma 3.3 and Assumptions 3.1, 3.4 and 3.5 hold. Then the proposed distributed control law in (3.43) together with (3.37) and (3.44) ensure that the semi-globally asymptotic robust consensus tracking objective for N*

agents with dynamics in (3.1) can be achieved in the sense: $\lim_{t \rightarrow \infty} q_i(t) - q_d(t) = \mathbf{0}_l$ and $\lim_{t \rightarrow \infty} \dot{q}_i(t) - \dot{q}_d(t) = \mathbf{0}_l$, provided that the control gain $k_{\varrho si}$ is selected sufficiently large and α_{qi} , α_{si} , $\alpha_{\varrho i}$, α_{ri} and $\beta_{\varrho 2i}$ in (3.37), (3.43) and (3.44) are selected according to the following conditions:

$$\alpha_{qi} > 0, \alpha_{si} > 0, \alpha_{\varrho i} > 0.5, \alpha_{ri} > 1, \beta_{\varrho 2i} > 0. \quad (3.50)$$

Proof. Let $\mathcal{D}_\varrho \subset \mathbb{R}^{4Nl+2}$ be a domain containing $y_\varrho(t)$ defined as $y_\varrho(t) \triangleq [z_\varrho^T(t), \tilde{\Pi}_{\varrho 1}^T(t), \sqrt{\mathcal{P}_\varrho(t)}, \sqrt{\Phi_\varrho(t)}]^T$, where $z_\varrho(t)$ is given in (3.49) and $\mathcal{P}_\varrho(t)$ and $\Phi_\varrho(t)$ are two positive semi-definite auxiliary functions, defined as:

$$\begin{aligned} \mathcal{P}_\varrho(t) &= s^T(0) \hat{\Pi}_{\varrho 1} \text{sgn}(s(0)) \mathbf{1}_{Nl} - s^T(0) \Delta_{d\varrho}(0) - S_\varrho(t), \\ \dot{S}_\varrho(t) &= r_s^T(\Delta_{d\varrho}(t) - \hat{\Pi}_{\varrho 1} \text{sgn}(s) \mathbf{1}_{Nl}), \quad S_\varrho(0) = 0, \\ \dot{\Phi}_\varrho(t) &= s \Pi_{\varrho 2} \text{sgn}(s) \mathbf{1}_{Nl}, \quad \Phi_\varrho(0) = s^T(0) \Pi_{\varrho 2} \text{sgn}(s(0)) \mathbf{1}_{Nl}, \end{aligned}$$

where $\hat{\Pi}_{\varrho 1} \triangleq \text{diag}(\hat{\beta}_{\varrho 11}, \dots, \hat{\beta}_{\varrho 1N}) \otimes I_l \in \mathbb{R}^{Nl \times Nl}$ is a subsequently designed matrix introduced in (3.51) and $\hat{\beta}_{\varrho 1i} > \|c_{3i}\|_\infty + \frac{1}{\alpha_{ri}} \|c_{4i}\|_\infty$ such that $\mathcal{P}_\varrho(t) \geq 0$.

Let $V_{\tilde{L}}: \mathcal{D}_\varrho \times [0, \infty) \rightarrow \mathbb{R}$ be a continuously differentiable, non-negative function (i.e., a Lyapunov candidate), defined as

$$V_{\tilde{L}}(y_\varrho, t) \triangleq v^T v + \frac{1}{2} s^T s + \frac{1}{2} r_s^T M r_s + \frac{1}{2} \tilde{\Pi}_{\varrho 1}^T \tilde{\Pi}_{\varrho 1} + \mathcal{P}_\varrho(t) + \Phi_\varrho(t), \quad (3.51)$$

where $\tilde{\Pi}_{\varrho 1}(t) = \Pi_{\varrho 1}(t) - \hat{\Pi}_{\varrho 1} \mathbf{1}_{Nl}$ and the term $\hat{\Pi}_{\varrho 1}(t)$ is an estimate of $\Pi_{\varrho 1}(t)$.

Next, the proof is similar to that in Theorem 3.1 to give $V_{\tilde{L}} \leq V_{\tilde{L}}(0) \in \mathcal{L}_\infty$ in $\mathcal{D}_\varrho \triangleq \{y_\varrho / \|y_\varrho\| < \rho_\varrho^{-1} [2\sqrt{\lambda_{\varrho 0} \lambda_{\min}(K_s)}]\}$, $\lambda_{\varrho 0} \triangleq \min\{2(\lambda_{\min}(\Lambda_\varrho) - \frac{1}{2}), \lambda_{\min}(\Lambda_r) - 1, 1\}$. Based on (3.36), (3.37), (3.41) and (3.42), Lemma 2.5 can be used to show $v(t) \rightarrow \mathbf{0}_{Nl}$, $s(t) \rightarrow \mathbf{0}_{Nl}$ and $r_s(t) \rightarrow \mathbf{0}_{Nl}$, as $t \rightarrow \infty$, $\forall y_\varrho(0) \in \Upsilon_\varrho$.

Next, to further show that $\lim_{t \rightarrow \infty} q_i(t) - q_d(t) = \mathbf{0}_l$ and $\lim_{t \rightarrow \infty} \dot{q}_i(t) - \dot{q}_d(t) = \mathbf{0}_l$ hold, we need linear input-to-state stability, (3.39) in Lemma 3.3 and the sliding mode design in (3.41). Specifically, substituting (3.38) into (3.41) gives

$$s_i = \dot{q}_i - \dot{q}_{ri} = \dot{q}_i - (\varrho_{i2} + \kappa_i \varrho_{di1}) + \alpha_{\varrho i}(q_i - \varrho_{i1}), \quad (3.52)$$

$$\dot{q}_i - \dot{\varrho}_{i1} + \alpha_{\varrho_i}(q_i - \varrho_{i1}) = s_i. \quad (3.53)$$

Since (3.53) can be viewed as a stable first-order differential equation with $s_i(t)$ as the input and this input is bounded for all $t \geq 0$ and tends to zero as $t \rightarrow \infty$, by exploiting the linear input-to-state stability, both $\dot{q}_i - \dot{\varrho}_{i1}$ and $q_i - \varrho_{i1}$ are bounded over $t \geq 0$ and will decay to zero. Thus, by the conclusion (3.39) in Lemma 4 and the sliding mode design in (3.41), it follows from

$$\begin{aligned} q_i(t) - q_d(t) &= q_i(t) - \varrho_{i1}(t) + \varrho_{i1}(t) - q_d(t), \\ \dot{q}_i(t) - \dot{q}_d(t) &= \dot{q}_i(t) - \dot{\varrho}_{i1}(t) + \dot{\varrho}_{i1}(t) - \dot{q}_d(t) = \dot{q}_i(t) - \varrho_{i2}(t) + \varrho_{i2}(t) - \dot{q}_d(t), \end{aligned}$$

that the robust consensus tracking result holds, i.e., $\lim_{t \rightarrow \infty} q_i(t) - q_d(t) = \mathbf{0}_l$ and $\lim_{t \rightarrow \infty} \dot{q}_i(t) - \dot{q}_d(t) = \mathbf{0}_l$. Therefore, the proof is completed. \square

Remark 3.6. *Based on the distributed two-layer design, all the gains are distributed. Moreover, $k_{\varrho_{si}}$ is not related to the global information on H , while k_{si} designed in Theorem 3.1 does need the global information on H . Therefore, this limitation is removed in Section 3.4 for a directed graph case.*

Remark 3.7. *The continuous distributed controller in (3.5) for the undirected graph case is distributed and relies on neighboring error signals. The use of these signals in (3.7) provides asymptotic consensus tracking of a time-varying leader, although it requires two-hop communication. However, in Section 3.4, the two-hop communication requirement is reduced to single-hop communication based on a distributed two-layer coordination design under a class of leader systems in (3.34) and (3.35). Distributed sufficient conditions are derived for both undirected and directed graph cases to achieve robust consensus tracking asymptotically.*

3.5 Numerical Example

Numerical simulations are presented to demonstrate the effectiveness of the proposed distributed control algorithms. As studied in [42–45], a group of robot manipulators are considered to model the networked Euler-Lagrange systems in (3.1).

We study the distributed coordinated tracking problem for six networked two-link robotic manipulators to track a desired time-varying trajectory. The classic manipulator's dynamics with unknown dynamics and disturbances are described as follows.

$$\begin{aligned}
& \begin{bmatrix} m_{1i} + 2m_{3i} \cos(q_{2i}) & m_{2i} + m_{3i} \cos(q_{2i}) \\ m_{2i} + m_{3i} \cos(q_{2i}) & m_{2i} \end{bmatrix} \begin{bmatrix} \ddot{q}_{1i} \\ \ddot{q}_{2i} \end{bmatrix} \\
& + \begin{bmatrix} -m_{3i} \sin(q_{2i}) \dot{q}_{2i} & -m_{3i} \sin(q_{2i}) (\dot{q}_{1i} + \dot{q}_{2i}) \\ m_{3i} \sin(q_{2i}) \dot{q}_{1i} & 0 \end{bmatrix} \begin{bmatrix} \dot{q}_{1i} \\ \dot{q}_{2i} \end{bmatrix} \\
& + \begin{bmatrix} g_{1i}(q_{1i}, q_{2i}) \\ g_{2i}(q_{1i}, q_{2i}) \end{bmatrix} + f_i(\dot{q}_i) + \delta_i = \tau_i, \tag{3.54}
\end{aligned}$$

where $i = 1, \dots, 6$, q_{1i} , q_{2i} denote joint angles, the uncertain dynamic parameters of each manipulator are set as $m_{1i} = i$, $m_{2i} = 0.1i$, $m_{3i} = 0.2i$, $g_{1i}(q_{1i}, q_{2i}) = 0.2i * \cos(q_{1i}) + 0.1i * \cos(q_{1i} + q_{2i})$, $g_{2i}(q_{1i}, q_{2i}) = 0.1i * \sin(q_{1i} + q_{2i})$, and the unknown dynamics and disturbances are $f_i(\dot{q}_i) = [0.1i * \dot{q}_{1i}, 0.2i * \dot{q}_{2i}]^T$ and $\delta_i = [0.1i * \sin(0.1i * t), 0.2i * \sin(0.2i * t)]^T$. The initial joint configuration and velocity are selected as $q_i(0) = [\pi/10i, -\pi/20i]^T$ rad and $\dot{q}_i(0) = [0, 0]^T$ rad/s, respectively.⁴

3.5.1 Robust consensus tracking under an undirected graph

An undirected communication graph of a team of agents is shown in Fig. 3.2. The controller gains in (3.5)-(3.8) are selected as $\alpha_{1i} = 10$, $\alpha_{2i} = 20$, $\beta_{2i} = 1$, $\beta_{1i}(0) = [0, 0]^T$, $k_{si} = 30$. Under the proposed distributed control algorithm, the state trajectories of the followers and the leader, and the tracking errors between the followers and the leader are shown in Figs. 3.3 and 3.4, respectively. Fig. 3.5 shows the trajectories of τ_i in (3.5) and the convergence of a time-varying gain β_{1i} in (3.8), respectively. It can be seen that robust consensus tracking is achieved for a group of unknown Euler-Lagrange systems under the undirected graph.

⁴For each simulation, the desired time-varying trajectory $q_d(t)$ for consensus tracking is given by $q_d(t) = [0.2 \sin(2t), 0.1 \cos(3t)]^T$ rad, which is only provided to the agents labeled by 3, 6 as indicated in the matrix $B = \text{diag}\{0, 0, 2, 0, 0, 2\}$.

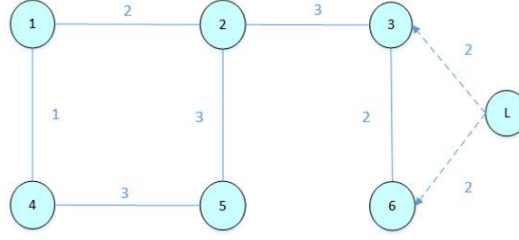


Figure 3.2: An information-exchange undirected graph. Circles denote the labeled agents and the connecting lines denote weighted information edges among all agents. The desired time-varying trajectory is denoted as a virtual leader.

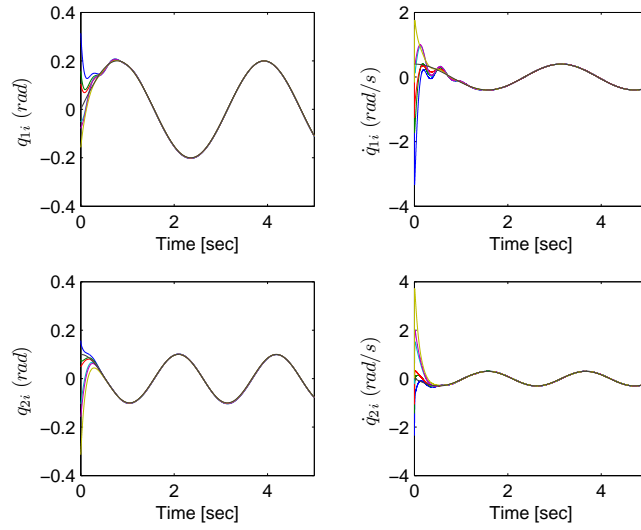


Figure 3.3: Trajectories of the states of the followers and the leader under (3.5)-(3.8).

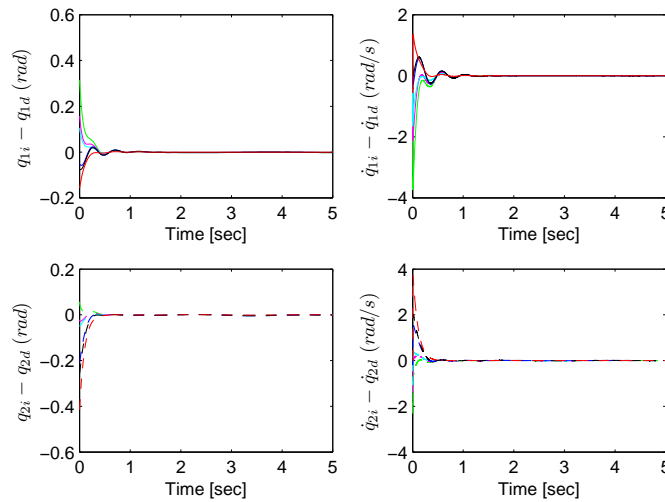


Figure 3.4: Tracking errors between the followers and the leader under (3.5)-(3.8).

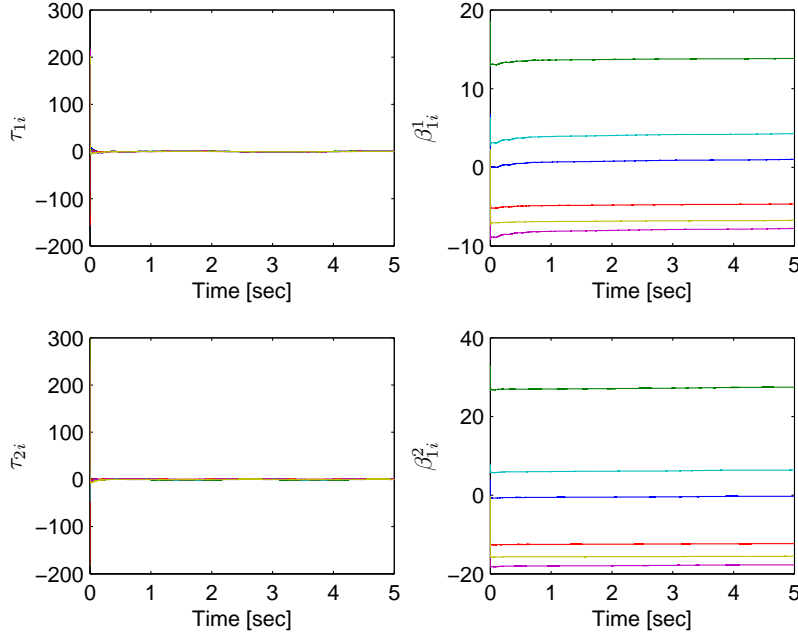


Figure 3.5: The control input τ_i in (3.5) and the convergence of β_{1i} in (3.8).

3.5.2 Robust consensus tracking under a directed graph

The directed communication graph of the team of six agents and one leader is provided in Fig. 3.6. For the desired time-varying trajectory, the expression in (3.34) holds, provided that

$$S_1 = \begin{bmatrix} -4 & 0 \\ 0 & -9 \end{bmatrix} \text{ and } S_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad (3.55)$$

which implies that Assumption 3.5 is satisfied.

According to the derived sufficient conditions in Theorem 3.2, the distributed controller gains in (3.43) with (3.37) and (3.44) are selected as $\kappa_i = 10$, $\alpha_{qi} = 5$, $\alpha_{si} = 10$, $\alpha_{\rho i} = 15$, $\alpha_{ri} = 20$, $\beta_{\rho 2i} = 1$, $k_{\rho si} = 30$. Under the developed distributed leader estimator in (3.37), the estimated state trajectories of the followers and the leader and the estimated tracking errors between the followers and the leader are shown in Figs. 3.7 and 3.8, respectively. Moreover, under the developed distributed

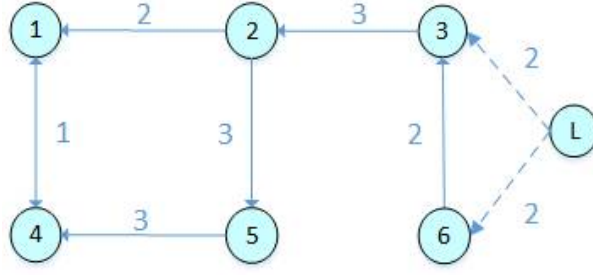


Figure 3.6: A directed graph. Circles denote the labeled agents and the connecting lines denote weighted information edges among all agents and a virtual leader.

control algorithm in (3.43), the state trajectories of the followers and the leader and the tracking errors between the followers and the leader are shown in Figs. 3.9 and 3.10, respectively. As a result, it can be seen from Figs. 3.7-3.10 that robust distributed cooperative tracking can be achieved for a group of heterogeneous unknown Euler-Lagrange systems under the directed communication graph using only relative measurement information.

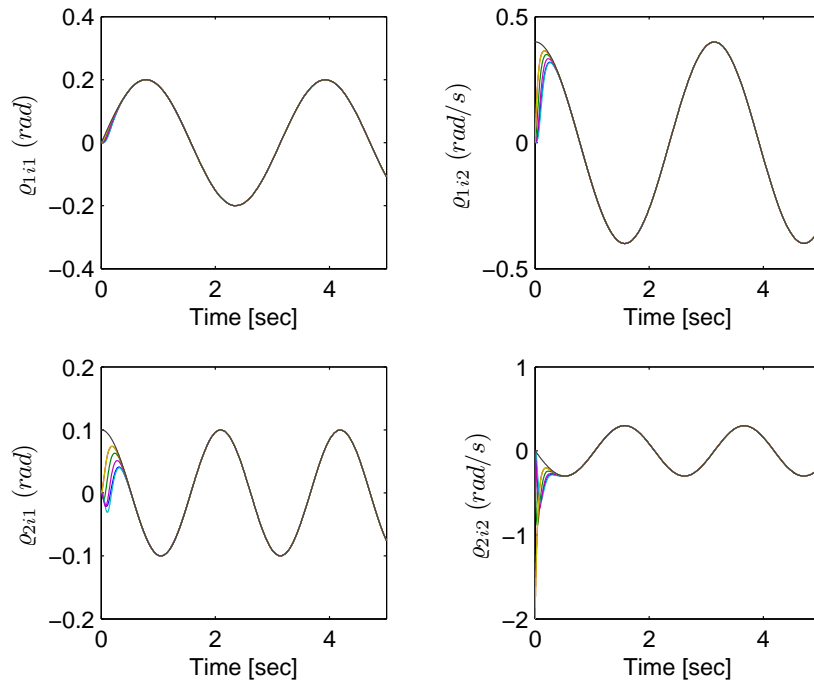


Figure 3.7: Trajectories of the estimated states of the followers and the leader under the developed distributed leader estimator (3.37).

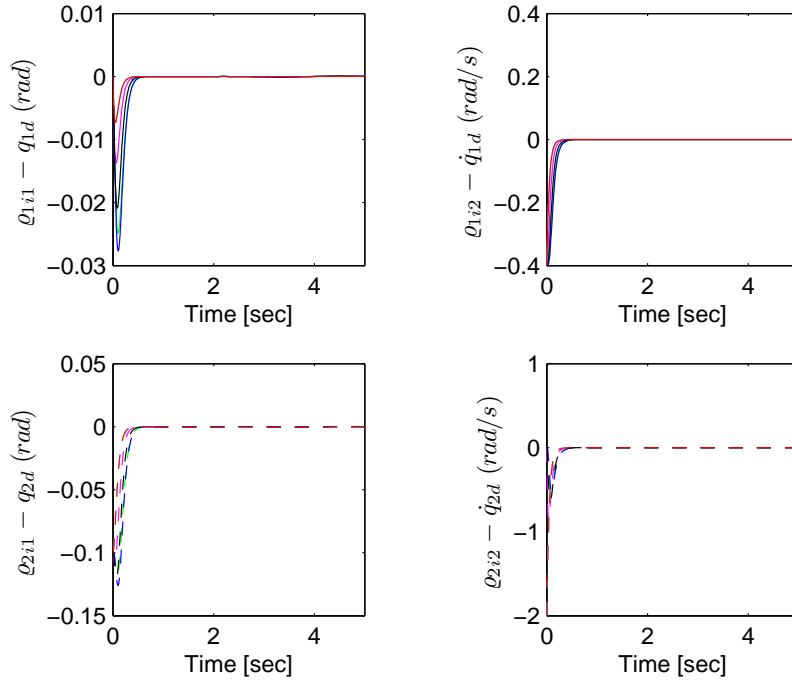


Figure 3.8: Estimated state tracking errors between the followers and the leader under the developed distributed leader estimator (3.37).

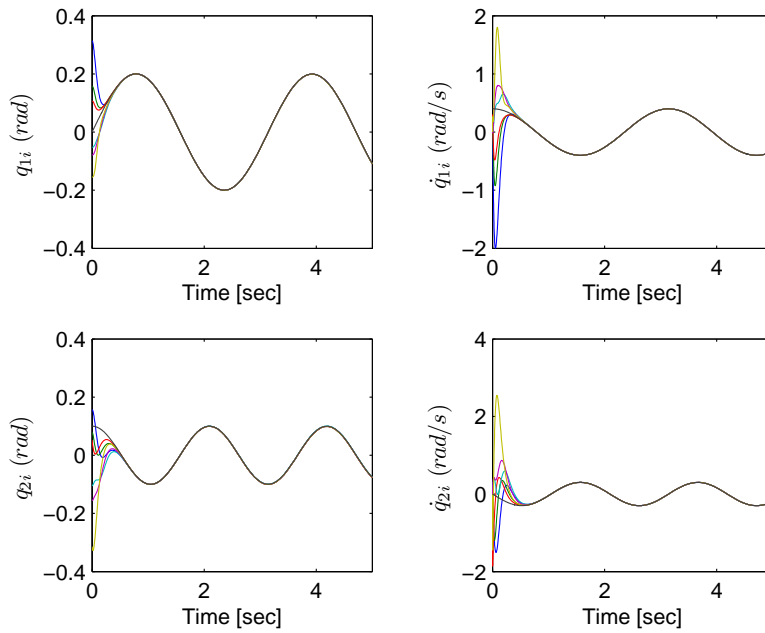


Figure 3.9: Trajectories of the states of the followers and the leader under (3.43).

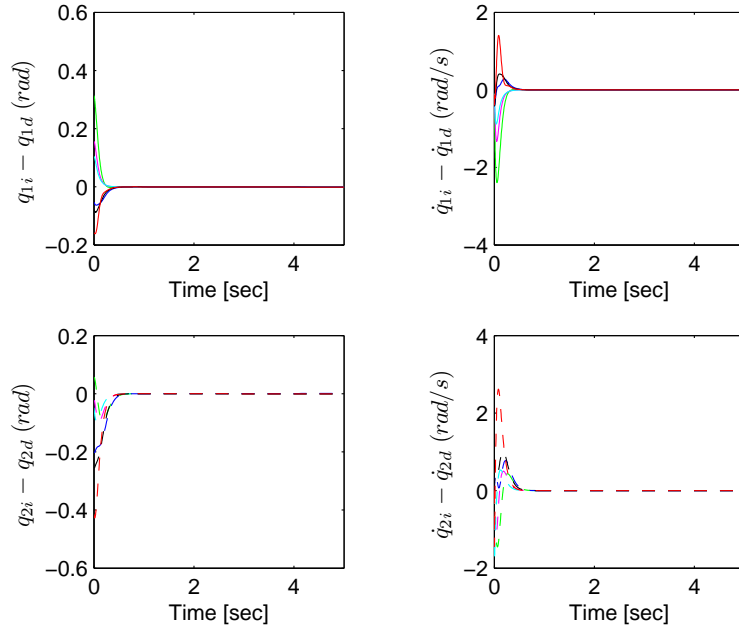


Figure 3.10: Tracking errors between the followers and the leader under (3.43).

3.6 Conclusion

In this chapter, a robust consensus tracking problem is considered for multiple unknown Euler-Lagrange systems under both undirected and directed communication graphs. The control objective is to enable all the agents to track the desired time-varying trajectory asymptotically. A distributed nonlinear identifier is firstly developed to compensate for the unknown nonlinear dynamics and disturbances. Then, a robust distributed control law combined with this identifier is developed to enable all the agents to reach robust consensus tracking asymptotically. Furthermore, in the directed case a distributed two-layer coordination scheme is developed to solve the robust consensus tracking problem. For both undirected and directed communication graphs, if the controller parameters are selected by the derived sufficient conditions, the stability of the closed-loop system is achieved via graph theory and Lyapunov analysis.

Chapter 4

Robust Connectivity Preserving Rendezvous of Multiple Mobile Robot Systems

4.1 Introduction

As stated in Chapter 1, network connectivity plays a key role in distributed cooperative control of multi-agent systems. However, many existing works (e.g., see [75–79,82] for example) study rendezvous relying on maintaining a connected network among robots, either for all time or over sequences of bounded time intervals. Since each mobile robot in practical has only limited sensing and communication capabilities. Thus, network connectivity preservation with robustness against the dynamic topology should be studied. In addition, few works consider connectivity preserving rendezvous for multi-robot systems under the unknown dynamics and disturbances. The authors in [72] studied this problem for second-order multi-agent systems with external disturbances generated by an exosystem. The exosystem is considered as a leader for all the followers. That is, the dynamics of

the leader and followers are coupled with each other. Based on a cooperative output regulation method, a distributed controller is proposed to solve this problem by using the hysteresis technique in [81,83].

In this chapter, we address a robust connectivity preservation rendezvous problem for multi-robot systems under the unknown nonlinear dynamics and disturbances. A gradient-based distributed control law is proposed to solve this problem. The designed controller not only maintains the connectivity of the multi-robot system, but also achieves robust asymptotic tracking of the leader. Compared with the existing literatures, the contributions of this chapter are summarized as follows.

1. The existing results in [22,72,73,75–87,90–93] for both leaderless and leader-following cases may not be directly applied due to the unknown nonlinear dynamics and disturbances. The proposed distributed control law is robust to the dynamic topologies, unknown nonlinear dynamics, and disturbances.
2. Although the hysteresis rule in [72,73,81,83,90] is employed, in contrast to a proportional controller used in the existing literature, a PID controller is developed in this work where additional interaction terms are introduced for achieving better rendezvous performance.
3. Sufficient conditions on the robust connectivity preservation rendezvous are derived via nonsmooth analysis and graph theory. Moreover, no upper bound information on the unknown nonlinear dynamics and disturbances is needed. The tracking errors are proven to converge to zero asymptotically.

The rest of the chapter is organized as follows. The robust connectivity preserving rendezvous problem is formulated in Section 4.2. In Section 4.3, the distributed control law design and stability analysis are developed in the main result part. A numerical example is used to verify the effectiveness of the proposed method in Section 4.4. Conclusions are given in Section 4.5.

4.2 Problem Formulation

4.2.1 Multi-Robot Model

Consider a second-order multi-robot system with a group of N non-identical mobile robots where the dynamics of the i th robot are denoted by

$$\begin{aligned}\dot{\xi}_i(t) &= v_i(t), \quad i = 1, 2, \dots, N, \\ \dot{v}_i(t) &= u_i(t) + f_i(\xi_i(t), v_i(t)) + \omega_i(t),\end{aligned}\tag{4.1}$$

where $\xi_i(t), v_i(t) \in \mathbb{R}^l$ represent the mobile robot states, $u_i(t) \in \mathbb{R}^l$ represents the control input to be designed later, $\omega_i(t) \in \mathbb{R}^l$ represents the unknown disturbances and $f(\xi_i(t), v_i(t)): \mathbb{R}^l \times \mathbb{R}^l \rightarrow \mathbb{R}^l$ denotes a continuously differentiable vector-valued function representing the intrinsic unknown nonlinear dynamics of the i th robot.

To facilitate the subsequent stability analysis of closed-loop systems, we assume that $\xi_i(t)$ and $v_i(t)$ are measurable. Moreover, we make the following assumptions.

Assumption 4.1. $f(\xi_i(t), v_i(t))$ is a continuously twice differentiable function.

Assumption 4.2. The disturbance term $\omega_i(t)$ and its first and second order time derivatives are bounded by some unknown constants (i.e., $\omega_i(t), \dot{\omega}_i(t), \ddot{\omega}_i(t) \in \mathcal{L}_\infty$).

Assumption 4.3. The desired reference trajectories $\xi_d(t), v_d(t), \dot{v}_d(t), \ddot{v}_d(t)$, and $\ddot{v}_d(t)$ are assumed to be bounded.

Remark 4.1. Assumption 4.1 given in [58,60,89] implies that $f(\xi_i(t), v_i(t))$ and its first and second order partial derivatives with respect to $\xi_i(t), v_i(t)$ are bounded, if $\xi_i(t), v_i(t)$ are bounded (i.e., $f(\xi_i(t), v_i(t)), \frac{\partial f(\xi_i(t), v_i(t))}{\partial \xi_i(t)}, \frac{\partial f(\xi_i(t), v_i(t))}{\partial v_i(t)}, \frac{\partial f(\xi_i(t), v_i(t))}{\partial \xi_i(t) \partial v_i(t)}, \frac{\partial^2 f(\xi_i(t), v_i(t))}{\partial^2 \xi_i(t)}, \frac{\partial^2 f(\xi_i(t), v_i(t))}{\partial^2 v_i(t)} \in \mathcal{L}_\infty$). Besides, Assumptions 4.2 and 4.3 are mild as shown in [54,55,58,60,88,89].

4.2.2 Connectivity Preservation Description

Consider a network of N mobile robots with integrated wireless communication capabilities and denote (i, j) a communication link between robot i and robot j . We assume that each robot has a limited communication capability and it can communicate with its neighboring robots within the limited transmission range given by a same sensing radius $R > 0$, as depicted in Fig. 4.1. Let $\mathcal{G}(t) = \{\mathcal{V}, \mathcal{E}(t)\}$ denote a new dynamic graph containing a virtual leader. It consists of a set of vertices $\mathcal{V} = \{0, 1, 2, \dots, N\}$ whose elements represent robots in the robot group and the vertex 0 is associated with the leader, and a time-varying set of edges $\mathcal{E}(t) = \{(i, j) : i, j \in 0, 1, 2, \dots, N\}$. Therefore, the time-varying communication sets for each mobile robot i corresponding to the sensing zone at each time instant can be further described as

$$\mathcal{N}_{\mathcal{G}i}(t) = \{j \neq i, \|\xi_j(t) - \xi_i(t)\| < R\}. \quad (4.2)$$

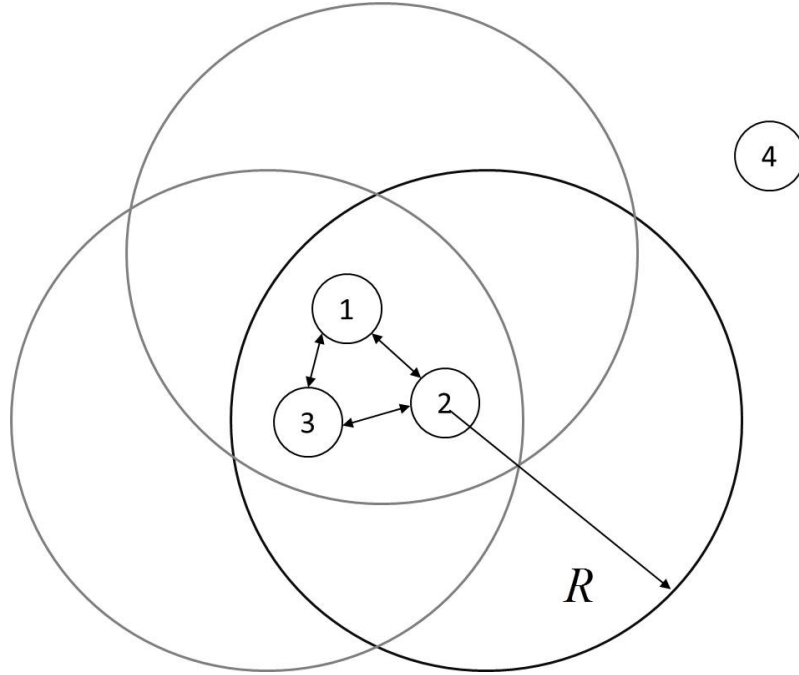


Figure 4.1: The model of mobile sensing robot networks. The robot 2 collects measurements from neighboring robots 1 and 3 in an R interactive range.

To obtain local controllers that guarantee invariance of $\mathcal{G}(t)$ with respect to connectivity, an equivalent algebraic representation of $\mathcal{G}(t) = \{\mathcal{V}, \mathcal{E}(t)\}$ is chosen as

$$L_{N+1}(t) \triangleq D_{N+1}(t) - A_{N+1}(t) \in \mathbb{R}^{(N+1) \times (N+1)},$$

where $D_{N+1}(t) \in \mathbb{R}^{(N+1) \times (N+1)}$ is a diagonal matrix with $d(t) = \sum_{j=0}^N a_{ij}(t)$, $i = 0, 1, \dots, N$, and $A_{N+1}(t) = a_{ij}(t) \in \mathbb{R}^{(N+1) \times (N+1)}$ represents the adjacency matrix of $\mathcal{G}(t)$, such that $a_{ij}(t) = 1$ if $(i, j) \in \mathcal{E}(t)$ and 0, otherwise.

Define a subgraph $\mathcal{G}_N(t) = \{\mathcal{V}_N, \mathcal{E}_N(t)\}$ of $\mathcal{G}(t)$ where $\mathcal{E}_N(t) \subseteq \mathcal{V}_N \times \mathcal{V}_N$ is obtained from $\mathcal{E}(t)$ by removing all edges from the leader to the followers in \mathcal{V}_N . Thus, $\mathcal{N}_i(t) = \{j \in \mathcal{V}_N, (v_i, v_j) \in \mathcal{E}_N(t)\}$. Clearly, $\mathcal{G}_N(t)$ is undirected and its Laplacian matrix is $L(t) \triangleq D(t) - A(t) \in \mathbb{R}^{N \times N}$. Thus, an information-exchange matrix is defined as $H(t) \triangleq L(t) + B(t) \in \mathbb{R}^{N \times N}$, where $B(t) = \text{diag}\{b_1(t), b_2(t), \dots, b_N(t)\}$ is a diagonal matrix with $b_i(t) = 1$ if the i -th robot has access to the leader and 0 otherwise.

The spectral properties of $L(t)$ is given as below.

Lemma 4.1. [81] *Let $\lambda_1(L(t)) \leq \lambda_2(L(t)) \leq \dots \leq \lambda_N(L(t))$ be all the ordered eigenvalues of $L(t)$. Then, it gets: 1). $\lambda_1(L(t)) = 0$ with the corresponding eigenvector equals to $\mathbf{1}_N$, i.e., the vector with all entries equal to 1; 2). $\lambda_2(L(t)) > 0$ if and only if $\mathcal{G}_N(t)$ is connected.*

In problem formulation, we will adopt the following revised network connectivity setting suggested in [72,73,81,83,90] to define the new edge sets for the multi-robot system (3.1), where the edge $\mathcal{E}(t)$ is denoted as follows:

- (1) Initial edges are generated by $\mathcal{E}(0) = \{(i, j) : \|\xi_j(0) - \xi_i(0)\| < R - \varepsilon, i, j = 1, 2, \dots, N\} \cup \{(0, j) : \|\xi_j(0) - \xi_0(0)\| < R - \varepsilon, j \in 1, 2, \dots, N\}$;
- (2) If $\|\xi_j(t) - \xi_i(t)\| \geq R$, then $(i, j) \notin \mathcal{E}(t)$;
- (3) $(i, 0) \notin \mathcal{E}(t)$, for $i = 0, 1, 2 \dots N$;
- (4) For $i = 0, 1, 2 \dots N$, $j = 1, 2, \dots, N$, if $(i, j) \notin \mathcal{E}(t^-)$ and $\|\xi_j(t) - \xi_i(t)\| < R - \varepsilon$, then $(i, j) \in \mathcal{E}(t)$;
- (5) For $i = 0, 1, 2 \dots N$, $j = 1, 2, \dots, N$, if $(i, j) \in \mathcal{E}(t^-)$ and $\|\xi_j(t) - \xi_i(t)\| < R$, then $(i, j) \in \mathcal{E}(t)$.

Remark 4.2. *It is clear, from the definition of the edge set, that there is a hysteresis of adding edge. That is, a new edge will not be added to the evolving graph $\mathcal{G}(t)$ until the distance between any two unconnected robots decreases to $R - \varepsilon$.*

Assumption 4.4. *Assume that the initial communication network $\mathcal{G}(t_0)$ with $t_0 = 0$ is a connected undirected multi-robot network and at least one follower robot is connected to the leader.*

Lemma 4.2. *Suppose Assumption 4.4 holds. If $\mathcal{G}(t)$, $t \neq t_0$ is a new multi-robot topology generated by adding some edge(s) into the graph $\mathcal{G}(t_0)$, then the minimal eigenvalue of the new graph $\mathcal{G}(t)$ satisfies: $\lambda_{\min}(H(t)) \geq \lambda_{\min}(H(t_0)) > 0$.*

4.2.3 Control Objective

The control objective is to design a distributed control law $u_i(t)$ such that the multi-robot system with a virtual leader $\tilde{\mathcal{V}}_0$ and agent dynamics modeled by (4.1) under $\mathcal{G}(t)$ reach robust connectivity preserving rendezvous. The robust connectivity preserving rendezvous problem is described as below.

Definition 4.1. (*Robust Connectivity Preserving Rendezvous*)

Given the multi-robot system (4.1) under a dynamic topology $\mathcal{G}(t)$ with $R > 0$, $\varepsilon \in (0, R)$ and arbitrary positive real numbers ϱ_{ξ_i} and ϱ_{v_i} , $i = 1, 2, \dots, N$, design a robust distributed control law $u_i(t)$ such that, for all the initial conditions $\xi_i(0)$, $\xi_d(0)$, $v_i(0)$ and $v_d(0)$ that make the initial graph $\mathcal{G}(0)$ connected and the initial energy finite satisfying $\|\xi_i(0) - \xi_d(0)\| \leq \varrho_{\xi_i}$ and $\|v_i(0) - v_d(0)\| \leq \varrho_{v_i}$, the closed-loop system has the following properties:

- (1). *The overall graph $\mathcal{G}(t)$ is connected for all $t \geq 0$.*
- (2). *The position and velocity states $\xi_i(t)$ and $v_i(t)$ of all the mobile robots converge to those of the desired trajectories $\xi_d(t)$ and $v_d(t)$ asymptotically in the sense that*

$$\xi_i(t) - \xi_d(t) \rightarrow \mathbf{0}_l \text{ and } v_i(t) - v_d(t) \rightarrow \mathbf{0}_l, \quad \text{as } t \rightarrow \infty, \quad (4.3)$$

for systems (4.1) under the unknown dynamics $f(\xi_i(t), v_i(t))$ and disturbances $\omega_i(t)$.

4.3 Robust Connectivity Preserving Rendezvous

In this section, we propose a distributed control law for each robot that relies only on relative information among the robots. Since not all the robots have access to the desired trajectory, the relative position and velocity tracking errors $e_{\xi_i}(t)$ and $e_{x_i}(t)$, and a sliding mode tracking variable $e_{f_i}(t) \in \mathbb{R}^l$ are defined respectively, using only local information exchanged from neighboring robots denoted by

$$e_{\xi_i} = \sum_{j=1}^N a_{ij}(t) (\xi_j - \xi_i) + b_i(t) (\xi_d - \xi_i), \quad (4.4)$$

$$e_{x_i} = \sum_{j=1}^N a_{ij}(t) (v_j - v_i) + b_i(t) (v_d - v_i), \quad (4.5)$$

$$\begin{aligned} e_{f_i} = & \sum_{j=1}^N a_{ij}(t) (\alpha_{1i}\pi_i - \alpha_{1j}\pi_j) + b_i(t)\alpha_{1i}\pi_i \\ & + \sum_{j=1}^N a_{ij}(t) (v_j - v_i) + b_i(t) (v_d - v_i), \end{aligned} \quad (4.6)$$

$$\pi_i = \sum_{j=1}^N \nabla_{e_{di}} \varphi(\|\xi_{ji}\|_\sigma) + b_i(t)e_{di}, \quad e_{di} = \xi_d - \xi_i, \quad (4.7)$$

where α_{1i} is a positive constant gain and $\nabla_{e_{di}} \varphi(\|\xi_{ji}\|_\sigma)$, $\xi_{ji} = \xi_j - \xi_i$, is a subsequently designed gradient-based term.

4.3.1 Potential Function

The function $\varphi(\|\xi_{ji}\|_\sigma)$ in (4.7) can be expressed in terms of potential functions that have been used in [72,81,83], while the difference is that the σ -norm in [75] has been employed to construct to a novel smooth collective potential. The following defines a general potential function $\varphi(\|\xi_{ji}\|_\sigma)$ which is a nonnegative function of the distance $\|\xi_{ji}\|_\sigma$ between the robot i and robot j and it is differentiable with respect to $\|\xi_{ji}\|_\sigma \in [0, R)$, such that

- (1) $\frac{\partial \varphi(\|\xi_{ji}\|_\sigma)}{\partial \|\xi_{ji}\|_\sigma} > 0$ for $\|\xi_{ji}\|_\sigma \in [0, R)$;
- (2) $\lim_{\|\xi_{ji}\|_\sigma \rightarrow 0} \left(\frac{\partial \varphi(\|\xi_{ji}\|_\sigma)}{\partial \|\xi_{ji}\|_\sigma} \cdot \frac{1}{1 + \epsilon \|\xi_{ji}\|_\sigma} \right)$ is nonnegative and bounded, where ϵ is a parameter of the σ -norm in [75];

- (3) $\varphi(\|\xi_{ji}\|_\sigma) = \tilde{Q} \in [Q_{\max}, +\infty)$ as $\|\xi_{ji}\|_\sigma \rightarrow R$, $Q_{\max} = \frac{N(N-1)}{2} \varphi(\|R - \varepsilon\|_\sigma) + V_L(0)$ where $V_L(0)$ is the initial energy of a subsequently selected Lyapunov function.

To be specific, for the defined problem, a bounded potential function can be selected as

$$\varphi(\|\xi_{ji}\|_\sigma) = \frac{\|\xi_{ji}\|_\sigma^{k_1}}{(R - \|\xi_{ji}\|_\sigma + \frac{R^{k_2}}{\tilde{Q}})^{k_3}}, \quad k_1 = k_2 k_3, \quad (4.8)$$

where $\|\xi_{ji}\|_\sigma \in [0, R)$, $\tilde{Q} > 0$ and $k_1 \geq 2$, $k_2 \geq 1$, $k_3 \geq 1$.

