Control coordination and monitoring of autonomous agents in agri–food field

Italian National Ph.D. Program in Autonomous Systems

ACADEMIC DISCIPLINE: SYSTEMS AND CONTROL ENGINEERING (IINF-04/A)

Final Dissertation

Control Coordination and Monitoring of Autonomous Agents in Agri–Food Field

by

Bushra Bushra

Administrative Headquarters:

Politecnico di Bari – Department of Electrical and Information Engineering

Hosting University:

Univrsity of L'Aquila – Department of Information Engineering, Computer Science and Mathematics

Referees:

Prof. Michael Defoort

Prof. Christoforos Hadjicostis

Supervisors:

Prof. Elena De Santis

Prof. Giordano Pola

Prof. Mario Di Ferdinando

Coordinator of Ph.D Program

Prof. Mariagrazia Dotoli

Course no. 38, 01/11/2022-31/10/2025

LIBERATORIA PER L'ARCHIVIAZIONE DELLA TESI DI DOTTORATO

Al Magnifico Rettore
del Politecnico di Bari

Il/la sottoscritto/a Bushra Bushra nato/a Thatta, Pakistan il 16-06-1993
residente a L'Aquila, Italy in via Acquasanta, 8/A e-mail b.shaikh@phd.poliba.it
iscritto al 3° anno di Corso di Dottorato di Ricerca in Autonomous Systems (DAUSY) ciclo XXXVIII
ed essendo stato ammesso a sostenere l'esame finale con la prevista discussione della tesi dal titolo:
Control, Coordination and Monitoring of Autonomous Agents in Agri–Food Field

DICHIARA

1) di essere consapevole che, ai sensi del D.P.R. n. 445 del 28.12.2000, le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del codice penale e delle Leggi speciali in materia, e che nel caso ricorressero dette ipotesi, decade fin dall'inizio e senza necessità di nessuna formalità dai benefici conseguenti al provvedimento emanato sulla base di tali dichiarazioni;
2) di essere iscritto al Corso di Dottorato di ricerca Autonomous Systems (DAUSY) ciclo XXXVIII, corso attivato ai sensi del "*Regolamento dei Corsi di Dottorato di ricerca del Politecnico di Bari"*, emanato con D.R. n.286 del 01.07.2013;
3) di essere pienamente a conoscenza delle disposizioni contenute nel predetto Regolamento in merito alla procedura di deposito, pubblicazione e autoarchiviazione della tesi di dottorato nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica;
4) di essere consapevole che attraverso l'autoarchiviazione delle tesi nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica del Politecnico di Bari (IRIS-POLIBA), l'Ateneo archivierà e renderà consultabile in rete (nel rispetto della Policy di Ateneo di cui al D.R. 642 del 13.11.2015) il testo completo della tesi di dottorato, fatta salva la possibilità di sottoscrizione di apposite licenze per le relative condizioni di utilizzo (di cui al sito http://www.creativecommons.it/Licenze), e fatte salve, altresì, le eventuali esigenze di "embargo", legate a strette considerazioni sulla tutelabilità e sfruttamento industriale/commerciale dei contenuti della tesi, da rappresentarsi mediante compilazione e sottoscrizione del modulo in calce (Richiesta di embargo);
5) che la tesi da depositare in IRIS-POLIBA, in formato digitale (PDF/A) sarà del tutto identica a quelle **consegnate**/inviate/da inviarsi ai componenti della commissione per l'esame finale e a qualsiasi altra copia depositata presso gli Uffici del Politecnico di Bari in forma cartacea o digitale, ovvero a quella da discutere in sede di esame finale, a quella da depositare, a cura dell'Ateneo, presso le Biblioteche Nazionali Centrali di Roma e Firenze e presso tutti gli Uffici competenti per legge al momento del deposito stesso, e che di conseguenza va esclusa qualsiasi responsabilità del Politecnico di Bari per quanto riguarda eventuali errori, imprecisioni o omissioni nei contenuti della tesi;
6) che il contenuto e l'organizzazione della tesi è opera originale realizzata dal sottoscritto e non compromette in alcun modo i diritti di terzi, ivi compresi quelli relativi alla sicurezza dei dati personali; che pertanto il Politecnico di Bari ed i suoi funzionari sono in ogni caso esenti da responsabilità di qualsivoglia natura: civile, amministrativa e penale e saranno dal sottoscritto tenuti indenni da qualsiasi richiesta o rivendicazione da parte di terzi;
7) che il contenuto della tesi non infrange in alcun modo il diritto d'Autore né gli obblighi connessi alla salvaguardia di diritti morali od economici di altri autori o di altri aventi diritto, sia per testi, immagini, foto, tabelle, o altre parti di cui la tesi è composta.

Luogo e data L'Aquila, 15-01-2026 Firma Bushra

Il/La sottoscritto, con l'autoarchiviazione della propria tesi di dottorato nell'Archivio Istituzionale ad accesso aperto del Politecnico di Bari (POLIBA-IRIS), pur mantenendo su di essa tutti i diritti d'autore, morali ed economici, ai sensi della normativa vigente (Legge 633/1941 e ss.mm.ii.),

CONCEDE

- al Politecnico di Bari il permesso di trasferire l'opera su qualsiasi supporto e di convertirla in qualsiasi formato al fine di una corretta conservazione nel tempo. Il Politecnico di Bari garantisce che non verrà effettuata alcuna modifica al contenuto e alla struttura dell'opera.
- al Politecnico di Bari la possibilità di riprodurre l'opera in più di una copia per fini di sicurezza, back-up e conservazione.