Remark 4.3. Under the selected local potential function (4.8), a distributed control law $u_i(t)$ can be designed to guarantee that there will be no edge loss during the evolution of the dynamic topology $\mathcal{G}(t)$, and a new edge is added to the evolving graph $\mathcal{G}(t)$ once the distance between any two unconnected robots decreases to $R - \varepsilon$. The used hysteresis rule guarantees that the local potential function (4.8) is finite when new edges are added. Moreover, the number ε in subsection 4.2.2 is used to introduce the effect of hysteresis. If the hysteresis parameter $\varepsilon = 0$, the potential function $\varphi(\|\xi_{ji}\|_\sigma)$ in (4.8) is $\tilde{Q}^{k_3} = +\infty$, which is similar to that in [81].

4.3.2 Filtered Error Design

To facilitate the subsequent stability analysis, a filtered error $r(t)$ is defined as

$$\tilde{H}(t)r(t) = \dot{E}_f(t) + \Lambda_2 E_f(t), \quad (4.9)$$

where $\tilde{H}(t) = H(t) \otimes I_l$, $\Lambda_2 \triangleq \text{diag}\{\alpha_{21}, \dots, \alpha_{2N}\} \otimes I_l \in \mathbb{R}^{Nl \times Nl}$, I_l is an $l \times l$ identity matrix and $E_f \triangleq \text{col}(e_{f1}, \dots, e_{fN}) \in \mathbb{R}^{Nl}$. Since $\tilde{H}(t)$ is positive symmetric definite according to Assumption 4.4 and Lemma 4.2, the convergence of $r(t)$ guarantees the convergence of $E_f(t)$.

4.3.3 Distributed Control Law Design

The distributed coordinated control law is designed as

$$\begin{aligned} u_i(t) &= \alpha_{1i} \dot{\pi}_i(t) + \alpha_{2i} e_{fi}(t) + \alpha_{0i} \int_0^t \pi_i(\tau) d\tau + \hat{f}_i(t), \\ \pi_i(t) &= \sum_{j \in \mathcal{N}_i(t)} \nabla_{e_{di}} \varphi(\|\xi_{ji}(t)\|_\sigma) + b_i(t) e_{di}(t), \end{aligned} \quad (4.10)$$

where α_{0i} , α_{1i} and α_{2i} are positive constant control gains, $\nabla_{e_{di}}\varphi(\|\xi_{ji}(t)\|_\sigma)$ is the gradient-based term to enforce the position of each robot i to converge to a common value, $b_i(t)e_{di}(t)$ is the navigational feedback term to enable robot i to track the desired trajectory, the velocity consensus term is given by $e_{fi}(t)$ in (3.3), and $\hat{f}_i(t)$ denotes a designed term to compensate for the unknown dynamics and disturbances.

A distributed learning law for $\hat{f}_i(t)$ can be designed as

$$\dot{\hat{f}}_i(t) = k_{si}(e_{fi}(t) - e_{fi}(0)) + \vartheta_i(t), \quad (4.11)$$

$$\dot{\vartheta}_i(t) = k_{si}\alpha_{2i}e_{fi}(t) + \theta_i(t) + b_i(t)\beta_i(t) \odot \eta_i(t), \quad (4.12)$$

$$\theta_i(t) = \sum_{j=1}^N a_{ij}(t)[\beta_i(t) \odot \eta_i(t) - \beta_j(t) \odot \eta_j(t)], \quad (4.13)$$

$$\eta_i(t) = \text{vsgn}(e_{fi}(t)), \vartheta_i(0) = \vartheta_{iO}, \quad (4.14)$$

where ϑ_{iO} is the initial condition, k_{si} is a positive control gain, the symbol \odot denotes the elementwise vector multiplication, $\text{vsgn}(e_{fi}) \triangleq \text{col}(\text{sgn}(e_{fi1}), \text{sgn}(e_{fi2}), \dots, \text{sgn}(e_{fil})) \in \mathbb{R}^l$, and $\beta_i(t) \in \mathbb{R}^l$ is a subsequently designed time-varying control gain (compensation for unknown nonlinear dynamics and disturbances) including a time-varying term $\beta_{1i}(t) \in \mathbb{R}^l$ and a positive constant part $\beta_{2i}\mathbf{1}_l \in \mathbb{R}^l$ as

$$\begin{aligned} \beta_i(t) &= \beta_{1i}(t) + \beta_{2i}\mathbf{1}_l, \beta_{1i}(0) = \mathbf{0}_l, \\ \beta_{1i}(t) &= |e_{fi}(t)| - |e_{fi}(0)| + \alpha_{2i} \int_0^t |e_{fi}(\tau)| d\tau. \end{aligned} \quad (4.15)$$

Remark 4.4. *Several distributed gradient-based algorithms using the local artificial potential functions have been developed for multi-agent systems in [22,72,73,81–87,90] to achieve rendezvous with preserved connectivity. However, these algorithms may not be able to guarantee the asymptotic convergence of the closed-loop error system in the presence of unknown dynamics and disturbances. Compared with the distributed control laws in [22,72,73,81–87,90], the proposed distributed PID controller in (4.10) with learning laws in (4.11)–(4.15) can compensate for the unknown dynamics and disturbances. Thus, this design enables robust connectivity preserving rendezvous. The tracking errors can be proven to converge to zero asymptotically.*

Let $U \triangleq \text{col}(u_1, \dots, u_N)$, $\Pi \triangleq \text{col}(\pi_1, \dots, \pi_N)$, $\hat{F} \triangleq \text{col}(\hat{f}_1, \dots, \hat{f}_N)$ denote some concatenated vectors, and $\Lambda_0 \triangleq \text{diag}\{\alpha_{01}, \dots, \alpha_{0N}\} \otimes I_l$ and $\Lambda_1 \triangleq \text{diag}\{\alpha_{11}, \dots, \alpha_{1N}\} \otimes I_l \in \mathbb{R}^{Nl}$ denote two diagonal matrices. Then, (4.10) can be expressed in a matrix form

$$U = \Lambda_1 \dot{\Pi} + \Lambda_2 E_f + \Lambda_0 \int_0^t \Pi(\tau) d\tau + \hat{F}. \quad (4.16)$$

Denote $\tilde{B}(t) \triangleq (B(t) \otimes I_l)$, $\tilde{v}_d \triangleq (\mathbf{1}_N \otimes \dot{v}_d)$, and $V \triangleq \text{col}(v_1, \dots, v_N)$, $F \triangleq \text{col}(f_1, \dots, f_N)$, $W \triangleq \text{col}(\omega_1, \dots, \omega_N) \in \mathbb{R}^{Nl}$. Substituting (4.4)-(4.7) into (4.9) yields the following closed-loop error system:

$$\begin{aligned} r &= \tilde{H}^{-1}(t)(-\tilde{H}(t)\dot{V} + \tilde{B}(t)\dot{\tilde{v}}_d + \tilde{H}(t)\Lambda_1\dot{\Pi} + \Lambda_2 E_f) \\ &= -U - F - W + \Lambda_1\dot{\Pi} + \tilde{H}^{-1}(t)(\tilde{B}(t)\dot{\tilde{v}}_d + \Lambda_2 E_f) \\ &= -F - W + \tilde{H}^{-1}(t)\tilde{B}(t)\dot{\tilde{v}}_d - \hat{F} - \Lambda_0 \int_0^t \Pi(\tau) d\tau + (\tilde{H}^{-1}(t) - I_{Nl})\Lambda_2 E_f. \end{aligned} \quad (4.17)$$

Based on the distributed learning laws in (4.11)-(4.14), the time derivative of \hat{F} can be written in the following matrix form

$$\dot{\hat{F}} = K_s(\dot{E}_f + \Lambda_2 E_f) + \tilde{H}(t)\text{sgn}(E_f)\Upsilon_1 + \tilde{H}(t)\text{sgn}(E_f)\Upsilon_2 \mathbf{1}_{Nl}, \quad (4.18)$$

$$\dot{\Upsilon}_1 = \text{sgn}(E_f)(\dot{E}_f + \Lambda_2 E_f), \quad (4.19)$$

where $\text{sgn}(E_f) \triangleq \text{diag}\{\text{dsgn}(e_{f1}), \dots, \text{dsgn}(e_{fN})\}$ with each element $\text{dsgn}(e_{fi}) \triangleq \text{diag}\{\text{sgn}(e_{fi1}), \dots, \text{sgn}(e_{fil})\}$, $K_s \triangleq \text{diag}\{k_{s1}, \dots, k_{sN}\} \otimes I_l$, $\Upsilon_2 \triangleq \text{diag}\{\beta_{21}, \dots, \beta_{2N}\} \otimes I_l$, and $\Upsilon_1 \triangleq \text{col}(\beta_{11}(t), \dots, \beta_{1N}(t)) \in \mathbb{R}^{Nl}$.

By taking the time derivative of (4.17) and rewriting it utilizing (4.9), (4.16), (4.18) and (4.19) yields the following global closed-loop error system

$$\begin{aligned} \dot{r} &= -\dot{\hat{F}} - \dot{F} - \dot{W} + \tilde{H}^{-1}(t)\tilde{B}(t)\ddot{\tilde{v}}_d - \Lambda_0 \Pi + (\tilde{H}^{-1}(t) - I_{Nl})\Lambda_2(\tilde{H}(t)r - \Lambda_2 E_f) \\ &= -K_s \tilde{H}(t)r - \Lambda_0 \Pi + \tilde{\Delta}(t) + \tilde{H}(t)(\Delta_d(t) - E_f - \text{sgn}(E_f)(\Upsilon_1 + \Upsilon_2 \mathbf{1}_{Nl})) \end{aligned} \quad (4.20)$$

where $\tilde{\Delta}(t)$ and $\Delta_d(t)$ denote the unmeasurable/uncertain auxiliary terms given by

$$\begin{aligned} \tilde{\Delta}(t) &\triangleq -\dot{F}(\Xi, V) + \dot{F}_d(\tilde{\xi}_d, \tilde{v}_d) + \tilde{H}(t)E_f + (\tilde{H}^{-1}(t) - I_{Nl})\Lambda_2(\tilde{H}(t)r - \Lambda_2 E_f), \\ \Delta_d(t) &\triangleq -\tilde{H}^{-1}(t)[\dot{F}_d(\tilde{\xi}_d, \tilde{v}_d) + \dot{W} - \tilde{H}^{-1}(t)\tilde{B}(t)\ddot{\tilde{v}}_d], \end{aligned} \quad (4.21)$$

where $\Xi \triangleq \text{col}(\xi_1, \dots, \xi_N)$, $\tilde{\xi}_d \triangleq (\mathbf{1}_N \otimes \xi_d)$ and the collective vector $\dot{F}_d(\tilde{\xi}_d, \tilde{v}_d)$ represents the time derivative of function $f(\xi_i(t), v_i(t))$ at the desired reference trajectory.

A mean value theorem in [58,59,68,89] is used to show that the upper bound of the uncertain auxiliary error term $\tilde{\Delta}(t)$ can be expressed as

$$\| \tilde{\Delta}(t) \| \leq \rho(\| z(t) \|) \| z(t) \|, \quad (4.22)$$

where $\rho(\| z(t) \|)$ is a positive, globally invertible, nondecreasing function with $z(t) \triangleq \text{col}(E_\xi(t), E_f(t), r(t)) \in \mathbb{R}^{3Nl}$, and it follows from Assumptions 4.1-4.3 that the auxiliary term $\Delta_d(t)$ and its time derivative satisfy:

$$\sup_{t \in [0, \infty)} |\Delta_{d_m}(t)| < k_{1m}, \quad \sup_{t \in [0, \infty)} \left| \dot{\Delta}_{d_m}(t) \right| < k_{2m}, \quad (4.23)$$

where $m = 1, 2, \dots, Nl$, $\Delta_{d_m}(t)$ and $\dot{\Delta}_{d_m}(t)$ denote the m^{th} element of $\Delta_d(t)$ and $\dot{\Delta}_d(t)$, respectively. Let $k_1 \triangleq \text{col}(k_{11}, k_{12}, \dots, k_{1N})$, $k_2 \triangleq \text{col}(k_{21}, k_{22}, \dots, k_{2N}) \in \mathbb{R}^{Nl}$, where $k_{1i}, k_{2i} \in \mathbb{R}^l$, $i \in \mathcal{V}_N$. Then, k_1 and k_2 can be used to denote some unknown upper bounds on the corresponding element of $\Delta_d(t)$ and $\dot{\Delta}_d(t)$, respectively.

4.3.4 Stability Analysis and Sufficient Condition

Theorem 4.1. *Suppose that Assumptions 4.1-4.4 hold. Then, the robust connectivity preserving rendezvous problem for N mobile robots with dynamics (4.1) and a virtual leader $\tilde{\mathcal{V}}_0$ is solvable by the proposed distributed control law in (4.10) with learning designs in (4.11)-(4.14). The following results hold:*

- (1). *The overall graph $\mathcal{G}(t)$ is connected for all $t \geq 0$.*
- (2). *The position and velocity states $\xi_i(t)$ and $v_i(t)$ of all the robots converge to those of the desired trajectories $\xi_d(t)$ and $v_d(t)$ asymptotically in the sense that*

$$\begin{aligned} \text{col}(\xi_1, \dots, \xi_N) - \mathbf{1}_N \otimes \xi_d(t) &\rightarrow \mathbf{0}_{Nl}, \\ \text{col}(v_1, \dots, v_N) - \mathbf{1}_N \otimes v_d(t) &\rightarrow \mathbf{0}_{Nl} \quad \text{as } t \rightarrow \infty, \end{aligned}$$

provided that α_{2i} and k_{si} are two positive constants¹, and the control gains α_{0i} , α_{1i} , β_{2i} in (4.10)-(4.14) are selected according to the following sufficient conditions:

$$\alpha_{0i} > 0, \quad 2\alpha_{1i} > \alpha_{0i}^2 + 1, \quad \beta_{2i} > 0, \quad \beta_{1i}(0) = \mathbf{0}_l. \quad (4.24)$$

Proof. Let $y(t) \in \mathbb{R}^{3Nl+3}$ be defined as $y(t) \triangleq \text{col}(E_f(t), r(t), \tilde{\Upsilon}_1(t), \sqrt{\mathcal{P}(t)}, \sqrt{\Phi(t)}, \sqrt{\Psi(t)})$, where the auxiliary functions $\mathcal{P}(t)$ is defined as

$$\mathcal{P}(t) = E_f^T(0)\hat{\Upsilon}_1 \text{sgn}(E_f(0))\mathbf{1}_{Nl} - E_f^T(0)\Delta_d(0) - S(t), \quad (4.25)$$

where $\hat{\Upsilon}_1 \triangleq \text{diag}\{\hat{\beta}_{11}, \dots, \hat{\beta}_{1N}\} \otimes I_l \in \mathbb{R}^{Nl \times Nl}$ is a subsequently designed matrix introduced in (4.26) and the function $S(t)$ is the Filippov generalized solution to:

$$\dot{S}(t) = r^T(t)\tilde{H}(t)(\Delta_d(t) - \hat{\Upsilon}_1 \text{sgn}(E_f(t))\mathbf{1}_{Nl}), S(0) = 0,$$

where $\hat{\beta}_{1i}$ in $\hat{\Upsilon}_1$ satisfies: $\hat{\beta}_{1i} > \|k_{1i}\|_\infty + \frac{1}{\alpha_{2i}} \|k_{2i}\|_\infty$ such that $\mathcal{P}(t) \geq 0$.

Similarly, another auxiliary function $\Phi(t)$ is the Filippov generalized solution to: $\dot{\Phi}(t) = \dot{E}_f^T(t)\Upsilon_2 \text{sgn}(E_f(t))\mathbf{1}_{Nl}$ and $\Phi(0) = E_f^T(0)\Upsilon_2 \text{sgn}(E_f(0))\mathbf{1}_{Nl}$.

Moreover, $\Psi(t)$ is an energy function for (4.1) defined as

$$\Psi(t) = \frac{1}{2} \sum_{i=1}^N \left(\sum_{j \in \mathcal{N}_i(t)} \varphi(\|\xi_{ji}\|_\sigma) + b_i(t)e_{di}^T e_{di} \right), \quad (4.26)$$

where $e_{di} = \xi_d - \xi_i$ and $\varphi(\|\xi_{ji}\|_\sigma)$ is a potential function.

Therefore, an energy-based Lyapunov function candidate $V_L(y(t), t)$ is chosen as

$$\begin{aligned} V_L(y(t), t) &= \Psi(t) + \frac{1}{2} E_f^T(t) E_f(t) + \frac{1}{2} r^T(t) r(t) \\ &\quad + \frac{1}{2} \tilde{\Upsilon}_1^T(t) \tilde{\Upsilon}_1(t) + \mathcal{P}(t) + \Phi(t), \end{aligned} \quad (4.27)$$

where $\tilde{\Upsilon}_1(t) = \Upsilon_1(t) - \hat{\Upsilon}_1 \mathbf{1}_{Nl}$ and the vector $\hat{\Upsilon}_1 \mathbf{1}_{Nl}$ is an estimate of $\Upsilon_1(t)$.

The main steps of this proof are as follows.

¹The parameters α_{2i} and k_{si} are related to communication topology information as shown in (4.24), and thus can be selected sufficiently large to yield a semi-global tracking result.

Step I. Since the topology $\mathcal{G}(t)$ is fixed on each time interval $[t_k, t_{k+1})$, $k \in \mathbb{N}$, this part will show the stability of the closed-loop multi-robot error system (4.20) for $t \in [t_k, t_{k+1})$.

Under Filippov's framework, the time derivative of $V_L(y, t)$ exists almost everywhere (a.e.), i.e., for almost all $t \in [0, \infty)$ and $\dot{V}_L \stackrel{a.e.}{\in} \tilde{V}_L$ where

$$\tilde{V}_L \triangleq \bigcap_{\xi \in \partial V_L(y, t)} \xi^T \mathbb{K}[\dot{E}_f^T, \dot{r}^T, \dot{\Upsilon}_1^T, \frac{1}{2} \mathcal{P}^{-\frac{1}{2}} \dot{\mathcal{P}}, \frac{1}{2} \Phi^{-\frac{1}{2}} \dot{\Phi}, \frac{1}{2} \Psi^{-\frac{1}{2}} \dot{\Psi}]^T, \quad (4.28)$$

where ∂V_L is the generalized gradient of $V_L(y, t)$. Since V_L is continuously differentiable in y , it has

$$\tilde{V}_L \subset \nabla V_L^T \mathbb{K}[\dot{E}_f^T, \dot{r}^T, \dot{\Upsilon}_1^T, \frac{1}{2} \mathcal{P}^{-\frac{1}{2}} \dot{\mathcal{P}}, \frac{1}{2} \Phi^{-\frac{1}{2}} \dot{\Phi}, \frac{1}{2} \Psi^{-\frac{1}{2}} \dot{\Psi}]^T, \quad (4.29)$$

where $\nabla V_L \triangleq \text{col}(E_f, r, \tilde{\Upsilon}_1, 2\mathcal{P}^{\frac{1}{2}}, 2\Phi^{\frac{1}{2}}, 2\Psi^{\frac{1}{2}})$.

After using (4.9), (4.20) and (4.25)-(4.27), the expression in (4.29) is rewritten as

$$\begin{aligned} \tilde{V}_L \subset & r^T \{-K_s \tilde{H}(t)r - \Lambda_0 \Pi + \tilde{\Delta}(t) + \tilde{H}(t) \Delta_d(t) - \tilde{H}(t) \mathbb{K}[\text{sgn}(E_f)](\Upsilon_1 + \Upsilon_2 \mathbf{1}_{Nl}) \\ & - \tilde{H}(t) E_f\} + E_f^T \dot{E}_f + (\tilde{H}(t)r - \Lambda_2 E_f)^T \Upsilon_2 \mathbb{K}[\text{sgn}(E_f)] \mathbf{1}_{Nl} + \dot{\Psi}(t) \\ & + (\Upsilon_1 - \hat{\Upsilon}_1 \mathbf{1}_{Nl})^T \mathbb{K}[\text{sgn}(E_f)] \tilde{H}(t)r - r^T \tilde{H}(t) (\Delta_d(t) \\ & - \hat{\Upsilon}_1 \mathbb{K}[\text{sgn}(E_f)] \mathbf{1}_{Nl}), \end{aligned} \quad (4.30)$$

where $\mathbb{K}[\text{sgn}(E_f)] = \text{SGN}(E_f)$ such that $\text{SGN}(E_{fik}) = 1$ if $E_{fik} > 0$, $[-1, 1]$ if $E_{fik} = 0$, and -1 if $E_{fik} < 0$, $i = 1, 2, \dots, N$, $k = 1, 2, \dots, l$ [65].

Hence, by substituting (4.26) and canceling the corresponding common terms, the expression in (4.30) can be written as

$$\begin{aligned} \tilde{V}_L \subset & r^T \tilde{\Delta}(t) - r^T K_s \tilde{H}(t)r - r^T \Lambda_0 \Pi - E_f^T \Lambda_2 E_f + \Pi^T \tilde{H}^{-1}(t) \\ & \times (E_f - \tilde{H}(t) \Lambda_1 \Pi) - E_f^T \Lambda_2 \Upsilon_2 \mathbb{K}[\text{sgn}(E_f)] \mathbf{1}_{Nl}, \end{aligned} \quad (4.31)$$

where $\dot{E}_f = \tilde{H}(t)r - \Lambda_2 E_f$ and $\tilde{H}(t)\dot{E}_d = \dot{E}_\xi = E_f - \tilde{H}(t)\Lambda_1\Pi$ are used via the error definition in (4.4)-(4.7).

Then the expression in (4.30) can be upper bounded as

$$\begin{aligned} \dot{V}_L \stackrel{a.e.}{\leq} & \|r\| \rho(\|z(t)\|) \|z(t)\| - \lambda_{\min}(\Theta) \|r\|^2 - \lambda_{\min}(\Lambda_2) \|E_f\|^2 \\ & - \lambda_{\min}(\Lambda_1) \|\Pi\|^2 + \|r\| \|\Lambda_0\| \|\Pi\| + \|\Pi\| \left\| \tilde{H}^{-1}(t) \right\| \|E_f\|, \end{aligned} \quad (4.32)$$

where $\Theta = \frac{1}{2}(K_s \tilde{H}(t) + \tilde{H}(t) K_s)$ and the set in (4.30) is reduced to the scalar inequality in (4.32) since the RHS is continuous a.e., i.e., the RHS is continuous except for the Lebesgue negligible set of times when $r^T \tilde{H}(t) \mathbb{k}[\text{sgn}(E_f)](\Upsilon_1 + \Upsilon_2 \mathbf{1}_{Nl}) - r^T \tilde{H}(t) \mathbb{k}[\text{sgn}(E_f)](\Upsilon_1 + \Upsilon_2 \mathbf{1}_{Nl}) \neq \{0\}$ and $r^T \tilde{H}(t) \tilde{\Upsilon}_1 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl} - r^T \tilde{H}(t) \tilde{\Upsilon}_1 \mathbb{k}[\text{sgn}(E_f)] \mathbf{1}_{Nl} \neq \{0\}$ [65].

Young's Inequality is used to show that

$$\begin{aligned} \|r^T \Lambda_0 \Pi\| & \leq \frac{1}{2} \|r\|^2 + \frac{\lambda_{\max}^2(\Lambda_0)}{2} \|\Pi\|^2, \\ \|\Pi^T \tilde{H}^{-1}(t) E_f\| & \leq \frac{1}{2} \|\Pi\|^2 + \frac{\lambda_{\max}^2(\tilde{H}^{-1}(t))}{2} \|E_f\|^2, \end{aligned} \quad (4.33)$$

which yields that the upper bound of (4.32) is expressed as

$$\begin{aligned} \dot{V}_L \stackrel{a.e.}{\leq} & -\frac{1}{2}[2\lambda_{\min}(\Lambda_1) - (\lambda_{\max}^2(\Lambda_0) + 1)] \|\Pi\|^2 - \frac{1}{2}[2\lambda_{\min}(\Lambda_2) \\ & - \lambda_{\max}^2(\tilde{H}^{-1}(t))] \|E_f\|^2 - \frac{1}{2}\lambda_{\min}(\Theta) \|r\|^2 + \rho(\|z(t)\|) \|z(t)\| \|r\| \\ & - \frac{1}{2}(\lambda_{\min}(\Theta) - 1) \|r\|^2 \\ \stackrel{a.e.}{\leq} & -\left(\delta_a - \frac{\rho^2(\|z(t)\|)}{2\lambda_{\min}(K_s \tilde{H}(t))} \right) \|z(t)\|^2, \end{aligned} \quad (4.34)$$

where $\delta_a \triangleq \min \frac{1}{2} \{ [2\lambda_{\min}(\Lambda_1) - (\lambda_{\max}^2(\Lambda_0) + 1)] \lambda_{\min}(\mathcal{M}^2(t)), 2\lambda_{\min}(\Lambda_2) - \lambda_{\max}^2(\tilde{H}^{-1}(t)), \lambda_{\min}(\Theta) - 1 \}$ with $\mathcal{M}(t)$ being a subsequently given matrix in (4.39). By selecting α_{0i} , α_{1i} , α_{2i} and k_{si} according to (4.24) and using the fact that $H(t)$ is of full rank, δ_a is positive.

Let $U(y) = \left(\delta_a - \frac{\rho^2(\|z(t)\|)}{2\lambda_{\min}(\Theta)} \right) \|z(t)\|^2 = \mu \|z(t)\|^2$ be a continuous positive semi-definite function defined on the domain:

$$\mathcal{D} \triangleq \left\{ y / \|y\| < \rho^{-1} \left(\sqrt{2\delta_a \lambda_{\min}(\Theta)} \right) \right\}. \quad (4.35)$$

Provided that the conditions in Theorem 4.1 are satisfied, the expression in (4.34) can be upper bounded as

$$\dot{V}_L \stackrel{a.e.}{\leq} -U(y) = -\mu \|z(t)\|^2, \quad (4.36)$$

for all $y \in \mathcal{D}$ and a positive constant $u \in \mathbb{R}$. The size of this domain \mathcal{D} can be increased by increasing k_{si} . Based on (4.27) and (4.36), Lemma 2.5 in chapter 2 can be used to show that $V_L \in \mathcal{L}_\infty$ in \mathcal{D} .

Next, we will show that the overall dynamic graph $\mathcal{G}(t)$ for all $t \geq 0$ is connected.

It follows from Step I that $\mathcal{G}(t)$ switches at time t_k and it is a fixed graph on each time interval $t \in [t_k, t_{k+1})$. Let the energy function $V_L(0)$ be given by (4.27). Thus, for all initial conditions $\xi_i(0)$, $\xi_d(0)$, $v_i(0)$, and $v_d(0)$, $V_L(0)$ is finite. According to the conditions in (4.24), the time derivative of $V_L(t)$ on $t \in [0, t_1)$ satisfies $\dot{V}_L < 0$ by selecting the parameters α_{0i} , α_{1i} , α_{2i} and β_{2i} appropriately. Furthermore, since $\mathcal{G}(0)$ is connected, it implies that

$$V_L(t) \leq V_L(0) < Q_{\max}, \quad \forall t \in [0, t_1).$$

By the definition of the selected local potential function (4.8), we can obtain that $\lim_{\|\xi_{ji}\|_\sigma \rightarrow R} \varphi(\|\xi_{ji}\|_\sigma) = Q^{k_3} > Q_{\max} > V_L(0)$. Thus, no edge-distances will tend to R for $t \in [0, t_1)$, which implies that no existing edges will be lost at time t_1 . Hence, new edges must be added in the interaction network at the time t_1 . Without loss of generality, assume that there are l_1 new links being added to the network graph at time t_1 . Clearly, $0 < l_1 < l_{\max} = \frac{(N-1)(N-2)}{2}$. Thus, it follows from (4.27) that it gives $V_L(t_1) = V_L(0) + l_1 \varphi(\|R - \varepsilon\|_\sigma) \leq Q_{\max}$. Thus, $\mathcal{G}(t_1) \supset \mathcal{G}(0)$.

Similarly, based on Lemma 4.2 and (4.24), it is thus obtained that

$$\begin{aligned}\mathcal{G}(t) &= \mathcal{G}(0), \quad t \in [0, t_1), \\ \mathcal{G}(t) &= \mathcal{G}(t_i) \supset \mathcal{G}(t_{i-1}), \quad t \in [t_{i-1}, t_i), \quad i = 1, \dots, k-1, \\ \mathcal{G}(t) &= \mathcal{G}(t_k) \supset \mathcal{G}(t_{k-1}), \quad t \in [t_k, \infty).\end{aligned}$$

Thus, no edges will be lost at time t_k and $V_L(t_k) \leq V_L(0) + (l_1 + l_2 + \dots + l_k)\varphi(\|R - \varepsilon\|_\sigma) \leq Q_{\max}$. Since $\mathcal{G}(0)$ is connected and no edges in $\mathcal{E}(0)$ have been lost, the graph $\mathcal{G}(t)$ will remain connected for all $t \geq 0$.

Step II. We will prove that $\xi_i(t) - \xi_d(t) \rightarrow \mathbf{0}_l$ and $v_i(t) - v_d(t) \rightarrow \mathbf{0}_l$, as $t \rightarrow \infty$.

According to the analysis in Step I, Lemma 2.5 and Barbalat's Lemma, it can be concluded that for all $t \geq 0$, $\Pi(t) \rightarrow \mathbf{0}_{Nl}$, $E_x(t) \rightarrow \mathbf{0}_{Nl}$, $E_f(t) \rightarrow \mathbf{0}_{Nl}$ and $r(t) \rightarrow \mathbf{0}_{Nl}$, as $t \rightarrow \infty$. Let $\tilde{L}(t) = L(t) \otimes I_l$. Based on the error definition in (4.4) and $E_x(t) = \mathbf{0}_{Nl}$, $-\tilde{L}(t)V - \tilde{B}(t)V = -\tilde{B}(t)\tilde{v}_d$ holds. Thus, it follows from $L(t)1_N = \mathbf{0}_N$ by Lemma 4.1 that

$$-\tilde{L}(t)V - \tilde{B}(t)V = -(L(t) \otimes I_l)(I_N \otimes v_d) - \tilde{B}(t)\tilde{v}_d = -\tilde{H}(t)\tilde{v}_d. \quad (4.37)$$

By Lemma 4.2, $H(t)$ is of full rank. Multiplying $\tilde{H}^{-1}(t)$ on both sides of (4.37) gives $V = \tilde{v}_d$ with $\tilde{v}_d = \mathbf{1}_N \otimes v_d(t)$, which implies that $v_i(t) - v_d(t) \rightarrow \mathbf{0}_l$, as $t \rightarrow \infty$.

Since $\Pi(t) = \mathbf{0}_{Nl}$, it can be obtained from (4.7) that

$$\begin{aligned}\pi_i(t) &= \sum_{j \in \mathcal{N}_i(t)} \nabla_{e_{di}} \varphi(\|\xi_{ji}(t)\|_\sigma) + b_i(t)e_{di}(t) \\ &= \sum_{j \in \mathcal{N}_i(t)} \frac{\partial \varphi(\|\xi_{ji}(t)\|_\sigma)}{\partial \|\xi_{ji}(t)\|_\sigma} \frac{1}{1 + \epsilon \|\xi_{ji}\|_\sigma} \xi_{ji}(t) + b_i(t)(\xi_d(t) - \xi_i(t)).\end{aligned} \quad (4.38)$$

Rewrite (4.38) in a matrix form:

$$\Pi = [\hat{L}(t) \otimes I_l + B(t) \otimes I_l]E_d = M(t)\tilde{H}^{-1}(t)E_\xi = \mathcal{M}(t)E_\xi = \mathbf{0}_{Nl}, \quad (4.39)$$

where $E_d \triangleq \text{col}(e_{d1}, \dots, e_{dN})$, $E_\xi \triangleq \text{col}(e_{\xi 1}, \dots, e_{\xi N})$, $e_{di} = \xi_d(t) - \xi_i(t)$, $\mathcal{M}(t) =$

$M(t)\tilde{H}^{-1}(t)$, $M(t) = \hat{L}(t) \otimes I_l + B(t) \otimes I_l$ and $\hat{L}(t) = [\hat{l}_{ij}]$ is a matrix with

$$\begin{aligned}\hat{l}_{ij} &= \frac{\partial \varphi(\|\xi_{ji}(t)\|_\sigma)}{\partial \|\xi_{ji}(t)\|_\sigma} \frac{1}{1 + \epsilon \|\xi_{ji}\|_\sigma}, \text{ if } i \neq j, \\ \hat{l}_{ii} &= -\sum_{j=1, j \neq i}^N \hat{l}_{ij}.\end{aligned}\tag{4.40}$$

By the definition of potential function in 4.8, it is obtained that $\frac{\partial \varphi(\|\xi_{ji}(t)\|_\sigma)}{\partial \|\xi_{ji}(t)\|_\sigma} \frac{1}{1 + \epsilon \|\xi_{ji}\|_\sigma}$ is positive for $\|\xi_{ji}(t)\|_\sigma \in [0, R)$ and $\lim_{\|\xi_{ji}(t)\|_\sigma \rightarrow 0} \frac{\partial \varphi(\|\xi_{ji}(t)\|_\sigma)}{\partial \|\xi_{ji}(t)\|_\sigma} \frac{1}{1 + \epsilon \|\xi_{ji}\|_\sigma}$ is nonnegative and bounded. Thus, it is not difficult to obtain that $M(t)$ in (4.39) is a positive-definite matrix and thus is nonsingular. Hence, it follows from (4.39) that $E_d = \mathbf{0}_{Nl}$, which implies that $\Xi = \tilde{\xi}_d$ with $\tilde{\xi}_d = \mathbf{1}_N \otimes \xi_d(t)$.

Thus, under the proposed distributed controller in (4.10) with learning designs in (4.11)-(4.14), the robust connectivity preserving rendezvous for N mobile robots with dynamics given in (4.1) can be achieved in the sense that $\text{col}(\xi_1, \dots, \xi_N) - \mathbf{1}_N \otimes \xi_d(t) \rightarrow \mathbf{0}_{Nl}$ and $\text{col}(v_1, \dots, v_N) - \mathbf{1}_N \otimes v_d(t) \rightarrow \mathbf{0}_{Nl}$, as $t \rightarrow \infty$. \square

Remark 4.5. Compared with the existing results in [58–60, 62, 72, 73, 89–93, 95, 96], this work possesses the following attributes. First, the works in [59, 62, 72, 73, 83, 90–93, 95, 96] for both leaderless and leader-following coordinations may not be directly applied due to unknown nonlinear dynamics and disturbances. Although an identifier-based scheme is developed in [58, 60, 89] to reach robust consensus tracking, the designs do not consider connectivity preservation. The robust connectivity preserving rendezvous problem in this paper is nontrivial. Second, the leader's information is available to only a portion of the follower robots in contrast to that in [83] where the leader's information (e.g., acceleration) is assumed to be available to all the followers. Third, although the hysteresis rule in [72, 73, 81, 83, 90] is employed, different from the used proportional controller, a distributed PID controller is developed in this paper where additional interaction terms are introduced. Fourth, different from the results in [58, 72, 73, 83], we remove the existing assumption that the upper bounds of both the disturbances and the leader's states are known constants.

4.4 Numerical Example

In this section, a numerical simulation example is presented to illustrate the effectiveness of our theoretical results. Consider a team of N mobile robots, the position of robot i is denoted as

$$\xi_i(t) = [x_i(t), y_i(t)]^T, i = 1, 2, \dots, N. \quad (4.41)$$

The velocity for each robot is thus described as

$$v_i(t) = \dot{\xi}_i(t), i = 1, 2, \dots, N. \quad (4.42)$$

Considering a group of 6 non-identical robots and taking into account the uncertainties yield the following second-order multi-robot system given by

$$\begin{aligned} \dot{\xi}_i(t) &= v_i(t), \quad i = 1, 2, 3 \dots 6, \\ \dot{v}_i(t) &= u_i(t) + f_i(\xi_i(t), v_i(t)) + \omega_i(t), \end{aligned} \quad (4.43)$$

where $f_i(\xi_i(t), v_i(t))$ and $\omega_i(t)$ are given by

$$\begin{aligned} f_i(t) &= 0.1 * \cos(\xi_i(t)) + 0.2 * \sin(v_i(t)), \\ \omega_i(t) &= [0.1i * \sin(0.1i * t), 0.2i * \sin(0.2i * t)]^T. \end{aligned} \quad (4.44)$$

The leader (labeled as 0) with second-order nonlinear dynamics is described as

$$\begin{aligned} \dot{\xi}_d(t) &= v_d(t), \quad \xi_d(0) = [1, 4.5]^T, \\ \dot{v}_d(t) &= f_d(\xi_d(t), v_d(t)), \quad v_d(0) = [0.5, 1]^T, \end{aligned} \quad (4.45)$$

where $\xi_d(t)$ and $v_d(t)$ are the position and velocity states of the desired reference trajectory, respectively, and $f_d(\xi_d(t), v_d(t))$ denotes the intrinsic unknown nonlinear dynamics given by $f_d(\xi_d(t), v_d(t)) = 2 * \sin(v_d(t))$.

Simulations are performed for the proposed algorithm in (4.10) with distributed learning laws in (4.11)-(4.14) on one leader and six follower robots moving in \mathbb{R}^2

with dynamics in (4.43)-(4.45). The initial condition for simulations is selected as

$$\begin{aligned}\Xi(0) &= [-1.5, -1.5, 3.5, -0.5, 8.5, -1.5, 1.5, -6.5, 3, -6, 10.5, -6]^T, \\ V(0) &= [-1, -1.5, -2, -2.5, 0, 1, 1, 1.5, 2, 3, 3, 2.5]^T.\end{aligned}\quad (4.46)$$

The initial topology is connected by setting the edges as $\mathcal{E}(0) = \{(0, 2), (1, 2), (1, 4), (2, 3), (2, 5), (3, 6), (4, 5)\}$. The sensing radius R is given by $R = 6$ and the parameter ε is chosen as $\varepsilon = 0.5$. Choose the positive constants $\varrho_{\xi i} = 10$ and $\varrho_{v i} = 15$, $i = 1, \dots, 6$. Then, the designed potential function in (4.8) can be expressed as

$$\varphi(\|\xi_{ji}\|_\sigma) = \frac{\|\xi_{ji}\|_\sigma^2}{(6 - \|\xi_{ji}\|_\sigma + \frac{36}{Q})}, \quad \tilde{Q} = 10000, \quad (4.47)$$

where the σ -norm of the distance $\|\xi_{ji}\|$ is defined as $\|\xi_{ji}\|_\sigma = \frac{1}{\epsilon}[\sqrt{1 + \epsilon \|\xi_{ji}\|^2} - 1]$ and its gradient is $\frac{\partial \|\xi_{ji}\|_\sigma}{\partial \xi_i} = \frac{\xi_j - \xi_i}{\sqrt{1 + \epsilon \|\xi_{ji}\|^2}} = \frac{\xi_j - \xi_i}{1 + \epsilon \|\xi_{ji}\|_\sigma}$.

Chose $\epsilon = 0.5$. It thus obtains that the gradient of potential function $\varphi(\|\xi_{ji}\|_\sigma)$ is

$$\begin{aligned}\nabla_{e_{di}} \varphi(\|\xi_{ji}\|_\sigma) &= \frac{\partial \varphi(\|\xi_{ji}\|_\sigma)}{\partial \|\xi_{ji}\|_\sigma} \frac{\partial \|\xi_{ji}\|_\sigma}{\partial \xi_i} \\ &= \frac{\|\xi_{ji}\|_\sigma (2R - \|\xi_{ji}\|_\sigma + \frac{2R^2}{Q})}{(R - \|\xi_{ji}\|_\sigma + \frac{R^2}{Q})^2 (1 + \epsilon \|\xi_{ji}\|_\sigma)} (\xi_j - \xi_i) \\ &= \frac{\|\xi_{ji}\|_\sigma (12 - \|\xi_{ji}\|_\sigma + \frac{64}{10000})}{(6 - \|\xi_{ji}\|_\sigma + \frac{36}{10000})^2 (1 + 0.5 \|\xi_{ji}\|_\sigma)} (\xi_j - \xi_i),\end{aligned}\quad (4.48)$$

where the σ -norm of $\|\xi_{ji}\|$ is given by $\|\xi_{ji}\|_\sigma = 2(\sqrt{1 + 0.5 \|\xi_j - \xi_i\|^2} - 1)$.

By the conditions in (4.24) of Theorem 4.1, the distributed controller in (4.10) with distributed learning laws in (4.11)-(4.14) are selected as

$$\alpha_{0i} = 1, \quad \alpha_{1i} = 10, \quad \alpha_{2i} = 10, \quad k_{si} = 15, \quad \beta_{2i} = 2. \quad (4.49)$$

The simulation results are shown in Figs. 4.2-4.8. Fig. 4.2 shows the distances among the robots. It can be seen that, for all $t \geq 0$, these distances are smaller than the sensing range $R = 6$. That is to say, the connectivity of the network is maintained for $t \geq 0$. Under the proposed distributed controller and learning laws in (4.10)-(4.14), Figs. 4.3 and 4.4 show that both the position and velocity of

all the followers can asymptotically track the position and velocity of the leader, respectively. Fig. 4.5 shows the rendezvous for one leader and six follower robots. The plot of the potential function $\varphi(\|\xi_{ji}\|_\sigma)$ is given in Fig. 4.6 and Figs. 4.7 and 4.8 show the trajectories of u_i in (4.10) and the convergence of β_{1i} in (4.15), respectively.

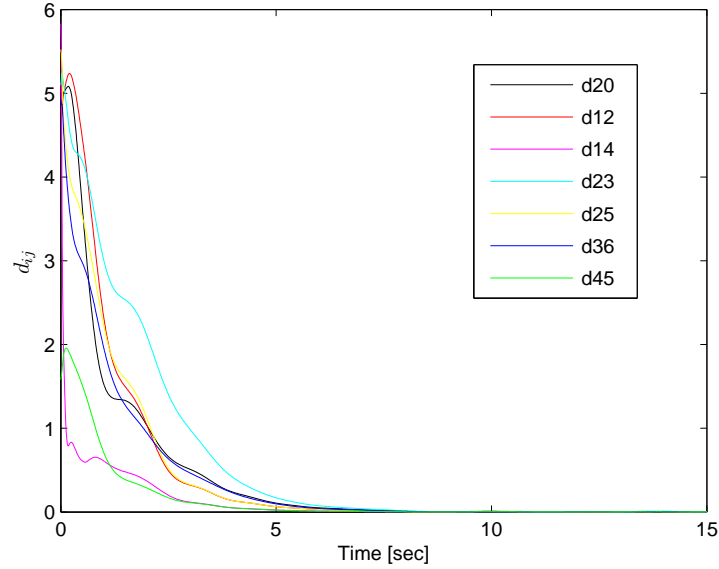


Figure 4.2: Distances among initially connected robots.

4.5 Conclusion

In this chapter, we studied a robust connectivity preserving rendezvous problem for leader-following multi-robot systems subject to unknown nonlinear dynamics and disturbances. Only a small group of mobile robots are informed to have access to the leader's information. The developed distributed PID control controller is robust to the dynamic topologies, unknown nonlinear dynamics, and disturbances. This robust distributed control law not only maintains the connectivity of the multi-robot system, but also achieves robust asymptotic tracking of the leader. Based on algebraic graph theory, Laypunov method and nonsmooth analysis, sufficient conditions on robust asymptotic convergence of closed-loop error systems are derived.