Luogo e data L'Aquila, 15-01-2026 Firma Bushra

Bushra Bushra

Control Coordination and Monitoring of Autonomous Agents in Agri–Food Field

Thesis submitted for the degree of Philosophiae Doctor

Italian National Ph.D. Program in Autonomous Systems
Politecnico di Bari
Univeristy of L'Aquila

Tutors
Prof. *Elena De Santis*
Prof. *Giordano Pola*
Prof. *Mario Di Ferdinando*

2026

The doctoral scholarship was funded by the European Union - Next Generation EU, Mission 4 Component [2] CUP [$D93D22001390001$].

Dissertation submitted for the degree of *Philosophiae Doctor*
Italian National Ph.D. Program in Autonomous Systems

Cycle:
38th

Administrative Headquarters:
Politecnico di Bari

Hosting University:
University of L'Aquila

Title:
Control Coordination and Monitoring of Autonomous Agents in Agri–Food Field

Ph.D Candidate:
Bushra Bushra, University of L'Aquila (L'Aquila, Italy)

Tutors:
Prof. Elena De Santis, University of L'Aquila (L'Aquila, Italy)
Prof. Giordano Pola, University of L'Aquila (L'Aquila, Italy)
Prof. Mario Di Ferdinando, University of L'Aquila (L'Aquila, Italy)

Coordinator:
Prof. Engr. Mariagrazia Dotoli, Politecnico di Bari (Bari, Italy)

External Reviewers:
Prof. Michael Defoort ,Université Polytechnique Hauts-de-France (Valenciennes, France)
Prof. Christoforos Hadjicostis, University of Cyprus (Nicosia, Cyprus)

Last version:
November 8, 2025

Abstract

Modern autonomous and distributed systems play an increasingly important role in applications ranging from precision agriculture to smart transportation and industrial automation. Ensuring reliable coordination, security, and fault management in such systems is a significant challenge due to practical limitations including communication delays, quantization, measurement noise, and partial observability. This thesis develops theoretical frameworks and methods to address these challenges, with all results validated through comprehensive numerical examples.

The thesis first focuses on the controlled and coordinated behaviour of multiple agents under realistic operational constraints. Robust controllers are designed to achieve consensus and stability in networks of nonlinear agents, such as fleets of *Unmanned Aerial Vehicle* (UAV)s for agricultural monitoring, while mitigating the effects of disturbances and measurement errors. The proposed approaches ensure that even under practical imperfections, agents can operate cohesively and effectively.

It then examines security threats in *Discrete Event Systems* (DES)s, addressing both active attacks that disrupt system operation and passive attacks that attempt to infer sensitive information. Methods are developed to detect and localize these attacks, preserving system integrity in both single and networked–systems. This work provides formal conditions and practical strategies to maintain reliability despite potential malicious interventions.

Finally the thesis investigates fault detection under partial observation, where sensor information is limited. Observer–based schemes are developed to identify input faults using limited sensor information, providing tools to enhance resilience and offering practical tools for monitoring complex systems.

Overall, this thesis presents novel methods to control, monitor, and secure autonomous systems, with the goal of making them more reliable, safe, and resilient in real–world conditions. Although the work emphasizes applications in agriculture, the approaches are flexible and can be applied to a wide range of autonomous technologies. The findings offer a strong theoretical foundation for building systems that can operate effectively and robustly in practical environments.

“No effort stands alone; it is shaped by the people who stand beside us”

I dedicate this thesis to my Mother, whose unconditional love, constant prayers, and belief in me gave me strength during every stage of this journey. Her support kept me going, especially during moments of doubt. I am deeply grateful to my Father for his quiet presence, patience, and encouragement, always standing by me without needing many words.

I also dedicate this work to my Brother and my two Sisters, whose support, understanding, and encouragement meant more to me than they know. Their belief in me played an important role in helping me reach this milestone.

Contents

List of Figures

Acronyms

CPS *Cyber-Physical System.* 1, 5, 7, 9

DCO *Decentralized Critical Observability.* 6, 55, 56, 84

DES *Discrete Event Systems.* ii, 4, 5, 7–11, 17, 43, 45, 65, 83, 84

FSM *Finite State Machines.* 1, 4, 5, 7, 8, 10–13, 15–17, 43–47, 49, 52, 61–68, 83, 84, 86

ISS *Input-to-State Stability.* 1, 3, 19, 23, 83

MAS *Multi-Agent System.* 1–4, 6, 7, 10–15, 19–21, 23, 24, 29, 30, 36, 69, 83–86

NoA *Network of Agents.* 52, 53, 55–59

PN *Petri Net.* 2, 5, 7–10, 12, 13, 17, 18, 69, 84, 86

POPN *Partially Observed Petri Net.* vi, 2, 8–13, 17, 18, 69–71, 73, 75–77, 83, 84, 86

QSE *Quantized Sampled-data Event-triggered.* 1, 3, 4, 11–13, 15, 19–21, 23, 24, 26, 28–30, 33, 35, 83

SDCF *Steepest Descent Consensus Feedback.* 1, 3, 19, 23–25, 29, 33, 36, 83

SDF *Steepest Descent Feedback.* 23, 25

UAV *Unmanned Aerial Vehicle.* ii, 1, 4, 7, 8, 19, 33–35, 37, 41, 83–86

Preface

This thesis is submitted in partial fulfillment of the requirements for the degree of *Philosophiae Doctor in Autonomous Systems* in the framework of the National PhD Program in Autonomous Systems (DAUSY). The research presented herein was primarily conducted at the University of L'Aquila under the administrative oversight of Politecnico di Bari, with additional work carried out during a mobility period in France at QUARTZ lab, National School of Electronics and its Applications - ENSEA.