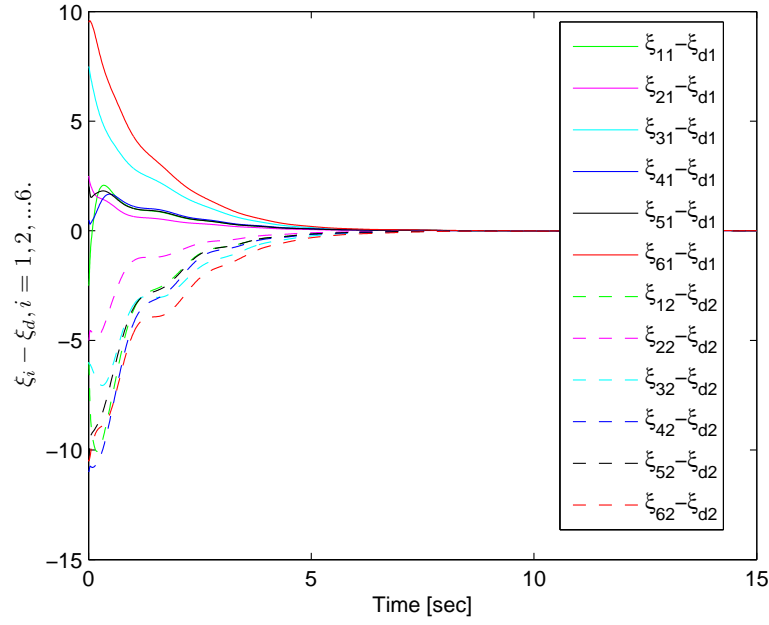


Figure 4.3: Position differences between the followers and the leader.

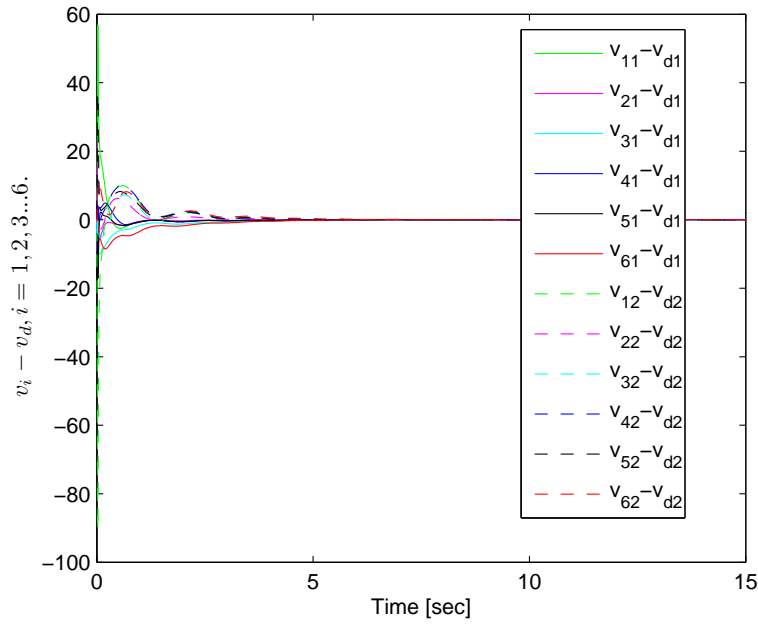


Figure 4.4: Velocity differences between the followers and the leader.

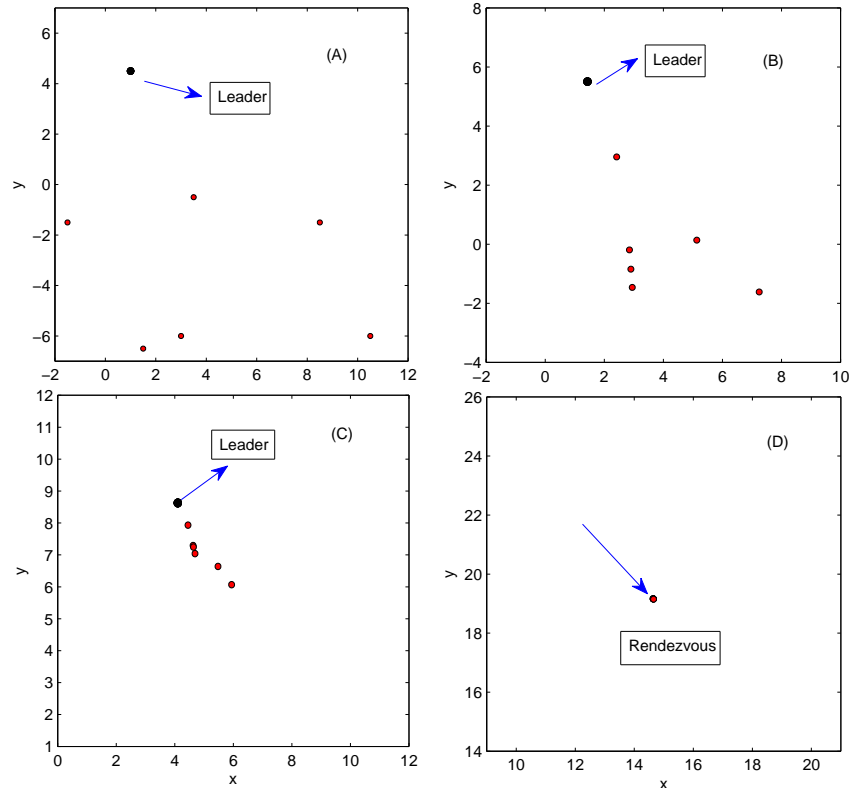


Figure 4.5: Rendezvous for one leader (black circle) and six follower robots (red circle): (A) initial configuration; (B) configuration at $t = 2.5s$; (C) configuration at $t = 5.6s$; (D) final configuration.

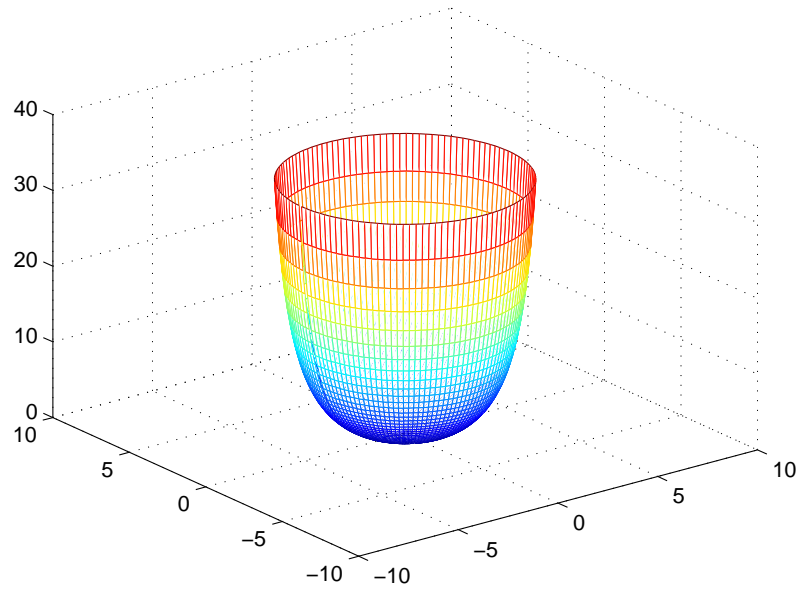


Figure 4.6: Plot of the potential function $\varphi(\|\xi_{ji}\|_\sigma)$ in (4.47).

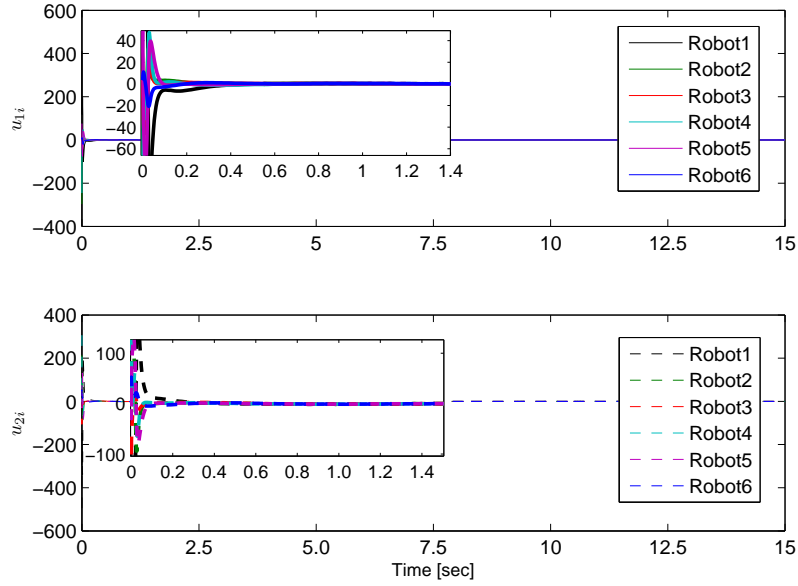


Figure 4.7: Control input u_i in (4.10).

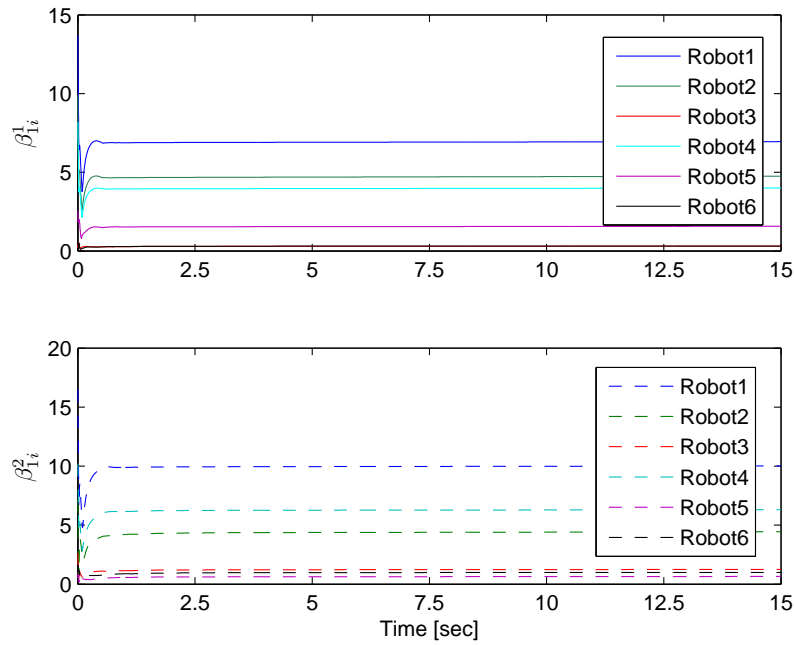


Figure 4.8: The convergence of the time-varying gain β_{1i} in (4.15).

Part II

Distributed Secure Coordination

Chapter 5

Distributed Consensus Tracking for Multi-Agent Systems under Two Types of Attacks

5.1 Introduction

As stated in Chapter 1, security of multi-agent systems is an interesting and important problem. Multi-agent systems, like all large-scale spatially distributed systems, are vulnerable to cyber-attacks due to the rapid development and widespread use of ICT. Typically, there are two different attack scenarios in a multi-agent system: attack on the dynamic behavior (or closed-loop dynamics) of the agents and attack on the communications among the agents. Both of these attacks can dramatically affect the consensus properties of the whole team of agents. Note that [101–103,106] show that an attack on a specific node is identical to node removal on the corresponding network graph. In reality, it is more general to consider the second attack scenario that a number of edges are attacked (e.g., [108–111], for just an example). To the best of knowledge, few distributed resilient control algorithms are proposed for secure coordinations.

In this chapter, a distributed coordinated control problem is addressed for a class of linear multi-agent systems under two types of attacks. Attacks on the edges instead of nodes may lead to loss of secure consensus performance. Compared with the existing works, the main contributions of this chapter are summarized as follows.

- Different from results in [11,13,22,24,58,99], the studied stochastic linear dynamics with state-dependent noise perturbation are quite general, which include systems of any order as special cases. Furthermore, the open-loop system matrix of linear agent dynamics may contain strictly unstable eigenvalues.
- Two types of attacks on the edges instead of nodes are considered. The studied topologies under these attacks indicate that the present problem cannot be solved by existing approaches (e.g., matrix analysis or CLF method) developed for an undirected or directed and balanced switching topology ([12,26,27,38, 99]). The results in [26,27,38] requires that the linear system matrix should have no unstable eigenvalues for undirected or jointly switching topologies.
- From a switching theoretical perspective, the connectivity-maintained attacks will have a destabilizing effect on systems. It is challenging to design an effective algorithm to ensure secure consensus tracking under these attacks. In addition, the effect of paralyzed topologies caused by the *connectivity-broken* attacks may make agents deviate from each other. Hence, it is challenging to get secure consensus under *connectivity-maintained/broken* attacks.
- Sufficient conditions for secure consensus tracking are firstly derived under only *connectivity-maintained* attacks. For the case with *connectivity-broken* attacks, the proposed distributed algorithm enables secure consensus tracking if the attack frequency and attack length rate satisfy certain conditions. Multi-step design procedures are developed to design distributed algorithms for both cases. An ADT-based MLF approach is developed for stability analysis.

The rest of the chapter is organized as follows. The distributed secure consensus tracking problem under two types of attacks is formulated in Section 5.2. In Section 5.3, the consensus tracking algorithm design and stability analysis are developed for multi-agent systems under only *connectivity-maintained* attacks, while the second case with mixed *connectivity-maintained/broken* attacks is studied in Section 5.4. In Section 5.5, numerical examples are provided to verify the effectiveness of the proposed methods. Conclusions on this chapter are given in Section 5.6.

5.2 Problem Formulation

Consider a class of $It\hat{o}$ stochastic linear multi-agent systems with a group of n agents described by the following stochastic differential equation:

$$dx_i(t) = [Ax_i(t) + Bu_i(t)]dt + f(x_i(t), t)d\omega(t), \quad (5.1)$$

where $i = 1, 2, \dots, n$, $x_i(t) \in \mathbb{R}^l$ is the system state, $u_i(t) \in \mathbb{R}^p$ is the control input to be designed, and $\omega(t)$ denotes a one-dimensional Brownian motion satisfying $E\{d\omega(t)\} = 0$ and $E\{d\omega^2(t)\} = dt$, $f(x_i(t), t)d\omega(t) \in \mathbb{R}^l$ represents the state-dependent noise perturbation, $A \in \mathbb{R}^{l \times l}$ and $B \in \mathbb{R}^{l \times p}$ indicates two time-invariant matrices. Let $f(x_i(t), t) = (f_1(x_i(t), t), \dots, f_l(x_i(t), t))^T$, $i = 1, 2, \dots, n$.

The objective of this paper is to design a distributed coordinated control law $u_i(t)$ such that all the states of the followers in (3.1) track that of a leader. The leader labeled as $i = 0$, is generated by the $It\hat{o}$ stochastic linear dynamics:

$$dx_0(t) = Ax_0(t)dt + f(x_0(t), t)d\omega(t). \quad (5.2)$$

Consider the information exchange between the n agents and the leader. A diagonal matrix $\mathcal{B} = \text{diag}\{b_1, b_2, \dots, b_n\} \in \mathbb{R}^{n \times n}$ is used to represent the access of agents to the desired trajectory. If b_i , $i = 1, 2, \dots, n$ is equal to 1, then the i^{th} agent has access to the desired trajectory and $b_i = 0$, otherwise. For further analysis, we denote a matrix $H \in \mathbb{R}^{n \times n}$ as $H = L + \mathcal{B}$ named as an information-exchange matrix.

Assumption 5.1. *The matrix pair (A, B) is stabilizable.*

Assumption 5.2. *There exists a constant $\rho > 0$, such that*

$$\|f(y, t) - f(z, t)\| \leq \rho \|y - z\|; \forall y, z \in \mathbb{R}^l, t \geq 0. \quad (5.3)$$

Remark 5.1. *The multi-agent state evolutions in (5.1) and (5.2) are modelled by stochastic differential equations which indeed exist in real world for general linear control systems [113]. If no stochastic noise appears, then it is a general deterministic linear multi-agent system including those with first-order [10,11], second-order [12,13], and high-order [25–27] dynamics as special cases. Assumption 5.1 is a standard assumption for linear systems. Assumption 5.2 is a Lipschitz condition for systems (5.1) and (5.2) with nonlinear state-dependent noise intensity.*

5.2.1 Attack Model

Compared with the existing results that an attack on a node (or a fraction of nodes) is identical to node removal (complete loss of its functionalities) on the corresponding network, in this work we consider attacks on the communication links \mathcal{E} but not on the nodes \mathcal{V} . That is, an attack removes or adds the edges instead of nodes in the network. The considered attacks on the edges may cause the loss of secure consensus tracking performance. To start, let us define two kinds of attacks for a directed communication graph.

Definition 5.1. *(Connectivity-maintained Attacks) Under connectivity-maintained attacks, the original network topology with a directed spanning tree still possesses a directed spanning tree, even though the topology changes due to attack-caused link failures or creation of new links.*

Definition 5.2. *(Connectivity-broken Attacks) Under connectivity-broken attacks, the original network topology with a directed spanning tree become disconnected (or paralyzed) due to attack-caused link failures or creation of new links.*

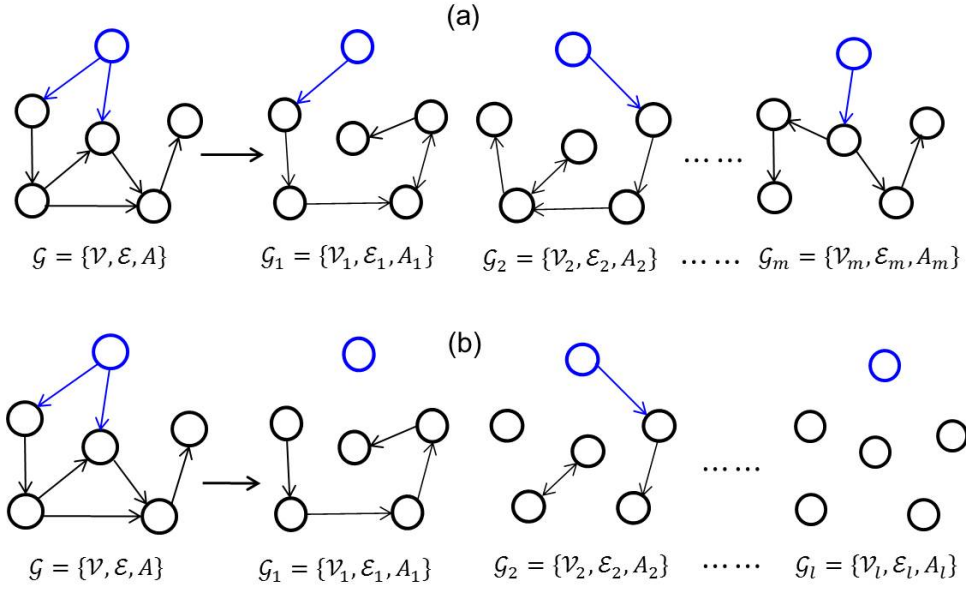


Figure 5.1: Examples of the network topology under two types of attacks: (a) network topology under m connectivity-maintained attacks; (b) network topology under l connectivity-broken attacks.

Examples of the network topology under these two attacks are shown in Fig. 5.1.

Remark 5.2. *Definition 5.1 implies that the topology with a directed spanning tree provides the possibility to guarantee consensus tracking security of the overall multi-agent systems, while in Definition 5.2, the topology under connectivity-broken attacks without any directed spanning trees will bring negative effect and might totally destroy the secure consensus tracking performance.*

Remark 5.3. *Definitions 5.1 and 5.2 are also motivated from some practical examples. Take the unmanned aerial vehicle (UAV) system for an instance, the communication among those UAVs would be blocked by some trees or buildings when they fly in a forested or urban area. In such a case, the communication network will result in a large number of topologies. Then, Definitions 5.1 and 5.2 can be used to model this situation. In addition, in a practical traffic network, the traffic congestion analysis was considered in [115] for a traffic switching network as the traffic jams do make the vehicles change their routes.*

5.2.2 Attacker and Defender Strategies

In a networked multi-agent system, the attacker aims to remove the connection edges in a network such that the possible network topologies don't have a directed spanning tree. The defender aims to reconstruct a number of edges in the network based on a recovery mechanism such that the network topology still has a spanning tree. A distributed algorithm is developed such that the network will not lose secure consensus performance. The framework of the attacker and defender strategies is shown in Fig. 5.2. The interactions between the cyber and physical systems are captured by their dynamics where the physical state $x_i(t)$ and cyber state $\sigma(t)$ are controlled by the defense mechanism used by the defender as well as attacker's action. This hybrid nature leads to adoption of a switched system model.

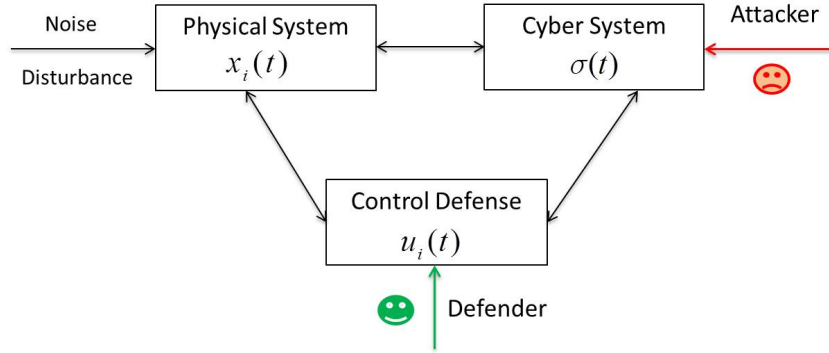


Figure 5.2: Framework of attacker and defender strategies in multi-agent systems.

5.2.3 Control Objective

The goal is to establish a framework for designing a distributed secure controller $u_i(t)$ for systems under two types of attacks.

Definition 5.3. (*Mean-Square Consensus Tracking*)

The distributed control law $u_i(t)$ is said to solve a secure consensus tracking problem in mean-square for systems (5.1) and (5.2) under these two types of attacks, if

$\forall t \geq t_0$, there exists a scalar $\kappa > 0$ and a decay rate $\lambda > 0$ such that

$$E\{\|x_i(t) - x_0(t)\|^2\} \leq \kappa e^{-\lambda(t-t_0)} E\{\|x_i(t_0) - x_0(t_0)\|^2\}. \quad (5.4)$$

5.3 Exponential Consensus Tracking Under Only Connectivity-Maintained Attacks

In this subsection, it is assumed that the switching of network topology is firstly triggered by only some connectivity-maintained attacks. A switching signal $\sigma(t) : [0, \infty) \rightarrow \Xi = \{1, 2, \dots, q\}$ is introduced to describe the switching among different topologies. Suppose that there exists an infinite sequence of uniformly bounded non-overlapping time intervals $[t_k, t_{k+1})$, $k \in \mathbb{N}$ across which the interaction graph is time-invariant. Obviously, $\{\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_q\}$, $q \geq 1$, denotes the set of possible directed switching graph $\mathcal{G}_{\sigma(t)}$. The information-exchange matrix for consensus tracking is denoted as H_1, H_2, \dots, H_q . Corresponding to $\sigma(t)$, the switching sequence is $\{(i_0, t_0), \dots, (i_k, t_k), \dots, | i_k \in \Xi, k = 0, 1, 2, \dots, Z\}$, which means that the i_k th subsystem is activated when $t \in [t_k, t_{k+1})$.

Assumption 5.3. *The connection graph $\mathcal{G}_{\sigma(t)}$ under connectivity-maintained attacks contains a directed spanning tree with the leader as the root.*

Based on Lemma 2.2 and Assumption 5.3, we get the following lemma.

Lemma 5.1. *[112] Suppose that Assumption 5.3 holds. Then, there exist positive definite diagonal matrices $\Theta_{\sigma(t)} = \text{diag}\{\theta_{\sigma(t),1}^{-1}, \dots, \theta_{\sigma(t),n}^{-1}\} \in \mathbb{R}^{n \times n}$, such that $Q_{\sigma(t)} = H_{\sigma(t)}^T \Theta_{\sigma(t)} + \Theta_{\sigma(t)} H_{\sigma(t)}$ is a symmetric positive definite matrix, where $\theta_{\sigma(t)} = [\theta_{\sigma(t),1}, \theta_{\sigma(t),2}, \dots, \theta_{\sigma(t),n}] = H_{\sigma(t)}^{-T} \mathbf{1}_n$.*

We propose the following distributed consensus tracking protocol for system (5.1) and (5.2) subject to connectivity-maintained attacks:

$$u_i(t) = \delta K \left\{ \sum_{j=1}^n a_{ij}^{\sigma(t)} (x_j(t) - x_i(t)) + b_i^{\sigma(t)} (x_0(t) - x_i(t)) \right\}, \quad (5.5)$$

where $\sigma(t) \in \Xi$, $a_{ij}^{\sigma(t)}$ is the adjacency element of $\mathcal{G}_{\sigma(t)}$, $b_i^{\sigma(t)}$ is equal to 1 when agent i has access to the leader and 0, otherwise, $\delta > 0$ denotes the coupling strength and K is the feedback controller gain matrix to be determined.

Denote the state tracking error as $e_i(t) = x_i(t) - x_0(t)$. Then, combining (5.1) with (5.5) gives the switched stochastic closed-loop error systems as

$$\begin{aligned} de_i(t) = & \{Ae_i(t) + \delta BK[\sum_{j=1}^n a_{ij}^{\sigma(t)}(e_j(t) - e_i(t)) - b_i^{\sigma(t)}e_i(t)]\}dt \\ & + (f(x_i(t), t) - f(x_0(t), t))d\omega(t). \end{aligned} \quad (5.6)$$

A multi-step design procedure is developed for selecting the control gains in (5.5).

Algorithm 5.1 Controller Parameter Design of (5.5).

Under Assumptions 5.1-5.3, a distributed secure algorithm in (5.5) is constructed:

(1) Solve an LMI $AP + PA^T - c\tilde{\theta}_r BB^T + \rho^2 P + \tau P < 0$ (5.7)

to get a matrix $P > 0$ and scalars $\tau, c > 0$. In (5.7), ρ satisfies Assumption 5.2 and $\tilde{\theta}_r = \min_{r,i} \theta_{r,i}$, $r \in \{1, \dots, q\}$, $i = 1, 2, \dots, n$ with $\theta_{r,i}$ defined in Lemma 5.1.

(2) Design the controller gain matrix K in (5.5) as

$$K = B^T P^{-1}. \quad (5.8)$$

(3) For matrix $Q_{\sigma(t)}$ defined in Lemma 5.1, denoting $\lambda_0 = \min\{\lambda_{\min}(Q_{\sigma(t)}) : \sigma(t) \in \Xi\}$ yields the coupling strength δ in (5.5) as $\delta \geq \delta th$:

$$\delta th = c/\lambda_0. \quad (5.9)$$

Remark 5.4. The feasibility analysis of LMI (5.7) is given below

First, we analyze the solvability of a matrix $\bar{P} > 0$ and a scalar $\bar{c} > 0$ for the following LMI:

$$A\bar{P} + \bar{P}A^T - \bar{c}BB^T + \rho^2 \bar{P} < 0. \quad (5.10)$$

If (A, B) is stabilizable but not completely controllable, then there exists a matrix X such that $(A + BX)$ is Hurwitz and the maximum real part of the eigenvalues of $(A + BX)$ is ϕ , where $\phi < 0$ is the largest real part of the uncontrollable modes of A . Based on Finsler's Lemma, LMI (5.10) is solvable if and only if there exists a positive definite matrix $Z = Z^T$ such that

$$(A + BX)Z + Z(A + BX)^T + \rho^2 Z < 0, \quad (5.11)$$

$$\text{i.e.,} \quad (A + BX + \frac{\rho^2}{2}I)Z + Z(A + BX + \frac{\rho^2}{2}I)^T < 0. \quad (5.12)$$

LMI (5.12) is solvable if and only if $\rho^2 < 2\theta_0$, where $\theta_0 = -\phi > 0$. If (A, B) is controllable, then LMI (5.12) is solvable for any given $\rho^2 \in \mathbb{R}^+$.

Next, we analyze the solvability equivalence between LMIs (5.7) and (5.10). If LMI (5.10) is valid, then based on the continuity of LMI (5.10), there exists an arbitrarily small positive scalar τ such that

$$A\bar{P} + \bar{P}A^T - \bar{c}BB^T + \rho^2\bar{P} + \tau\bar{P} < 0. \quad (5.13)$$

Then, there exist a matrix $P > 0$ and a scalar $c > 0$ such that LMI (5.7) is valid which implies LMI (5.10) is valid by continuity. The feasibility analysis is finished.

Next, sufficient conditions on secure consensus tracking are developed for systems subject to only connectivity-maintained attacks.

Theorem 5.1. Consider a class of Itô stochastic linear multi-agent systems (5.1) and (5.2) subject to only connectivity-maintained attacks. Suppose Assumptions 5.1-5.3 hold and the LMI (5.7) has a feasible solution. Then the agents modeled by (5.1) and (5.2) under the proposed protocol (5.5) constructed by Algorithm 5.3 can achieve mean-square exponential consensus tracking of the leader modeled by (3.2) under the switching signal $\sigma(t) \in \Xi$ with the average dwell time satisfying $T_a > T_a^* = \frac{\ln(\mu_1)}{\tau}$.

Moreover, the error state estimation is given by

$$E\{\|e_i(t)\|^2\} \leq \hat{\mu}e^{-\lambda(t-t_0)}E\{\|e_i(t_0)\|^2\}, \quad (5.14)$$

where $\lambda = (\tau - \frac{\ln \mu_1}{T_a})$, $\hat{\mu} = \frac{a}{b}e^{N_0 \ln \mu_1}$, $a = \lambda_{\max}(\theta_{r,i}^{-1}P^{-1})$, $b = \lambda_{\min}(\theta_{r,i}^{-1}P^{-1})$, $\mu_1 = \frac{\bar{\theta}_r}{\theta_r} \geq 1$, $\tilde{\theta}_r = \min_{r,i} \theta_{r,i}$, and $\bar{\theta}_r = \max_{r,i} \theta_{r,i}$, $r \in \{1, \dots, q\}$, $i = 1, 2, \dots, n$.

Proof. Choose a Multiple Lyapunov functional candidate as

$$V(e_i(t), \sigma(t)) = \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} P^{-1} e_i(t). \quad (5.15)$$

Based on the $It\hat{o}$ stochastic formula, the stochastic derivative is

$$\begin{aligned} d(V(e_i(t), \sigma(t))) &= \mathcal{L}V(e_i(t), \sigma(t))dt + 2 \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} P^{-1} \\ &\quad \times (f(x_i(t), t) - f(x_0(t), t)) d\omega(t), \end{aligned} \quad (5.16)$$

$$\begin{aligned} \mathcal{L}V(e_i(t), \sigma(t)) &= 2 \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} P^{-1} \{Ae_i(t) + \delta BK[\sum_{j=1}^n a_{ij}^{\sigma(t)}(e_j(t) - e_i(t)) \\ &\quad - b_i^{\sigma(t)} e_i(t)]\} + \sum_{i=1}^n (f(x_i(t), t) - f(x_0(t), t))^T \theta_{\sigma(t),i}^{-1} P^{-1} \\ &\quad \times (f(x_i(t), t) - f(x_0(t), t)). \end{aligned} \quad (5.17)$$

According to Algorithm 5.3, substituting (5.8) into (5.17) yields

$$\begin{aligned} \mathcal{L}V(e_i(t), \sigma(t)) &= \sum_{i=1}^n e_i^T(t) (\theta_{\sigma(t),i}^{-1} P^{-1} A + \theta_{\sigma(t),i} A^T P^{-1}) e_i(t) + 2\delta \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} \\ &\quad \times P^{-1} B B^T P^{-1} [\sum_{j=1}^n a_{ij}^{\sigma(t)} (e_j(t) - e_i(t)) - b_i^{\sigma(t)} e_i(t)] \\ &\quad + \sum_{i=1}^n (f(x_i(t), t) - f(x_0(t), t))^T \theta_{\sigma(t),i}^{-1} P^{-1} (f(x_i(t), t) - f(x_0(t), t)). \end{aligned}$$

Based on Assumption 5.2, we have

$$\begin{aligned} \mathcal{L}V(e_i(t), \sigma(t)) &\leq \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} (P^{-1} A + A^T P^{-1} + \rho^2 P^{-1}) e_i(t) + 2\delta \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} \\ &\quad \times P^{-1} B B^T P^{-1} [\sum_{j=1}^n a_{ij}^{\sigma(t)} (e_j(t) - e_i(t)) - b_i^{\sigma(t)} e_i(t)]. \end{aligned} \quad (5.18)$$

Let $\varsigma(t) = (\varsigma_1^T(t), \dots, \varsigma_n^T(t))^T$, where $\varsigma_i(t) = P^{-1} e_i(t)$, $i = 1, \dots, n$. Obviously, $e(t) = (I_n \otimes P) \varsigma(t)$. It thus follows from Assumption 5.3, Lemma 5.1 and (5.18) that

$$\begin{aligned} \mathcal{L}V(e(t), \sigma(t)) &\leq \varsigma^T(t) [\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)] \varsigma(t) \\ &\quad - \delta \varsigma^T(t) [(\Theta_{\sigma(t)} H_{\sigma(t)} + H_{\sigma(t)}^T \Theta_{\sigma(t)}) \otimes BB^T] \varsigma(t) \\ &\leq \varsigma^T(t) [\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)] \varsigma(t) \\ &\quad - \delta \lambda_0 \varsigma^T(t) (I \otimes BB^T) \varsigma(t), \end{aligned} \quad (5.19)$$

where $\lambda_0 = \min\{\lambda_{\min}(Q_{\sigma(t)}) : \sigma(t) \in \Xi\}$ with $Q_{\sigma(t)}$ defined in Lemma 5.1.

Since $\delta > \frac{c}{\lambda_0}$, the expression in (5.19) can be rewritten as

$$\begin{aligned} \mathcal{L}V(e_i(t), \sigma(t)) &\leq \varsigma^T(t)[\Theta_{\sigma(t)} \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ &\quad - \tilde{\theta}_r \varsigma^T(t)(\Theta_{\sigma(t)} \otimes cBB^T)\varsigma(t). \end{aligned} \quad (5.20)$$

According to Algorithm 5.3, (5.7) implies that $AP + PA^T - c\tilde{\theta}_r BB^T + \rho^2 P < -\tau P$.

Thus it gets from (5.15) and (5.16) that

$$\mathcal{L}V(e_i(t), \sigma(t)) \leq -\tau \varsigma^T(t)(\Theta_{\sigma(t)} \otimes P)\varsigma(t) = -\tau \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} P^{-1} e_i(t). \quad (5.21)$$

Substituting (5.21) into (5.16) leads to

$$\begin{aligned} d(V(e_i(t), \sigma(t))) &\leq -\tau V(e_i(t), \sigma(t))dt + 2 \sum_{i=1}^n e_i^T(t) \theta_{\sigma(t),i}^{-1} P^{-1} \\ &\quad \times (f(x_i(t), t) - f(x_0(t), t))d\omega(t). \end{aligned} \quad (5.22)$$

Integrating both sides of (5.22) over $[t_k, t_{k+1})$ and taking expectation yield

$$E\{V(e_i(t), \sigma(t))\} \leq e^{-\tau(t-t_k)} E\{V(e_i(t_k), \sigma(t_k))\}. \quad (5.23)$$

It is noted that the communication topology $\mathcal{G}_{\sigma(t)}$ is fixed for $t \in [t_k, t_{k+1})$, $k \in \mathbb{N}$. After deriving the change relationship of (5.15) in the time interval of active subsystem, combining (5.21) with (5.22), at switching instant t_k yields

$$E\{V(e_i(t_k), \sigma(t_k))\} \leq \mu_1 E\{V(e_i(t_k^-), \sigma(t_k^-))\}. \quad (5.24)$$

Thus, based on (5.23), (5.24), and Definition 2.4, we can get

$$\begin{aligned} E\{V(e_i(t), \sigma(t))\} &\leq \mu_1 e^{-\tau(t-t_k)} E\{V(e_i(t_k^-), \sigma(t_k^-))\} \\ &\leq \mu_1 e^{-\tau(t-t_{k-1})} E\{V(e_i(t_{k-1}), \sigma(t_{k-1}))\} \\ &\leq \dots \leq \mu_1^k e^{-\tau(t-t_0)} E\{V(e_i(t_0), \sigma(t_0))\} \\ &\leq e^{N_0 \ln \mu_1} e^{-(\tau - \frac{\ln \mu_1}{T_a})(t-t_0)} E\{V(e_i(t_0), \sigma(t_0))\}. \end{aligned} \quad (5.25)$$

From (5.15), it is obtained that

$$E\{\|e_i(t)\|^2\} \leq \hat{\mu} e^{-\lambda(t-t_0)} \|e_i(t_0)\|^2, \quad (5.26)$$

where $\hat{\mu} = \frac{a}{b} e^{N_0 \ln \mu_1}$, $a = \lambda_{\max}(\theta_{r,i}^{-1} P^{-1})$, $b = \lambda_{\min}(\theta_{r,i}^{-1} P^{-1})$, and $\lambda = (\tau - \frac{\ln \mu_1}{T_a})$. \square

5.4 Exponential Consensus Tracking Under Mixed Connectivity-Maintained /Broken Attacks

In the above section, secure consensus tracking is solved under only connectivity-maintained attacks. However, when further considering a class of connectivity-broken attacks, the agents may be isolated partly or totally. The goal is to design an effective algorithm to achieve secure consensus tracking, which is resilient to these mixed connectivity-maintained/broken attacks. A new switching signal $\tilde{\sigma}(t) : [0, \infty) \rightarrow \tilde{\Xi} = \{1, 2, \dots, m, m+1, \dots, l\}$, $m \geq 1$, $l \geq 2$ is introduced to describe the evolution of the underlying topologies subject to the m and b ($b = l - m$) connectivity-maintained/broken attacks, respectively. Obviously, $\{\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_m, \mathcal{G}_{m+1}, \dots, \mathcal{G}_l\}$ denote the set of all possible new directed topologies $\mathcal{G}_{\tilde{\sigma}(t)}$ caused by these two types of attacks.

Some notations are introduced to be used later for systems (5.1) and (5.2) subject to mixed connectivity-maintained/broken attacks. The index set $\tilde{\Xi}$ of $\tilde{\sigma}(t)$ is divided into two subsets Ξ_m and Ξ_b ($\Xi_m \cup \Xi_b = \tilde{\Xi}$), where Ξ_m and Ξ_b are used to index the sets of the connectivity-maintained/broken attacks, respectively. Let T_m and T_b denote the total activation time of the connectivity-maintained/broken attacks on $[t_0, t)$, respectively. Denoting t_k ($k = 0, 1, 2, \dots, Z$) as the switching instants in $[t_0, t)$, and letting $t_{Z+1} = t$, we can obtain that

$$T_m(t_0, t) = \sum_{\substack{k=0, \\ \tilde{\sigma}(t_k) \in \Xi_m}}^Z (t_{k+1} - t_k), \quad (5.27)$$

$$T_b(t_0, t) = \sum_{\substack{k=0, \\ \tilde{\sigma}(t_k) \in \Xi_b}}^Z (t_{k+1} - t_k). \quad (5.28)$$

Assumption 5.4. *The network topology $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_m$ under the connectivity-maintained attacks contains a directed spanning tree with the leader as the root, while all the other paralyzed topology $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_b$ under the connectivity-broken attacks does not contain any directed spanning trees with the leader as the root.*

Assumption 5.5. *The paralyzed topology $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_b$ can be recovered into connectivity-maintained topologies $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_m$ after a connectivity restoration mechanism (i.e, the sensing and communication devices are able to recover through some backup or repairing efforts).*

Remark 5.5. *The connectivity-maintained topology $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_m$ with a directed spanning tree in Assumption 5.4 provides the possibility of consensus tracking for system (5.1). However, each paralyzed topology $\mathcal{G}_{\tilde{\sigma}(t)}$, $\tilde{\sigma}(t) \in \Xi_b$ under the connectivity-broken attacks might totally destroy the secure performance of the whole multi-agent systems. Thus, Assumption 5.5 implies that the secure consensus tracking objective can be achieved if there exists a connectivity restoration mechanism through internal recovery/tolerance capacities of the system or repairing efforts, even though it may take a short period of time.*

To achieve the secure consensus tracking objective, the following protocol is proposed for systems (5.1) and (5.2) under mixed two attacks as

$$u_i(t) = \gamma F \left\{ \sum_{j=1}^n a_{ij}^{\tilde{\sigma}(t)} (x_j(t) - x_i(t)) + b_i^{\tilde{\sigma}(t)} (x_0(t) - x_i(t)) \right\}, \quad (5.29)$$

where $\tilde{\sigma}(t) \in \tilde{\Xi}$, $\tilde{\Xi} = (\Xi_m \cup \Xi_b)$, $a_{ij}^{\tilde{\sigma}(t)}$ is the adjacency element of the network topology $\mathcal{G}_{\tilde{\sigma}(t)}$, and γ and F are new coupling strength and feedback gain matrix, respectively.

Thus, combining (5.1), (5.2) and (5.29) yields the closed-loop error systems as

$$de(t) = [(I_n \otimes A)e(t) - \gamma(H_{\tilde{\sigma}(t)} \otimes BF)e(t)]dt + \tilde{f}(x(t), t)d\omega(t), \quad \tilde{\sigma}(t) \in \tilde{\Xi}. \quad (5.30)$$

Remark 5.6. *Section 5.3 shows that the secure consensus tracking is achieved under only connectivity-maintained attacks. However, the existence of paralyzed topologies (e.g., $H_{\tilde{\sigma}(t)}$ $\tilde{\sigma}(t) \in \tilde{\Xi}$ in (5.30)) may totally destroy the secure consensus tracking. To overcome this difficulty, a requirement on the ratio of the total activation time of these mixed connectivity-maintained/broken attacks should be specified as well as a switching signal constraint to handle the effect of switching.*

Inspired by the above definition of ADT in [117,118], and controller failure in [119], the following notions are introduced to solve the problem.

Definition 5.4. (*Connectivity-broken attack frequency*) For a switching signal $\tilde{\sigma}(t) \in \tilde{\Xi}$ and $\forall T_2 > T_1 \geq 0$, let $N_f(T_1, T_2)$ denote the number of connectivity-broken attacks over (T_1, T_2) . $F_f(T_1, T_2) = \frac{N_f(T_1, T_2)}{T_2 - T_1}$ is defined as the connectivity-broken attack frequency over (T_1, T_2) .

A multi-step design procedure is developed for selecting the corresponding controller parameters γ and F in protocol (5.29).

Algorithm 5.2 Controller Parameter Design of (5.29).

Under Assumptions 5.1, 5.2, 5.4, and 5.5, a distributed protocol (5.29) can be constructed as follows.

(1) Solve an LMI

$$AP + PA^T - d\tilde{\theta}_s BB^T + \rho^2 P + \beta P < 0, \quad (5.31)$$

to get a matrix $P > 0$ and scalars $\beta, d > 0$.

(2) Solve an LMI $AP + PA^T + \varepsilon BB^T + \rho^2 P - \alpha P < 0$, (5.32)

to get scalars $\varepsilon, \alpha > 0$.

(3) Design the feedback gain matrix F of (5.29) as

$$F = B^T P^{-1}. \quad (5.33)$$

(4) Choose the coupling strength γ satisfying:

$$\varepsilon / |\bar{\lambda}_0| \geq \gamma \geq d / \tilde{\lambda}_0. \quad (5.34)$$

In (5.31), $\tilde{\theta}_s$ is given as $\tilde{\theta}_s = \min_{s,i} \theta_{s,i}$, $s \in \{1, \dots, m\}$, $i = 1, 2, \dots, n$, $\bar{\lambda}_0$ and $\tilde{\lambda}_0$ are described as $\bar{\lambda}_0 = \min\{\lambda_{\min}(H_{\tilde{\sigma}(t)}^T + H_{\tilde{\sigma}(t)}) : \tilde{\sigma}(t) \in \tilde{\Xi}_b\}$ and $\tilde{\lambda}_0 = \min\{\lambda_{\min}(Q_{\tilde{\sigma}(t)}) : \tilde{\sigma}(t) \in \tilde{\Xi}_m\}$, respectively, with $Q_{\tilde{\sigma}(t)}$ given in Lemma 5.1.

Remark 5.7. In Algorithm 5.4, one only needs to solve the LMI (5.31) first and its feasibility analysis is provided in Remark 5.4. Then, it is not difficult to verify that there exists a scalar α such that the LMI (5.32) holds if $\alpha > (d\tilde{\theta}_s + \varepsilon)\lambda_{\max}(BB^T P^{-1})$, where P is a feasible solution of (5.31). Thus, it implies that under Assumption 5.1, there always exist some positive scalars $\alpha, \beta, \varepsilon$, and d such that the LMIs (5.31) and (5.32) share a common positive solution $P > 0$. The obtained matrix P is successfully used to construct the distributed control law (5.29).

Theorem 5.2. *Consider stochastic linear multi-agent systems (5.1) and (5.2) subject to mixed connectivity-maintained/broken attacks. Suppose Assumptions 5.1, 5.2, 5.4 and 5.5 hold and the LMIs (5.31) and (5.32) have feasible solutions. Then under the proposed protocol (5.29) constructed by Algorithm 5.4, the agents modeled by (5.1) can achieve mean-square exponential consensus tracking of the leader in (5.2) under the new switching signal $\tilde{\sigma}(t)$, $\tilde{\sigma}(t) \in \tilde{\Xi} = (\Xi_m \cup \Xi_b)$, provided that:*

1. *For a constant $\eta^* \in (0, \beta)$, the connectivity-broken attack length rate satisfies:*

$$\frac{T_b(t_0, t)}{t - t_0} \leq \frac{\beta - \eta^*}{\alpha + \beta}. \quad (5.35)$$

2. *For a constant $\eta \in (0, \eta^*)$, the connectivity-broken attack frequency $F_f(t_0, t)$ for the whole time interval satisfies:*

$$F_f(t_0, t) = \frac{N_f(t_0, t)}{t - t_0} \leq F_f^* = \frac{\eta^* - \eta}{2 \ln(\mu_2)}, \quad (5.36)$$

where $\mu_2 = \frac{\bar{\theta}_s}{\bar{\theta}_s} \geq 1$, $\bar{\theta}_s = \min_{s,i} \theta_{s,i}$, $\bar{\theta}_s = \max_{s,i} \theta_{s,i}$, $s \in \{1, \dots, m\}$, $i = 1, 2, \dots, n$.

Thus, the average recovery time is less than $\frac{\beta - \eta^*}{(\alpha + \beta) F_f(t_0, t)}$. Moreover, the state decay estimation of consensus tracking error is given as

$$E\{\|e_i(t)\|^2\} \leq \varphi e^{-\eta(t-t_0)} E\{\|e_i(t_0)\|^2\}, \quad (5.37)$$

where $\varphi = \frac{\tilde{a}}{\tilde{b}}$, $\tilde{a} = \max\{\lambda_{\max}(\theta_{s,i}^{-1} P^{-1}), \lambda_{\max}(P^{-1})\}$, $\tilde{b} = \min\{\lambda_{\min}(\theta_{s,i}^{-1} P^{-1}), \lambda_{\min}(P^{-1})\}$, $s \in \{1, \dots, m\}$, $i = 1, 2, \dots, n$.

Proof. Choose the following multiple Lyapunov functional candidate for the stochastic switched closed-loop error systems (5.30) as

$$V(\sigma(t), e(t)) = \begin{cases} e^T(t)(\Theta_{\tilde{\sigma}(t)} \otimes P^{-1})e(t), & \tilde{\sigma}(t) \in \Xi_m, \\ e^T(t)(I_n \otimes P^{-1})e(t), & \tilde{\sigma}(t) \in \Xi_b. \end{cases} \quad (5.38)$$

where $\Theta_{\tilde{\sigma}(t)} = \text{diag}\{\theta_{\tilde{\sigma}(t),1}^{-1}, \dots, \theta_{\tilde{\sigma}(t),m}^{-1}\}$ is defined in Lemma 5.1.

Next, the proof for Theorem 5.2 will be presented with the following steps.

(I) The multi-agent systems (5.1) and (5.2) are subject to m connectivity-maintained attacks. When $\tilde{\sigma}(t) \in \Xi_m$, it follows from the $It\hat{o}$ stochastic formula that the stochastic derivative of (5.38) along system (5.30) is given by

$$d(V(\tilde{\sigma}(t), e(t))) = LV(\tilde{\sigma}(t), t)dt + 2e^T(t)(\Theta_{\tilde{\sigma}(t)} \otimes P^{-1})\tilde{f}(x(t), t)d\omega(t), \quad (5.39)$$

$$\begin{aligned} LV(\tilde{\sigma}(t), e(t)) &= 2e^T(t)(\Theta_{\tilde{\sigma}(t)} \otimes P^{-1})[(I_n \otimes A) - \gamma(H_{\tilde{\sigma}(t)} \otimes BF)e(t)] \\ &\quad + \tilde{f}^T(x(t), t)(\Theta_{\tilde{\sigma}(t)} \otimes P^{-1})\tilde{f}(x(t), t). \end{aligned} \quad (5.40)$$

Similar to (5.16)-(5.23) in Theorem 5.1, it is obtain that for $t \in [t_k, t_{k+1})$,

$$E\{V(\tilde{\sigma}(t), e(t))\} \leq e^{-\beta(t-t_k)} E\{V(\tilde{\sigma}(t_k), e(t_k))\}. \quad (5.41)$$

(II) The multi-agent systems are subject to b connectivity-broken attacks. When $\tilde{\sigma}(t) \in \Xi_b$, similarly, the stochastic derivative of (5.38) along system (5.30) is

$$d(V(\tilde{\sigma}(t), e(t))) = LV(\tilde{\sigma}(t), t)dt + 2e^T(t)(I_n \otimes P^{-1})\tilde{f}(x(t), t)d\omega(t), \quad (5.42)$$

$$\begin{aligned} LV(\tilde{\sigma}(t), e(t)) &= e^T(t)[I_n \otimes (P^{-1}A + A^T P^{-1} - 2\gamma P^{-1}BF)]e(t) \\ &\quad + \tilde{f}^T(x(t), t)(I_n \otimes P^{-1})\tilde{f}(x(t), t). \end{aligned} \quad (5.43)$$

Similar to (5.17)-(5.20) in Theorem 5.1, it follows from Algorithm 5.4 that

$$\begin{aligned} LV(\tilde{\sigma}(t), e(t)) &\leq \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) \\ &\quad - \gamma\varsigma^T(t)[(H_{\tilde{\sigma}(t)} + H_{\tilde{\sigma}(t)}^T) \otimes BB^T]\varsigma(t) \\ &\leq \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P)]\varsigma(t) + \gamma|\bar{\lambda}_0|\varsigma^T(t)[I_n \otimes BB^T]\varsigma(t) \\ &\leq \varsigma^T(t)[I_n \otimes (AP + PA^T + \rho^2 P) + \varepsilon BB^T]\varsigma(t), \end{aligned} \quad (5.44)$$

where $\varepsilon \geq \gamma|\bar{\lambda}_0|$ and $\bar{\lambda}_0 = \min\{\lambda_{\min}(H_{\tilde{\sigma}(t)}^T + H_{\tilde{\sigma}(t)}), \tilde{\sigma}(t) \in \Xi_b\}$.

Based on (5.32) in Algorithm (5.4), it is not difficult to obtain

$$LV(\tilde{\sigma}(t), e(t)) \leq \alpha\varsigma^T(t)(I_n \otimes P)\varsigma(t) = \alpha e^T(t)(I_n \otimes P^{-1})e(t). \quad (5.45)$$

Thus, it follows from (5.42) and (5.45) that for for any $t \in [t_k, t_{k+1})$,

$$E\{V(\tilde{\sigma}(t), e(t))\} \leq e^{\alpha(t-t_k)} E\{V(\tilde{\sigma}(t_k), e(t_k))\}. \quad (5.46)$$

(III) Synthesizing the above two circumstances (I)-(II) into one, it can be obtained from (5.41) and (5.46) that for any $t \in [t_k, t_{k+1})$,

$$E\{V(\tilde{\sigma}(t), e(t))\} \leq \begin{cases} e^{-\beta(t-t_k)} E\{V(\tilde{\sigma}(t_k), e(t_k))\}, & \tilde{\sigma}(t) \in \Xi_m, \\ e^{\alpha(t-t_k)} E\{V(\tilde{\sigma}(t_k), e(t_k))\}, & \tilde{\sigma}(t) \in \Xi_b. \end{cases} \quad (5.47)$$

Therefore, under $\tilde{\sigma}(t) \in \tilde{\Xi} = (\Xi_m \cup \Xi_b)$, it further yields for any $t \in [t_k, t_{k+1})$,

$$E\{V(\tilde{\sigma}(t), e(t))\} \leq e^{\alpha T_b(t_k, t) - \beta T_m(t_k, t)} E\{V(\tilde{\sigma}(t_k), e(t_k))\}. \quad (5.48)$$

When $t = t_k$, we assume that $\tilde{\sigma}(t_k)$ is activated during $t \in [t_k, t_{k+1})$, and $\tilde{\sigma}(t_{k-1})$ is identified at t_{k-1} . Besides, it is assumed that there is no jump in the state $x_i(t)$ at the switching instant, i.e., $x_i(t_k) = x_i(t_k^-)$. It follows from (5.38) that

$$E\{V(\tilde{\sigma}(t_k), e(t_k))\} \leq \mu_2 E\{V(\tilde{\sigma}(t_k^-), e(t_k^-))\}. \quad (5.49)$$

For the whole switching interval, (5.48) and (5.49) give

$$\begin{aligned} E\{V(\tilde{\sigma}(t), e(t))\} &\leq \mu_2 e^{\alpha T_b(t_k, t) - \beta T_m(t_k, t)} E\{V(\tilde{\sigma}(t_k^-), e(t_k^-))\} \\ &\leq \mu_2 e^{\alpha T_b(t_{k-1}, t) - \beta T_m(t_{k-1}, t)} E\{V(\tilde{\sigma}(t_{k-1}), e(t_{k-1}))\} \\ &\leq \dots \\ &\leq \mu_2^{N_{\tilde{\sigma}(t)}(t_0, t)} e^{\alpha T_b(t_0, t) - \beta T_m(t_0, t)} E\{V(\tilde{\sigma}(t_0), e(t_0))\} \\ &= e^{N_{\tilde{\sigma}(t)}(t_0, t) \ln(\mu_2) + \alpha T_b(t_0, t) - \beta T_m(t_0, t)} E\{V(\tilde{\sigma}(t_0), e(t_0))\}. \end{aligned} \quad (5.50)$$

According to the condition (5.35), it holds that

$$-\beta T_m(t_0, t) + \alpha T_b(t_0, t) \leq -\eta^*(t - t_0), \quad (5.51)$$

Based on Definition 6.2 and the condition (5.36), it is clear that

$$e^{N_{\tilde{\sigma}(t)}(t_0, t) \ln(\mu_2)} \leq e^{2N_f(t_0, t) \ln(\mu_2)} \leq e^{(\eta^* - \eta)(t - t_0)}. \quad (5.52)$$

Hence, it follows from (5.50)-(5.52) that (5.37) holds, which implies that $e_i(t) \rightarrow 0$ as $t \rightarrow +\infty$, i.e., $x_i(t) \rightarrow x_0(t)$, as $t \rightarrow +\infty$. \square

5.5 Numerical Example

In this section, three numerical simulations are provided to demonstrate the effectiveness of results for systems under two types of attacks. The dynamics of the i th agent are given by (5.1) with $x_i(t) = (x_{i1}, x_{i2}, x_{i3}, x_{i4})^T \in \mathbb{R}^4$ and $f(x_i(t), t) = (0.3 \cos(x_{i1}), 0, 0, 0.3 \sin(x_{i4}))^T \in \mathbb{R}^4$, $i = 0, 1, \dots, 4$. It is easy to check that (A, B) is stabilizable. In view of Assumption 5.2, $\rho = 0.3$.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -48.6 & -1.26 & 48.6 & 0 \\ 0 & 0 & 0 & 10 \\ 1.95 & 0 & -1.95 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 21.6 \\ 0 \\ 0 \end{bmatrix}. \quad (5.53)$$

Example 5.1. Connectivity-Maintained Attacks

In this example, consensus tracking for multi-agent systems with connectivity-maintained attacks is numerically studied. The network topology switches among \mathcal{G}_1 and \mathcal{G}_2 caused by only two different connectivity-maintained attacks are shown in Fig. 5.3. Both \mathcal{G}_1 and \mathcal{G}_2 has a directed spanning tree with agent 0 as the leader.

Based on Algorithm 5.3, constructing (5.5) with $c = 1.5$ and $\tau = 1.6$ yields $K = [1.2293, 0.2619, -0.4736, 4.7397]$. Some calculations give the parameters $\tilde{\theta}_r = 1.6667$, $\mu_1 = 2.2$, $\lambda_0 = 0.2093$, and $\delta th = \frac{c}{\lambda_0} = 7.1684$. Set the coupling strength

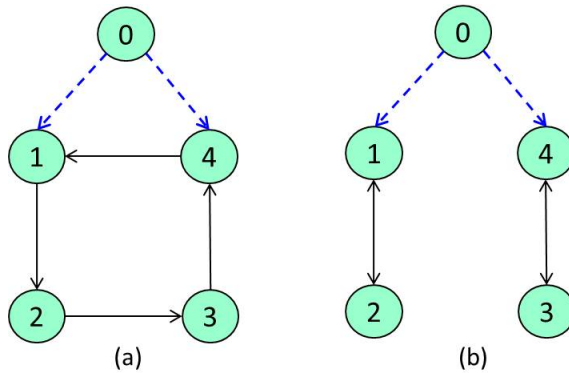


Figure 5.3: Switching topologies \mathcal{G}_1 and \mathcal{G}_2 in Example 5.1.

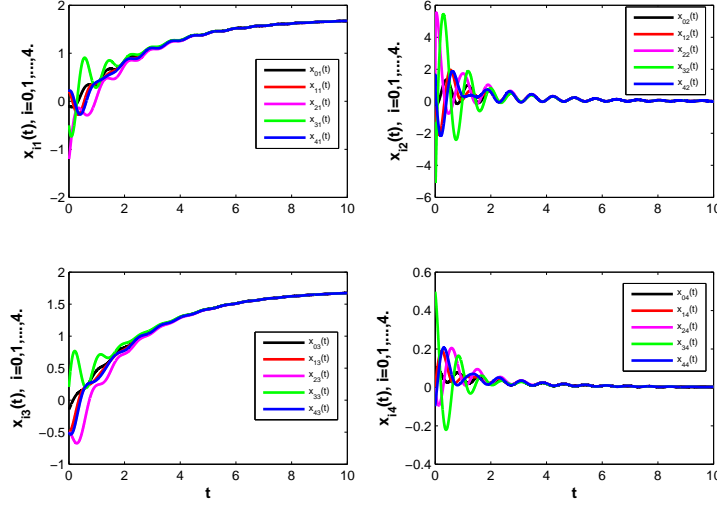


Figure 5.4: State trajectories $x_{ij}(t)$, $i = 0, 1, 2, \dots, 4$, $j = 1, 2, 3, 4$ under (5.5).

$\delta = 15.5 > \delta_{th}$. It follows from Theorem 5.1 that mean-square consensus tracking can be achieved if the ADT satisfies $T_a = 1 > T_a^* = \frac{\ln(\mu_1)}{\tau} = 0.5257$. The state trajectories of the close-loop multi-agent systems (5.6) are shown in Fig. 5.4.

Example 5.2. *Mixed Connectivity-Maintained/Broken Attacks*

In this example, consensus tracking for multi-agent systems with connectivity-maintained/broken attacks is numerically studied. The agent dynamics are taken as the same as those in Example 5.1. According to Definitions 5.1 and 5.2, the switching topologies \mathcal{G}_3 , \mathcal{G}_4 , and \mathcal{G}_5 caused by one connectivity-maintained attack and two different connectivity-broken attacks are shown in Fig. 5.5, respectively. It can be seen from Fig. 5.5 that only network topology \mathcal{G}_3 contains a directed spanning tree with agent 0 as the leader, while the two other network topologies \mathcal{G}_4 , and \mathcal{G}_5 are paralyzed topologies without a directed spanning tree.

According to Algorithm 5.4, Some calculations give the parameters $\tilde{\theta}_s = 1$, $\mu_2 = 2$, $\tilde{\lambda}_0 = 0.7134$, and $\frac{d}{\lambda_0} = 6.7281$. Set the coupling strength $\gamma = 8$, it follows from Theorem 5.2 that mean-square consensus tracking for system with protocol (5.29) can be achieved if two conditions in (5.35) and (5.36) are satisfied. The total activation

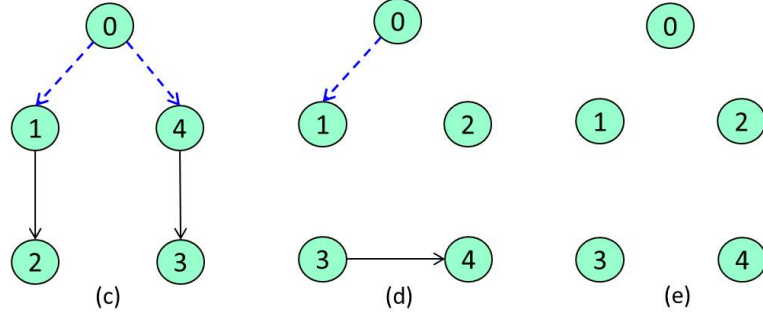


Figure 5.5: Switching topologies \mathcal{G}_3 , \mathcal{G}_4 , and \mathcal{G}_5 in Example 5.2.

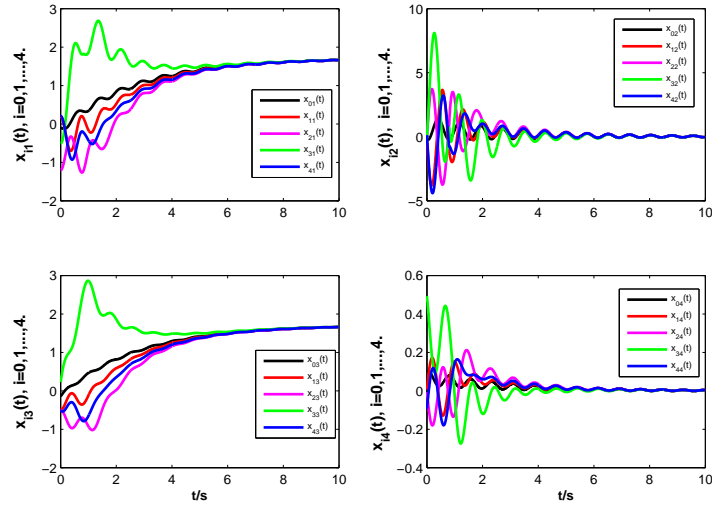


Figure 5.6: State trajectories $x_{ij}(t)$, $i = 0, 1, 2, \dots, 4$, $j = 1, 2, 3, 4$ under (5.29).

time of the connectivity-maintained and broken attacks is 8.4s and 1.6s, respectively. The state trajectories of systems (5.6) are shown in Fig. 5.6. It can be seen from Fig. 5.6 that the four followers achieve consensus and track the leader, respectively. The details on the conditions provided in Theorem 5.2 are shown as follows.

As given in (5.36), the *connectivity-broken attack frequency* $F_f(t_0, t)$ is

$$F_f(t_0, t) = \frac{N_f(t_0, t)}{t - t_0} \leq F_f^* = \frac{\eta^* - \eta}{2 \ln(\mu)} = \frac{0.41 - 0.01}{2 \ln(2)} = 0.2886, \quad (5.54)$$

which implies that attacks cannot happen more than 0.2886 times in a unit time.

Besides, it follows from (5.35) that the *connectivity-broken attack length rate* is

$$\frac{T_b(t_0, t)}{t - t_0} \leq \frac{\beta - \eta^*}{\alpha + \beta} = \frac{1.51 - 0.41}{5.1 + 1.51} = 0.1664, \quad (5.55)$$

which means that average recovery time is less than $\frac{\beta - \eta^*}{(\alpha + \beta)F_f(t_0, t)} = 0.5766$ unit time.

Example 5.3. A Power Network Example Under Attacks

A power network example is considered here. The distributed voltage regulation of microgrid is formulated as a consensus tracking problem, where all DGs try to synchronize their terminal voltage amplitude to a reference value. However, this system is vulnerable to cyber attacks as the communication lines connected among DGs might be subject to attacks. A power system from [121] is used and its single-line diagram is shown in Fig. 5.7 (a), while the network graph is given in Fig. 5.7 (b). The red nodes are generator nodes whose edges are attacked, while the rest are load nodes. The detailed attack cases are shown in Fig. 5.7 (b): (i)-(iv). The parameters of the DGs, lines, and loads are adopted from [121]. The goal is to design a distributed algorithm such that $y_i \rightarrow y_0$, where $\dot{y}_i = Ay_i + Bu_i$ and $\dot{y}_0 = Ay_0$ with $y_i = [v_{o, magi}, \dot{v}_{o, magi}]^T$, $y_0 = [v_{ref}, 0]^T$, $B = [0, 1]^T$, and $A = [0, 1; 0, 1]^T$.

Constructing (5.33) with parameters $d = 4.0$, $\rho = 0$, $\alpha = 5.2$, and $\beta = 1.6$ yields $F = [0.8262, 1.0185]$. It is assumed that the microgrid is islanded from the main grid at $t = 0$, while the secondary control is active at $t = 1.2$. Fig. 5.8 shows the DG terminal voltage amplitudes under attacks and the reference voltage value is set to 1 p.u. As analyzed in Section 5.4, Fig. 5.8: (a) implies that the distributed secondary control can regulate the DG terminal voltage amplitude to the prespecified reference value under the connectivity-maintained attacks, while Fig. 5.8: (b) shows that it fails under the connectivity-broken attacks. Fortunately, Fig. 5.8: (c) presents that under mix connectivity-maintained/broken attacks, the DG terminal voltage amplitude can track the prespecified reference value if conditions in Theorem 5.2 are satisfied. Fig. 5.8: (d) shows the switching signal $\tilde{\sigma}(t) \in \tilde{\Xi}$.

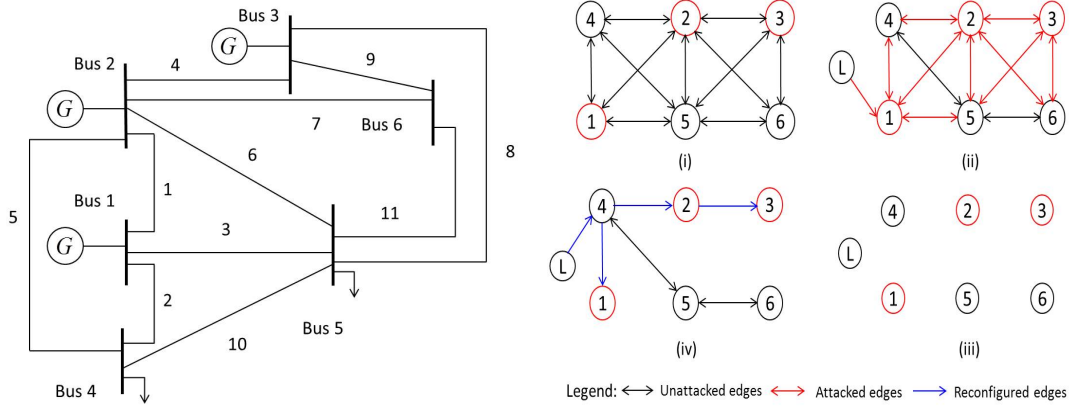


Figure 5.7: IEEE 6-bus test system: (a) the single-line diagram, (b) the corresponding communication graph under attacks.

5.6 Conclusion

In this chapter, a distributed secure consensus tracking problem is studied for multi-agent systems under two types of attacks. We formulate this problem from the perspective of a switched system subject to connected and paralyzed topologies caused by different attacks. Under the proposed distributed secure protocols, sufficient conditions on secure consensus tracking are derived.

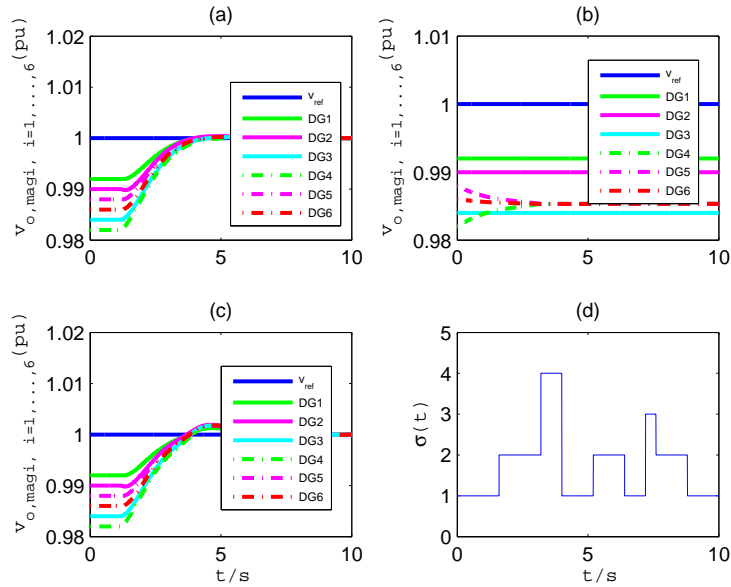


Figure 5.8: (a), (b) and (c) represent DG voltage magnitudes under different attack cases, respectively. (d) represents the signal $\tilde{\sigma}(t) \in \tilde{\Xi}$.

Chapter 6

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

6.1 Introduction

As stated in Chapter 5, two types of attacks, connectivity-maintained/broken attacks, were studied and a hybrid secure control scheme was provided. However, on one hand, the attacks on graphs are modeled by using a deterministic switching signal that determines the switching among various network topologies. That is, it is assumed that the system has complete access to the attacker moves. This similar switching attacks are also considered in [136] from the perspective of sliding mode. On the other hand, sufficient conditions for existence of consensus algorithms are established by solving two linear matrix inequalities (LMIs) to get a common solution for designing Lyapunov functions afterwards. The set of LMIs are dependent on the eigenvalues of the Laplacian matrix of all the information graph topologies. Besides, the time-complexity of solving an LMI is $O(N^2s^4)$, where N and s are the number of agents and the dimension number of agent dynamics, respectively. Overall, LMI techniques are conservative.

In this chapter, a distributed secure coordinated control problem is addressed for linear multi-agent systems under strategic attacks in cyber space whose dynamics are captured by a random Markov process. Exponential consensus tracking in mean-square sense is achieved based on a novel hybrid stochastic secure control approach, provided that two conditions are satisfied with respect to the attack frequency and attack length rate. A piecewise quadratic Lyapunov function is explored, which is determined by solving an algebraic Riccati equation and an algebraic Riccati inequality and the existence of solutions can be guaranteed [137,138]. Compared with the existing works, the main contributions of this chapter are summarized:

1. In contrast to consensus problems for lower-order multi-agent systems, we consider both continuous-time and discrete-time linear agent dynamics. The open-loop system matrix of linear agent dynamics may not contain stable eigenvalues as required in [26,27,124].
2. Different from deterministic attacks in [95], this work studies strategic attacks, whose dynamics are captured by a random Markov process. A connectivity restoration mechanism is assumed such that after a short period of time, the networks can recover from attacks. A switching sequence forms a random Markov chain to model strategic attacks.
3. An explicit analysis of the attack frequency and length rate is provided to achieve secure consensus tracking. By virtue of a slowly switching mechanism, certain conditions are obtained to ensure that the attacks do not occur frequently and the average recovery time is not too large.
4. Different from solving two LMIs to obtain a common solution in [95], the distributed controllers can be designed by solving the algebraic Riccati equation and inequality, with the time-complexity of $O(s^4)$ [137], which are independent of graphs under strategic attacks.

The rest of the chapter is organized as follows. The distributed secure coordinated control problem is formulated in Section 6.2. The main results are presented in Section 6.3. The distributed design and stability analysis are first developed for continuous-time systems under attacks. Then, an extension to discrete-time case is studied. In Section 6.4, numerical examples are provided to verify the effectiveness of the proposed methods. A brief conclusion on this chapter is given in Section 6.5.

6.2 Problem Formulation

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

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad t \in \mathbb{R}_{\geq 0}, \quad (6.1)$$

$$x_i(t+1) = \tilde{A}x_i(t) + \tilde{B}u_i(t), \quad t \in \mathbb{N}_0, \quad (6.2)$$

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

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

$$\delta_i(t) = \sum_{j=1}^N a_{ij}(x_i(t) - x_j(t)) + b_i(x_i(t) - x_0(t)), \quad (6.3)$$

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

The objective of distributed coordination is to design

$$u_i(t) = -cK\delta_i(t), \quad i = 1, 2, \dots, N, \quad (6.4)$$

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

6.2.1 Attack Model

In [95], two types of attacks are modeled by using a deterministic switching signal to determine switchings among various network topologies. The model in [95] assumes that the system has complete access to the attacker moves. In this work, we study a new attack model partly motivated by [133] and [134].

Cyber System: Different from [95], the state of cyber systems is described by $\theta(t)$. The evolution of $\theta(t)$ depends on the attacker's action a and cyber defense action d . For a given pair (a, d) , $\theta(t)$ is modeled as a right-continuous, time-homogeneous, ergodic, random Markov process. $\mathcal{S} = \{1, 2, \dots, s\}$ is the finite state space corresponding to all possible topologies under attacks. Let the infinitesimal generator of Markov process be $\Upsilon = (\gamma_{pq})$, which is given by

$$P_{pq}(t) = \Pr\{r(t+h) = q | r(t) = p\} = \begin{cases} \gamma_{pq}h + o(h), & p \neq q, \\ 1 + \gamma_{pp}h + o(h), & p = q, \end{cases} \quad (6.5)$$

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

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

$$f(k) = [f_p(k)]_{p=1}^n \in \mathcal{F}_k, \quad g(k) = [g_q(k)]_{q=1}^m \in \mathcal{G}_k, \quad (6.6)$$

$$\tilde{\mathcal{F}}_k : = \{f(k) \in [0, 1]^n : \sum_{p=1}^n f_p(k) = 1\}, \quad (6.7)$$

$$\tilde{\mathcal{G}}_k : = \{g(k) \in [0, 1]^m : \sum_{q=1}^m g_q(k) = 1\}, \quad (6.8)$$

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

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

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

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

$$\gamma_{pq}(f(k), g(k)) = \sum_{p=1}^n \sum_{q=1}^m f_p(k) g_q(k) \tilde{\gamma}_{pq}(k). \quad (6.9)$$

6.2.2 Hybrid Stochastic Secure Control Framework

In a networked multi-agent system, an interaction between the physical space and cyber space is captured by their dynamics. Clearly, equations (6.1) and (6.5) describe a hybrid system with continuous-time and discrete-time states. The multi-agent physical system state $x_i(t)$ is controlled by a distributed secure controller $u_i(t)$. In cyber space under attacks modeled by a random Markov jump process, the cyber system state $\theta(t)$ is controlled by a cyber defense mechanism d used by the network administrator as well as the attacker's action a . The attacker intends to remove the connection edges in a networked multi-agent system by launching strategic attacks on graphs, which results in all kinds of new possible graph topologies. These topologies are paralyzed when the graph connectivity is broken. A distributed secure control algorithm will be developed such that the network won't lose secure consensus performance. The hybrid nature of systems leads to the adoption of a class of hybrid systems model. Thus, a hybrid stochastic secure control framework for networked multi-agent systems is illustrated in Fig. 6.1.

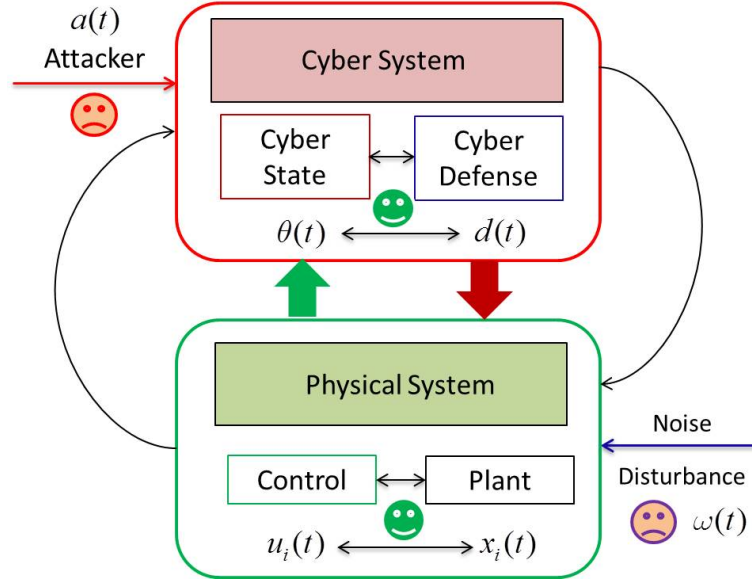


Figure 6.1: Hybrid stochastic secure control framework in a multi-agent system.

6.2.3 Control Objective

The objective is to design a distributed secure control law $u_i(t)$ for multi-agent systems (6.1) with strategic attacks on communication graphs modeled by a random Markov jump process. Thus, a secure consensus problem is defined as follows.

Definition 6.1. Mean-Square Consensus under Strategic Attacks

The distributed secure control law $u_i(t)$ is said to solve a secure consensus tracking problem in a mean-square sense for multi-agent systems (6.1) under strategic attacks, if there exist a scalar $\kappa > 0$ and a decay rate $\rho > 0$ such that for all $t > t_0$,

$$E \{ \|x_i(t) - x_0(t)\|^2 \} \leq \kappa e^{-\rho(t-t_0)} E \{ \|x_i(t_0) - x_0(t_0)\|^2 \}. \quad (6.10)$$

6.3 Mean-Square Consensus Under A Class of Strategic Attacks

Based on the attack model in subsection 6.2.1, a distributed secure consensus tracking control problem will be studied for multi-agent systems (6.1) under strategic attacks. In the context of multi-agent systems, the initial connectivity graph of the agents often meets some connection conditions [72]. Thus, motivated by this

observation, we assume that the initial graph without being attacked by any strategic attacks contains a directed spanning tree with the leader being the root. However, strategic attacks satisfying a random Markov jump process may make the networks paralyzed as the connectivity is broken, which results in the loss of secure consensus for systems. Next, the following graph description under attacks is presented.

6.3.1 Time-varying Markovian Graph

Based on descriptions of attack model in Section 6.2.1, let $\mathcal{G}_{r(t)} = \{\mathcal{V}, \mathcal{E}_{r(t)}, A_{r(t)}\}$ represent a directed time-varying graph of order N with the set of nodes \mathcal{V} , $\mathcal{E}_{r(t)}$ is the set of edges and $A_{r(t)} = [a_{ij}^{r(t)}] \in \mathbb{R}^{N \times N}$ denotes the adjacency matrix of $\mathcal{G}_{r(t)}$, where $a_{ij}^{r(t)} > 0$ if and only if $(j, i) \in \mathcal{E}_{r(t)}$ else $a_{ij}^{r(t)} = 0$. An edge of $\mathcal{G}_{r(t)}$ is an ordered pair $(i, j) \in \mathcal{E}_{r(t)}$ if agent j can be directly supplied with information from agent i . The set of neighbors of node v_i is denoted by $\mathcal{N}_{r(t)} = \{v_i \in \mathcal{V}, (v_j, v_i) \in \mathcal{E}_{r(t)}, j \neq i\}$. Graph $\mathcal{G}_{r(t)}$ contains a directed spanning tree if there is a node which can reach all the other nodes through a directed path. The Laplacian matrix of a graph $\mathcal{G}_{r(t)}$ is defined as $\mathcal{L}_{r(t)} = D_{r(t)} - A_{r(t)} \in \mathbb{R}^{N \times N}$, where $D_{r(t)} = \text{diag}\{d_1^{r(t)}, d_2^{r(t)}, \dots, d_N^{r(t)}\}$ with $d_i^{r(t)} = \sum_{j=1}^N a_{ij}^{r(t)}$. Thus, an information-exchange matrix for consensus tracking is written as $H_{r(t)} = \mathcal{L}_{r(t)} + \mathcal{B}_{r(t)}$, where $\mathcal{B}_{r(t)} = \text{diag}\{b_1^{r(t)}, b_2^{r(t)}, \dots, b_N^{r(t)}\}$ represents the access of followers to the leader under attacks. If $b_i^{r(t)} = 1$, the i th agent accesses to leader, and $b_i^{r(t)} = 0$, otherwise.

6.3.2 Connectivity Restoration Mechanism

In order to achieve secure consensus tracking for systems (6.1) under strategic attacks, the following assumption introduces a connectivity recovery mechanism.

Assumption 6.1. $\mathcal{G}_{r(t)}$ can be recovered into connectivity-maintained topologies after a connectivity restoration mechanism (i.e., the sensing and communication devices are able to recover through some backup or repairing efforts).

Remark 6.1. *Although the initial graph without being attacked can provide the possibility of consensus tracking for system (6.1), each paralyzed topology $\mathcal{G}_{r(t)}$ under strategic attacks might totally destroy the secure consensus performance of the whole multi-agent systems. Thus, Assumption 6.1 implies that the secure consensus tracking problem can be solved if there exists a connectivity restoration mechanism through internal recovery/tolerance capacities of the system or repairing efforts, even though it may take a short period of time.*

6.3.3 Distributed Secure Control Law Design

Without loss of generality, one may suppose that there exists an infinite sequence $k = 0, 1, 2, \dots$, for $[t_{2k}, t_{2(k+1)})$, such that when $t = t_{2k+1}$, the multi-agent system is subject to strategic attacks. That is, the multi-agent network $\mathcal{G}_{r(t)}$ is paralyzed during $[t_{2k+1}, t_{2(k+1)})$, while it works well during $[t_{2k}, t_{2k+1})$ for an initial graph \mathcal{G}_0 without being attacked by any strategic attacks. Based on the recovery mechanism in Assumption 6.1, when $t = t_{2k}^+$, the multi-agent network is recovered to a connectivity-maintained topology.

The objective is to construct a distributed control law to achieve secure consensus tracking for system (6.1) under strategic attacks. Specifically, based on the above analysis the protocol can be designed as

$$u_i(t) = \begin{cases} \varrho K[\sum_{j=1}^N a_{ij}^0(x_j(t) - x_i(t)) + b_i^0(x_0(t) - x_i(t))], \\ \quad t \in [t_{2k}, t_{2k+1}), \\ \\ \vartheta F[\sum_{j=1}^N a_{ij}^{r(t)}(x_j(t) - x_i(t)) + b_i^{r(t)}(x_0(t) - x_i(t))], \\ \quad t \in [t_{2k+1}, t_{2(k+1)}), \end{cases} \quad (6.11)$$

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

Denote the state tracking error between the followers and the leader as $e_i(t) = x_i(t) - x_0(t)$ and let $e(t) = (e_1^T(t), e_2^T(t), \dots, e_N^T(t))^T$. Then, substituting (6.11) into the multi-agent system (6.1) yields the following closed-loop error dynamic system in a compact form

$$\dot{e}(t) = \begin{cases} [I_N \otimes A - \varrho(H_0 \otimes BK)]e(t), & t \in [t_{2k}, t_{2k+1}), \\ [I_N \otimes A - \vartheta(H_{r(t)} \otimes BF)]e(t), & t \in [t_{2k+1}, t_{2(k+1)}), \end{cases} \quad (6.12)$$

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

6.3.4 Attack Frequency and Attack Length Rate

Based on [95], it is obvious that the attack amount is not arbitrary and suitable conditions must be imposed. Motivated by a slowly switching mechanism in [118], the following definitions are introduced to solve the studied problem.

Definition 6.2. (*Attack Frequency*) For any $T_2 > T_1 \geq t_0$, let $N_f(T_1, T_2)$ denote the number of attacks taking place over $[T_1, T_2)$. Thus, $F_f(T_1, T_2) = \frac{N_f(T_1, T_2)}{T_2 - T_1}$ is defined as the attack frequency over $[T_1, T_2)$ for all $T_2 > T_1 \geq t_0$.

Definition 6.3. (*Attack Length Rate*) For any $t > 0$, denote $T_a(t_0, t)$ as the total time interval for multi-agent systems under attacks during $[t_0, t)$. Thus, $\frac{T_a(t_0, t)}{t - t_0}$ is defined as the attack length rate over $[t_0, t)$.

Remark 6.2. Note that H_0 is a nonsingular matrix, while $H_{r(t)}$ may be a reducible matrix. Even though H_0 provides the possibility of consensus tracking, the existence of paralyzed topologies $H_{r(t)}$ may totally destroy the secure consensus tracking performance. To overcome this difficulty, suitable conditions must be imposed on both attack frequency and length rate as it is important to determine the amount of attacks that a system can tolerate before undergoing instability.

6.3.5 Stability Analysis

The following two lemmas are provided as a basis for developments of main results.

Lemma 6.1. *For multi-agent systems (6.1) without being attacked by any strategic attacks, if there exists a unique symmetric positive definite matrix $P > 0$ such that the following algebraic Riccati equation (ARE) is satisfied*

$$PA + A^T P - PBR^{-1}B^T P + Q = 0, \quad (6.13)$$

where $R > 0$ and $Q > I$ are two symmetric positive definite matrices. Then, under the proposed distributed controller (6.11), for a selected Lyapunov function $V_a(e(t))$ and a positive constant $\alpha = \lambda_{\min}(Q)/\lambda_{\max}(P) > 0$, it holds that

$$V_a(e(t)) \leq e^{-\alpha(t-t_0)} V_a(e(t_0)). \quad (6.14)$$

Proof. Choose a Lyapunov function candidate as:

$$V_a(e(t)) = \sum_{i=1}^N e_i^T(t) \theta_i^{-1} P e_i(t), \quad i = 1, 2, \dots, N, \quad (6.15)$$

where θ_i^{-1} is similarly given as in Lemma 4 [135] such that $\Phi = \Theta H_0 + H_0^T \Theta > 0$.

One such Θ is given by $\text{diag}\{\theta_1^{-1}, \dots, \theta_N^{-1}\}$ where $\theta = [\theta_1^{-1}, \dots, \theta_N^{-1}]^T = (H_0^T)^{-1} \mathbf{1}$.