The thesis, entitled *Control, Coordination, and Monitoring of Autonomous Agents*, addresses key challenges in the field of autonomous systems, with a particular focus on enabling multiple agents to operate cooperatively, reliably, and safely in complex and uncertain environments. Autonomous systems are becoming increasingly important in modern society, offering the potential to perform tasks that are too complex, repetitive, or dangerous for humans. These systems rely heavily on multi–agent architectures, where autonomous agents must work together seamlessly, communicate reliably, and respond quickly to disturbances, faults, or external challenges. Ensuring that such systems are properly controlled, coordinated, and monitored is therefore critical for productivity, safety, and long–term sustainability.

During my PhD, I had the opportunity to undertake a mobility period in France at the QUARTZ Lab, focusing on the study of fault detection and monitoring in autonomous systems. This part of the research explored theoretical approaches to identify and isolate faults in networked systems, providing a complementary perspective to the work carried out at the University of L'Aquila. This international experience was particularly valuable, as it provided exposure to diverse research environments, facilitated collaboration with new colleagues, and offered alternative perspectives on problem–solving in autonomous systems.

The journey of this research has been both intellectually stimulating and personally rewarding. Conducting research in the field of autonomous systems requires not only mastery of technical concepts but also creativity, persistence, and the ability to integrate ideas from multiple domains. I have learned to navigate complex theoretical challenges, design and implement simulation studies, and critically analyse results to extract meaningful conclusions. Beyond the technical achievements, the thesis reflects perseverance, curiosity, and a commitment to personal and professional growth, fostering abilities such as critical thinking, problem–solving, and the capacity to tackle complex challenges effectively.

I hope that the work presented in this thesis will help advance understanding in the field of autonomous systems, especially in areas that require reliable coordination and effective monitoring. The methodologies and results developed here may provide a foundation for future research and support the design of autonomous agents capable of operating efficiently, handling unexpected situations, and functioning safely in a variety of environments.

In conclusion, this thesis represents a combination of theoretical exploration, practical analysis, and personal growth that has shaped my doctoral journey. It is intended as a contribution to the ongoing development of autonomous systems, offering insights and approaches that may inspire further research and practical applications in the control, coordination, and monitoring of autonomous agents.

Acknowledgements

Completing this PhD has been a long and challenging journey, one that would not have been possible without the support, guidance, and encouragement of many people.

First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. Elena De Santis, whose expertise, patience, and guidance have been invaluable throughout this research. Your insightful comments, constructive feedback, and encouragement have shaped not only this work but also my growth as a researcher. I am also deeply grateful to my co–supervisor, Prof. Giordano Pola, for his constant support, thoughtful guidance, and meticulous attention to detail. His constructive suggestions and careful review at critical stages of the research were instrumental in refining the work and ensuring its rigor. I would also like to express my sincere gratitude to my other co–supervisor, Prof. Mario Di Ferdinando, whose guidance and support were essential for the work on control and coordination. Without his direction and encouragement, completing that part of the research would not have been possible.

I would like to sincerely thank Prof. Mohamed Djemai at QUARTZ Lab, National School of Electronics and its Applications - ENSEA, France, for welcoming me during my mobility period and for his invaluable guidance on fault detection and monitoring for autonomous systems. His mentorship and thoughtful discussions greatly enriched this part of the research and provided a broader perspective on theoretical approaches. I am also grateful to Prof. Maria Domenica Di Benedetto, whose advice and support have been invaluable, not only academically but also personally, helping me navigate the challenges of the PhD journey.

I would also like to thank the administrative and academic staff at the University of L'Aquila, Politecnico di Bari, and QUARTZ Lab for their support during my doctoral studies, I am also grateful to my fellow PhD colleagues and friends, for providing a collaborative, motivating, and stimulating environment throughout these years.

Finally, I want to express my heartfelt gratitude to my family. I am especially thankful to my mother, whose encouragement and motivation inspired me to embark on this PhD journey. Special thanks also go to my father and the rest of my family, whose love, patience, and unwavering support have been a constant source of strength.

To all of you, thank you for making this journey not only possible but also meaningful and memorable.

Chapter 1

Introduction

1.1 Background and Motivation

The rapid growth of autonomous systems has opened up a new era of intelligent technologies that can operate independently in complex and uncertain environments. In modern agriculture, these systems are playing an increasingly important role by automating tasks such as crop monitoring, precision irrigation, soil analysis, and coordinated field operations. Many of these applications rely on *Multi-Agent System* (MAS), where multiple autonomous agents whether in the form of robotic swarms, distributed sensor networks, or components of larger *Cyber-Physical System* (CPS), need to work together seamlessly, communicate reliably, and respond quickly to faults or external challenges like equipment malfunctions or cyber threats.