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

$$\begin{aligned} \dot{V}_a(e(t)) &= e^T(t) (\Theta \otimes PA + \Theta \otimes A^T P) e(t) \\ &\quad - \varrho e^T(t) ((\Theta H_0 + H_0^T \Theta) \otimes PBK) e(t). \end{aligned} \quad (6.16)$$

Denote $\theta_{\min} = \min_i \theta_i$, $i = 1, 2, \dots, N$, and $\lambda_{\min} = \lambda_{\min}(\Phi)$. Substituting $K = R^{-1}B^T P$ into (6.16) yields

$$\begin{aligned} \dot{V}_a(e(t)) &= e^T(t) (\Theta \otimes PA + \Theta \otimes A^T P) e(t) \\ &\quad - \varrho e^T(t) ((\Theta H_0 + H_0^T \Theta) \otimes PBR^{-1}B^T P) e(t) \\ &\leq e^T(t) (\Theta \otimes (PA + A^T P)) e(t) - \varrho \lambda_{\min} \theta_{\min} \\ &\quad \times e^T(t) (\Theta \otimes PBR^{-1}B^T P) e(t). \end{aligned} \quad (6.17)$$

Provided the coupling strength $\varrho > (\lambda_{\min}\theta_{\min})^{-1}$, it follows from (6.13) that the expression in (6.17) can be rewritten as

$$\begin{aligned}\dot{V}_a(e(t)) &\leq e^T(t)[\Theta \otimes (PA + A^T P - PBR^{-1}B^T P)]e(t) \\ &= -e^T(t)(\Theta \otimes Q)e(t).\end{aligned}\tag{6.18}$$

Given that $-Q \leq -\lambda_{\min}(Q)I = -\alpha\lambda_{\max}(P)I \leq -\alpha P$ and $\alpha = \lambda_{\min}(Q)/\lambda_{\max}(P)$, (6.18) is further rewritten as

$$\dot{V}_a(e(t)) \leq -\alpha e^T(t)(\Theta \otimes P)e(t) = -\alpha V_a(e(t)).\tag{6.19}$$

Integrating both sides of (6.18) over $[t_0, t]$ leads to (6.14) in Lemma 6.1. \square

Next, we consider that the multi-agent system (6.1) is subject to strategic attacks satisfying a random Markov process. Before presenting the result, the following assumption is given on possible graphs under strategic attacks.

Assumption 6.2. *The paralyzed topology $\mathcal{G}_{r(t)}$ under strategic attacks are balanced and the union of all digraphs consisting of the leader and the N followers contains a spanning tree rooted at the leader.*

Lemma 6.2. *For multi-agent systems (6.1), if there exists a symmetric positive definite matrix $S > 0$ such that the following ARI is satisfied*

$$SA + A^T S - SBT^{-1}B^T S - \beta S < 0,\tag{6.20}$$

where $T > 0$ is a symmetric positive definite matrix, then, under the proposed distributed controller (6.11) with Assumption 6.2, for a selected Lyapunov function $V_b(e(t))$ and a constant $\beta > 0$, the following expression can be obtained:

$$E\{V_b(e(t))\} \leq e^{\beta(t-t_0)} E\{V_b(e(t_0))\}.\tag{6.21}$$

Proof. Choose a Lyapunov function candidate as

$$V_b(e(t)) = \sum_{i=1}^N e_i^T(t) S e_i(t), \quad i = 1, 2, \dots, N.\tag{6.22}$$

Based on (Lemma 4.2, [139]), the stochastic Lyapunov function of (6.22) w.r.t the Markov jump process is

$$V_b^p(e(t)) = E[e^T(t)(I_N \otimes S)e(t)\chi_{\{r(t)=p\}}], \forall p \in \mathcal{S}, \quad (6.23)$$

where $r(t)$ used to model the strategic attacks on graphs is given in Section 6.2.1 and for a real function $r(t)$, its indicator function of event $r(t) = p$ is defined by

$$\chi_{\{r(t)=p\}} = \begin{cases} 1, & \text{if } r(t) = p, \\ 0, & \text{if } r(t) \neq p. \end{cases} \quad (6.24)$$

Based on (Lemma 4.2 in [139]), the stochastic derivative of $V_b^p(e(t))$ along the closed-loop error system is expressed as

$$\begin{aligned} V_b^p(e(t)) &= E[(de(t))^T(I_N \otimes S)e(t)\chi_{\{r(t)=p\}}] + E[e^T(t)(I_N \otimes S)de(t)\chi_{\{r(t)=p\}}] \\ &\quad + \sum_{q=1}^s \gamma_{qp} V_b^q(e(t))dt + o(dt) \\ &= E\{e^T(t)[I_N \otimes SA + I_N \otimes A^T S - \vartheta(H_p \otimes SBF + (H_p \otimes SBF)^T)]e(t) \\ &\quad + \sum_{q=1}^s \gamma_{qp} V_b^q(e(t))dt + o(dt)\}, \end{aligned} \quad (6.25)$$

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

Suppose that the signal $\gamma(t)$ starts at an invariant distribution $\pi = [\pi_1, \dots, \pi_s]$ as given in [140], selecting $\vartheta \geq (2\pi_{\min}\lambda_{\min}(\hat{H}_{un}))^{-1}$ with $\pi_{\min} = \min_{p \in \mathcal{S}}\{\pi_p\}$, $\mathcal{S} = \{1, 2, \dots, s\}$, and substituting the controller gain matrix $F = T^{-1}B^T S$ into (6.25) yield the following expression by bearing in mind that $\pi_p \geq \pi_{\min}$,

$$\begin{aligned} \frac{dV_b(e(t))}{dt} &\leq E[e^T(t)(I_N \otimes SA + I_N \otimes A^T S)e(t)] \\ &\quad - E[e^T(t)(\tilde{H} \otimes SBT^{-1}B^T S)e(t)], \end{aligned} \quad (6.26)$$

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

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

$$\begin{aligned} & e^T(t)[I_N \otimes (SA + A^T S) - \tilde{H} \otimes SBT^{-1}B^T S]e(t) \\ &= \sum_{j=1}^N \tilde{e}_j^T(t)(SA + A^T S - \frac{\lambda_j(\hat{H}_{un})}{\lambda_{\min}(\hat{H}_{un})} SBT^{-1}B^T S)\tilde{e}_j(t) \\ &\leq \sum_{j=1}^N \tilde{e}_j^T(t)(SA + A^T S - SBT^{-1}B^T S)\tilde{e}_j(t). \end{aligned} \quad (6.27)$$

Since $SA + A^T S - SBT^{-1}B^T S - \beta S < 0$ in (7.59), (6.26) is rewritten as

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

which yields (6.21) and the proof is completed. \square

Next, a multi-step design procedure is developed for (6.11).

Algorithm 6.1 Controller Parameter Design for (6.11).

Under Assumptions 6.1 and 6.2, the proposed distributed control law (6.11) can be constructed as follows.

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

$$PA + A^T P - PBR^{-1}B^T P + Q = 0, \quad (6.28)$$

to get a matrix $P > 0$.

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

$$SA + A^T S - SBT^{-1}B^T S - \beta S < 0, \quad (6.29)$$

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

(3) Design the feedback control gains of (6.11) as

$$K = R^{-1}B^T P, \quad F = T^{-1}B^T S, \quad (6.30)$$

where $R > 0$ and $T > 0$ are two given symmetric positive definite matrices, P and S are obtained by solving ARE (6.28) and ARI (6.29), respectively.

(4) Choose the coupling strength satisfying:

$$\varrho > (\lambda_{\min} \theta_{\min})^{-1}, \quad \vartheta \geq (2\pi_{\min} \lambda_{\min}(\hat{H}_{un}))^{-1}, \quad (6.31)$$

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

Based on Algorithm 6.1, the main result is thus described as follows.

Theorem 6.1. *Consider the multi-agent systems (6.1) subject to strategic attacks. Suppose that Assumptions 6.1 and 6.2 hold. The proposed control law $u_i(t)$ in (6.11) enables secure consensus tracking in a mean-square sense, provided that*

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

$$\frac{T_a(t_0, t)}{t - t_0} \leq \frac{\alpha - \eta^*}{\alpha + \beta}. \quad (6.32)$$

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

$$F_f(t_0, t) = \frac{N_f(t_0, t)}{t - t_0} \leq F_f^* = \frac{\eta^* - \eta}{2 \ln(\mu)}, \quad (6.33)$$

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

Moreover, the state decay estimation is given by

$$E\{\|e_i(t)\|^2\} \leq \phi e^{-\eta(t-t_0)} E\{\|e_i(t_0)\|^2\}, \quad (6.34)$$

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

Proof. Based on Lemmas 6.1 and 6.2, the following piecewise Lyapunov-like functional candidate is defined as $V(t) = V_{\sigma(t)}(e(t))$, where $\sigma(t) = a$ or b is a switching signal, specifically, to activate the running time of the controller.

$$V(t) = \begin{cases} V_a(e(t)), & \text{if } t \in [t_{2k}, t_{2k+1}), \\ V_b(e(t)), & \text{if } t \in [t_{2k+1}, t_{2(k+1)}), \end{cases} \quad (6.35)$$

where $V_a(e(t))$ and $V_b(e(t))$ are defined in (6.15) and (6.22), respectively.

Suppose V_a is activated in $[t_{2k}, t_{2k+1})$ and V_b is activated in $[t_{2k+1}, t_{2(k+1)})$. It follows from Lemmas 6.1 and 6.2 that

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

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

Case I: if $t \in [t_{2k}, t_{2k+1})$, it follows from (6.36) that

$$\begin{aligned}
E\{V(t)\} &\leq e^{-\alpha(t-t_{2k})} E\{V_a(t_{2k})\} \leq \mu e^{-\alpha(t-t_{2k})} E\{V_b(t_{2k}^-)\} \\
&\leq \mu e^{-\alpha(t-t_{2k})} [e^{\beta(t_{2k}-t_{2k-1})} E\{V_b(t_{2k-1})\}] \\
&\leq \mu e^{-\alpha(t-t_{2k})} [e^{\beta(t_{2k}-t_{2k-1})} \mu E\{V_a(t_{2k-1}^-)\}] \\
&= \mu^2 e^{-\alpha(t-t_{2k})} e^{\beta(t_{2k}-t_{2k-1})} E\{V_a(t_{2k-1}^-)\} \\
&\leq \mu^2 e^{-\alpha(t-t_{2k})} e^{\beta(t_{2k}-t_{2k-1})} \times [e^{-\alpha(t_{2k-1}-t_{2(k-1)})} E\{V_a(t_{2(k-1)})\}] \\
&\leq \dots \\
&\leq \mu^{2k} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V_a(t_0)\}.
\end{aligned} \tag{6.36}$$

Case II: if $t \in [t_{2k+1}, t_{2(k+1)})$, it follows from (6.36) that

$$\begin{aligned}
E\{V(t)\} &\leq e^{\beta(t-t_{2k+1})} E\{V_b(t_{2k+1})\} \leq \mu e^{\beta(t-t_{2k+1})} E\{V_a(t_{2k+1}^-)\} \\
&\leq \mu e^{\beta(t-t_{2k+1})} [e^{-\alpha(t_{2k+1}-t_{2k})} E\{V_a(t_{2k})\}] \leq \dots \\
&\leq \mu^{2k+1} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V_a(t_0)\}.
\end{aligned} \tag{6.37}$$

According to Definition 6.2, $N_f(t_0, t) = k$ for $t \in [t_{2k}, t_{2k+1})$ and $N_f(t_0, t) = k + 1$ for $t \in [t_{2k+1}, t_{2(k+1)})$. Thus, for $\forall t \geq t_0$, it follows from (6.36) and (6.37) that

$$E\{V(t)\} \leq \mu^{2N_f(t_0,t)} e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} E\{V(t_0)\}. \tag{6.38}$$

Based on (6.32), it holds that

$$e^{-\alpha(t-t_0-T_a(t_0,t))} e^{\beta T_a(t_0,t)} \leq e^{-\eta^*(t-t_0)}. \tag{6.39}$$

Based on (6.33), it is clear that

$$e^{2N_f(t_0,t) \ln(\mu)} \leq e^{(\eta^*-\eta)(t-t_0)}. \tag{6.40}$$

Thus, substituting (6.39) and (6.40) into (6.38) yields

$$E\{V(t)\} \leq e^{-\eta(t-t_0)} E\{V_0(t_0)\}, \tag{6.41}$$

which yields (6.34) and the proof is finished. \square

6.3.6 Extension to Discrete-time Case

The objective is to design a distributed controller $u_i(k)$ for a discrete-time linear multi-agent system (6.2) under strategic attacks satisfying a random discrete-time Markov process with a transition probability matrix $\Lambda = (\Lambda_{pq})$, which is given by

$$\Lambda_{pq} = \text{Pr ob}\{r(k+1) = q | r(k) = p\}, \quad k \in \mathbb{N}_0. \quad (6.42)$$

Thus, a distributed secure consensus tracking control problem for discrete-time systems (6.2) is defined as follows.

Definition 6.4. *The distributed secure control law $u_i(k)$ solves a secure consensus tracking problem in a mean-square sense for discrete-time linear multi-agent system (6.2) under strategic attacks, if there exists a scalar $c > 0$ and a decay rate $0 < v < 1$ such that for all $k > k_0$,*

$$E \{ \|x_i(k) - x_0(k)\|^2 \} \leq cv^{(k-k_0)} E \{ \|x_i(k_0) - x_0(k_0)\|^2 \}.$$

Similar to Section 6.3.3, the following distributed control law is proposed to achieve secure consensus tracking

$$u_i(k) = \begin{cases} \tilde{q}\tilde{K}\delta_i^0(k), & k \in [k_{2m}, k_{2m+1}), \\ \tilde{\vartheta}\tilde{F}\delta_i^{r(k)}(k), & k \in [k_{2m+1}, k_{2(m+1)}), \end{cases} \quad (6.43)$$

where $\delta_i^{\tilde{h}}(k) = \sum_{j=1}^N a_{ij}^{\tilde{h}}(x_i(k) - x_j(k)) + b_i^{\tilde{h}}(x_i(k) - x_0(k))$, $\tilde{h} = 0, r(k)$.

Thus, substituting (6.43) into system (6.2) yields the following closed-loop error systems in a compact form

$$e(k+1) = \begin{cases} [I_N \otimes \tilde{A} - \tilde{q}(H_0 \otimes \tilde{B}\tilde{K})]e(k), & \text{if } k \in \Omega_1, \\ [I_N \otimes \tilde{A} - \tilde{\vartheta}(H_{r(k)} \otimes \tilde{B}\tilde{F})]e(k), & \text{if } k \in \Omega_2, \end{cases} \quad (6.44)$$

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

Next, sufficient conditions on secure consensus tracking are given for systems (6.2).

Algorithm 6.2 Controller Parameter Design for (6.43).

The proposed distributed control law (6.43) can be constructed as follows.

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

$$\tilde{A}^T \tilde{P} \tilde{A} - \tilde{P} - \tilde{A}^T \tilde{P} \tilde{B} (\tilde{B}^T \tilde{P} \tilde{B} + \tilde{R})^{-1} \tilde{B}^T \tilde{P} \tilde{A} + \tilde{Q} = 0, \quad (6.45)$$

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

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

$$\tilde{A}^T \tilde{S} \tilde{A} - \lambda_+ \tilde{S} - \gamma \tilde{A}^T \tilde{S} \tilde{B} (\tilde{B}^T \tilde{S} \tilde{B} + \tilde{T})^{-1} \tilde{B}^T \tilde{S} \tilde{A} < 0, \quad (6.46)$$

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

(3) Design the feedback control gains of (6.43) as

$$\tilde{K} = (\tilde{B}^T \tilde{P} \tilde{B} + \tilde{R})^{-1} \tilde{B}^T \tilde{P} \tilde{A}, \quad \tilde{F} = (\tilde{B}^T \tilde{S} \tilde{B} + \tilde{T})^{-1} \tilde{B}^T \tilde{S} \tilde{A}, \quad (6.47)$$

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

(4) Choose the coupling strength satisfying

$$|\tilde{\varrho} \lambda_i(H_0) - 1| < \gamma_0, \quad \tilde{\vartheta} \in \mathfrak{S}, \quad (6.48)$$

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

Theorem 6.2. Consider the multi-agent system (6.2) subject to strategic attacks.

Under the proposed $u_i(k)$ in (6.43), all the agents can achieve secure consensus tracking in mean-square sense, provided that

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

$$\frac{T_a(k_0, k)}{k - k_0} \leq \frac{\ln \lambda_* - \ln \lambda_-}{\ln \lambda_+ - \ln \lambda_-}. \quad (6.49)$$

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

$$F_f(k_0, k) = \frac{N_f(k_0, k)}{k - k_0} \leq F_f^* = \frac{2 \ln \lambda_d - \ln \lambda_*}{2 \ln(\tilde{\mu})}. \quad (6.50)$$

Moreover, the state decay estimation is given by

$$E\{\|e_i(k)\|^2\} \leq \tilde{\phi} v^{(k-k_0)} E\{\|e_i(k_0)\|^2\}, \quad (6.51)$$

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

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

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

(I) The system (6.2) is not subject to any attacks. Similar to the above analysis for continuous-time case, it follows from (Algorithm 6.2 and Theorem 2 in [138]) that $\Delta \tilde{V}_a(e(k)) \leq -e^T(k) \tilde{Q} e(k) \leq -\lambda_a \tilde{V}_a(e(k))$, $\lambda_a = \lambda_{\min}(\tilde{Q})/\lambda_{\max}(\tilde{P}) \in (0, 1)$, which implies that

$$\tilde{V}_a(k+1) \leq \lambda_- \tilde{V}_a(k), \quad \lambda_- = 1 - \lambda_a < 1. \quad (6.52)$$

(II) The system (6.2) is subject to strategic attacks on graphs. Similarly, it gets that since $\gamma(k)$ starts at the invariant distribution $\tilde{\pi}$, it follows from $\tilde{\pi} \geq \tilde{\pi}_{\min}$ that

$$\begin{aligned} \Delta \tilde{V}_b(e(k)) - \lambda_b \tilde{V}_b(e(k)) &\leq E\{e^T[I_N \otimes \tilde{A}^T \tilde{S} \tilde{A} + \tilde{\vartheta}^2(\sum_{p=1}^s H_p^T H_p) \otimes \tilde{F}^T \tilde{B}^T \tilde{S} \tilde{B} \tilde{F}] \\ &\quad - 2\tilde{\vartheta} \tilde{\pi}_{\min} \lambda_{\min}(\hat{H}_{un}) \frac{H_{un} + H_{un}^T}{2\lambda_{\min}(\hat{H}_{un})} \otimes \tilde{A}^T \tilde{S} \tilde{B} \tilde{F}]\} e(k) \\ &\quad - \lambda^+ E\{e^T(k)(I_N \otimes \tilde{S})e(k)\}. \end{aligned} \quad (6.53)$$

Substituting $\tilde{F} = (\tilde{B}^T \tilde{S} \tilde{B} + \tilde{T})^{-1} \tilde{B}^T \tilde{S} \tilde{A}$ into (6.53) and it follows from Algorithm 6.3.6 and Theorem 1 in [138] that $\Delta \tilde{V}_b(e(k)) - \lambda_b \tilde{V}_b(e(k)) \leq 0$ holds, which means

$$E\{\tilde{V}_b(k+1)\} \leq \lambda_+ E\{\tilde{V}_b(k)\}, \quad \lambda_+ = 1 + \lambda_b > 1. \quad (6.54)$$

(III) Synthesizing the above two circumstances (I)-(II) into one, it follows from (6.52) and (6.54) that for any $k > 0$,

$$E\{\tilde{V}(k)\} \leq \begin{cases} \lambda_-^{k-k_{2m}} E\{\tilde{V}_a(k_{2m})\}, & \text{if } k \in \Omega_1, \\ \lambda_+^{k-k_{2m+1}} E\{\tilde{V}_b(k_{2m+1})\}, & \text{if } k \in \Omega_2, \end{cases} \quad (6.55)$$

where $0 < \lambda_- = 1 - \lambda_a < 1$ and $\lambda_+ = 1 + \lambda_b > 1$ imply that the Lyapunov function along systems (6.44) has an exponential decay rate λ_- or increase rate λ_+ .

Similar to (6.36) and (6.37) in Theorem 6.1, we can obtain

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

$$\begin{aligned}
E\{\tilde{V}(k)\} &\leq \lambda_+^{k-k_{2m+1}} E\{\tilde{V}_b(k_{2m+1})\} \leq \tilde{\mu} \lambda_+^{k-k_{2m+1}} E\{\tilde{V}_a(k_{2m+1}^-)\} \\
&\leq \tilde{\mu} \lambda_+^{k-k_{2m+1}} \lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_a(k_{2m})\} \leq \tilde{\mu}^2 \lambda_+^{k-k_{2m+1}} \lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_b(k_{2m}^-)\} \\
&\leq \tilde{\mu}^3 \lambda_+^{k-k_{2m+1}+k_{2m}-k_{2m-1}} \lambda_-^{k_{2m+1}-k_{2m}} E\{\tilde{V}_a(k_{2m-1}^-)\} \leq \cdots \\
&\leq \tilde{\mu}^{2m+1} \lambda_+^{T_a(k_0, k)} \lambda_-^{k-k_0-T_a(k_0, k)} E\{\tilde{V}_a(k_0)\}. \tag{6.56}
\end{aligned}$$

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

$$E\{\tilde{V}(k)\} \leq \tilde{\mu}^{2m} \lambda_+^{T_a(k_0, k)} \lambda_-^{k-k_0-T_a(k_0, k)} E\{\tilde{V}_a(k_0)\}. \tag{6.57}$$

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

$$E\{\tilde{V}(k)\} \leq \tilde{\mu}^{2N_f(k_0, k)} \lambda_+^{T_a(k_0, k)} \lambda_-^{k-k_0-T_a(k_0, k)} E\{\tilde{V}_a(k_0)\}. \tag{6.58}$$

Based on (6.49), it holds that

$$(\ln \lambda_- - \ln \lambda_+) T_a(k_0, k) \geq (\ln \lambda_- - \ln \lambda_*)(k - k_0). \tag{6.59}$$

Based on (6.50), it is clear that

$$\tilde{\mu}^{2N_f(k_0, k)} \leq e^{(2 \ln \lambda_- - \ln \lambda_*)(k-k_0)} = \left(\frac{\lambda_-^2}{\lambda_*}\right)^{k-k_0}. \tag{6.60}$$

Thus, substituting (6.59) into (6.58) yields: $E\{\tilde{V}(k)\} \leq \lambda_d^{2(k-k_0)} E\{\tilde{V}(k_0)\}$, which implies (6.51) in Theorem 6.2 and the proof is finished. \square

Remark 6.3. Theorems 6.1 and 6.2 show mean-square exponential consensus tracking. The divergence of tracking errors with the exponential increasing rates β in (6.21) and λ_+ in (6.54) are caused by strategic attacks. Fortunately, it follows from conditions (6.32) and (6.33) for continuous-time case and conditions (6.49) and (6.50) for discrete-time case that exponential convergence with decay rates η and v are eventually obtained in (6.34) and (6.51), respectively.

6.4 Numerical Example

Two numerical examples are provided to demonstrate the effectiveness of our approaches for systems under strategic attacks.

Example 6.1. *Continuous-Time Consensus Tracking*

In this example we consider a cooperative tracking problem with 1 leader agent and 6 follower agents. Each agent is a two-mass-spring system with a single force input, except for the leader agent, which is unforced. The dynamics of the i th agent are given in the form of (6.1) as provided in [141]:

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad t \in \mathbb{R}_{\geq 0}, \quad (6.61)$$

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

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

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

Let these agents receive information from their neighbors according to a communication topology. As described in Section 6.2.1, we consider two cases:

(1) When the cyber system is not subject to an attack, the communication topology is shown in Fig. 6.2(a).

(2) When the cyber system is under strategic attacks modeled by a random Markov jump process, the communication topologies are shown in Fig. 6.2 (b)-(d). It can be seen that each topology $\mathcal{G}_{r(t)}$, $r(t) = 1, 2, 3$, is paralyzed while the union of $\mathcal{G}_{r(t)}$ has a spanning tree satisfying Assumption 6.2.

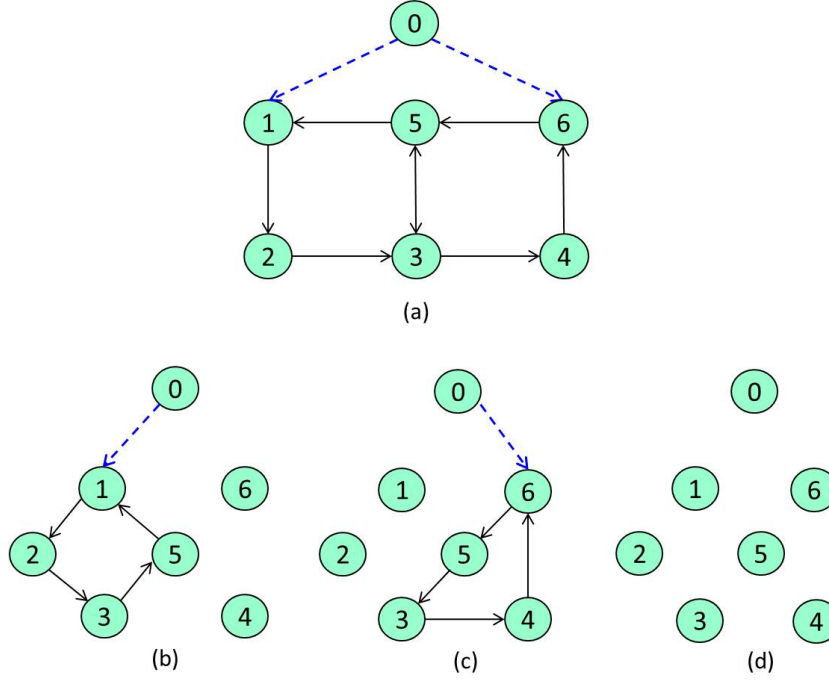


Figure 6.2: Initial communication topologies \mathcal{G}_0 (a) and topologies under strategic attacks $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ (b-(d)) in Example 6.1.

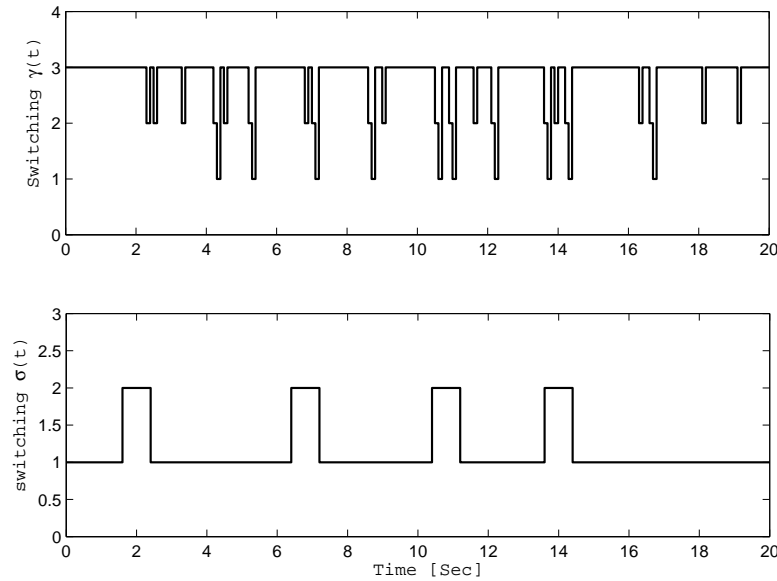
The objective of the secure consensus tracking control problem in mean-square sense is to design a distributed secure controller $u_i(t)$ for systems (6.61) under strategic attacks modeled by a random Markov jump process.

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

$$\Upsilon = \begin{bmatrix} -0.1 & 0.02 & 0.08 \\ 0.3 & -0.5 & 0.2 \\ 0.1 & 0.1 & -0.2 \end{bmatrix}, \quad (6.62)$$

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

Based on Algorithm 6.1, constructing (6.11) with $R = 2$, $T = 0.05$, $Q = 10I$, I is a 4×4 identity matrix, $\alpha = 4.31$, and $\beta = 0.19$ yields $K = [3.2477, 3.4850, -1.2477, 2.4193]$ and $F = [0.0386, 0.0873, -0.0155, 0.0272]$. Some calculations give $\lambda_{\min} = 0.0842$, $\theta_{\min} = 2.5$, $\lambda_{\min}(\hat{H}_{un}) = 0.1433$, $\mu = 11.1843$. According to Algorithm 6.3.5, set the coupling strength $\varrho = 15$ and $\vartheta = 25$. It follows from Theorem 6.1 that mean-square consensus tracking for system (6.61) with protocol (6.11) can be achieved if two conditions in (6.32) and (6.33) are satisfied. The switching signal is shown in Fig. 6.3, where $r(t) = 1, 2, 3$ is to describe the evolution of cyber states under $\mathcal{G}_{r(t)}$ and $\sigma(t)$ is to describe the switching in high level to activate the running time of the designed controller. The total activation time of attacks is 3.2 seconds, which implies that (6.32) and (6.33) are satisfied. The state trajectories of systems are shown in Fig. 6.4 which imply that the agents can achieve consensus and track the leader. Use $E_c(t) = (1/6)\sqrt{\sum_{j=1}^6 \|x_j(t) - x_0(t)\|}$ in Fig. 6.5 to denote the consensus tracking error. This simulation demonstrates that secure consensus tracking can be achieved. The details on (6.32) and (6.33) are provided.

Figure 6.3: Switching signal $\gamma(t)$ and $\sigma(t)$ in Example 6.1.

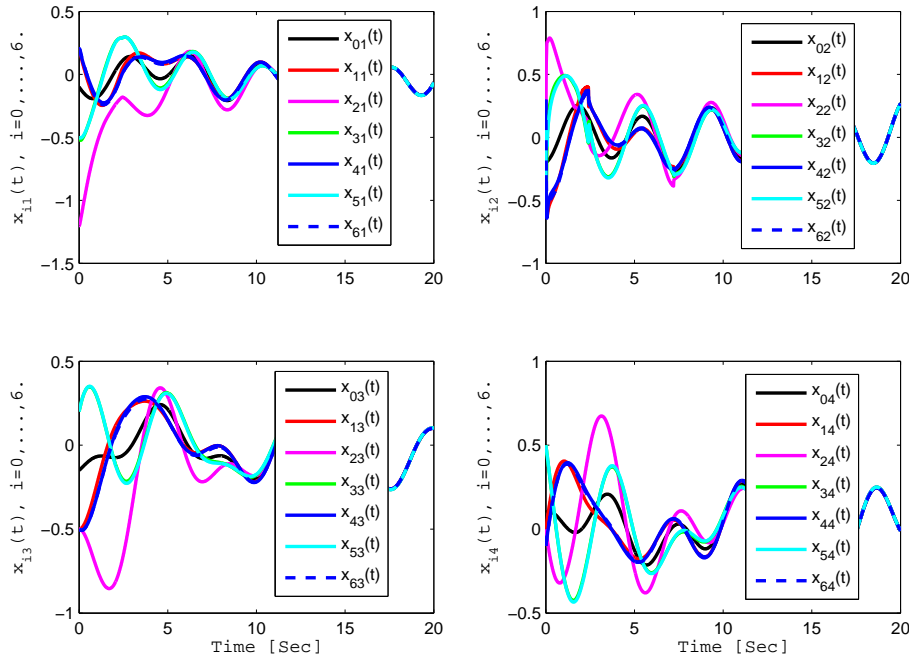


Figure 6.4: State trajectories $x_{ij}(t)$ under the distributed control law (6.11).

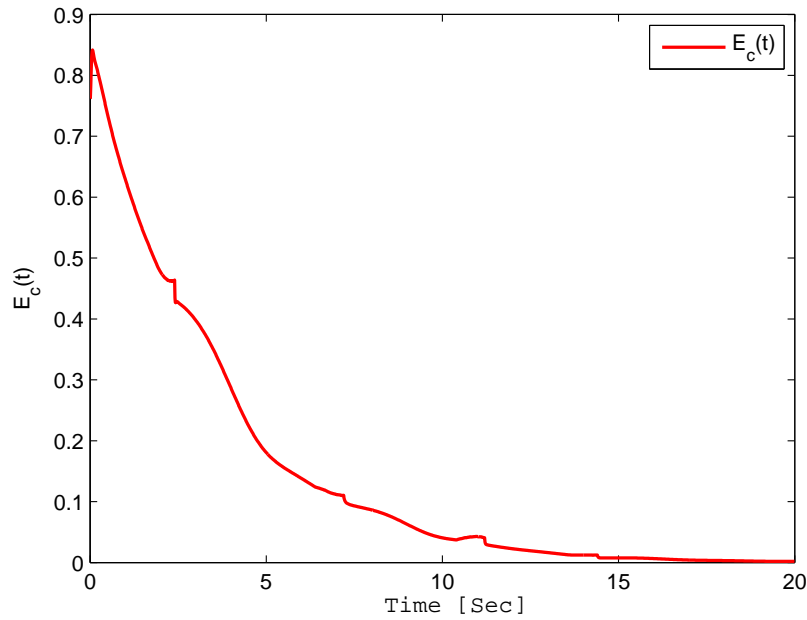


Figure 6.5: Consensus tracking errors $E_c(t)$.

Example 6.2. Discrete-time consensus tracking

Consider the discrete-time dynamics of the i th agent as

$$x_i(k+1) = \tilde{A}x_i(k) + \tilde{B}u_i(k), \quad k \in \mathbb{N}_0, \quad (6.63)$$

$$\tilde{A} = \begin{bmatrix} -1.5 & 2.5 & 0 & 0 \\ -0.5 & -1 & 0.5 & 0 \\ 0 & 0 & 0 & 1 \\ 1.5 & 0 & -2 & 0 \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}. \quad (6.64)$$

The communication topologies in cyber space are the same as that in Example 6.1.

The Markov process starts at its invariant distribution $\tilde{\pi} = [0.2165, 0.4021, 0.3814]$.

The transition probability matrix is given by

$$\Lambda = \begin{bmatrix} 0.1 & 0.4 & 0.5 \\ 0.2 & 0.5 & 0.3 \\ 0.3 & 0.3 & 0.4 \end{bmatrix}. \quad (6.65)$$

Based on Algorithm 6.3.6, we construct (6.43) with $\tilde{R} = 0.5$, $\tilde{T} = 0.8$, $\tilde{Q} = 0.4I$, $\lambda_- = 0.0035$, $\lambda_* = 0.6$, $\lambda_+ = 1.6$. According to Theorem 6.2, the simulation results are shown in Figs. 6.6-6.8. Use $E_d(k) = (1/6)\sqrt{\sum_{j=1}^6 \|x_j(k) - x_0(k)\|^2}$ in Fig. 6.8 to denote the consensus tracking errors. This simulation demonstrates that secure consensus tracking can be achieved for discrete-time agent systems under strategic attacks. The details on the conditions provided in Theorem 6.2 are shown as follows.

As given in (6.50), the *attack frequency* $F_f(k_0, k)$ satisfies

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

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

It follows from (6.49) that the *attack length rate* satisfies

$$\frac{T_a(k_0, k)}{k - k_0} \leq \frac{\ln \lambda_+ - \ln \lambda_*}{\ln \lambda_+ - \ln \lambda_-} = \frac{-0.5108 + 0.5108}{0.4700 + 5.6550} = 0.8399, \quad (6.66)$$

which means that in a statistical sense, the average recovery time is less than 3.6549.

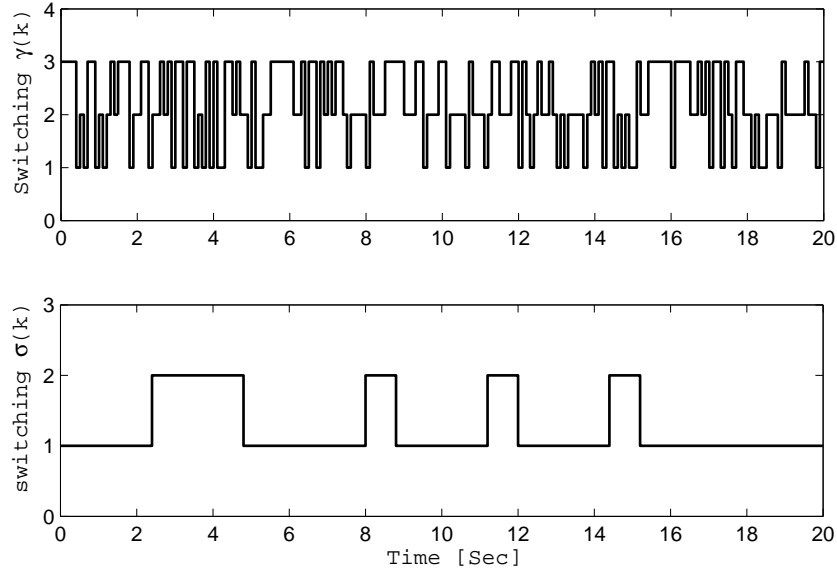


Figure 6.6: Switching signal $\gamma(k)$ and $\sigma(k)$ in Example 6.2.

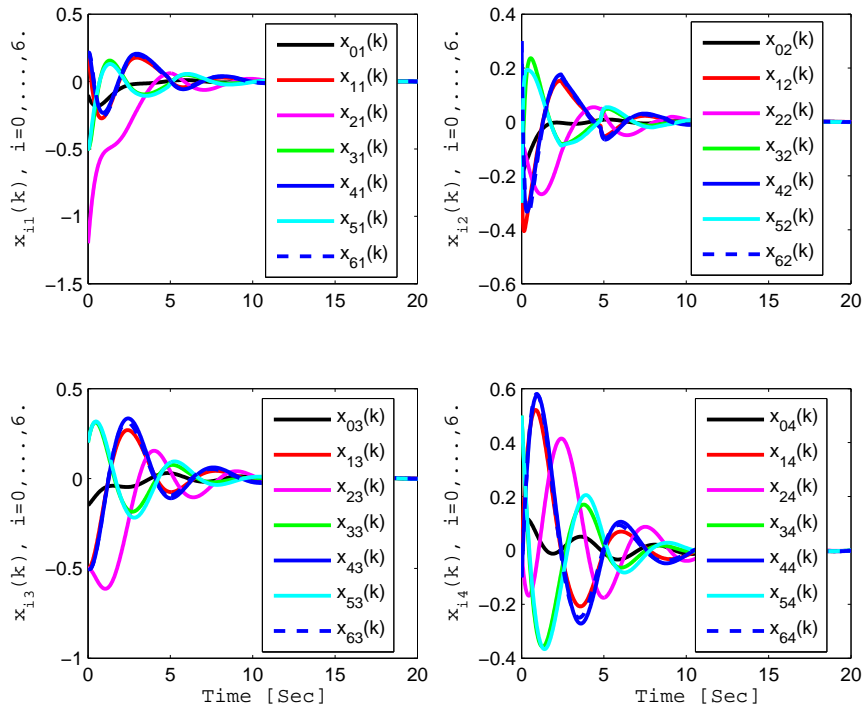
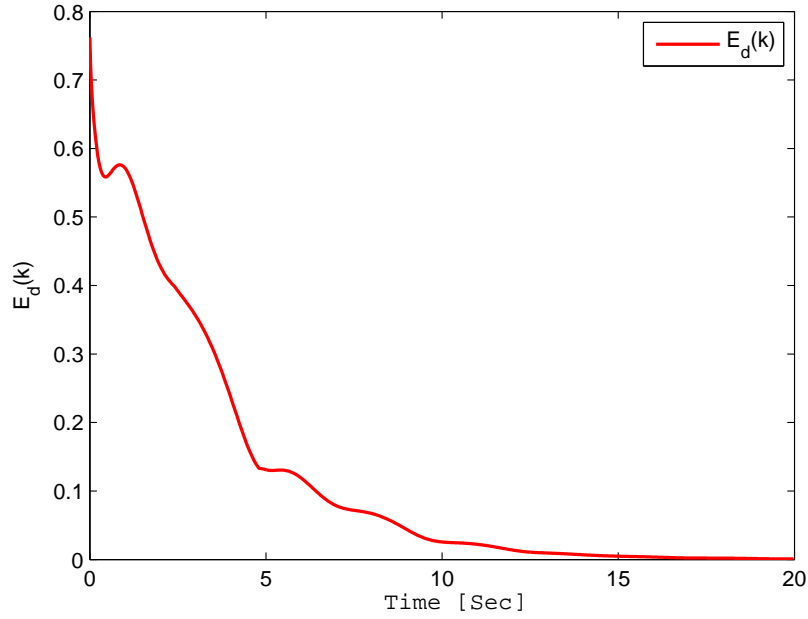


Figure 6.7: State trajectories $x_{ij}(k)$ under the distributed control law (6.43).

Figure 6.8: Consensus tracking errors $E_d(k)$.

6.5 Conclusion

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

Chapter 7

Distributed Event-Triggered Control of Linear Multi-Agent Systems Subject to DoS Attacks

7.1 Introduction

Different from previous works [94–96] presented in chapters 5 and 6 where the system has complete or part access to the attacker moves, this paper concerns with DoS attacks for multi-agent systems in which the attacker follows an unknown strategy. The authors in [149] proposed a centralized event-based controller to address energy-constrained DoS attacks by assuming that the known attacks occur periodically. [150,151] extended this centralized design to deal with packet losses and unavailable measurements, respectively. In [152], event-triggered control strategies were studied for systems subject to DoS attacks and stability was achieved if attack duration was upper bounded. [151] extended this centralized event-based design to deal with DoS attacks and unavailable measurements. A sign-function based ternary controller was further proposed in [153] for self-triggered coordination with practical consensus. Motivated by [94–96,151–153], this work investigates DoS attacks for multi-agent systems where the attacker follows an unknown strategy.

We will focus on the following two problems:

- How to design an event-based distributed resilient controller to achieve secure consensus against DoS attacks?
- To implement this controller, how to ensure a positive inter-execution time interval bounded away from zero?

Specifically, the resilience is concerned with secure consensus under DoS attacks and meanwhile, the positive inter-execution time interval is required for controller implementations over a network. The main contributions of this chapter are:

1. This paper studies secure consensus for linear agent dynamics with event-based samplings. Unlike [145–151, 154–156], a time-sequence-based DoS attack model is considered in which the DoS attacks are allowed to occur aperiodically in an unknown attack strategy. Besides, these works find optimal control policies and attack strategies for a pure single discrete-time system, while we study resilient coordination for a continuous-time multi-agent system.
2. Based on previous works in [94–96], another contribution is an explicit analysis of the frequency and duration of DoS attacks. By virtue of a slowly switching mechanism, upper bounds of the frequency and duration of DoS attacks are obtained to ensure that the attacks do not occur frequently and average recovery time is not too large.
3. Two secure consensus problems are solved by event-based distributed control schemes. The event condition is used to determine when the agent updates its control input and broadcasts the measurements to its neighbors. First, secure leaderless consensus is achieved to provide resilience against DoS attacks. By specifying a positive inter-execution time interval for each agent, Zeno behavior can be avoided for controller implementations. It shows that with the proposed design, the agent group can achieve secure leaderless consensus. Second, secure leader-following consensus is further achieved under a directed graph.

The rest of the chapter is organized as follows. We formulate the problem in Section 7.2. An event-based distributed controller design and stability analysis are presented for solving a secure leaderless consensus problem in Section 7.3. Then, secure leader-following consensus is studied in Section 7.4. Numerical examples are presented to verify the effectiveness of the proposed methods in Section 7.5. Conclusions on this chapter are given in Section 7.6.

7.2 Problem Formulation

7.2.1 Multi-Agent Network Model

In this work, we consider a multi-agent network of N agents with identical general linear dynamics described by

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad t \in \mathbb{R}_{\geq 0}, \quad (7.1)$$

where $x_i(t) \in \mathbb{R}^n$ and $u_i(t) \in \mathbb{R}^l$, $i = 1, 2, \dots, N$, are the state and control input, respectively, $A \in \mathbb{R}^{n \times n}$, and $B \in \mathbb{R}^{n \times l}$ are the time-invariant system and input matrices of (7.1), respectively. We assume that A is not Hurwitz stable, while a standard assumption is that (A, B) is stabilizable.

The goal of coordination is to design the following controller with a gain matrix K so that agents reach consensus.

$$u_i(t) = K\xi_i(t), \quad \xi_i(t) = \sum_{j=1}^N a_{ij}(x_j(t) - x_i(t)). \quad (7.2)$$

7.2.2 DoS Attack Model

DoS attack [145–151, 154–156] refer to a class of attacks where an adversary renders certain or all components of a control system. The DoS attacks can simultaneously affect both measurement and control channels, which leads to loss of data availability. This described situation is illustrated in Fig. 7.1 for a multi-agent system.

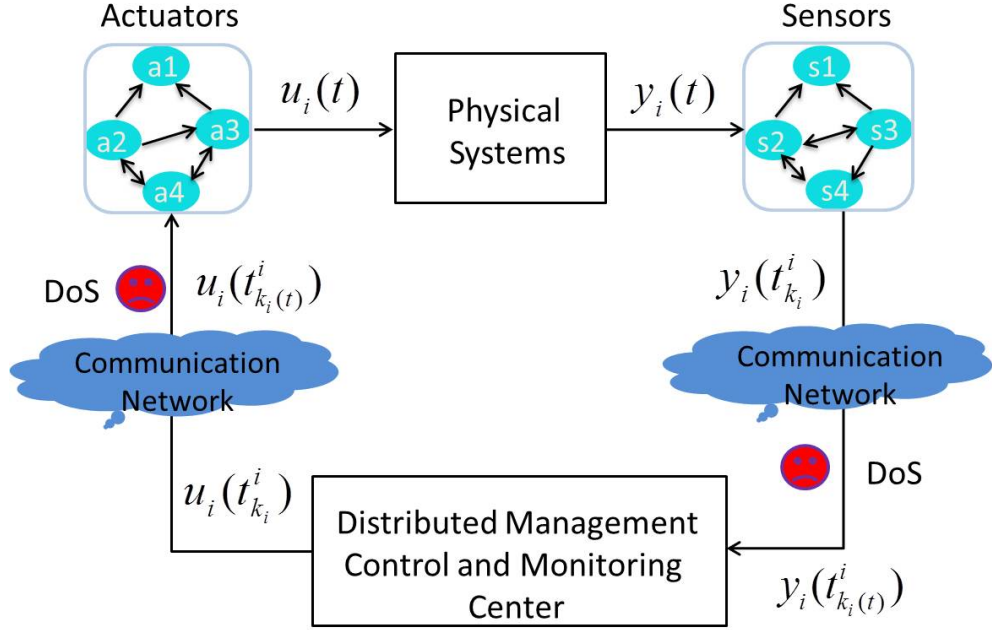


Figure 7.1: Framework of the closed-loop multi-agent system under DoS attacks.

DoS Attack Sequence: In the presence of DoS attacks, although agents have the communication ability, data availability is violated. Without loss of generality, it is assumed that the attacker in Fig. 7.1 can attack the communication network in a varying active period. Next, it needs to terminate attack activities and shift to a sleep period to supply its energy for next attacks. Suppose that there exists an $m \in \mathbb{N}$ and denote $\{\tilde{t}_m\}_{m \in \mathbb{N}}$ as an attack sequence when a DoS attack is launched at \tilde{t}_m . For a length $\tilde{\Delta}_m > 0$, the m -th DoS time-interval is $\mathcal{A}_m = [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m)$ with $\tilde{t}_{m+1} > \tilde{t}_m + \tilde{\Delta}_m$ for all $m \in \mathbb{N}$. Thus, for given $t \geq \tau \in \mathbb{R}$, the sets of time instants where the communication is denied are denoted as

$$\Xi_a(\tau, t) := \cup \mathcal{A}_m \cap [\tau, t], \quad m \in \mathbb{N}, \quad (7.3)$$

which implies that the sets of time instants where the communication is allowed are: $\Xi_s(\tau, t) := [\tau, t] \setminus \Xi_a(\tau, t)$. Suppose that there exists a $k_i \in \mathbb{N}$ and denote $\{t_{k_i}^i\}_{k_i \in \mathbb{N}}$ as an event-based control update sequence to be determined later. We say that it has a finite sampling rate property if there exists Δ_*^i such that $\Delta_{k_i}^i = t_{k_i+1}^i - t_{k_i}^i \geq \Delta_*^i$.

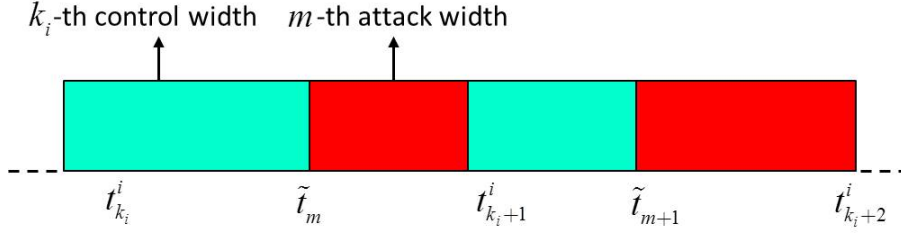


Figure 7.2: Sketch map of aperiodic time sequences: $\{\tilde{t}_m\}_{m \in \mathbb{N}}$ and $\{t_{k_i}^i\}_{k_i \in \mathbb{N}}$.

Next, the problem of interest is to develop the distributed event-triggered controller $u_i(t)$ to achieve resilience against DoS attacks, while ensuring that the positive inter-execution time interval is bounded away from zero. The resilience is concerned with stability and performance of the closed-loop system under DoS attacks, while the positive inter-execution time interval is required for controller implementation over a network. To illustrate the described two aperiodic time sequences $\{t_{k_i}^i\}_{k_i \in \mathbb{N}}$ and $\{\tilde{t}_m\}_{m \in \mathbb{N}}$, a sketch map is given in Fig. 7.2.

7.2.3 Control Objective

Definition 7.1. *Secure Leaderless Consensus*

Given the system (7.1) and a fixed graph \mathcal{G} , the distributed event-triggered secure control law $u_i(t)$ is said to solve a secure leaderless consensus problem for multi-agent systems (7.1) under DoS attacks described in subsection 7.2.2, if

$$\lim_{t \rightarrow \infty} [\|x_i(t) - x_j(t)\|^2] = 0, \quad \forall i, j \in \mathcal{V}. \quad (7.4)$$

There is another consensus problem named leader-following consensus where the solution of each subsystem is required to approach some signal, i.e., the leader state $x_0(t) \in \mathbb{R}^n$ generated by:

$$\dot{x}_0(t) = Ax_0(t). \quad (7.5)$$

Associated with systems (7.1) and (7.5), we define another graph $\tilde{\mathcal{G}} = (\tilde{\mathcal{V}}, \tilde{\mathcal{E}})$, where $\tilde{\mathcal{V}} = \{0, 1, \dots, N\}$ and $(i, j) \in \tilde{\mathcal{E}}$. Clearly, \mathcal{G} is a subgraph of $\tilde{\mathcal{G}}$ and can be obtained by removing the vertex 0 from $\tilde{\mathcal{V}}$ and all edges on vertex 0 from $\tilde{\mathcal{E}}$. $\mathcal{N}_i(\tilde{\mathcal{G}})$ denotes the new neighborhood set of vertex $i \in \tilde{\mathcal{V}}$.

Definition 7.2. Secure Leader-Following Consensus

Given the follower system (7.1) and leader system (7.5), and a fixed graph $\tilde{\mathcal{G}}$, the distributed event-triggered secure control law $u_i(t)$ is said to solve a secure leader-following consensus problem for multi-agent systems (7.1) and (7.5) under DoS attacks, if there exists a scalar $\kappa > 0$ and a decay rate $\rho > 0$ such that for all $t > 0$

$$\|x_i(t) - x_0(t)\|^2 \leq \kappa e^{-\rho t} \|x_i(0) - x_0(0)\|^2. \quad (7.6)$$

7.3 Event-Triggered Secure Leaderless Consensus

7.3.1 Distributed Event-triggered Controller Design

Define $t_0 = t_0^i, t_1^i, \dots, t_{k_i}^i, \dots$ as the sequence of event times for each agent i . For $t \in [t_{k_i}^i, t_{k_i+1}^i)$, a distributed control law for multi-agent systems (7.1) under the modeled time-sequence DoS attacks can be designed as

$$u_i(t) = K\hat{\xi}_i(t), \quad \hat{\xi}_i(t) = \sum_{j \in \mathcal{N}_i(\mathcal{G})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t)), \quad (7.7)$$

where $\hat{x}_i(t)$ is the latest broadcast state of agent i , and the computation of $\hat{\xi}_i(t)$ only requires the estimates of agent i and its neighboring followers' state estimate (i.e., $\hat{x}_j(t)$), instead of using their true states $x_j(t)$ via continuous communication as required in [164–166]. The subscript $k_i(t)$ denotes last successful update:

$$k_i(t) = \begin{cases} -1, & \text{if } \Xi_s(0, t) = \emptyset, \\ \sup\{k_i \in \mathbb{N} \mid t_{k_i}^i \in \Xi_s(0, t)\}, & \text{otherwise,} \end{cases} \quad (7.8)$$

where $\{t_{k_i}^i\}$ is the control sequence and we assume $k_i(0) = -1$ and when $\tilde{t}_0 = 0$, $u_i(0) = 0$ with $\hat{\xi}_i(t_{-1}^i) = 0$.

In (7.7), the estimate $\hat{x}_j(t)$ is obtained by the following state estimator:

$$\dot{\hat{x}}_j(t) = A\hat{x}_j(t), \quad t_{k_j}^j \leq t < t_{k_j+1}^j, \quad (7.9)$$

$$\hat{x}_j(t_{k_j}^j) = x_j(t_{k_j}^j), \quad j \in \mathcal{N}_i(\mathcal{G}), \quad k_j \in \mathbb{N}, \quad (7.10)$$

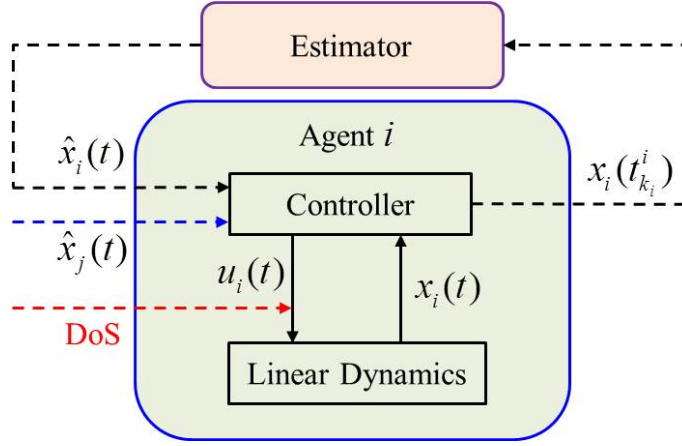


Figure 7.3: Framework of event-based secure control setup with an estimator.

where $\hat{x}_j(t)$ evolves along its dynamics during $[t_{k_j}^j, t_{k_j+1}^j)$ and is updated via x_j communicated from the neighboring agent j at its discrete time $t_{k_j}^j$. For agent i , the state estimate $\hat{x}_i(t)$ is updated continuously with the dynamics in (7.9) and discretely at the time instance described in (7.10). It can be seen that the discrete-time signal $x_i(t_{k_i}^i)$ is thus converted into the continuous-time signal $\hat{x}_i(t)$ until the next event occurs. Fig. 7.3 gives this event-based secure control setup with an estimator under DoS attacks.

Note that under DoS attacks the states of system are unavailable. Therefore, this estimator has been used to estimate the state and to design the controllers.

In the current setup, each agent has to measure $\hat{\xi}_i(t)$ to generate (7.7). To determine the event time instants, we define the following measurement error:

$$e_i(t) = \hat{x}_i(t) - x_i(t). \quad (7.11)$$

It is desired to employ the distributed controller law so that $e_i(t)$ satisfies

$$\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|, \quad \beta_i > 0, \quad (7.12)$$

which implies that the update rule is triggered by measuring the state $\hat{\xi}_i(t)$ and triggering a control when

$$\|e_i(t)\| = \|\hat{x}_i(t) - x_i(t)\| = \beta_i \|\hat{\xi}_i(t)\|. \quad (7.13)$$

To ensure that no agent will exhibit Zeno behavior, which is called as a “Zeno-free trigger”, a hybrid approach in [165] is adopted such that for agent i ,

$$t_{k_i+1}^i = t_{k_i}^i + \Delta_{k_i}^i, \quad \Delta_{k_i}^i = \max\{\tau_{k_i}^i, b_i\}, \quad (7.14)$$

where $\Delta_{k_i}^i$ is the inter-execution interval, b_i is a strictly positive real number which will be given in the subsequent theorem and $\tau_{k_i}^i$ is determined as

$$\tau_{k_i}^i = \inf_{t > t_{k_i}^i} \{t - t_{k_i}^i \mid \|e_i(t)\| = \beta_i \|\hat{\xi}_i(t)\|\}. \quad (7.15)$$

Note that [162–166] show the achievements of average consensus in the absence of DoS when the triggered condition is satisfied. This is always possible in the absence of DoS. However, in the presence of DoS failing to reset $e_i(t)$ may cause condition (7.12) to be violated and consensus can be lost. Thus, it is challenging to study how to achieve secure consensus to account for the DoS attacks.

7.3.2 DoS Attack Frequency and Attack Duration

According to DoS attack model in subsection 7.2.2, a natural question is to determine the amount of DoS attacks that systems can tolerate before losing secure consensus. It is obvious that this amount is not arbitrary and that suitable conditions must be imposed on both DoS attack frequency and duration defined in [94–96]. Motivated by the slowly switching mechanism in previous work [118], the following definitions are given for the convenience of subsequent developments.

Definition 7.3. (*Attack Frequency*) For any $T_2 > T_1 \geq t_0$, let $N_a(T_1, T_2)$ denote the number of DoS attacks occurring over $[T_1, T_2)$. Thus, $F_a(T_1, T_2) = \frac{N_a(T_1, T_2)}{T_2 - T_1}$ is defined as the attack frequency over $[T_1, T_2)$ for all $T_2 > T_1 \geq t_0$.

Definition 7.4. (*Attack Duration*) For any $T_2 > T_1 \geq t_0$, denote $T_a(T_1, T_2)$ as the total time interval for multi-agent systems under DoS attacks during $[T_1, T_2)$. The attack duration over $[T_1, T_2)$ is defined as: there exists $T_0 \geq 0$ and $\tau_a > 0$ such that $T_a(T_1, T_2) \leq T_0 + (T_2 - T_1)/\tau_a$.

Remark 7.1. *As stated in [94–96] for multi-agent systems under attacks, Definitions 7.3 and 7.4 can specify the class of DoS attack signals in terms of their frequency and duration. By virtue of a slowly switching mechanism in [118], Definitions 7.3 and 7.4 express the property that the DoS attacks satisfy a slow-on-the-average type condition. Thus, an explicit analysis of attack frequency and duration can be obtained to ensure that the DoS attacks do not occur frequently and the average recovery time of systems is not too large [94–96].*

7.3.3 Stability Analysis of Secure Leaderless Consensus

Assumption 7.1. *The undirected graph \mathcal{G} is connected.*

Denote the collective vectors $e(t) = \text{col}(e_1(t), \dots, e_N(t))$, $x(t) = \text{col}(x_1(t), \dots, x_N(t))$ and $\hat{x}(t) = \text{col}(\hat{x}_1(t), \dots, \hat{x}_N(t)) \in \mathbb{R}^{Nn}$. From the definitions of $u_i(t)$ in (7.7) and $e_i(t)$ in (7.11), the dynamics of agent group are written by

$$\dot{x}(t) = [I_N \otimes A - (\mathcal{L} \otimes BK)]x(t) - (\mathcal{L} \otimes BK)e(t). \quad (7.16)$$

Denote the state average of agents as: $\bar{x}(t) = \frac{1}{N} \sum_{i=1}^N x_i(t)$. Defining a disagreement vector $\delta_i(t) = x_i(t) - \bar{x}(t)$ gives

$$\delta(t) = [(I_N - \frac{1_N 1_N^T}{N}) \otimes I_n]x(t) = (\mathcal{M} \otimes I_n)x(t), \quad (7.17)$$

where $\delta(t) = \text{col}(\delta_1(t), \dots, \delta_N(t))$ and \mathcal{M} is given by

$$\mathcal{M} = \frac{1}{N} \begin{bmatrix} N-1 & -1 & \cdots & -1 \\ -1 & N-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & N-1 \end{bmatrix}.$$

Under Assumption 7.1, the Laplacian matrix \mathcal{L} is symmetric and positive semi-definite [14]. By the definition of $\delta(t)$, it is easy to see that $(1_N^T \otimes I_n)\delta(t) = 0$. Thus, there always exists an orthogonal matrix $\Psi = [1_N/\sqrt{N}, \Phi] \in \mathbb{R}^{N \times N}$, where $\Phi = (\phi_2, \dots, \phi_N) \in \mathbb{R}^{N \times (N-1)}$ and $\phi_i \in \mathbb{R}^N$, $i = 2, \dots, N$, is an orthogonal eigenvector

of \mathcal{L} associated with eigenvalue $\lambda_i(\mathcal{L})$, i.e., $\phi_i^T \mathcal{L} = \lambda_i(\mathcal{L}) \phi_i^T$. Therefore, we can have the following properties [64]:

$$\begin{aligned}\Psi^T \Psi &= I_N, \quad \Phi \Phi^T = \mathcal{M} = I_N - (1_N 1_N^T)/N, \\ \mathcal{L} \mathcal{M} &= \mathcal{M} \mathcal{L} = \mathcal{L}, \quad \Psi^T \mathcal{L} \Psi = \text{diag}\{0, \lambda_i(\mathcal{L})\}.\end{aligned}\quad (7.18)$$

Based on (7.16) and (7.18), the time derivative of (7.17) is given by

$$\dot{\delta}(t) = (\mathcal{M} \otimes I_n) \dot{x}(t) = [I_N \otimes A - (\mathcal{L} \otimes BK)] \delta(t) - (\mathcal{L} \otimes BK) e(t). \quad (7.19)$$

Theorem 7.1. *Consider a group of N agents with dynamics in (7.1). Suppose that Assumption 7.1 holds. Given any positive symmetric definite matrices $R > 0$ and $Q > 0$, there exists a unique symmetric positive definite matrix $P > 0$ such that the following algebraic Riccati equation (ARE) is satisfied.*

$$PA + A^T P - PBR^{-1}B^T P + Q = 0. \quad (7.20)$$

Let $\gamma_1, \gamma_2 > 0$ satisfy: $\gamma_1 + \gamma_2 = \gamma < 1$. If $\beta_i^2 = \frac{s_i}{2\lambda_N^2(\mathcal{L})} \leq \gamma_1$, $s_i \in (0, 1)$ and b_i in (7.14) is strictly positive with

$$b_i \leq \frac{1}{c_1} \ln\left(\frac{c_1}{c_2} \sqrt{\frac{2\gamma_2 \lambda_N^2(\mathcal{L})}{N(1-s_{\max})}} + 1\right),^1 \quad (7.21)$$

then under the proposed distributed event-triggered control law (7.7) with $K = \tau R^{-1} B^T P$, $\tau \geq (2\lambda_2(\mathcal{L}))^{-1}$, the agent group will achieve secure leaderless consensus, provided that the following two conditions are satisfied:

1. There exists a constant $\eta_1^* \in (0, \alpha_1)$ such that the attack frequency $F_a(t_0, t)$ in Definition 7.3 satisfies

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \leq \frac{\eta_1^*}{\ln(\mu) + (\alpha_1 + \alpha_2)\Delta_*}, \quad (7.22)$$

2. There exists a positive constant τ_a in attack duration Definition 7.4 so that

$$\tau_a > (\alpha_1 + \alpha_2)/(\alpha_1 + \eta_1^*), \quad (7.23)$$

¹ $s_{\max} = \max_i s_i$, $s_{\max} < \lambda_{\min}^2(Q)/(4k_0^2 \lambda_N^2(\mathcal{L}) + \lambda_{\min}^2(Q)) < 1$, $k_0 = \|PBK\|$, $c_1 = 2\|A\| + c_2$, $c_2 = \lambda_N(\mathcal{L}) \|BK\| (1 + \sqrt{Nc})$, $c = 2\gamma_2 \lambda_N^2(\mathcal{L})/(N(1 - s_{\max}))$.

where $\alpha_1 = (\lambda_{\min}(Q)/2 - \frac{2k_0^2\lambda_N^2(\mathcal{L})s_{\max}}{\lambda_{\min}(Q)(1-s_{\max})})/\lambda_{\max}(P) > 0$, $\alpha_2 > 0$ such that for $S > 0$, $SA + A^T S - \alpha_2 S < 0$, $\mu = \max\{\lambda_{\max}(P)/\lambda_{\min}(S), \lambda_{\max}(S)/\lambda_{\min}(P)\}$, and Δ_* is a nonnegative constant satisfying: $\sup_{(i,k_i) \in \mathcal{F}} \Delta_{k_i}^i \leq \Delta_*$.

The event detection time instants are determined by (7.14) and no agent will exhibit Zeno behavior.

Proof. (I) Resilience analysis

The idea is to decompose the time axis into intervals where it is possible to satisfy the condition (7.12) and intervals where (7.12) needs not to hold due to the occurrence of DoS attacks. Similar to the analysis in [94–96], we then consider the closed-loop dynamics as a hybrid system with switches between stable and unstable modes. Thus, the proof is divided into the following steps for clarity of expositions.

Step 1: Two intervals classification

In this step, the intervals of time where (7.12) holds and does not hold are characterized which is essential for Lyapunov analysis in Step 2.

Consider the control update sequence $\{t_{k_i}^i\}_{k_i \in \mathbb{N}}$ along with the DoS attack sequence $\{\tilde{t}_m\}_{m \in \mathbb{N}}$. The set of integers related to a control update attempt occurring under the DoS attacks is

$$\mathcal{F} = \{(i, k_i) \in \mathcal{V} \times \mathbb{N} \mid t_{k_i}^i \in \cup_{m \in \mathbb{N}} \mathcal{A}_m\}. \quad (7.24)$$

Due to the finite sampling rate, a time interval will necessarily elapse from the time $\tilde{t}_m + \tilde{\Delta}_m$, to the time at which the agents successfully sample and transmit. It can be upper bounded as: $\sup_{(i,k_i) \in \mathcal{F}} \Delta_{k_i}^i \leq \Delta_*$. Notice that the last control update of agent i over the m -th attack interval necessarily falls within $[\tilde{t}_m + \tilde{\Delta}_m - \Delta_*, \tilde{t}_m + \tilde{\Delta}_m)$. That is, the next sampling falls within $[\tilde{t}_m + \tilde{\Delta}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$. Hence, a DoS free interval of a length greater than Δ_* guarantees that the agents are able to sample and transmit. The m -th time interval where (7.12) needs not to hold is given by

$$\mathfrak{A}_m = \{\tilde{t}_m\} \cup (\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*). \quad (7.25)$$

Thus, the time interval $[\tau, t)$ consists of the following two union of sub-intervals:

$[\tau, t) = \tilde{\Xi}_s(\tau, t) \cup \tilde{\Xi}_a(\tau, t)$ with

$$\tilde{\Xi}_a(\tau, t) := \cup \mathfrak{A}_m \cap [\tau, t], \tilde{\Xi}_s(\tau, t) := [\tau, t] \setminus \tilde{\Xi}_a(\tau, t). \quad (7.26)$$

Step 2: Lyapunov stability analysis

(1). Consider the time interval $\tilde{\Xi}_s(\tau, t)$ over which (7.12) holds. Choose a Lyapunov function candidate as:

$$V(t) = \delta^T(t)(I_N \otimes P)\delta(t). \quad (7.27)$$

Computing the time derivative of (7.27) yields

$$\begin{aligned} \dot{V}(t) &= \dot{\delta}^T(I_N \otimes P)\delta + \delta^T(I_N \otimes P)\dot{\delta} \\ &= \delta^T(I_N \otimes (PA + A^T P))\delta - 2\delta^T(\mathcal{L} \otimes PBK)(\delta + e). \end{aligned} \quad (7.28)$$

Based on (7.18), defining $\tilde{\delta} = (\Psi^T \otimes I_n)\delta$ yields that $\tilde{\delta}_1 = (\frac{1}{N}\mathcal{M} \otimes I_n)x = 0$. Since $\tau \geq (2\lambda_2(\mathcal{L}))^{-1}$, one has

$$\begin{aligned} &\delta^T[I_N \otimes (PA + A^T P) - 2\tau(\mathcal{L} \otimes PBR^{-1}B^T P)]\delta \\ &\leq \sum_{i=2}^N \tilde{\delta}_i^T (PA + A^T P - PBR^{-1}B^T P)\tilde{\delta}_i. \end{aligned} \quad (7.29)$$

By using Young's inequality: $x^T y \leq \frac{\varrho}{2}x^T x + \frac{1}{2\varrho}y^T y$ for any $\varrho > 0$ and any $x, y \in \mathbb{R}^{nN}$, it follows that for $k_0 = \|PBK\|$, $\omega = \lambda_N^2(\mathcal{L})$, and $\tilde{e} = (\Phi^T \otimes I_n)e$,

$$-2\tau\delta^T(\mathcal{L} \otimes PBR^{-1}B^T P)e \leq k_0 \sum_{i=2}^N (\omega\varrho\tilde{\delta}_i^T \tilde{\delta}_i + \varrho^{-1}\tilde{e}_i^T \tilde{e}_i).$$

Since $PA + A^T P - PBR^{-1}B^T P + Q = 0$, (7.28) can be given by

$$\begin{aligned} \dot{V}(t) &\leq -\lambda_{\min}(Q) \sum_{i=1}^N \delta_i^T \delta_i + k_0 \sum_{i=2}^N (\omega\varrho\tilde{\delta}_i^T \tilde{\delta}_i + \frac{1}{\varrho}\tilde{e}_i^T \tilde{e}_i) \\ &= -(\lambda_{\min}(Q) - k_0\omega\varrho) \sum_{i=1}^N \delta_i^T \delta_i + \frac{k_0}{\varrho} \sum_{i=2}^N \tilde{e}_i^T \tilde{e}_i \\ &\leq -\frac{\lambda_{\min}(Q)}{2} \sum_{i=1}^N \delta_i^T \delta_i + \frac{2k_0^2\lambda_N^2(\mathcal{L})}{\lambda_{\min}(Q)} \sum_{i=1}^N e_i^T e_i, \end{aligned} \quad (7.30)$$

where $\varrho = \lambda_{\min}(Q)/(2k_0\omega)$, $\omega = \lambda_N^2(\mathcal{L})$, and $\|\tilde{e}\| \leq \|\Phi^T \otimes I_n\| \|e\| \leq \|e\|$ is used.

Let $\hat{\xi}(t) = \text{col}(\hat{\xi}_1(t), \hat{\xi}_2(t), \dots, \hat{\xi}_N(t))$. By the definition of $\hat{\xi}_i(t) = \sum_{j \in \mathcal{N}_i(G)} a_{ij}(\hat{x}_j(t) -$

$\hat{x}_i(t)$) in (7.7) and $e_i(t) = \hat{x}_i(t) - x_i(t)$ in (7.11), it is obtained that

$$\begin{aligned} \|\hat{\xi}(t)\| &= \|-(\mathcal{L} \otimes I_n)\hat{x}\| = \|-(\mathcal{L} \otimes I_n)(x + e)\| \\ &= \|\xi - (\mathcal{L} \otimes I_n)e\| \leq \|\xi\| + \|(\mathcal{L} \otimes I_n)e\| \\ &\leq \|\xi\| + \lambda_N(\mathcal{L})\|e\|, \end{aligned} \quad (7.31)$$

where $\xi(t) = \text{col}(\xi_1(t), \xi_2(t), \dots, \xi_N(t))$.

By using the properties in (7.18), it gives $\mathcal{L}^2 \leq \lambda_N^2(\mathcal{L})\mathcal{M}^2$, which implies that the following inequality holds

$$\begin{aligned} \|\xi\|^2 &= x^T(\mathcal{L}^T \otimes I_n)(\mathcal{L} \otimes I_n)x = x^T(\mathcal{L}^2 \otimes I_n)x \\ &\leq \lambda_N^2(\mathcal{L})x^T(\mathcal{M}^2 \otimes I_n)x = \lambda_N^2(\mathcal{L})\|\delta\|^2, \end{aligned} \quad (7.32)$$

where $\delta(t) = (\mathcal{M} \otimes I_n)x(t)$ is used in (7.17).

Combining (7.31) with (7.32) yields

$$\|\hat{\xi}(t)\| \leq \lambda_N(\mathcal{L})(\|\delta\| + \|e\|). \quad (7.33)$$

Since $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$, it follows from $\beta_i^2 = \frac{s_i}{2\lambda_N^2(\mathcal{L})}$ and (7.33) that for $s_{\max} = \max_i s_i$, $i \in \mathcal{V}$,

$$\|e(t)\|^2 \leq \frac{s_{\max}}{2\lambda_N^2(\mathcal{L})} \|\hat{\xi}(t)\|^2 \leq \frac{s_{\max}}{2}(\|\delta\| + \|e\|)^2 \leq s_{\max}(\|\delta\|^2 + \|e\|^2), \quad (7.34)$$

which leads to

$$\|e(t)\|^2 \leq \frac{s_{\max}}{1 - s_{\max}} \|\delta\|^2. \quad (7.35)$$

If we choose $s_{\max} < \lambda_{\min}^2(Q)/(4k_0^2\lambda_N^2(\mathcal{L}) + \lambda_{\min}^2(Q))$, then it follows from (7.30) and (7.35) that

$$\begin{aligned} \dot{V}(t) &\leq -\left(\frac{\lambda_{\min}(Q)}{2} - \frac{2k_0^2\lambda_N^2(\mathcal{L})s_{\max}}{\lambda_{\min}(Q)(1 - s_{\max})}\right) \sum_{i=1}^N \delta_i^T \delta_i \\ &\leq -\alpha_1 \delta^T(t)(I_N \otimes P)\delta(t) = -\alpha_1 V(t), \end{aligned} \quad (7.36)$$

where $\alpha_1 > 0$ is given in Theorem 7.1.

By using the Comparison lemma (Lemma 3.4 in [74]), it follows from (7.36) that

for $\forall t \in [\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}, \tilde{t}_m)$,

$$V(t) \leq e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} V(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}). \quad (7.37)$$

(2). Consider the time interval $\tilde{\Xi}_s(\tau, t)$ over which (7.12) does not necessarily hold. Choose a Lyapunov function candidate:

$$V(t) = \delta^T(t)(I_N \otimes S)\delta(t), \quad (7.38)$$

which yields that the time derivative of (7.38) is $\dot{V}(t) = \delta^T[I_N \otimes (SA + A^T S)]\delta \leq \alpha_2 V(t)$, where $\alpha_2 > 0$ such that $SA + A^T S - \alpha_2 S < 0$ is used.

Thus, it is obtained that for $\forall t \in [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$,

$$V(t) \leq e^{\alpha_2(t-\tilde{t}_m)} V(\tilde{t}_m). \quad (7.39)$$

Denote $\sigma(t) \in \{a, b\}$ as a piecewise constant function. The chosen piecewise Lyapunov function is thus given by: $V(t) = V_{\sigma(t)}$, where V_a and V_b are defined in (7.27) and (7.38), respectively. Suppose that V_a is activated in $[\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}, \tilde{t}_m)$ and V_b is activated in $[\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$. It follows from (7.37) and (7.39) that

$$V(t) \leq \begin{cases} e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} V_a(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}), \\ e^{\alpha_2(t-\tilde{t}_m)} V_b(\tilde{t}_m). \end{cases} \quad (7.40)$$

Case I: if $t \in [\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}, \tilde{t}_m)$, it follows from (7.40) that

$$\begin{aligned} V(t) &\leq e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} V_a(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}) \leq \mu e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} V_b(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}) \\ &\leq \mu e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} [e^{\alpha_2(t-\tilde{t}_{m-2}-\tilde{\Delta}_{m-2})} \times V_b(\tilde{t}_{m-2} + \tilde{\Delta}_{m-2})] \\ &\leq \mu^2 e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} e^{\alpha_2(t-\tilde{t}_{m-2}-\tilde{\Delta}_{m-2})} \\ &\quad \times [e^{-\alpha_1(\tilde{t}_{m-2}+\tilde{\Delta}_{m-2}-\tilde{t}_{m-3}-\tilde{\Delta}_{m-3})} \times V_a(\tilde{t}_{m-3} + \tilde{\Delta}_{m-3})] \\ &\leq \dots \\ &\leq \mu^m e^{-\alpha_1|\tilde{\Xi}_s(t_0, t)|} e^{\alpha_2|\tilde{\Xi}_a(t_0, t)|} V_a(t_0). \end{aligned} \quad (7.41)$$

Case II: if $t \in [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$, similarly it has

$$\begin{aligned}
V(t) &\leq e^{\alpha_2(t-\tilde{t}_m)} V_b(\tilde{t}_m) \leq \mu e^{\alpha_2(t-\tilde{t}_m)} V_a(\tilde{t}_m^-) \\
&\leq \mu e^{\alpha_2(t-\tilde{t}_m)} [e^{-\alpha_1(\tilde{t}_m-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})} \times V_a(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1})] \\
&\leq \dots \\
&\leq \mu^{m+1} e^{-\alpha_1|\tilde{\Xi}_s(t_0,t)|} e^{\alpha_2|\tilde{\Xi}_a(t_0,t)|} V_a(t_0).
\end{aligned} \tag{7.42}$$

Step 3: Bounds on DoS attack frequency and duration According to Definition 7.3, $N_a(t_0, t) = m$ for $t \in [\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}, \tilde{t}_m)$ and $N_a(t_0, t) = m + 1$ for $t \in [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$. Thus, for $\forall t \geq t_0$, it follows from (7.41) and (7.42) that

$$V(t) \leq \mu^{N_a(t_0,t)} e^{-\alpha_1|\tilde{\Xi}_s(t_0,t)|} e^{\alpha_2|\tilde{\Xi}_a(t_0,t)|} V(t_0). \tag{7.43}$$

Notice that for all $t \geq t_0$, $|\tilde{\Xi}_s(t_0, t)| = t - t_0 - |\tilde{\Xi}_a(t_0, t)|$ and $|\tilde{\Xi}_a(t_0, t)| \leq |\Xi_a(t_0, t)| + (1 + N_a(t_0, t))\Delta_*$, where $N_a(t_0, t)$ represents the numbers of DoS attacks during $[t_0, t)$ and Δ_* satisfies: $\sup_{(i,k_i) \in \mathcal{F}} \Delta_{k_i}^i \leq \Delta_*$. Hence, it follows from Definition 7.4 that

$$\begin{aligned}
&-\alpha_1(t - t_0 - |\tilde{\Xi}_a(t_0, t)|) + \alpha_2|\tilde{\Xi}_a(t_0, t)| = -\alpha_1(t - t_0) + (\alpha_1 + \alpha_2)|\tilde{\Xi}_a(t_0, t)| \\
&= -\alpha_1(t - t_0) + (\alpha_1 + \alpha_2)[|\Xi_a(t_0, t)| + (1 + N_a(t_0, t))\Delta_*] \\
&\leq -\alpha_1(t - t_0) + (\alpha_1 + \alpha_2)[T_0 + (t - t_0)/\tau_a + (1 + N_a(t_0, t))\Delta_*].
\end{aligned} \tag{7.44}$$

Substituting (7.44) into (7.43) yields

$$\begin{aligned}
V(t) &\leq \mu^{N_a(t_0,t)} e^{-\alpha_1(t-t_0-|\tilde{\Xi}_a(t_0,t)|)} e^{\alpha_2|\tilde{\Xi}_a(t_0,t)|} V(t_0) \\
&\leq e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)} e^{-\alpha_1(t-t_0)} e^{\frac{(\alpha_1+\alpha_2)}{\tau_a}(t-t_0)} \times e^{[\ln(\mu)+(\alpha_1+\alpha_2)\Delta_*]N_a(t_0,t)} V(t_0).
\end{aligned}$$

Based on (7.22), it gets $e^{[\ln(\mu)+(\alpha_1+\alpha_2)\Delta_*]N_a(t_0,t)} \leq e^{\eta_1^*(t-t_0)}$, which implies that

$$V(t) \leq e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)} e^{-[\alpha_1 - \frac{(\alpha_1+\alpha_2)}{\tau_a} - \eta_1^*](t-t_0)} V(t_0).$$

Thus, by (7.23) there exists a $\eta_1 = \alpha_1 - \frac{(\alpha_1+\alpha_2)}{\tau_a} - \eta_1^* > 0$ such that

$$V(t) \leq e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)} e^{-\eta_1(t-t_0)} V(t_0). \tag{7.45}$$

(II). Minimal inter-event interval

At time t , the inter-event time of an agent is determined either by $\tau_{k_i}^i$ or b_i based on (7.14). Let $R_1(t)$ and $R_2(t)$ be the agent sets consisting of agents whose latest inter-event time of an agent is determined by $\tau_{k_i}^i$ and b_i , respectively. Then, $R_1(t) \cup R_2(t) = \{1, 2, \dots, N\}$ and $R_1(t) \cap R_2(t) = \emptyset$. To guarantee $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$ in (7.12), one can choose

$$\sum_{i \in R_1(t)} \|e_i(t)\|^2 \leq \gamma_1 \sum_{i \in R_1(t)} \|\hat{\xi}_i(t)\|^2 \leq \gamma_1 \sum_{i=1}^N \|\hat{\xi}_i(t)\|^2, \quad (7.46)$$

and

$$\sum_{i \in R_2(t)} \|e_i(t)\|^2 \leq \gamma_2 \sum_{i \in R_2(t)} \|\hat{\xi}_i(t)\|^2 \leq \gamma_2 \sum_{i=1}^N \|\hat{\xi}_i(t)\|^2, \quad (7.47)$$

where $\gamma_1, \gamma_2 > 0$ satisfy: $\gamma_1 + \gamma_2 = \gamma < 1$.

A sufficient condition for (7.46) is that for each agent in $R_1(t)$, $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$ with $\beta_i^2 \leq \gamma_1$. Next, a sufficient condition for (7.47) is that for each agent in $R_2(t)$,

$$\|e_i(t)\|^2 \leq \sum_{j=1}^N \frac{\gamma_2}{N} \|\hat{\xi}_j(t)\|^2 \leq \frac{2\gamma_2 \lambda_N^2(\mathcal{L})}{N(1-s_{\max})} \|\delta(t)\|^2, \quad (7.48)$$

where (7.33)-(7.35) are used to get (7.48).

Let $c = \frac{2\gamma_2 \lambda_N^2(\mathcal{L})}{N(1-s_{\max})}$. Then, (7.48) is $\|e_i(t)\|^2 \leq c \|\delta(t)\|^2$. If we have a lower bound, i.e., b_i , for the evolution time of $\|e_i(t)\| / \|\delta(t)\|$ from 0 to \sqrt{c} , then for all the agents in $R_2(t)$, letting $t_{k_i+1}^i = t_{k_i}^i + b_i$ will be sufficient to ensure (7.47).

To show the existence of a positive inter-execution interval, i.e., find the lower time bound b_i , one can estimate the time derivative of $\|e_i\| / \|\delta\|$ as

$$\begin{aligned} \frac{d}{dt} \frac{\|e_i(t)\|}{\|\delta(t)\|} &= \frac{e_i^T(t) \dot{e}_i(t)}{\|e_i(t)\| \|\delta(t)\|} - \frac{\|e_i(t)\| \delta^T(t) \dot{\delta}(t)}{\|\delta(t)\|^3} \\ &\leq \frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} + \frac{\|e_i(t)\|}{\|\delta(t)\|} \frac{\|\dot{\delta}(t)\|}{\|\delta(t)\|}. \end{aligned} \quad (7.49)$$

Since $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$, it follows from $\beta_i^2 = \frac{s_i}{2N\lambda_N^2(\mathcal{L})}$ and (7.33) that for $s_{\max} = \max_i s_i$, $i \in \mathcal{V}$,

$$\frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} \leq \|A\| \frac{\|e_i(t)\|}{\|\delta(t)\|} + \lambda_N(\mathcal{L}) \|BK\| \left(\frac{\|e(t)\|}{\|\delta(t)\|} + 1 \right). \quad (7.50)$$

By using (7.19) and $\|e(t)\| = \sum_{i=1}^N \|e_i(t)\| \leq \sqrt{Nc} \|\delta(t)\|$, the expression in (7.49) is rewritten as

$$\begin{aligned} \frac{d}{dt} \frac{\|e_i(t)\|}{\|\delta(t)\|} &\leq \|A\| \frac{\|e_i(t)\|}{\|\delta(t)\|} + \lambda_N(\mathcal{L}) \|BK\| \left(\frac{\|e(t)\|}{\|\delta(t)\|} + 1 \right) \\ &\quad + (\|A\| + \lambda_N(\mathcal{L}) \|BK\|) \frac{\|e_i(t)\|}{\|\delta(t)\|} + \sqrt{Nc} \lambda_N(\mathcal{L}) \|BK\| \frac{\|e_i(t)\|}{\|\delta(t)\|} \\ &= c_1 \frac{\|e_i(t)\|}{\|\delta(t)\|} + c_2, \end{aligned} \quad (7.51)$$

where $c_1 = 2\|A\| + c_2$ and $c_2 = \lambda_N(\mathcal{L}) \|BK\| (1 + \sqrt{Nc})$. Hence, we conclude that $\|e_i(t)\| / \|\delta(t)\|$ satisfies the bound $\|e_i(t)\| / \|\delta(t)\| < y(t, y_0)$, where $y(t, y_0)$ is the solution of $\dot{y}(t) = c_1 y(t) + c_2$, $y(0) = 0$.

Then the evolution time of $\|e_i(t)\| / \|\delta(t)\|$ from 0 to \sqrt{c} is lower bounded by

$$\mathfrak{B} = \frac{1}{c_1} \ln\left(\frac{c_1}{c_2} \sqrt{c} + 1\right) = \frac{1}{c_1} \ln\left(\frac{c_1}{c_2} \sqrt{\frac{2\gamma_2 \lambda_N^2(\mathcal{L})}{N(1-s_{\max})}} + 1\right). \quad (7.52)$$

Thus, for each agent in $R_2(t)$ the inter-event time is chosen as a strictly positive real number $b_i \leq \mathfrak{B}$ to guarantee (7.47). It therefore concludes that the distributed secure controller (7.7) with the event trigger (7.14) for $t_{k_i}^i \notin \mathcal{A}_m$ guarantee that (7.45) holds for all the agents in $R_1(t) \cup R_2(t) = \{1, 2, \dots, N\}$, which implies that $V(t)$ converges to zero. Specifically, it follows from (7.27) and (7.38) that

$$b_1 \|\delta_i(t)\|^2 \leq V(t), \quad V(0) \leq a_1 \|\delta_i(0)\|^2, \quad (7.53)$$

where $a_1 = \max\{\lambda_{\max}(P), \lambda_{\max}(S)\}$ and $b_1 = \min\{\lambda_{\min}(P), \lambda_{\min}(S)\}$. Let $\kappa_1 = \frac{a_1}{b_1} e^{(\alpha_1 + \alpha_2)(T_0 + \Delta^*)}$. Thus, combining (7.45) and (7.53) yields

$$\|\delta_i(t)\|^2 \leq \kappa_1 e^{-\eta_1 t} \|\delta_i(0)\|^2, \quad (7.54)$$

which implies that all the agents will exponentially achieve secure leaderless consensus. Furthermore, it is trivial that (7.4) in Definition 7.1 holds because $\|\delta_i(t)\|^2 = 0$ as $t \rightarrow +\infty$. That is, $\lim_{t \rightarrow +\infty} x_i(t) = \frac{1}{N} \sum_{i=1}^N x_i(0)$. \square

7.4 Secure Leader-Following Consensus

For the defined graph $\tilde{\mathcal{G}}$, its Laplacian matrix is $\tilde{\mathcal{L}} = \begin{pmatrix} 0_{1 \times 1} & 0_{1 \times N} \\ -\mathcal{B}1_N & \mathcal{L} + \mathcal{B} \end{pmatrix}$, where \mathcal{B} is a nonnegative diagonal matrix whose i th diagonal element is a_{i0} , where $a_{i0} > 0$ if $(0, i) \in \tilde{\mathcal{E}}$ and $a_{i0} = 0$ if otherwise. Define an information-exchange matrix $\mathcal{H} = \mathcal{L} + \mathcal{B}$, then \mathcal{H} is asymmetric for a digraph. In such a case, if we choose a Lyapunov function $\delta^T \mathcal{H} \delta$, then the term $-\delta^T \mathcal{H} \delta$ will appear in its derivative. Thus, it is unclear how the aforementioned controller can be applied. Hence, a distributed event-triggered control scheme is needed to solve the problem under a directed graph.