As agriculture continues to adopt automation, ensuring that these systems can be properly controlled, well–coordinated, and effectively monitored is becoming more important than ever. Reliable operation plays a key role in improving productivity and maintaining safety across modern agricultural systems. To achieve these objectives, this thesis investigates three main areas: control and coordination, security analysis, and fault detection and isolation. Together, these three form the core pillars of the research, aiming to build the foundation for developing autonomous agricultural systems that can perform efficiently and consistently under real–world conditions.

This work first addresses the robust control and coordination of nonlinear MAS with time delays, considering the effects of actuation disturbances and measurement errors. A novel methodology is developed for designing *Quantized Sampled-data Event-triggered* (QSE) controllers that ensure consensus tracking despite state delays. By leveraging *Steepest Descent Consensus Feedback* (SDCF) and *Input-to-State Stability* (ISS) redesign techniques, the approach can attenuate bounded disturbances and measurement errors in the digital control framework. Theoretical results guarantee that, with sufficiently fast sampling and appropriately quantized channels, the robustified SDCF controllers achieve semiglobal practical consensus tracking, even under discontinuities or non-uniform quantization. This methodology is demonstrated on a class of nonlinear time–delay MAS, including a numerical example involving the coordination of an *Unmanned Aerial Vehicle* (UAV) swarm.

In addition to achieving controlled coordinated behaviors, it is equally critical to monitor MAS to ensure that they operate securely and reliably. MAS function within a networked environment, and the complex and interdependent nature of these systems makes them vulnerable to faults and cyber attacks, as an attack on a single system or fault in a single system can rapidly spread across the network and can easily compromise the reliability of the whole network. Monitoring plays a fundamental role in the dependability of autonomous systems by offering a way to identify such undesired events and lessen their impact. This thesis investigates the monitoring of agents through security analysis and fault detection and isolation. Formal, model–based methods are developed to detect and interpret abnormal behaviors.

For security analysis, this thesis employs the *Finite State Machines* (FSM) modeling formalism to model agent behaviors and analyze their vulnerability to malicious attacks. Mainly, two types of attacks are addressed in this work: Active and Passive attacks. For active attacks, the focus is to develop necessary and sufficient conditions to ensure detectability and localizability of attacks in both single–agent and networked–systems, modeled using FSM. The work is then extended to passive attacks, which aim to infer secret or sensitive states of the system without directly altering its behavior. The focus here is on opacity, which determines whether sensitive information (e.g., the agent being

in a critical or secret state) can be inferred by an external observer. Observers are typically employed to verify or analyze opacity for this purpose. However, in large–scale systems, the use of classical or traditional observers can lead to unnecessary and complex computations. To reduce computational complexity, a decomposition technique that breaks the observer into sub–observers is developed. The work also discusses how these sub–observers can reduce the computational complexity involved in analyzing opacity.

In terms of fault detection, the thesis utilizes *Petri Net* (PN) modeling, and in particular, *Partially Observed Petri Net* (POPN), to capture the concurrent behavior of MAS. In this model, agents are represented by places or nodes, and the system's evolution is governed by transitions. The proposed fault detection method focuses on identifying and isolating faults occurring in the input channels of agents due to communication failures. A known–input observer–based fault detection algorithm is presented to identify or detect the presence of faults in the unmeasurable input space. Furthermore, utilizing the developed observer, a residual–based fault isolation scheme is also presented. It is important to clarify that, although PN and POPN models naturally arise in distributed and networked environments such as MAS, the fault detection framework developed in this thesis is formulated at the level of a single POPN model. The connection to MAS is therefore conceptual and motivational, rather than an explicit multi–agent modeling or cooperative control formulation.

Together, these findings provide comprehensive approaches for achieving well–coordinated, safe, and reliable operation of MAS. This thesis looks at control and coordination, and monitoring as separate but connected areas, focusing on the real–world challenges of using intelligent agents in agriculture, where both teamwork and reliability are important. For instance, farming tasks such as crop monitoring, irrigation, and field operations rely on precise coordination and consistent performance. The methods developed in this thesis provide a strong foundation to help autonomous agents work together effectively in these settings.

1.2 Literature Survey

In recent years, MAS have shown great promise in agriculture, where autonomous agents are being used more and more for tasks like crop monitoring, precision irrigation, soil analysis, and coordinated field operations [1], [2], [3], [4], [5], [6]. These applications require agents to work together seamlessly, communicate reliably, and respond quickly to unexpected events, such as equipment failures, dynamic enviroments, or even cyber threats [7], [8], [9], [10]. This emphasizes that study of control, coordination, and monitoring of MAS is not only technically interesting but also highly relevant for real–world agricultural systems, where performance of the overall system depends on the reliable performance of autonomous agents.

While the primary focus of this thesis is to develop methodologies for controlled, coordinated, and monitored behavior of MAS, the approaches presented here are readily applicable to agricultural settings. By highlighting this connection, the importance of creating robust, secure, and fault–tolerant MAS frameworks becomes clear. The following sections review the technical literature in three main areas control and coordination, security, and fault detection, showing how existing approaches tackle these challenges and setting the stage for the methods developed in this thesis.

1.2.1 Control and Cordination of Multi Agent Systems

Research in control and coordination of MAS has attracted significant attention over the past decades. A central challenge in this field lies in designing control strategies that not only stabilize individual agents but also ensure their coordinated behavior under practical constraints, such as communication delays, measurement errors, limited actuation, etc. In particular, the consensus problem of MAS concerns the design of a distributed control protocol such that a group of autonomous agents reach an agreement

in some sense. Many results have been provided for the consensus problem of linear and nonlinear MAS making use of continuous–time control laws (see, for instance, [11], [12]). On the other hand, it is well–known that in most practical applications, the quantized sampled–data transmission is unavoidable due to the involved technological devices and, consequently, the digital implementation of the control law is required [13]. Many approaches have been proposed in the literature for the study of the digital consensus control problem in the case of delay–free MAS (see [14], [15], [16]). In practical engineering applications, another important aspect to take into account is the unavoidable presence of measurement errors and actuation disturbances affecting sensors and actuators and which can deteriorate the performances of the consensus protocol preventing the agreement to be reached. In the case of delay–free MAS, the robust consensus problem has been widely investigated by exploiting continuous-time/digital controllers (see, for instance, [14], [17], [18], [19], [20]). On the other hand, results concerning the robust quantized sampled–data consensus of nonlinear MAS with state–delays are very few in the literature (see, for instance, [21]). Recently, in [17], the robust quantized sampled–data consensus tracking problem of a class of nonlinear globally Lipschitz MAS with state–delays in presence of actuation disturbances and measurement errors and described by bounded functions was investigated by exploiting the notion of *Steepest Descent Consensus Feedback* (SDCF). It is here highlighted that the results in [17] do not take into account: (i) general nonlinear time-delay MAS described by locally Lipschitz functions; (ii) known external disturbances affecting the system at hand introduced to characterize tracking control problems; (iii) event-triggered strategies for the update of the control input signals in order to properly manage the communication resources. To the best of our knowledge, no result is available in the literature concerning quantized sampled–data protocols achieving the consensus tracking of nonlinear MAS with state–delays in presence of measurement errors and actuation disturbances taking into account points (i)-(iii).

In this work, we fill this gap by providing, for the first time in the literature, a methodology for the design of robust *Quantized Sampled-data Event-triggered* (QSE) controllers for the consensus tracking of nonlinear locally Lipschitz MAS with state–delays affected by bounded actuation disturbances and suitably bounded measurement errors. In particular, the recent results provided in [22], concerning the robust QSE stabilization problem of nonlinear time–delay systems, are here extended to the case of the tracking consensus control problem in the context of nonlinear MAS with state–delays. The proposed methodology relies on the Artstein's approach (see, for instance, [23], [24], [25]), which is here used in order to provide a new guideline for the design of robust QSE protocols for the consensus tracking of nonlinear time–delay MAS taking into account points (i)-(iii). The notion of SDCFs [17] is here suitably accommodated in order to: (a) cope with nonlinear time–delay MASs described by locally Lipschitz functions; (b) be used together with the *Input-to-State Stability* (ISS) redesign methodology for the design of robust QSE protocols. For the first time in the literature, it is shown that there exist a suitably small maximum inter–sampling time and a suitably accurate quantization of the input/output channels such that the QSE implementation of SDCFs (continuous or not), together with the new added control term, ensures the consensus tracking agreement in finite–time of the related closed—loop MAS in a semiglobal practical sense, with arbitrarily small final tracking error and regardless of the above uncertainties. The design procedure here provided allows for possible discontinuities in the function describing the SDCF at hand, widely enlarging the possibilities of successfully constructing robust QSE protocols for the consensus tracking of nonlinear MASs with state–delays because the continuity issue is no more a constraint. In the theory here developed, the case of time–varying sampling intervals and of non–uniform quantization of both input/output channels, as well as the stability analysis of the intersampling system behaviour, are included. The stabilization in the sample–and–hold sense theory [26], [27], [28], [22], [29], [30] is properly revised and used as a tool for proving the results. We highlight that, differently from the results here provided, in [22]: (1) tracking control problems characterized thorough the presence of known exogenous disturbances are not considered; (2) MASs are not addressed excluding the consideration of consensus control problems.

Moreover, differently from [17], here: (1) event–triggered strategies introduced to properly manage the communication resources are considered; (2) nonlinear MASs with state delays described by locally Lipschitz functions and in presence of known exogenous disturbances are studied; (3) spline approximation methods in order to cope with the possible non–availability in the buffer of required past values of the state measurements. The provided results are validated through an application concerning a particular class of nonlinear MASs.

While the above results are developed for a general class of nonlinear MASs, similar control challenges explicitly arise in agricultural UAV applications, where coordinated drones must operate under sampling constraints, communication limitations, disturbances, and measurement errors. Robust control strategies have demonstrated significant success in precision farming applications. For instance, tube–based robust Model Predictive Control (MPC) schemes for fixed–wing UAVs have been shown to follow waypoints with high accuracy while effectively compensating for disturbances across agricultural fields [31]. Extending beyond individual UAVs, multi–UAV coordination and optimal control frameworks have been developed for large–scale farm coverage and agricultural spraying, highlighting the practical advantages of consensus–based control strategies in smart agriculture [32]. Reviews of precision farming drones consistently stress that advanced, robust flight control methods are crucial for successful coordinated UAV operations [33] reinforcing the practical relevance of the robust QSE consensus–tracking framework presented in this thesis. Taken together, these studies clearly illustrate the significance and applicability of robust, sampled–data, and event–triggered consensus control approaches for UAV systems in agriculture.