7.4.1 Leader-Following Event-Triggered Controller Design

Similar to that in section 7.3, a distributed event-triggered control law for systems (7.1) and (7.5) is designed as:

$$u_i(t) = \tilde{K} \left(\sum_{j=1}^N a_{ij} (\hat{x}_j(t) - \hat{x}_i(t)) + a_{i0} (\hat{x}_0(t) - \hat{x}_i(t)) \right), \quad (7.55)$$

where \tilde{K} is the controller gain matrix to be determined, and $\hat{x}_i(t)$ and $\hat{x}_j(t)$ are similarly designed in (7.9) and (7.10). We assume that the leader knows its own state, i.e., $\hat{x}_0(t) = x_0(t)$ when the leader is a neighbor of the followers.

Based on the defined measurement error $e_i(t)$ in (7.11), it is desired to employ the control update rule that can keep $e_i(t)$ small in a suitable sense:

$$\begin{aligned} \|e_i(t)\| &= \|\hat{x}_i(t) - x_i(t)\| \leq \tilde{\beta}_i \|\hat{z}_i(t)\|, \quad \tilde{\beta}_i > 0, \\ \hat{z}_i(t) &= \sum_{j \in \mathcal{N}_i(\tilde{\mathcal{G}})} a_{ij} (\hat{x}_j(t) - \hat{x}_i(t)), \quad i \in \tilde{\mathcal{V}}. \end{aligned} \quad (7.56)$$

Similar to that in section 7.3, the following scheme is proposed for agent i

$$t_{k_i+1}^i = t_{k_i}^i + \tilde{\Delta}_{k_i}^i, \quad \tilde{\Delta}_{k_i}^i = \max\{\tilde{\tau}_{k_i}^i, \tilde{b}_i\}, \quad (7.57)$$

where $\tilde{\Delta}_{k_i}^i$ is the new inter-execution interval, \tilde{b}_i is a strictly positive real number to

be determined, and $\tilde{\tau}_{k_i}^i$ is given by $\tilde{\tau}_{k_i}^i = \inf_{t > t_{k_i}^i} \{t - t_{k_i}^i \mid \|e_i(t)\| = \tilde{\beta}_i \|\hat{z}_i(t)\|\}$.

7.4.2 Stability Analysis of Secure Leader-Following Case

Assumption 7.2. Assume that the communication graph $\tilde{\mathcal{G}}$ is directed and the leader is globally reachable in $\tilde{\mathcal{G}}$.

Lemma 7.1. [64] Under Assumption 7.2, \mathcal{H} is nonsingular and all the eigenvalues of \mathcal{H} have positive real parts.

Lemma 7.2. [135] Under Assumption 7.2 and Lemma 7.1, there exists a positive diagonal matrix Ω such that $\Omega = \Theta\mathcal{H} + \mathcal{H}^T\Theta > 0$. One such Θ is given by $\text{diag}\{\theta_1^{-1}, \dots, \theta_N^{-1}\}$ where $\theta = [\theta_1^{-1}, \dots, \theta_N^{-1}]^T = (\mathcal{H}^T)^{-1}\mathbf{1}_N$.

Define the state tracking error between the followers and leader as $\eta_i(t) = x_i(t) - x_0(t)$. Let $\eta(t) = \text{col}(\eta_1, \dots, \eta_N)$. From the definitions of $u_i(t)$ and $\eta_i(t)$, it is obtained that the dynamics of the agent group can be written in a compact form:

$$\dot{\eta}(t) = [I_N \otimes A - (\mathcal{H} \otimes BK)]\eta(t) - (\mathcal{H} \otimes BK)e(t). \quad (7.58)$$

Theorem 7.2. Consider a group of N agents with dynamics in (7.1) and (7.5). Suppose that Assumption 7.2 holds. Given any positive symmetric definite matrices $\tilde{R} > 0$ and $\tilde{Q} > 0$, there exists a unique symmetric positive definite matrix $\tilde{P} > 0$ such that the following ARE is satisfied.

$$\tilde{P}A + A^T\tilde{P} - \tilde{P}B\tilde{R}^{-1}B^T\tilde{P} + \tilde{Q} = 0. \quad (7.59)$$

Let $\tilde{\gamma}_1, \tilde{\gamma}_2 \in \mathbb{R}^+$ satisfy: $\tilde{\gamma}_1 + \tilde{\gamma}_2 = \tilde{\gamma} < 1$. If $\tilde{\beta}_i^2 = \tilde{s}_i(\tilde{k}_2 - \frac{\tilde{k}_4}{\tilde{\varrho}})/(\tilde{k}_3 + \tilde{k}_4\tilde{\varrho}) \leq \tilde{\gamma}_1$, $\tilde{s}_i \in (0, 1)$, $\tilde{\varrho} > \tilde{k}_4/\tilde{k}_2 > 0$ and \tilde{b}_i in (7.57) is strictly positive with

$$\tilde{b}_i \leq \frac{1}{\tilde{c}_1} \ln(\frac{\tilde{c}_1}{\tilde{c}_2} \sqrt{\frac{\tilde{\gamma}_2}{N}} + 1),^2 \quad (7.60)$$

then under the proposed event-based distributed control law (7.55) with $\tilde{K} = \tilde{\tau}\tilde{R}^{-1}B^T\tilde{P}$, $\tilde{\tau} \geq \lambda_{\min}^{-1}(\Omega)\theta_{\min}^{-1}$, where $\Omega = \Theta\mathcal{H} + \mathcal{H}^T\Theta > 0$ is defined in Lemma 7.2, the agent group will achieve secure leader-following consensus, provided that

$$\frac{2\tilde{k}_2}{\tilde{H}} = k_{\min}^2 \sigma_{\min}(\tilde{\mathcal{H}}^T \tilde{\mathcal{H}}), \tilde{k}_3 = \sigma_{\max}(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K}) - k_{\min}^2, \tilde{k}_4 = \sigma_{\max}(\tilde{\mathcal{H}}^T \Theta\mathcal{H} \otimes \tilde{P}B\tilde{K} - k_{\min}^2 \tilde{\mathcal{H}}^T), \tilde{\mathcal{H}} = \mathcal{H}^{-1} \otimes I_n, k_{\min} = k_{\min}^1 + k_{\min}^2 = \lambda_{\min}(\Theta \otimes \tilde{Q}), \tilde{c}_1 = 2\|A\| \text{ and } \tilde{c}_2 = 2\|\mathcal{H} \otimes BK\| \sqrt{\tilde{\gamma}_2} + \|BK\|.$$

1. There exists a constant $\tilde{\eta}_1^* \in (0, \tilde{\alpha}_1)$ such that the attack frequency $F_a(t_0, t)$ is

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \leq \frac{\tilde{\eta}_1^*}{\ln(\tilde{\mu}) + (\tilde{\alpha}_1 + \tilde{\alpha}_2)\tilde{\Delta}_*}, \quad (7.61)$$

2. There exists a constant τ_a in the attack duration Definition 7.4 such that

$$\tau_a > (\tilde{\alpha}_1 + \tilde{\alpha}_2)/(\tilde{\alpha}_1 + \tilde{\eta}_1^*), \quad (7.62)$$

where $\tilde{\alpha}_1 = k_{\min 1} \lambda_{\max}^{-1}(\theta_i^{-1} \tilde{P})$, $\tilde{\alpha}_2 > 0$ such that for $\tilde{S} > 0$, $\tilde{S}A + A^T \tilde{S} - \tilde{\alpha}_2 \tilde{S} < 0$, $\tilde{\mu} = \max\{\lambda_{\max}(\tilde{P})/\lambda_{\min}(\tilde{S}), \lambda_{\max}(\tilde{S})/\lambda_{\min}(\tilde{P})\}$ and $\tilde{\Delta}_*$ satisfies: $\sup_{(i, k_i) \in \mathcal{F}} \tilde{\Delta}_{k_i}^i \leq \tilde{\Delta}_*$.

The event instants are obtained by (7.57) and no agent will exhibit Zeno behavior.

Proof. **(I) Resilience analysis**

Step 1: Two intervals classification

This part is similar to that in (7.24)-(7.26) for the new controller update sequence $\{t_{k_i}^i\}$ determined by (7.57) and thus is omitted.

Step 2: Lyapunov stability analysis

(1). Consider the time interval $\tilde{\Xi}_s(\tau, t)$ over which (7.56) holds. Let

$$V(\eta(t)) = \sum_{i=1}^N \theta_i^{-1} \eta_i^T(t) \tilde{P} \eta_i(t), \quad i = 1, 2, \dots, N. \quad (7.63)$$

Taking the time-derivative of $V(\eta(t))$ along the closed-loop error system (7.58) yields the following equality for $\Omega = \Theta \mathcal{H} + \mathcal{H}^T \Theta > 0$ is used in Lemma 7.2,

$$\begin{aligned} \dot{V}(t) &= 2\eta^T(t)(\Theta \otimes \tilde{P})[I_N \otimes A - (\mathcal{H} \otimes B\tilde{K})]\eta(t) - 2\eta^T(t)(\Theta \otimes \tilde{P})(\mathcal{H} \otimes B\tilde{K})e(t) \\ &= \eta^T(t)[\Theta \otimes (\tilde{P}A + A^T \tilde{P}) - \Omega \otimes \tilde{P}B\tilde{K}]\eta(t) - \eta^T(t)(\Theta \mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t). \end{aligned}$$

Substituting $\tilde{K} = \tilde{\tau} \tilde{R}^{-1} B^T \tilde{P}$ into the above inequality yields

$$\begin{aligned} \dot{V}(t) &\leq \eta^T(t)(\Theta \otimes (\tilde{P}A + A^T \tilde{P}))\eta(t) - \tilde{\tau} \lambda_{\min}(\Omega) \theta_{\min} \times \eta^T(t)(\Theta \otimes \tilde{P}B\tilde{R}^{-1}B^T \tilde{P})\eta(t) \\ &\quad - \eta^T(t)(\Theta \mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) \\ &\leq \eta^T(t)[\Theta \otimes (\tilde{P}A + A^T \tilde{P} - \tilde{P}B\tilde{R}^{-1}B^T \tilde{P})]\eta(t) - \eta^T(t)(\Theta \mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t), \end{aligned}$$

where $\theta_{\min} = \min \theta_i^{-1}$, $i \in \mathcal{V}$ and $\tilde{\tau} \geq \lambda_{\min}^{-1}(\Omega) \theta_{\min}^{-1}$.

By using (7.59) and denoting $k_{\min} = \lambda_{\min}(\Theta \otimes \tilde{Q})$, it has

$$\begin{aligned}\dot{V}(t) &\leq -\eta^T(t)(\Theta \otimes \tilde{Q})\eta(t) - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) \\ &\leq -k_{\min}\eta^T(t)\eta(t) - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t).\end{aligned}\quad (7.64)$$

Since $\eta_i(t) = x_i(t) - x_0(t)$, $e_i(t) = \hat{x}_i(t) - x_i(t)$ and $\hat{z}_i(t) = \sum_{j \in \mathcal{N}_i(\tilde{\mathcal{G}})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t))$, it is obtained that

$$\eta(t) = \hat{x}(t) - (1_N \otimes x_0(t)) - e(t), \hat{z}(t) = (\mathcal{H} \otimes I_n)(1_N \otimes x_0(t) - \hat{x}(t)), \quad (7.65)$$

which implies that

$$\eta(t) = -(\mathcal{H} \otimes I_n)^{-1}\hat{z}(t) - e(t), \quad (7.66)$$

where $\hat{z}(t) = \text{col}(\hat{z}_1, \dots, \hat{z}_N)$ is governed by the dynamics: $\dot{\hat{z}}(t) = (I_N \otimes A)\hat{z}(t)$ obtained from (7.5), (7.9) and (7.10).

After substituting (7.66) into (7.64) and letting $k_{\min} = k_{\min}^1 + k_{\min}^2$, it has

$$\begin{aligned}\dot{V}(t) &\leq -k_{\min 1}\eta^T(t)\eta(t) - k_{\min 2}\hat{z}^T(t)(\mathcal{H}^{-T}\mathcal{H}^{-1} \otimes I_n)\hat{z}(t) \\ &\quad - 2k_{\min 2}e^T(t)(\mathcal{H}^{-1} \otimes I_n)\hat{z}(t) - k_{\min 2}e^T(t)e(t) \\ &\quad + \hat{z}(t)^T(\mathcal{H}^{-T}\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) + e^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t).\end{aligned}\quad (7.67)$$

By using Young's inequality: $x^T y \leq \frac{\tilde{\varrho}}{2}x^T x + \frac{1}{2\tilde{\varrho}}y^T y$ for any $\tilde{\varrho} > 0$, one has

$$\begin{aligned}\dot{V}(t) &\leq -k_{\min 1}\eta^T(t)\eta(t) - \tilde{k}_2\hat{z}^T(t)\hat{z}(t) + \tilde{k}_3e^T(t)e(t) \\ &\quad + 2\tilde{k}_4\left(\frac{\tilde{\varrho}}{2}e^T(t)e(t) + \frac{1}{2\tilde{\varrho}}\hat{z}^T(t)\hat{z}(t)\right) \\ &\leq -k_{\min 1}\eta^T(t)\eta(t) - \left(\tilde{k}_2 - \frac{\tilde{k}_4}{\tilde{\varrho}}\right)\hat{z}^T(t)\hat{z}(t) + (\tilde{k}_3 + \tilde{k}_4\tilde{\varrho})e^T(t)e(t),\end{aligned}\quad (7.68)$$

where $\tilde{k}_2 = k_{\min}^2\sigma_{\min}(\tilde{\mathcal{H}}^T\tilde{\mathcal{H}})$, $\tilde{k}_3 = \sigma_{\max}(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K}) - k_{\min}^2$, $\tilde{k}_4 = \sigma_{\max}(\tilde{\mathcal{H}}^T\Theta\mathcal{H} \otimes \tilde{P}B\tilde{K} - k_{\min}^2\tilde{\mathcal{H}}^T)$ and $\tilde{\mathcal{H}} = \mathcal{H}^{-1} \otimes I_n$.

Let $\|e_i(t)\| \leq \tilde{\beta}_i \|\hat{z}_i(t)\|$ with $\tilde{\beta}_i^2 = \tilde{s}_i(\tilde{k}_2 - \frac{\tilde{k}_4}{\tilde{\varrho}})/(\tilde{k}_3 + \tilde{k}_4\tilde{\varrho})$, $\tilde{\varrho} > \tilde{k}_4/\tilde{k}_2$ and $\tilde{s}_i \in$

(0, 1). Given $\tilde{\alpha}_1 = k_{\min}^1 \lambda_{\max}^{-1}(\Theta \otimes \tilde{P})$, then (7.68) can be rewritten as

$$\begin{aligned} \dot{V}(t) &\leq -k_{\min} \sum_{i=1}^N \eta_i^T(t) \eta_i(t) - \sum_{i=1}^N (1 - \tilde{s}_i) \hat{z}^T(t) \hat{z}(t) \\ &\leq -k_{\min} \lambda_{\max}^{-1}(\theta_i^{-1} \tilde{P}) \sum_{i=1}^N \theta_i^{-1} \eta_i^T(t) \tilde{P} \eta_i(t) = -\tilde{\alpha}_1 V(t). \end{aligned} \quad (7.69)$$

(2). Consider the time interval $\tilde{\Xi}_s(\tau, t)$ over which (7.12) does not necessarily hold.

Choose a Lyapunov function:

$$V(t) = \eta^T(t) (I_N \otimes \tilde{S}) \eta(t), \quad (7.70)$$

which yields that for $\tilde{S}A + A^T \tilde{S} - \tilde{\alpha}_2 \tilde{S} < 0$, it has

$$\dot{V}(t) = \eta^T(t) [I_N \otimes (\tilde{S}A + A^T \tilde{S})] \eta(t) \leq \tilde{\alpha}_2 V(t). \quad (7.71)$$

Denote $\tilde{\sigma}(t) \in \{\tilde{a}, \tilde{b}\}$ as a new piecewise constant function. Similar to that in (7.40), it follows from (7.69) and (7.71) that

$$V(\eta(t)) \leq \begin{cases} e^{-\alpha_1(t - \tilde{t}_{m-1} - \tilde{\Delta}_{m-1})} V_{\tilde{a}}(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}), \\ e^{\alpha_2(t - \tilde{t}_m)} V_{\tilde{b}}(\tilde{t}_m). \end{cases} \quad (7.72)$$

Step 3: Bounds on DoS attack frequency and duration

Similar to (7.41)-(7.45), when the DoS attack frequency and duration conditions in (7.61) and (7.62) are satisfied, then there exists a constant $\tilde{\eta}_1 = \tilde{\alpha}_1 - \frac{(\tilde{\alpha}_1 + \tilde{\alpha}_2)}{\tau_a} - \tilde{\eta}_1^* > 0$

$$V(\eta(t)) \leq e^{(\tilde{\alpha}_1 + \tilde{\alpha}_2)(T_0 + \tilde{\Delta}_*)} e^{-\tilde{\eta}_1(t - t_0)} V(\eta(t_0)). \quad (7.73)$$

(II). Minimal inter-event interval

Following a similar way in above subsection, one can estimate the time derivative of $\|e_i(t)\| / \|\hat{z}(t)\|$ to obtain $\|\dot{e}_i(t)\| / \|\hat{z}(t)\| \leq \tilde{c}_1 \frac{\|e_i(t)\|}{\|\hat{z}(t)\|} + \tilde{c}_2$ with $\tilde{c}_1 = 2\|A\|$ and $\tilde{c}_2 = 2\|\mathcal{H} \otimes BK\| \sqrt{\tilde{\gamma}_2} + \|BK\|$. The evolution time of $\|e_i(t)\| / \|\hat{z}(t)\|$ from 0 to $\sqrt{\tilde{c}}$ is thus lower bounded by $\tilde{\mathfrak{B}} = \frac{1}{\tilde{c}_1} \ln(\frac{\tilde{c}_1}{\tilde{c}_2} \sqrt{\tilde{c}} + 1)$ with $\tilde{c} = \tilde{\gamma}_2/N$. Moreover, denote $\tilde{\kappa}_1 = (\tilde{a}_1/\tilde{b}_1) e^{(\tilde{\alpha}_1 + \tilde{\alpha}_2)(T_0 + \tilde{\Delta}_*)}$ with $\tilde{a}_1 = \max\{\lambda_{\max}(\Theta \otimes \tilde{P}), \lambda_{\max}(\tilde{S})\}$ and $\tilde{b}_1 = \min\{\lambda_{\min}(\Theta \otimes \tilde{P}), \lambda_{\min}(\tilde{S})\}$. By (7.73), $\|\eta_i(t)\|^2 \leq \tilde{\kappa}_1 e^{-\tilde{\eta}_1 t} \|\eta_i(0)\|^2$, which implies (7.6). \square

7.5 Numerical Example

In this subsection, to analyze the performance of the proposed distributed control algorithms for multi-agent systems in the presence of DoS attacks, two distributed control applications are provided: 1) Distributed multi-robot coordination; (2) Distributed voltage regulation of Microgrid.

Example 7.1. *Distributed Multi-Robot Coordination*

7.5.1 Multi-Robot Simulation Setup & Conditions

In this example, a multi-robot system simulator is developed in MATLAB/Simulink to validate the effectiveness of the proposed event-based distributed controller designs. Repeatable simulations can be designed under a wide range of network environments, system conditions and network settings. The following control task is tested in the simulation: keep all the six robots in a line and achieve consensus on their position and velocity.

Consider a group of 6 robots in \mathbb{R}^2 with dynamics given by

$$\dot{x}_i(t) = \begin{bmatrix} 0 & -0.5 \\ 0.5 & 0 \end{bmatrix} x_i(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_i(t),$$

where $x_i(t) = [x_{i1}(t), x_{i2}(t)]^T$ is the state for agent $i = 1, \dots, 6$, and $u_i(t)$ is the control input. The eigenvalues of matrix A are: $0 \pm 0.5i$ ($i = \sqrt{-1}$). One can easily verify that the matrix pair (A, B) is controllable.

7.5.2 Secure Leaderless Consensus

The undirected communication topology is given in Fig. 7.4(a). According to Theorem 7.1, $K = [-0.2500, 0.4330]$, $\alpha_1 = 0.0289$ and $\alpha_2 = 0.0611$, given that $\lambda_2(\mathcal{L}) = 2.0$, $R = 0.5$, $Q = I_2$. Choose $s_i = 0.05 < s_{\max} = 0.0588$ and $\beta_i = 0.04$. Fig. 7.5 provides the simulation results under the proposed distributed event-triggered controller (7.7) with an estimator in (7.9) and (7.10). The DoS attack signal is

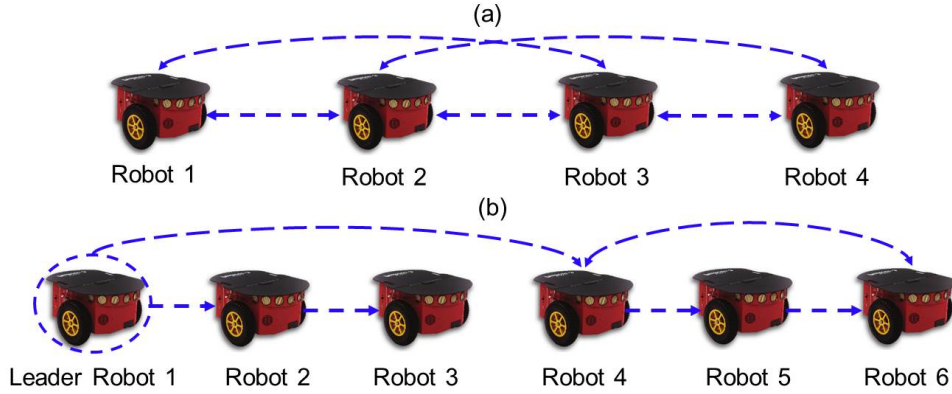


Figure 7.4: Communication topology of a multi-robot system: (a) in a leaderless consensus case; and (b) in a leader-follower consensus case.

simulated in Fig. 7.5(A) with $\tau_a = 6.25s$. Thus, the two conditions in (7.22) and (7.23) are satisfied with $F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \leq 0.01$ and $\tau_a > (\alpha_1 + \alpha_2)/(\alpha_1 + \eta_1^*) = 3$, which means that the DoS attack cannot occur more than 0.01 times during a unit of time and its duration is smaller than 6.25s. Fig. 7.5(B) shows the state $x_{ij}(t)$ and Fig. 7.5(C) shows the error $Error_\delta(t) = 0.25\sqrt{\sum_{i=1}^4 \delta_i^T(t)\delta_i(t)}$. The sawtooth waves display the jumps of controller when events are triggered and Fig. 7.5(D) shows the triggered events for each robot.

7.5.3 Secure Leader-Following Consensus

The directed communication topology is shown in Fig. 7.4(b). By Theorem 7.2, $\tilde{K} = [-3.9957, 6.9208]$, $\tilde{\alpha}_1 = 0.48$, and $\tilde{\alpha}_2 = 1.02$. Choose $\tilde{\beta}_i = 0.2$. The simulation results are provided in Fig. 7.6 by the controller (7.55) with (7.9) and (7.10). The DoS attack signal is simulated in Fig. 7.6(A) with $\tau_a = 5s$. (7.61) and (7.62) are satisfied. Fig. 7.6(B) shows the state $\eta_{ij}(t), i = 1, \dots, 6, j = 1, 2$ and Fig. 7.6(C) shows the consensus error $Error_\eta(t) = 0.2\sqrt{\sum_{i=2}^6 \|x_i(t) - x_1(t)\|^2}$. Fig. 7.6(D) shows the triggered events for each robot.

Example 7.2. Distributed Voltage Regulation

A power system example is provided to demonstrate the effectiveness of designs.

Consider a power system with the dynamics of distributed generators (DGs) given in [105] where distributed secondary voltage control of microgrid can be formulated as the following leader-following consensus problem, i.e., all DGs synchronize their terminal voltage amplitude to a prespecified reference value with:

$$\dot{y}_i(t) = Ay_i(t) + Bu_i(t), \quad \dot{y}_0(t) = Ay_0(t), \quad (7.74)$$

where $y_i(t) = [v_{o,magi}, \dot{v}_{o,magi}]^T$, $y_0(t) = [v_{ref}, 0]^T$, $B = [0, 1]^T$ and $A = [0, 1; 0, 0]$.

However, this multi-agent microgrid consists of large-scale physical processes monitored and controlled over a set of communication networks and computers. Due to

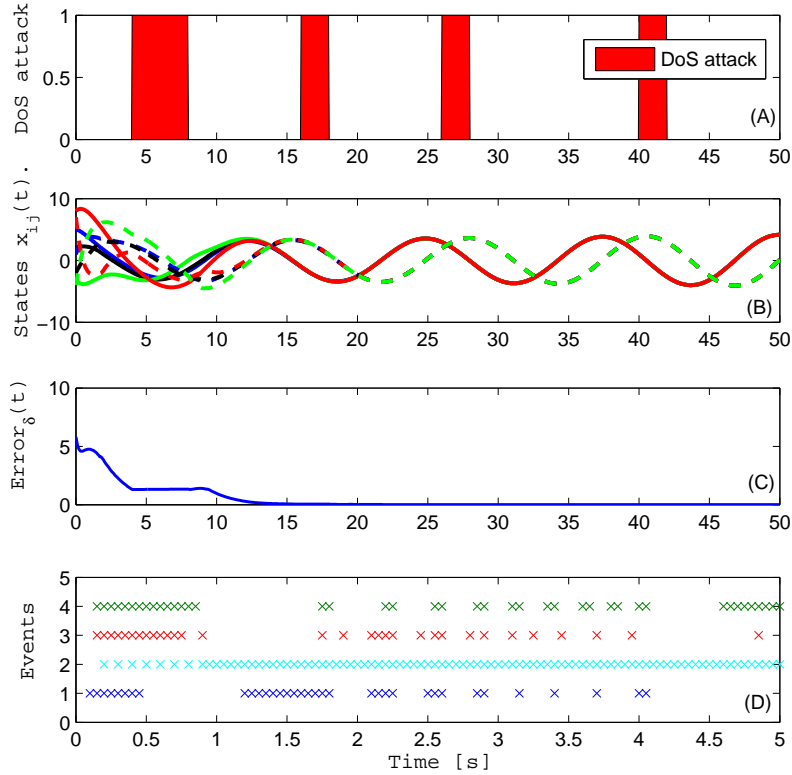


Figure 7.5: Simulation results for secure consensus in the presence of DoS attack: (A) a sustained DoS attack with varying period and duty cycle, generated randomly. The vertical red stripes represent the time-intervals over which a DoS attack is active and it has an average duty cycle of 24%; (B) state trajectory $x_{ij}(t)$, $i = 1, 2, 3, 4, j = 1, 2$; (C) consensus error $Error_\delta(t)$; (D) occurrences of the events for all the robots.

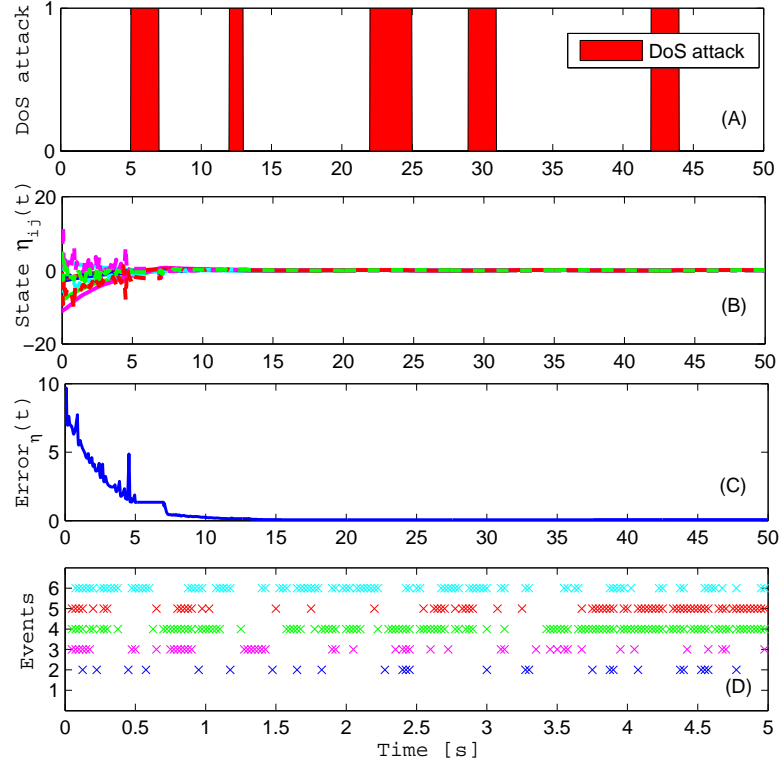


Figure 7.6: Simulation results for secure leader-following consensus in the presence of DoS attack: (A) a sustained DoS attack with an average duty cycle of 20%; (B) state trajectory $\eta_{ij}(t)$, $i = 2, \dots, 6, j = 1, 2$; (C) consensus tracking error $Error_\eta(t)$; (D) occurrences of the events for all the robots.

the use of modern network ICT, the cyber layer for distributed secondary control in Fig. 7.7 is vulnerable to cyber-attacks, e.g., DoS attacks: interruptions of communication on distributed secondary control channels carried out by an intelligent adversary. The DoS attack model is described in subsection 7.2.2. Next, the goal is to design an event-based distributed controller $u_i(t) = \tilde{K} \sum_{j \in \mathcal{N}_i(\bar{g})} a_{ij}(\hat{y}_j(t) - \hat{y}_i(t))$ with $\hat{y}_j(t)$ similarly defined in (7.9), so that $y_i(t) \rightarrow y_0(t)$.

7.5.4 Microgrid Simulation Setup & Conditions

In order to test the designed distributed secondary controller, a 220-V (per phase rms) 50-Hz islanded microgrid is considered as the test system. The simulation is conducted in MATLAB/Simulink environment. Fig. 7.8 illustrates the single-line

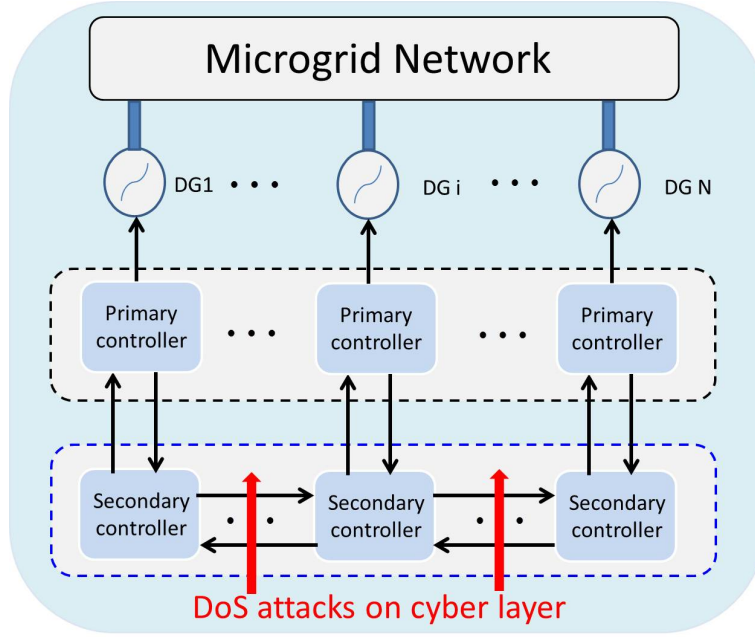


Figure 7.7: Distributed secondary control diagram of an islanded MG.

diagram of the microgrid test system. This islanded microgrid consists of four DGs and the lines between buses are modeled as series RL branches. The parameters of the whole test system are given in [105] and the reference voltage is 1.05 p.u. In this example, we assume that DGs communicate with each other through the communication digraph. This communication digraph for distributed secondary voltage control is also shown in Fig. 7.8 where the reference voltage values are only known to DG1, i.e., $a_{10} = 1$ and $a_{i0} = 0$, $i = 2, 3, 4$.

7.5.5 Secure Voltage Regulation

By Theorem 7.2, $\tilde{K} = [5.0, 8.6603]$, $\tilde{\alpha}_1 = 0.6$ and $\tilde{\alpha}_2 = 1.4$. The microgrid is islanded from the main grid at $t = 0s$, while the secondary control is applied at $t = 2.5s$. Choose $\tilde{\beta}_i = 0.5$. The simulation results are provided in Fig. 7.9. The DoS attack signal is simulated in Fig. 7.9(A) with $\tau_a = 5s$. As seen in Fig. 7.9(B), while the primary control keeps the voltage amplitudes stable, the secondary control returns all terminal voltage amplitudes to the prespecified reference values after 2.5s. Fig. 7.9(C) shows the voltage regulation error $Error_V(t) = 0.25\sqrt{\sum_{i=1}^4 \|y_i(t) - y_0(t)\|^2}$.

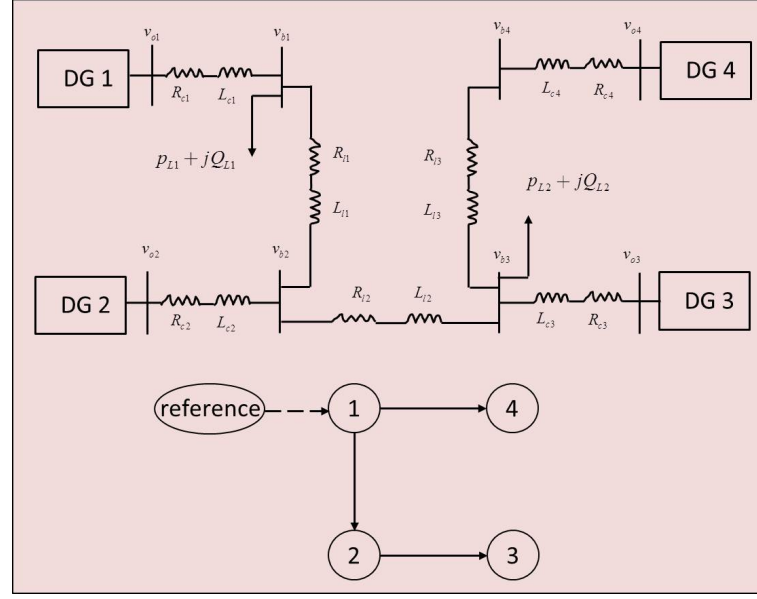


Figure 7.8: Simulation microgrid test system.

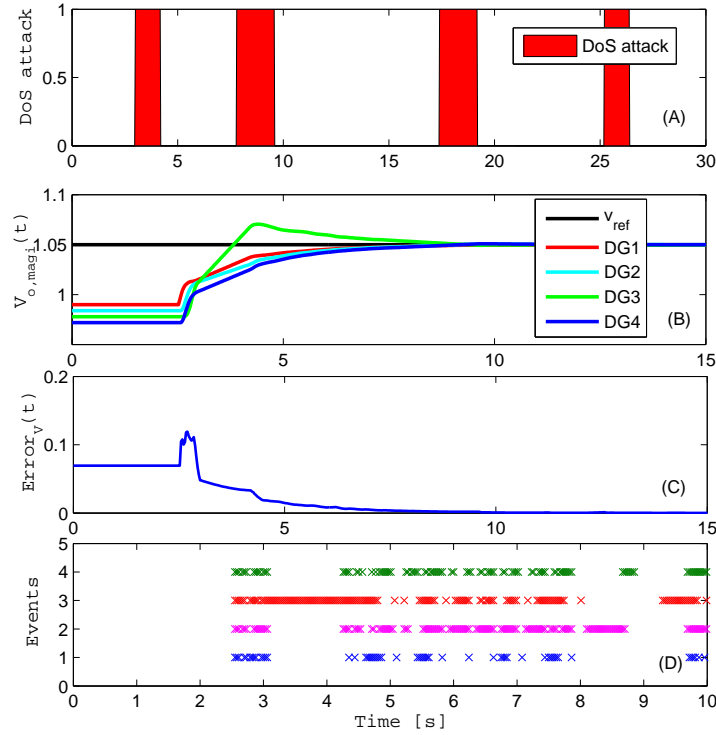


Figure 7.9: Simulation results for distributed voltage regulation of microgrid in the presence of DoS attack: (A) a sustained DoS attack with an average duty cycle of 20%; (B) state trajectory $V_{o, magi}(t)$, $i = 1, \dots, 4$; (C) voltage regulation error $Error_V(t)$; (D) occurrences of the events for all DGs.

7.6 Conclusion

In this work, we studied event-triggered secure coordination of linear multi-agent systems under DoS attacks. Both secure leaderless and leader-following consensus are investigated, respectively. Distributed event-triggered control schemes are developed. It is proven that under the proposed algorithms, the agent group can achieve secure consensus exponentially, provided that the frequency and duration of DoS attacks satisfy certain conditions.

Chapter 8

Conclusions and Future Work

8.1 Conclusions

In this dissertation, distributed resilient coordination is investigated for networked multi-agent systems in complex environments. On one hand, when the systems are subject to unknown uncertainties and disturbances, distributed robust cooperative control is studied. On the other hand, when the systems are subject to different types of cyber-attacks, distributed secure coordination is considered. Several methods are proposed to solve distributed robust and secure coordination problems, respectively. To demonstrate the practical applications of proposed algorithms, distributed multi-robot coordination and distributed voltage regulation of microgrid are considered, respectively. More specifically, the distributed resilient coordination problem in this dissertation is studied from the following aspects:

- Robust distributed coordinated control of multiple Euler-Lagrange systems via an identifier-based distributed control approach;
- Robust connectivity preserving rendezvous of multi-robot systems based on a potential function design;
- Distributed secure coordinated control under two types of switching attacks;
- Event-based distributed resilient coordination under DoS attacks.

First of all, a robust consensus tracking problem is addressed for multiple unknown Euler-Lagrange systems under both undirected and directed graphs. A distributed nonlinear identifier is developed to compensate for these uncertainties and distributed control law combined with this identifier is then developed to ensure robust consensus tracking asymptotically. Furthermore, a distributed two-layer coordination scheme is developed in the directed case to enable the agent group to achieve robust consensus tracking asymptotically.

The application of this identifier-based distributed design is studied in robust connectivity preserving rendezvous for multi-robot systems. The problem is solved by using a gradient-based approach. A distributed PID controller is thus proposed. This robust distributed control law not only maintains the connectivity of the multi-robot system, but also achieves asymptotic consensus tracking.

In addition, we deal with distributed secure coordination issues for multi-agent systems under two types of switching attacks. Attack scenarios where the attackers launch attacks on communication links instead of agents are considered. Firstly, we model a class of connectivity-maintained/broken attacks and a distributed secure controller is developed to achieve secure consensus from a switching perspective. Secondly, this work is extended to secure cooperative control in the presence of strategic attacks whose dynamics are captured by a random Markov process. A hybrid stochastic secure control framework is proposed and secure consensus tracking is obtained in a mean-square sense.

At last, a distributed control strategy is proposed to solve an event-based resilient coordination problem for linear multi-agent systems under DoS attacks. We model a time-sequence-based DoS attack allowed to occur aperiodically in an unknown attack strategy. An explicit analysis of frequency and duration of DoS attacks is studied for two linear secure consensus issues. An event-based distributed control scheme is proposed and suitable scheduling of controller updating times is determined in the presence of DoS attacks such that the agent group can achieve secure consensus.

8.2 Future Work

As stated in chapter 1, a hierarchical distributed resilient monitoring and control framework is proposed for studying resilient coordination problems in this thesis. In Part I, we developed distributed robust schemes to deal with uncertainties and disturbances on physical plants in the bottom layer. In Part II, we developed distributed secure schemes against malicious attacks on cyber space. In the top layer, we will study risk security management involving human decision makers who are in charge of economic and social control optimization. Resilience of networked multi-agent systems can be built via this multi-layer distributed resilient design. The following studies several research directions to explore extending the works.

Exploration and study of distributed robust coordination

In Part I, the model-free distributed control law design requires an undirected graph with two-hop communication. A directed graph case is studied to remove this requirement for a specified leader system. The distributed leader estimator imposes assumptions that the desired time-varying trajectory is generated by some linear autonomous systems and the S matrix is known by all followers. It is of significance to extend the work to directed graph case for an arbitrary time-varying leader system. The studied model-free distributed design can thus cover more general cases in many practical problems. On the other hand, the performance requirements e.g., fast consensus tracking, are not studied in this work. The research on how to optimize the network topology and parameters to obtain faster convergence rate is still very limited. One of the potential future directions is to design the distributed integral sliding mode or super twisting algorithms to solve this problem.

Attack diagnosis and resilient control for specific malicious attacks

In part II, two types of switching attacks and DoS attacks are studied. Nevertheless, we only solve resilient control problems via a hybrid secure control approach.

(1) There is a growing need for attack diagnosis techniques for more skilled and specific malicious attacks with certain capacities.

(2) Much research is required for detecting and identifying the attack strategies and studying how the attacker selects its strategies.

(3) Novel attack-resilient control methods and trade-offs between system performance and resilience are needed to study for best resilient designs.

Distributed resilient optimization under vulnerability environments

The objective is to optimize the integrated influences of multiple vulnerabilities, such as uncertainties from physical space, malicious attacks from cyber space as well as strategic decision makers in the design process. As proposed in chapter 1, a hierarchical distributed resilient framework can be developed to solve optimal issues.

(1) How game theory and distributed optimization approaches can be employed to provide optimal resilient solutions? The challenges will be designs of both player and attacker objective functions and distributed optimal resilient schemes to achieve the optimal time-varying solutions.

(2) How to develop this comprehensive distributed optimal resilient framework with associated theory, algorithms and testbeds for systems involving physical components, cyber communications and social human decision makers?

(3) Some other issues are studied on communication topologies, complex dynamics, and learning and designs of architectures for performance improvement under optimal solutions. Game theory combined with potential approaches like model predictive control, event triggered control and other tools can be employed.

In summary, this thesis considers resilient coordination techniques for networked multi-agent systems from different perspectives. More efforts will be dedicated to studies on distributed optimal learning and control designs, cyber-security and resilience to diverse malicious attacks as well as the design and analysis of mechanisms in practical applications e.g., smart infrastructures.

Appendix A

$\mathcal{P}(t)$ Is Nonnegative (Chapter 3)

Lemma A.1. *Given the differential equation (3.24) in Chapter 3, a function $\mathcal{P}(t)$ defined as below is positive semi-definite*

$$\mathcal{P}(t) = E_f^T(0)\hat{\Pi}_1 \text{sgn}(E_f(0))\mathbf{1}_{Nl} - E_f^T(0)\Delta_d(0) - \mathcal{S}(t), \quad (\text{A.1})$$

where $\hat{\Pi}_1 \triangleq \text{diag}(\hat{\beta}_{11}, \dots, \hat{\beta}_{1N}) \otimes I_l \in \mathbb{R}^{Nl \times Nl}$ and $\mathcal{S}(t)$ is the Filippov generalized solution to the following defined differential equation

$$\dot{\mathcal{S}}(t) = r^T(t)\tilde{H}(\Delta_d(t) - \hat{\Pi}_1 \text{sgn}(E_f(t))\mathbf{1}_{Nl}), \quad (\text{A.2})$$

provided that the control gain $\hat{\beta}_{1i}$ satisfies for all $i \in \mathcal{V}$,

$$\hat{\beta}_{1i} > \|c_{1i}\|_\infty + \frac{1}{\alpha_{2i}} \|c_{2i}\|_\infty. \quad (\text{A.3})$$

Proof. The term $\mathcal{S}(t)$ is given by $\mathcal{S}(t) = \int_0^t r^T(\tau)\tilde{H}(\Delta_d(\tau) - \hat{\Pi}_1 \text{sgn}(E_f(\tau))\mathbf{1}_{Nl})d\tau$.

Since $\tilde{H}r = \dot{E}_f + \Lambda_2 E_f$, $\mathcal{S}(t)$ can be rewritten as

$$\begin{aligned} \mathcal{S}(t) &= \int_0^t (\dot{E}_f^T(\tau)\Delta_d(\tau) + E_f^T\Lambda_2\Delta_d(\tau))d\tau \\ &\quad - \int_0^t [\dot{E}_f^T(\tau)\hat{\Pi}_1 \text{sgn}(E_f(\tau))\mathbf{1}_{Nl} + E_f^T\Lambda_2\hat{\Pi}_1 \text{sgn}(E_f(\tau))\mathbf{1}_{Nl}]d\tau. \end{aligned} \quad (\text{A.4})$$

(A.4) can be rewritten as

$$\begin{aligned}\mathcal{S}(t) &= \int_0^t E_f^T \Lambda_2(\Delta_d(\tau) - \hat{\Pi}_1 \text{sgn}(E_f(\tau)) \mathbf{1}_{Nl}) d\tau \\ &+ \int_0^t \dot{E}_f^T(\tau) \Delta_d(\tau) d\tau + \int_0^t \dot{E}_f^T(\tau) \hat{\Pi}_1 \text{sgn}(E_f(\tau)) \mathbf{1}_{Nl} d\tau.\end{aligned}\quad (\text{A.5})$$

Integrating $\dot{E}_f^T(\tau) \hat{\Pi}_1 \text{sgn}(E_f(\tau)) \mathbf{1}_{Nl}$ and $\dot{E}_f^T(\tau) \Delta_d(\tau)$ gives

$$\begin{aligned}\int_0^t \dot{E}_f^T(\tau) \hat{\Pi}_1 \text{sgn}(E_f(\tau)) \mathbf{1}_{Nl} d\tau &= E_f^T(t) \hat{\Pi}_1 \text{sgn}(E_f(t)) \mathbf{1}_{Nl} - E_f^T(0) \hat{\Pi}_1 \text{sgn}(E_f(0)) \mathbf{1}_{Nl}, \\ \int_0^t \dot{E}_f^T(\tau) \Delta_d(\tau) d\tau &= E_f^T(t) \Delta_d(t) - E_f^T(0) \Delta_d(0) - \int_0^t E_f^T \dot{\Delta}_d(\tau) d\tau,\end{aligned}\quad (\text{A.6})$$

Thus, $\mathcal{S}(t)$ in (A.5) satisfies

$$\begin{aligned}\mathcal{S}(t) &= \int_0^t \left(\sum_m^{Nl} E_{f_m}(\tau) [\Lambda_{2m,m} \Delta_{d_m}(\tau) - \dot{\Delta}_{d_m}(\tau)] \right) d\tau + \sum_m^{Nl} |E_{f_m}(\tau)| \hat{\Pi}_{1m,m} \big|_0^t \\ &- \int_0^t \left(\sum_m^{Nl} |E_{f_m}(\tau)| \Lambda_{2m,m} \hat{\Pi}_{1m,m} \right) d\tau + E_f^T(t) \Delta_d(t) - E_f^T(0) \Delta_d(0),\end{aligned}\quad (\text{A.7})$$

Based on the fact that $\sup_{t \in [0, \infty)} |\Delta_{d_m}(t)| < c_{1m}$, and $\sup_{t \in [0, \infty)} |\dot{\Delta}_{d_m}(t)| < c_{2m}$ in (3.20), the upper bound of (A.7) is given by

$$\begin{aligned}\mathcal{S}(t) &\leq \int_0^t \left(\sum_m^{Nl} |E_{f_m}(\tau)| [\Lambda_{2m,m} c_{1m} + c_{2m} - \Lambda_{2m,m} \Pi_{1m,m}] \right) d\tau \\ &+ \sum_m^{Nl} |E_{f_m}(t)| (c_{1m} - \Pi_{1m,m}) + \sum_m^{Nl} |E_{f_m}(0)| - E_f^T(0) \Delta_d(0),\end{aligned}\quad (\text{A.8})$$

where c_{1m} and c_{2m} represent the m^{th} element of c_1 and c_m , $m = 1, 2, \dots, Nl$, respectively. Provided that the gain condition for $\hat{\beta}_{1i}$ in (A.3) is satisfied for each $i \in \mathcal{V}$, then $\mathcal{S}(t) \leq \sum_m^{Nl} |E_{f_m}(0)| - E_f^T(0) \Delta_d(0)$. Therefore, $\mathcal{S}(t)$ can be upper bounded as

$$\mathcal{S}(t) \leq E_f^T(0) \hat{\Pi}_1 \text{sgn}(E_f(0)) \mathbf{1}_{Nl} - E_f^T(0) \Delta_d(0), \quad (\text{A.9})$$

which yields that the function $\mathcal{P}(t) \geq 0$. \square

Appendix B

System (3.40) Is Stable.

Lemma B.1. *Given the following closed-loop error system and Assumption 3.5, then the origin of this error system is exponentially stable. That is, for all $i = 1, 2, \dots, N$, $\lim_{t \rightarrow \infty} \tilde{q}_i(t) = \mathbf{0}_l$. As a result, it can be seen that $\lim_{t \rightarrow \infty} q_{i1}(t) - q_d(t) = \mathbf{0}_l$ and $\lim_{t \rightarrow \infty} q_{i2}(t) - \dot{q}_d(t) = \mathbf{0}_l$ hold.*

$$\dot{\tilde{q}}(t) = [(I_N \otimes S) - \kappa(H \otimes I_{2l})]\tilde{q}(t). \quad (\text{B.1})$$

Proof. Define $\tilde{H} = \text{diag}\{k_1, k_2, \dots, k_N\}H$. Let $\lambda_i(S)$ and $\lambda_j(\tilde{H})$ be the eigenvalues of S and \tilde{H} , respectively. Let two matrices T and P be such that $T\tilde{H}T^{-1} = \Lambda_1$ and $PSP^{-1} = \Lambda_2$ where Λ_1 and Λ_2 are the Jordan form of \tilde{H} and S , respectively. Thus,

$$\begin{aligned} & (T \otimes P)[(I_N \otimes S) - (\tilde{H} \otimes I_{2l})](T^{-1} \otimes P^{-1}) \\ &= I_N \otimes (PSP^{-1}) - (T\tilde{H}T^{-1}) \otimes I_{2l} = I_N \otimes \Lambda_2 - \Lambda_1 \otimes I_{2l} \triangleq W. \end{aligned}$$

Note that the eigenvalues of W are the same as those of $(I_N \otimes S) - (\tilde{H} \otimes I_{2l})$ after similar transformation. The eigenvalues of W are given by

$$\{\lambda_i(\Lambda_2) - \lambda_j(\Lambda_1) : i = 1, 2, \dots, 2l, j = 1, 2, \dots, N\}, \quad (\text{B.2})$$

Based on Lemma 3.2 and Lemma 1 in [71], the real parts of $\lambda_j(\tilde{H})$ are all positive and so the real parts of $\lambda_j(\Lambda_1)$ are also all positive. Since all the eigenvalues of S have nonpositive real parts, the real parts of (B.2) are always negative. \square

AUTHOR'S PUBLICATIONS

1. Z. Feng, G. Hu, W. Ren, W. E. Dixon, J. Mei, "Distributed coordination of multiple unknown Euler-Lagrange systems," *IEEE Transactions on Control of Network Systems*, to appear, DOI: 10.1109/TCNS.2016.2578039, 2016. (Regular Paper)
2. Z. Feng, C. Sun, G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," *IEEE Transactions on Control of Network Systems*, to appear, DOI: 10.1109/TCNS. 2016. 2545869. (Regular Paper)
3. Z. Feng, G. Wen, G. Hu, "Distributed secure coordinated control for multi-agent systems under strategic attacks," *IEEE Transactions on Cybernetics*, vol. 47, no. 5, pp. 1273-1284, 2017. (Regular Paper)
4. Z. Feng, G. Hu, G. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks," *International Journal of Robust Nonlinear Control*, vol. 26, no. 5, pp. 896-918, 2015. (Regular Paper)
5. Z. Feng, G. Hu, "Passivity-based consensus for stochastic multi-agent systems with switching topologies," *Control Theory and Technology*, vol. 12, no. 3, pp. 304-316, 2014. (Invited)
6. Z. Feng, G. Hu, "Distributed event-triggered control of linear multi-agent systems subject to DoS Attacks," submitted, 2016.
7. Z. Feng, G. Hu, K. H. Johansson, A. V. Vasilakos, B. Chen, "An overview of resilient cyber physical systems," submitted, 2016.

8. Z. Feng, G. Hu, "Distributed secure average consensus for linear multi-agent systems under DoS attacks," *American Control Conference*, May 24-26, Seattle, WA, USA, 2017.
9. Z. Feng, C. Sun, G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," *The 54th IEEE Conference on Decision and Control*, Osaka, Japan, December 15-18, pp. 4266-4271, 2015.
10. Z. Feng, G. Hu, "Distributed fault-tolerant control for a large-scale power generator network," *American Control Conference*, Chicago, USA, July 1-3, pp. 5521-5526, 2015.
11. Z. Feng, G. Hu, "Distributed Tracking Control for Multi-Agent Systems Under Two Types of Attacks," *The 19th World Congress of IFAC*, South Africa, August 24-29, pp. 5790-5795, 2014.
12. Z. Feng, G. Hu, "Distributed fault identification and fault-tolerant control for multi-agent system," *Chinese Control Conference*, Nanjing, China, July 1-3, pp. 1476-1481, 2014.
13. Z. Feng, G. Hu, "Robust distributed consensus tracking for stochastic linear multi-agent systems with directed switching topologies", *The 11th IEEE International Conference on Control and Automation*, Taichung, June 18-24, pp. 174-179, 2014.
14. Z. Feng, G. Hu, "Distributed coordinated tracking control for multiple unknown nonlinear Euler-Lagrange systems", *The 10th IEEE International Conference on Control and Automation*, Hangzhou, China, June 12-14, pp. 123-128, 2013.

Bibliography

- [1] I. Korhonen, J. Parkka, M. V. Gils, “Health monitoring in the home of the future,” *IEEE Eng. Med. Biol. Mag.*, vol. 22, no. 3, pp. 66-73, 2003.
- [2] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. M. Fortino, S. Park, A. Roederer, K. K. Venkatasubramanian, “Challenges and research directions in medical cyber-physical systems,” *Proc. IEEE*, vol. 100, no. 1, pp. 75-90, 2012.
- [3] J. Kleissl, Y. Agarwa, “Cyber-physical energy systems: focus on smart buildings,” *Proceeding of the 47th IEEE on Design Automation Conference*, 13-18 June, Anaheim, CA, USA, pp. 749-754, 2010.
- [4] J. Fink, A. Ribeiro, V. Kumar, “Robust control for mobility and wireless communication in cyber-physical systems with application to robot teams,” *Proc. IEEE*, vol. 100, no. 1, pp. 75-90, 2012.
- [5] N. Nigam, S. Bieniawski, I. Kroo, J. Vian, “Control of multiple UAVs for persistent surveillance: algorithm and flight test results,” *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1236-1251, 2012.
- [6] K. Sampigethaya, R. Poovendran, “Aviation cyber-physical systems foundations for future aircraft and air transport,” *Proc. IEEE*, vol. 101, no. 8, pp. 1834-1855, 2013.
- [7] A. R. Metke, R. L. Ekl, “Security technology for smart grid networks,” *IEEE Trans. Smart Grid*, vol. 53, no. 1, pp. 99-107, 2010.
- [8] S. Sridhar, A. Hahn, M. Govindarasu, “Cyber-physical system security for the electric power grid,” *Proc. IEEE*, vol. 100, no. 1, pp. 210-224, 2012.
- [9] Department of Energy, “The smart grid: An introduction,” 2011.
- [10] A. Jadbabaie, J. Lin, A. S. Morse, “Coordination of groups of mobile autonomous agents using nearest neighbor rules,” *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 988-1001, 2003.
- [11] R. Olfati-Saber, R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” *IEEE Trans. Autom. Control*, vol. 49, no.9, pp. 1520-1533, 2004.

- [12] X. Wang, Y. Hong, J. Huang, Z. Jiang, "A distributed control approach to a robust output regulation problem for multi-agent linear systems," *IEEE Trans. Autom. Control*, vol. 55, no.12, pp. 2891-2895, 2010.
- [13] Y. Cao, W. Ren, "Distributed coordinated tracking with reduced interaction via a variable structure approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 33-48, 2012.
- [14] R. Olfati-Saber, J. A. Fax, R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215-233, 2007.
- [15] Y. Cao, W. Yu, W. Ren, G. Chen, "An overview of recent progress in the study of distributed multi-agent coordination," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 427-438, 2007.
- [16] W. Ren, "Distributed cooperative attitude synchronization and tracking for multiple rigid bodies," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 2, pp. 383-392, 2010.
- [17] Y. Hong, J. Hu, L. Gao, "Tracking control for multi-agent consensus with an active leader and variable topology," *Automatica*, vol. 42, no. 7, pp. 1177-1182, 2012.
- [18] Y. Hong, G. Cheng, L. Bushnell, "Distributed observer design for leader-following control of multi-agent networks," *Automatica*, vol. 44, no. 3, pp. 846-850, 2008.
- [19] X. Wang, N. Wei, X. Wang, "Leader-following formation of switching multi-robot systems via internal model," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 42, no. 3, pp. 817-826, 2012.
- [20] H. Bai, M. Arcak, J. T. Wen, "Adaptive design for reference velocity recovery in motion coordination," *Syst. Control Lett.*, vol. 57, no. 8, pp. 602-610, 2008.
- [21] M. Cao, C. Yu, B. Anderson, "Formation control using range-only measurements," *Automatica*, vol 47, no. 4, pp. 776-781, 2011.
- [22] Q. Hui, "Finite-Time rendezvous algorithms for mobile autonomous agents," *IEEE Trans. Autom. Control*, vol. 56, no. 1, pp. 207-211, 2011.
- [23] H. Bai, M. Arcak, J. T. Wen, "Adaptive motion coordination: using relative velocity feedback to track a reference velocity," *Automatica*, vol. 45, no. 4, pp. 1020-1025, 2009.
- [24] Q. Song, F. Liu, J. Cao, W. Yu, "Pinning-controllability analysis of complex networks: An M -matrix approach," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol 59, no. 11, pp. 2692-2701, 2012.

- [25] G. Wen, G. Hu, W. Yu, J. Cao, G. Chen, "Consensus tracking for higher-order multi-agent systems with switching directed topologies and occasionally missing control inputs," *Syst. Control Lett.*, vol 62, no. 12, pp. 1151-1158, 2013.
- [26] L. Scardovi, R. Sepulchre, "Synchronization in networks of identical linear systems," *Automatica*, vol 45, no. 11, pp. 2557-2562, 2009.
- [27] H. Su, Michael. Z. Q. Chen, J. Lam, Z. Lin, "Semi-global leader-following consensus of linear multi-agent systems with input saturation via low gain feedback," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol 60, no. 7, pp. 1881-1889, 2013.
- [28] Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, 2008.
- [29] J. P. Farwell, R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23-40, 2011.
- [30] J. Slay, M. Miller. Lessons learned from the Maroochy water breach. *Critical Infrastructure Protection*, pp. 73-82, 2007.
- [31] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur Priv.*, vol. 9, no. 3, pp. 49-51, 2011.
- [32] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computer World*, 2010.
- [33] A. Cárdenas, S. Amin, S. Sastry, "Research challenges for the security of control systems," *Proceedings of the 3rd Conference on Hot Topics in Security*, 6-25 July, Berkeley, CA, USA, 2008.
- [34] B. Miller, D. Rowe, "A survey of SCADA and critical infrastructure incidents," *Proceedings of the 1st Annual Conference on Research in information technology*, New York, NY, USA, pp. 51-56, 2012.
- [35] <https://ics-cert.us-cert.gov/monitors>.
- [36] S. Amin, B. Sinopoli, A. Giani, A. A. Perrig, S. S. Sastry, "Challenges for securing cyber physical systems," *Workshop on Future Directions in Cyber-physical Systems Security*, Newark, NJ, USA, 23 July, 2009.
- [37] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283-299, 2012.
- [38] Y. Su, J. Huang, "Cooperative output regulation of linear multi-agent systems," *IEEE Trans. Autom. Control*, vol. 57, no. 4, pp. 1062-1066, 2012.

- [39] G. Wen, Z. Duan, G. Chen, W. Yu, "Consensus tracking of multi-agent systems with Lipschitz-type node dynamics and switching topologies," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 2, pp. 499-511, 2014.
- [40] S. Chung, J. J. E. Slotine, "Cooperative robot control and concurrent synchronization of Lagrangian systems," *IEEE Trans. Robotics*, vol. 25, no. 3, pp. 686-700, 2009.
- [41] S. Chung, S. Bandyopadhyay, I. Chang, F. Y. Hadaegh, "Phase synchronization control of complex networks of Lagrangian systems on adaptive digraphs," *Automatica*, vol. 49, no. 5, pp. 1148-1161, 2013.
- [42] L. Cheng, Z. Hou, M. Tan, "Decentralized adaptive leader-follower control of multi-manipulator system with uncertain dynamics," *Proceedings of The 34th Annual Conference of the IEEE Industrial Electronics Society, USA*, 2008.
- [43] G. Chen, Frank L. Lewis, "Distributed adaptive tracking control for synchronization of unknown networked Lagrangian systems," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 41, no. 3, pp. 805-816, 2011.
- [44] J. Mei, W. Ren, G. Ma, "Distributed coordinated tracking with a dynamic leader for multiple Euler-Lagrange systems," *IEEE Trans. Autom. Control*, vol. 56, no. 6, pp. 1415-1421, 2011.
- [45] J. Mei, W. Ren, G. Ma, "Distributed containment control for Lagrangian networks with parametric uncertainties under a directed graph," *Automatica*, vol. 48, no. 4, pp. 653-659, 2012.
- [46] F. Zhi, G. Hu, "Distributed coordinated tracking control for multiple unknown nonlinear Euler-Lagrange systems," *The 10th IEEE International Conference on Control and Automation*, 2013.
- [47] J. Klotz, Z. Kan, J. M. Shea, E. L. Pasiliao, W. E. Dixon, "Asymptotic synchronization of leader-follower networks of uncertain Euler-Lagrange systems," *The 53th IEEE Conference on Decision and Control*, December 15-17, Los Angeles, CA, USA, 2013.
- [48] A. Abdessameud, I. G. Polushin, A. Tayebi, "Synchronization of Lagrangian systems with irregular communication delays," *IEEE Trans. Autom. Control*, vol. 59, no. 1, pp. 187-193, 2014.
- [49] H. Wang, "Consensus of networked mechanical systems with communication delays: a unified framework," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1571-1576, 2014.
- [50] S. Khoo, L. Xie, Z. Man, "Robust finite-time consensus tracking algorithm for multirobot systems," *IEEE/ASME Trans. Mechatronics*, vol. 14, no. 2, pp. 219-228, 2009.

- [51] S. Li, H. Du, X. Lin, "Finite-time consensus algorithm for multi-agents with double-integrator dynamics," *Automatica*, vol. 47, no. 8, pp. 1706-1712, 2011.
- [52] X. Li, X. Wang, G. Chen, "Pinning a complex dynamical network to its equilibrium," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 10, pp. 2074-2087, 2004.
- [53] Z. Hou, L. Cheng, M. Tan, "Decentralized robust adaptive control for the multiagent system consensus problem using neural networks," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 39, no. 3, pp. 636-647, 2009.
- [54] L. Cheng, Z. Hou, M. Tan, Y. Lin, W. Zhang, "Neural-network-based adaptive leader-following control for multiagent systems with uncertainties," *IEEE Trans. Neural Netw.*, vol. 21, no. 8, pp. 1351-1358, 2010.
- [55] H. Zhang, F. L. Lewis, "Adaptive Cooperative tracking control for high-order nonlinear systems with unknown nonlinearities," *Automatica*, vol. 48, no. 7, pp. 1432-1439, 2012.
- [56] S. E. Ferik, A. Qureshi, F. L. Lewis, "Neuro-adaptive cooperative tracking control of unknown higher-order affine nonlinear systems," *Automatica*, vol. 50, no. 3, pp. 798-808, 2014.
- [57] G. Hu, "Robust consensus tracking of an integrator-type multi-agent system with disturbance and unmodelled dynamics," *Int. J. Control*, vol. 84, no. 1, pp. 1-8, 2011.
- [58] G. Hu, "Robust consensus tracking of a class of second-order multi-agent dynamic systems," *Syst. Control Lett.*, vol. 61, no. 1, pp. 134-142, 2012.
- [59] Z. Feng, C. Sun, G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," *The 54rd IEEE Conference on Decision and Control*, December 15-18, Osaka, Japan, 2015.
- [60] C. Sun, G. Hu, L. Xie, "Robust consensus tracking for a class of high-order multi-agent systems," *Int. J. Robust Nonlinear Control*, vol. 26, no. 3, pp. 578-598, 2015.
- [61] Z. Meng, Z. Lin, W. Ren, "Leader-follower swarm tracking for networked Lagrange systems", *Syst. Control Lett.*, vol. 61, no. 1, pp. 117-126, 2012.
- [62] X. Dong, J. Xi, G. Lu, Y. Zhong, "Formation control for high-order linear time-invariant multiagent systems with time delays," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 3, pp. 232-240, 2014.
- [63] J. Qin, C. Yu, H. Gao, "Collective behavior for group of generic linear agents interacting under arbitrary network topology," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 3, pp. 288-297, 2015.

- [64] W. Ren, Y. Cao, Distributed coordination of multi-agent networks, Communications and Control Engineering Series, Springer-Verlag, London, 2011.
- [65] N. Fischer, R. Kamalapurkar, W. E. Dixon, “LaSalle–Yoshizawa corollaries for nonsmooth systems,” *IEEE Trans. Autom. Control*, vol. 58, no. 9, pp. 2333-2338, 2013.
- [66] D. Shevitz, B. Paden, “Lyapunov stability theory of nonsmooth systems,” *IEEE Trans. Autom. Control*, vol. 39, no. 9, pp. 1910-1914, 1994.
- [67] B. Xian, D. M. Dawson, M. S. de Queiroz, J. Chen, “A continuous asymptotic tracking control strategy for uncertain nonlinear systems,” *IEEE Trans. Autom. Control*, vol. 49, no. 7, pp. 1206-1211, 2004.
- [68] C. Makkar, G. Hu, W. G. Sawyer, W. E. Dixon, “Lyapunov-based tracking control in the presence of uncertain nonlinear parameterizable friction,” *IEEE Trans. Autom. Control*, vol. 52, no. 10, pp. 1988-1994, 2007.
- [69] P. M. Patre, W. MacKunis, K. Dupree, W. E. Dixon, “Modular adaptive control of uncertain Euler–Lagrange systems with additive disturbances,” *IEEE Trans. Autom. Control*, vol. 56, no. 1, pp. 155-160, 2011.
- [70] G. Hu, W. E. Dixon, H. Ding, “Robust tracking control of an array of nanoparticles moving on a substrate,” *Automatica*, vol. 48, no. 4, pp. 442-448, 2012.
- [71] Y. Su, J. Huang, “Cooperative robust output regulation of a class of heterogeneous linear uncertain multi-agent systems,” *Int. J. Robust Nonlinear Control*, vol. 24, no. 17, pp. 2819-2839, 2014.
- [72] Y. Dong, J. Huang, “A leader-following rendezvous problem of double integrator multi-agent systems,” *Automatica*, vol. 49, no. 5, pp. 1386-1391, 2013.
- [73] Y. Dong, J. Huang, “Leader-following connectivity preservation rendezvous of multiple double integrator systems based on position measurement only,” *IEEE Trans. Autom. Control*, vol. 59, no. 9, pp. 2598-2603, 2014.
- [74] H. K. Khalil, Nonlinear systems 3rd edition, Prentice Hall, Englewood Cliffs, NJ, 2003.
- [75] R. Olfati-Saber, “Flocking for multi-agent dynamics systems: algorithms and theory,” *IEEE Trans. Autom. Control*, vol. 51, no. 3, pp. 401-420, 2006.
- [76] H. Su, X. Wang, Z. Lin, “Flocking of multi-agents with a virtual leader,” *IEEE Trans. Autom. Control*, vol. 54, no. 12, pp. 293-307, 2009.
- [77] G. Wen, Z. Duan, Z. Li, G. Chen, “Flocking of multi-agent dynamical systems with intermittent nonlinear velocity measurements,” *Int. J. Robust Nonlinear Control*, vol. 22, no. 2, pp. 1790-1805, 2012.

- [78] H. G. Tanner, A. Jadbabaie, G. J. Pappas, "Flocking in fixed and switching networks," *IEEE Trans. Autom. Control*, vol. 52, no. 5, pp. 863-868, 2007.
- [79] H. Zhang, C. Zhai, Z. Chen, "A general alignment repulsion algorithm for flocking of multi-agent systems," *IEEE Trans. Autom. Control*, vol. 56, no. 2, pp. 430-435, 2011.
- [80] M. Zavlanos, G. Pappas, "Potential fields for maintaining connectivity of mobile networks," *IEEE Trans. Robotics*, vol. 23, no. 4, pp. 812-816, 2007.
- [81] M. Ji, M. Egerstedt, "Distributed coordination control of multi-agent systems while preserving connectedness," *IEEE Trans. Robotics*, vol. 23, no. 4, pp. 693-703, 2007.
- [82] M. Zavlanos, H. Tanner, A. Jadbabaie, G. Pappas, "Hybrid control for connectivity preserving flocking," *IEEE Trans. Autom. Control*, vol. 54, no. 12, pp. 2869-2875, 2009.
- [83] H. Su, X. Wang, G. Chen, "Rendezvous of multiple mobile agents with preserved network connectivity," *Syst. Control Lett.*, vol. 59, no. 5, pp. 313-322, 2010.
- [84] D. V. Dimarogonas, K. J. Kyriakopoulos, "On the rendezvous problem for multiple nonholonomic agents," *IEEE Trans. Autom. Control*, vol. 52, no. 5, pp. 916-922, 2007.
- [85] T. Gustavi, D. V. Dimarogonas, M. Egerstedt, X. Hu, "Sufficient conditions for connectivity maintenance and rendezvous in leader-follower networks," *Automatica*, vol. 46, no.1, pp. 133-139, 2010.
- [86] F. Xiao, L. Wang, T. Chen, "Connectivity preservation for multi-agent rendezvous with link failure," *Automatica*, vol. 48, no. 1, pp. 25-35, 2012.
- [87] Z. Kan, A. P. Dani, J. M. Shea, W. E. Dixon, "Network connectivity preserving formation stabilization and obstacle avoidance via a decentralized controller," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 207-211, 2012.
- [88] J. Mei, W. Ren, G. Ma, "Distributed coordination for second-order multi-agent systems with nonlinear dynamics using only relative position measurements," *Automatica*, vol. 49, no. 5, pp. 1419-1427, 2013.
- [89] Z. Feng, G. Hu, W. Ren, W. E. Dixon, J. Mei, "Distributed coordination of multiple unknown Euler-Lagrange systems," *IEEE Trans. Control Netw. Syst.*,, accepted, 2015.
- [90] I. Saboori, H. Nayyeri, K. Khorasani, "A distributed control strategy for connectivity preservation of multi-agent systems subject to actuator saturation," *American Control Conference*, June 17-19, Washington, DC, USA, pp. 4044-4049, 2013.

- [91] S. Ghapani, J. Mei, W. Ren, "Flocking with a moving leader for multiple uncertain lagrange systems," *American Control Conference*, June 4-6, Portland, Oregon, USA, pp. 3189-3194, 2014.
- [92] A. Roza, M. Maggiore, L. Scardovi, "A class of rendezvous controllers for underactuated thrust-propelled rigid bodies," *The 53rd IEEE Conference on Decision and Control*, December 15-17, Los Angeles, California, USA, pp. 1649-1654, 2014.
- [93] M. Ouimet, J. Cortes, "Coordinated rendezvous of underwater drifters in ocean internal waves," *The 53rd IEEE Conference on Decision and Control*, December 15-17, Los Angeles, California, USA, pp. 6099-6104, 2014.
- [94] Z. Feng, G. Hu, "Distributed coordinated tracking control for multi-agent systems under two types of attacks with an application to power system," *Proceedings of the 19th IFAC World Congress*, August 24-29, South Africa, 2014.
- [95] Z. Feng, G. Hu, G. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks," *Int. J. Robust. Nonlinear Control*, vol. 26, no. 5, pp. 896-918, 2015.
- [96] Z. Feng, G. Wen, G. Hu, "Distributed secure coordinated control for multi-agent systems under strategic attacks," *IEEE Trans. Cybern.*, *accepted, to appear*, 2016.
- [97] M. Huang, J. H. Manton, "Coordination and consensus of networked agents with noisy measurement: stochastic algorithms and asymptotic behavior," *SIAM J. Control and Optimization*, vol 48, no. 1, pp. 134-161, 2009.
- [98] L. Cheng, Z. Hou, M. Tan, X. Wang, "Necessary and sufficient conditions for consensus of double-integrator multi-agent systems with measurement noises," *IEEE Trans. Autom. Control*, vol 56, no. 8, pp. 1958-1963, 2011.
- [99] J. Hu, G. Feng, "Distributed tracking control of leader-follower multiagent systems under noisy measurements," *Automatica*, vol 46, no. 8, pp. 1382-1387, 2010.
- [100] Z. Zhou, H. Fang, Y. Hong, "Distributed estimation for moving target based on state-consensus strategy," *IEEE Trans. Autom. Control*, vol 58, no. 8, pp. 2096-2101, 2013.
- [101] A. Teixeira, H. Sandberg, K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," *In IEEE Conference of American Control Conference*, MD, USA, 2010.
- [102] I. Shames, A. Teixeira, H. Sandberg, K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol 47, no. 12, pp. 2757-2764, 2011.

- [103] H. J. LeBlanc, X. D. Koutsoukos, "Consensus in networked multi-agent systems with adversaries," *Proceedings of the 14th International Conference on Hybrid systems: Computation and Control*, Chicago, IL, 2011.
- [104] F. Pasqualetti, R. Carli, F. Bullo, "A distributed method for state estimation and false data detection in power networks," *In IEEE International Conference on Smart Grid Communications*, 2011.
- [105] A. Bidram, A. Davoudi, F. L. Lewis, J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Trans. Power Syst.*, vol 28, no. 3, pp. 3462-3470, 2013.
- [106] F. Pasqualetti, R. Carli, F. Bullo, "Attack Detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol 58, no. 11, pp. 2715-2729, 2013.
- [107] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, 2014, doi:10.1109/TAC.2013.2279896.
- [108] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol 65, no. 1, pp. 056109, 2002.
- [109] A. N. Bishop, I. Shames, "Link operations for slowing the spread of disease in complex networks," *Europhys. Lett.*, vol 95, no. 1, pp. 18005, 2011.
- [110] H. Tong, B. A. Prakash, T. E. Rad, M. Faloutsos, C. Faloutsos, "Gelling, and melting, large graphs by edge manipulation," *Proceedings of the 21st ACM international conference on Information and knowledge management*, 2012.
- [111] S. Meloni, N. Perra, A. Arenas, S. Gomez, Y. Moreno, A. Vespignani, "Modeling human mobility responses to the large-scale spreading of infectious diseases," *Scientific Reports*, 2012, DOI: 10.1038/srep00062.
- [112] Z. Qu, *Cooperative Control of Dynamical Systems: Applications to Autonomous Vehicles*. Springer-Verlag: New York, 2009.
- [113] B. Ksendar, *Stochastic Differential Equations*. Springer-Verlag, New York, 2000.
- [114] P. Kundur, J. Paserba, C. Ajjarapu, N. Hatziargyriou, "Definition and classification of power system stability," *IEEE Trans. Power Syst.*, vol 19, no. 2, pp. 1387-1401, 2004.
- [115] A. Rausch, J. Coe, J. Gerencser, L. Patterson, D. Walters, "Traffic congestion analysis of the public switched network," *IEEE Conference on Military Communications*, Boston, MA, pp. 917-921, 1993.

- [116] J. Zhao, D. J. Hill, T. Liu, "Synchronization of complex dynamical networks with switching topology: A switched system point of view," *Automatica*, vol 45, no. 11, pp. 2502-2511, 2009.
- [117] J. P. Hespanha, A. S. Morse, "Stability of switched systems with average dwell time," *Proceedings of the 38th IEEE Conference on Decision and Control*, Phoenix, AR, pp. 2655-2660, 1999.
- [118] J. Lian, Z. Feng, P. Shi, "Observer design for switched recurrent neural networks: An average dwell time approach," *IEEE Trans. Neural Netw.*, vol 22, no. 10, pp. 1547-1556, 2011.
- [119] X. Sun, G. Liu, D. Rees, W. Wei, "Stability of systems with controller failure and time-varying delay," *IEEE Trans. Autom. Control*, vol 53, no. 10, pp. 2391-2396, 2008.
- [120] G. Zhai, B. Hu, K. Yasuda, A. N. Michel, "Piecewise Lyapunov functions for switched system with average dwell time," *Asian J. Control*, vol 2, no. 3, pp. 192-197, 2000.
- [121] A. J. Wood, B. F. Wollenberg, *Power generation, operation, and control*. New York, NY, USA: Wiley, 2013.
- [122] W. Ren, "Synchronization of coupled harmonic oscillators with local interaction," *Automatica*, vol. 44, no. 12, pp. 3195-3200, 2008.
- [123] Z. Feng, C. Sun, G. Hu, "Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances," *IEEE Trans. Control Netw. Syst.*, 2016, DOI:10.1109/TCNS.2016.2545869.
- [124] Y. Su, J. Huang, "Two consensus problems for discrete-time multi-agent systems with switching topology," *Automatica*, vol. 48, no. 9, pp. 1988-1997, 2012.
- [125] S. Chen, Daniel W. C. Ho, L. Li, M. Liu, "Fault-tolerant consensus of multi-agent system with distributed adaptive protocol," *IEEE Trans. Cybern.*, vol. 44, no. 10, pp. 2142-2155, 2015.
- [126] D. Wang, N. Zhang, J. Wang, W. Wang, "A PD-like protocol with a time delay to average consensus control for multi-agent systems under an arbitrarily fast switching topology," *IEEE Trans. Cybern.*, 2016, DOI:10.1109/TCYB.2016.2532898.
- [127] I. Shames, A. Teixeira, H. Sandberg, K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2024-2037, 2014.
- [128] L. Zhao, K. Park, Y. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Phys. Rev. E*, vol. 70, no. 3, pp. 035101(R), 2004.

- [129] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 60, no. 5, pp. 056109, 2009.
- [130] A. N. Bishop, I. Shames, "Link operations for slowing the spread of disease in complex networks," *Europhys. Lett.*, vol. 95, no. 1, pp. 18005, 2011.
- [131] W. Zeng, M. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2038-2049, 2014.
- [132] D. Meng, K. Moore, "Studies on resilient control through multiagent consensus networks subject to disturbances," *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2050-2064, 2014.
- [133] J. Moon, T. Basar, "Control over lossy networks: A dynamic game approach," *American Control Conference*, June 4-6, Portland, 2014.
- [134] Q. Zhu, T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Trans. Syst. Mag.*, vol. 35, no. 1, pp. 46-65, 2015.
- [135] Z. Li, G. Wen, Z. Duan, W. Ren, "Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs," *IEEE Trans. Autom. Control*, vol. 60, no. 6, pp. 1152-1157, 2015.
- [136] S. Liu, B. Chen, T. Zourntos, D. Kundur, K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183-1195, 2014.
- [137] D. A. Bini, B. Iannazzo, F. Poloni, "A fast newton's method for anonsymmetric algebraic Riccati equation," *SIAM J. Matrix Anal. Appl.*, vol. 30, no. 1, pp. 276-290, 2008.
- [138] K. H. Movric, K. You, F. Lewis, L. Xie, "Synchronization of discrete-time multi-agent systems on grphs using Riccati design," *Automatica*, vol. 49, no. 2, pp. 414-423, 2013.
- [139] M. D. Fragoso, O. L. V. Costa, "A unified approach for stochastic and mean square stability of continuous-time linear systems with Markovian jumping parameters and additive disturbances," *SIAM J. Control Optim.*, vol. 44, no. 4, pp. 1165-1191, 2005.
- [140] W. Li, Z. Wu, "Output tracking of stochastic high-order nonlinear systems with Markovian switching," *IEEE Trans. Autom. Control*, vol. 58, no. 6, pp. 1585-1590, 2013.

- [141] H. Zhang, F. Lewis, Z. Qu, "Lyapunov, adaptive, and optimal design techniques for cooperative systems on directed communication graphs," *IEEE Trans. Ind. Electronics*, vol. 59, no. 7, pp. 3026-3041, 2012.
- [142] D. M. Naedele, T. P. Hoff, M. Crevatin, "Security for industrial communication systems," *Proc. IEEE*, vol 93, no. 6, pp. 1152-1177, 2005.
- [143] Q. Zhu. Game-theoretic methods for security and resilience in cyber-physical systems. PhD thesis, Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 2013.
- [144] G. D. Torre, T. Yucelen, J. D. Peterson, "Resilient networked multi-agent systems: a distributed adaptive control approach," *Proceedings of the 53rd IEEE Conference on Decision and Control*, December 15-17, Los Angeles, California, USA, pp. 5367-5372, 2014.
- [145] S. Amin, A. Cardenas, S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *In Hybrid Systems: Computation and Control*, pp. 31-45, 2009.
- [146] A. Gupta, C. Langbort, T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," *Proceedings of the 49th IEEE Conference on Decision and Control*, December 15-17, Atlanta, Georgia, USA, pp. 1096-1101, 2010.
- [147] C. De Persis, P. Tesi, "On resilient control of nonlinear systems under denial-of-service," *Proceedings of the 53rd IEEE Conference on Decision and Control*, December 15-17, Los Angeles, California, USA, pp. 5254-5259, 2014.
- [148] H. Zhang, P. Cheng, L. Shi, J. Chen, "Optimal denial of service attack scheduling against linear quadratic gaussian control," *American Control Conference*, Portland, Oregon, USA, June 4-6, 2014.
- [149] H. Shishah Foroush, S. Martínez, "On event-triggered control of linear systems under periodic denial-of-service attacks," *Proceedings of the 51st IEEE Conference on Decision and Control*, December 15-17, Maui, HI, USA, pp. 2551-2556, 2012.
- [150] A. Cetinkaya, H. Ishii, T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," *The 54th IEEE Conference on Decision and Control*, December 15-18, Osaka, Japan, pp. 4818-4823, 2015.
- [151] V. S. Dolk, P. Tesi, C. De Persis, W. P. M. H. Heemels, "Output-based event-triggered control systems under denial-of-service Attacks," *The 54th IEEE Conference on Decision and Control*, December 15-18, Osaka, Japan, pp. 4824-4829, 2015.
- [152] C. De. Persis, P. Tesi, "Resilient Control under Denial-of-Service," *Proceedings of the 19th IFAC World Congress*, August 24-29, South Africa, 2014.

- [153] D. Senejohnny, C. De. Persis, P. Tesi, "Self-triggered coordination over a shared network under denial-of-service," *The 54th IEEE Conference on Decision and Control*, December 15-18, Osaka, Japan, pp. 4824-4829, 2015.
- [154] H. Zhang, P. Cheng, L. Shi, J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol 60, no. 11, pp. 3223-3328, 2015.
- [155] G. K. Befekadu, V. Gupta, P. J. Antsaklis, "Risk-sensitive control under markov modulated denial-of-service attack strategies," *IEEE Trans. Autom. Control*, vol 60, no. 12, pp. 3299-3304, 2015.
- [156] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol 51, no. 1, pp. 135-148, 2015.
- [157] M. Zhu, S. Martínez, "On distributed formation control in operator-vehicle adversarial networks," *Automatica*, vol 49, no. 2, pp. 3571-3582, 2013.
- [158] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, "Efficient computations of a security index for false data attacks in power networks" *IEEE Trans. Autom. Control*, vol 58, no. 11, pp. 3194-3208, 2014.
- [159] Y. Mo, S. Weerakkody, B. Sinopoli, "Physical authentication of control systems designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst. Mag.*, vol 35, no. 1, pp. 93-109, 2015.
- [160] K. J. Astrom, B. Bernhardsson, "Comparison of periodic and event based sampling for first-order stochastic systems," *IFAC World Congress, Beijing, China*, 1999.
- [161] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control*, vol 52, no. 9, pp. 1680-1685, 2007.
- [162] X. Wang, M. D. Lemmon, "Event-triggering in distributed networked control systems," *IEEE Trans. Autom. Control*, vol 56, no. 3, pp. 586-601, 2011.
- [163] D. V. Dimarogonas, E. Frazzoli, K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *IEEE Trans. Autom. Control*, vol 57, no. 5, pp. 1291-1297, 2012.
- [164] Y. Fan, G. Feng, Y. Wang, C. Song, "Distributed event-triggered control of multi-agent systems with combinational measurements," *Automatica*, vol 49, no. 2, pp. 671-675, 2013.
- [165] Y. Fan, G. Hu, "Event-triggered rendezvous control of multi-agent systems with limited communication ranges," *submitted to Automatica*, 2015.

- [166] H. Li, X. Liao, T. Huang, W. Zhu, “Event-triggering sampling based leader-following consensus in second-order multi-agent systems,” *IEEE Trans. Autom. Control*, vol 60, no. 7, pp. 1998-2003, 2015.
- [167] T. H. Cheng, Z. Kan, J. R. Klotz, J. M. Shea, W. E. Dixon, “Decentralized event-triggered control of networked systems-Part 2: containment control,” *Am. Control Conf.*, July 1-3, Chicago, USA, pp. 5444-5448, 2015.
- [168] T. H. Cheng, Z. Kan, J. R. Klotz, J. M. Shea, W. E. Dixon, “Decentralized Event-Triggered Control of Networked Systems-Part 1: Leader-Follower Consensus Under Switching,” *Am. Control Conf.*, July 1-3, Chicago, USA, pp. 5444-5448, 2015.
- [169] T. H. Cheng, Z. Kan, J. R. Klotz, J. M. Shea, W. E. Dixon, “Event-triggering control of multi-agent systems for fixed and time-varying network topologies,” *IEEE Trans. Autom. Control*, 2018.