1.2.2 Security Analysis

In parallel to control and coordination, monitoring autonomous agents to ensure reliable and secure operation has become increasingly important, especially as systems grow in complexity and scale.

For security analysis, FSM modeling provides a natural and expressive formalism for representing agent behaviors and interactions. While the control and coordination framework in this thesis is based on nonlinear system models, previous research has shown that such nonlinear dynamics can be effectively abstracted into FSM representations, thereby justifying the use of FSMs for security–related studies [34]. Numerous studies further validate the choice of FSM / automaton–based modelling for analyzing security in MAS and networked–systems. For example, [35] discusses security and diagnosability under cyber–attacks by using the FSM modeling formalism to represent both the system and the attacker. Similarly, In [36], intrusion detection in Mobile Ad Hoc Networks (MANETs) was addressed for a specific class of attacks, namely Denial of Service, using an FSM–based framework. In [37], the problem of multiple attack detection in *Discrete Event Systems* (DES) is addressed, where attacker influence is represented through altered observations, while using the FSM modelling formalism. Lastly, [38] demonstrates the use of FSM modeling to represent reconfigurable MAS, supporting the idea that agent behavior, communication, and dynamic reconfiguration can be effectively captured using FSM. All of these works show that FSM and DES modeling is a preferable choice for capturing both normal and malicious behavior, thus justifying their use in this thesis for security analysis.

A thorough summary of studies examining attack and defensive strategies in the context of DES, taking into account Fault Diagnosis, Opacity and Cyber Security, was provided by [39]. Another detailed systematic survey can be found in [40] that reviews research based on all types of attacks.

Building upon the general motivation for using FSM in security analysis, we now examine more specific literature, beginning with a single system and extending to networked or MAS.

Active Attack on Single Systems: The authors in [41] investigate the problem of attack detection and prevention in supervisory control systems under actuator enablement attacks,

using the notion of AE–safe controllability. An extension of this work, considering the effect of control delays, is presented in [42]. The results in [43] characterize the existence of a successful attacker and present an algorithm to synthesize the supremal successful normal attackers. The research done in [44] proposes a method to obfuscate an (insecure) supervisor, in order to maintain the behavior of the initial closed–loop system while making it resilient to actuator enablement attacks. Similarly, the authors in [45] address the problem of resilient supervisory control in DES under indefinite actuator attacks, where any controllable event may be targeted by an intruder.

A general framework for attack mitigation in supervisory control systems is presented in [46], where the goal is to minimize tolerated but undesirable behaviour while maximizing desirable behaviour under partial observation. A Finite State Transducer (FST) model for the supervisor–known sensor and actuator attacks is proposed and analyzed in [47]. In a related direction, the research in [48] provides a quantitative representation of the system under specific categories of actuator attacks, sensor erasure, or sensor insertion attacks, and proposes a defense strategy based on the disablement of all controllable events once an attack is detected.

From the discussion above, it can be concluded that most of the available literature on actuator attacks using the FSM or automaton modeling formalism either utilizes a specific class of actuator attacks (e.g., actuator enablement attacks in [41], [42], [44]), focuses on synthesizing the attacker ([43]), or deals with synthesizing a resilient supervisor to mitigate the effect of attacks ([45], [46], [47], [48]). This highlights a gap in research on attack detection at the actuator side that considers a more generic class of attacks. In this thesis, we address this problem in detail by proposing a unique approach for actuator attack detection, based on the composition of the plant and attacker models. With the proposed approach, one can pre–analyze the system behavior for possible attack models and design an appropriate controller to ensure safety.

Few researchers have also addressed the problem of security and attack detection in DES by using PN formalism instead of automaton modelling. The research presented in [49] deals with the detection of replay and covert attacks. The detection technique is based on the comparison of the received signal from the network and the expected behaviour of the system model. Paper [50] proposes a defence strategy to detect actuator enablement attacks. A different approach based on cryptography, to protect CPS against actuator attacks is provided in [51]. The idea is to encrypt the controllable events before transmitting, leading intruders to mistakenly infer the supervisor's control actions.

In contrast to these approaches, the method developed in this thesis uses an FSM–based framework and addresses both attack detection under actuator attacks. Unlike [50] and [49], this thesis provides necessary and sufficient conditions to identify the attacked channel. Additionaly, the work done in [51] is effective in reducing attack impact, but assumes secure key distribution and does not support post–attack analysis as done in this thesis.

The existing literature available on cyber–attacks in the context of DES, mostly deals with attack detection [49],[52], [50], [41], [48] and supervisor synthesis [41], [48], [45], [46], [44], [47]. However, only a few research articles can be found related to the localization of attack, see e.g. [52]. The work presented in [52], refers to the term "attack localization", to identify the attacked subsystem. A subsystem contains a subset of sensors, and it is assumed that the attacker has access to a limited number of sensor signals and the attacked subset of sensor signals remains fixed. In contrast, this thesis defines attack localization as the identification of the compromised channel type, i.e., whether the sensor or actuator is under attack, rather than narrowing down to a fixed subset of sensor signals. Moreover, the proposed approach does not assume prior knowledge of which signals are accessible to the attacker.

While the above works focus on attack detection and isolation for a single system, the increasing deployment of interconnected systems necessitates extending these security measures to networked or multi–agent settings. In what follows, we review existing literature that addresses attack detection and resilience in such distributed or networked DES.

Active Attacks in Networked/Multi-Agent Systems: Similar to the case of single system, the existing literature discussing the security of networked systems can be classified into three main categories (i) attack detection [53], [54], [55], [56], [57], [58], [59], [60], (ii) attack isolation [54], [59], [61], and (iii) control strategies to minimize the effect of attacks [47], [62], [63], [64]. Further discussion related to the security of MASs can be found in these survey articles [65], [66], [67].

Drawing from these primary concepts a distribution attack detection strategy, for interconnected systems is proposed in [53]. The proposed technique utilizes two observers, distributed Luenberger observer and a decentralized unknown input observer, to locally detect the attack in the communication channel connecting neighbouring sub-systems and their respective local controllers. The extended results discussing the isolation of covert attacks and the effect of disturbances were then addressed in [54] and [55] respectively.

Some papers address the security of interconnected systems along with network optimization. The authors of [62], presented an event–triggered mechanism (ETM) to address the security of networked interconnected systems (NISs), the proposed ETM allows the control unit to gather more information from the local subsystem for improved control performance in the presence of cyber–attacks, ensuring the efficient usage of communication and computation resources.

Papers [53], [54], [55], [62] mainly address the problem of attacks in the communication channel connecting subsystems with their local controller, but in contrast, the focus of this work is to address the problem of decentralized attack detection, when the communication channels connecting the subsystems are vulnerable to attacks.

Using the same interconnected system framework introduced in [53], the notion of distributed attack detectability was discussed in [56]. Both local and interconnection attacks were discussed and the ability to detect interconnection attacks was linked to the input observability of neighbour's states through interconnection, but the proposed approach in [56], requires physical coupling (secure communication channel) amongst the subsystems and the interconnection attack refers to the attacks on the communication channel linking the distributed controllers. However, the conditions developed in this thesis for attack detectability and localizability do not require any physical coupling or secure communication channel among the agents.

While most research focuses on attack detectability and control strategies, the work in [57] explores networked system vulnerabilities through graph theory. In [57], conditions were developed to ensure that the attack remains undetectable; however, these conditions were based on the assumption that the network must contain one rooted directed spanning tree. In contrast, the proposed method in this thesis develops conditions for attack detectability without imposing constraints on the network topology.

The problem of co–diagnosability in the presence of deception and denial of service (DoS-D) attacks was discussed in [58], which focused on a decentralized network that utilized one plant and multiple communication channels to gather data from various measurement sites. On the contrary, we discuss the problem of attack detection in a network of two agents in a decentralized framework.

Some researchers also investigated the concept of security from a control perspective. The research presented in [47] provides attack–resilient control strategies for scenarios where an attack occurs on the sensor, actuator, or both sides. These proposed control strategies were derived using a Finite State Transducer (FST) model of the attacker. An enhanced version of this work, utilizing FST (instead of automaton) modeling of plants, was presented in [63]. Similar to [47], [63], we also used an attack model; however, in our work, the focus is on attack detectability within a network of two agents, utilizing the concept of *Decentralized Critical Observability* (DCO) while the research in [47], [63] focuses on synthesizing a supervisor in the presence of attacks.

While many studies focus on detection and control strategies, few work address attack isolation in networked systems. A recent work discussing a distributed attack isolation strategy was presented in [61], which provides necessary and sufficient conditions for the localization to occur. These conditions put structural constraints on the physical coupling

on the network of agents. In contrast, the conditions for attack detection and localization provided here do not require any physical connection among the agents.

While much of the literature discussing security of MAS or Networked systems focuses on attack detection, isolation, or mitigation assuming specific communication models or structural constraints, our work diverges by developing conditions for both attack detectability and localization in a network of two agents without requiring physical coupling or secure inter–agent channels.

Unlike existing works that often depend on strong assumptions about network topology, controller structure, or secure links, the work done in this thesis provides a more relaxed framework that still ensures rigorous detection guarantees in a decentralized setting.

Passive Attack analysis through Opacity: Building on the analysis of active attack detection and isolation in networked systems, the next component of this thesis moves towards passive attacks, which manipulate or leak information without directly altering system behavior. In the context of DES, opacity has emerged as a widely accepted property for formalizing and analyzing such information–flow security concerns.

A system is said to be opaque if an external observer, with limited observation capabilities, cannot determine whether the system has visited a set of secret (or sensitive) states [68]. Several notions of opacity have been introduced in the literature and the intruder is modelled as a passive observer with complete knowledge of the structure of the system [69]-[70]. There are two general concepts of opacity in the literature [71]:

- Execution–based opacity (Language–based opacity) [72] which has two categories: Strong opacity and Weak opacity;
- State–based opacity considers two kinds of opacity: Current state opacity [73] and Initial state opacity [74].

It was discussed in [75], that the different notions of opacity can be transformed into each other. Wintenberg et. al. [76] provide a general framework that unifies different notions of opacity including language–based and state–based ones. Strong current state opacity and strong initial state opacity as more robust forms of opacity, were introduced in [77] for partially observed non–deterministic finite state automata. Paper [78] proposed an approach to verify current state opacity for bounded PN by using Multi–valued decision diagrams with partial observable transitions. Worthy opacity was introduced in [79] for PN, which characterizes the value of the information that a system may leak over its evolution. While literature recalled above addresses opacity analysis, the works presented in [80] and [81] address opacity enforcing via supervisory control design.

The notion of opacity allows for the modeling and verification of privacy against passive observers and has been applied in various CPS settings to ensure that confidential behaviors remain hidden [82], [83]. Motivated by this, the current work explores opacity as a means to characterize and assess the vulnerability of FSM under passive attacks. To this end, many existing approaches rely on observer–based methods, as the observer captures the intruder's knowledge of the system [83]. In fact, opacity verification is typically performed through the computation of the system's observer (see, e.g., [84]), and the complexity of this process has been widely studied in the literature [85]. This motivates the work on observer decomposition, which aims to reduce the complexity by constructing smaller, local observers instead of the full global one, enabling more scalable verification of opacity–related properties.

Building on the discussion of opacity for passive attacks, the FSM/DES–based security analysis developed in this work–including both active attack detectability and localizability as well as passive attack opacity has clear relevance to agriculture oriented UAV systems. Discrete–event modeling has already been applied to multi–UAV agricultural systems to represent mission stages, state transitions, and coordination, showing that DES/FSM frameworks are suitable for capturing the behavior of complex agricultural operations [86]. From a security perspective, UAVs and IoT–enabled agricultural networks face a variety of cyber threats, including communication attacks and sensor spoofing, which highlights

the practical importance of formally analyzing attack detectability and localizability [87], [88].

Beyond UAV coordination, formal state–based and hybrid automata models have also been adopted in smart agriculture to represent and control complex greenhouse processes, including crop growth, pathogen dynamics, and climate regulation. Such works demonstrate that automata–based modeling provides a suitable abstraction for composing heterogeneous agricultural subsystems and enabling formal analysis and control [89].

Hybrid formal models have been proposed in smart agriculture to ensure system resilience, demonstrating that structured modeling approaches can help protect critical agricultural operations [90]. In the case of passive attacks, opacity offers a formal framework to evaluate privacy and potential information leakage in DES–based systems, supporting observer–based verification methods that help protect sensitive behaviors [91]. Similarly, formal threat modeling in IoT–enabled precision agriculture emphasizes the importance of systematically evaluating system vulnerabilities to safeguard both data and autonomous operations [92]. Overall, these findings show that the DES–based framework developed in this work covering both active and passive attacks is not only theoretically robust but also directly applicable to modern UAV–enabled agricultural systems, offering a practical and well–structured approach to protecting precision farming operations against a broad range of cyber threats.

1.2.3 Fault Detection

After discussing security analysis in FSM–based models, particularly in the context of passive and active attacks, we now shift focus to another important reliability concern in DES: fault detection. While FSM–based frameworks are well–suited for applications relying solely on control logic and sequential behavior, they become increasingly limited when modeling systems with concurrency or resource sharing. To address these structural limitations, PN and POPN have been widely adopted as an alternate modelling formalism in distributed and concurrent systems.

Several works have demonstrated the applicability of POPN in fault diagnosability and isolation in complex and partially observed systems, e.g. the results presented in [83], [93] provide structured methods to predict and detect faults without requiring full system observability or exhaustive reachability analysis. Given these advantages, PN modeling, particularly POPN is adopted in this thesis to address fault detection problems.

A major challenge in POPN is state estimation under partial observation particularly reconstructing the marking (system state) and the sequence of transition firings based on limited sensor data. Early work by Giua [94] addressed this by proposing an algorithm to estimate the marking from observed transitions, assuming the net structure is known. In another contribution, Giua and co–authors [95] investigated the estimation of markings in labeled PN with nondeterministic transitions, where different transitions may share the same label and be simultaneously enabled. They demonstrated that the set of possible consistent markings can be expressed as the solution of a linear system with fixed structure, whose parameters can be recursively determined. This methodology was later applied in [96] to address the estimation problem in the presence of silent transitions, i.e., transitions whose firings cannot be directly observed.

Alternative approaches have also been developed to tackle estimation in PN systems. For instance, Bourjij [97] proposed a reduced–order observer for generalized PN systems, where the token flow is represented using state equations analogous to those in continuous dynamic systems. This observer design was subsequently employed in [98] for detecting active modes in hybrid systems, and later applied to hybrid photovoltaic systems in [99]. In a different line of work, Ramírez et al. [100] examined the recovery of the initial marking when only partial information about transition firings is accessible. Their formulation incorporates both the available output measurements and the notion of observability into the observer design. For Interpreted PN, Salas [101] proposed a construction procedure for asymptotic observers under partial observation, while Hadjicostis [102] studied state estimation under the combined presence of nondeterministic and unobservable transitions.

Despite these numerous efforts, relatively little work has been devoted to the estimation of firing transitions themselves. Lingxi [103] introduced an approach for determining the least–cost transition firing sequence that matches the observed label sequence generated by transition activities in a labeled PN. Similarly, Lefebvre et al. [104] analyzed the problem of estimating transition firing sequences under the assumption that the marking of the PN is known.

This work builds upon previous research in the field. In [105], the focus was on designing an unknown input observer for POPN. The objective in that study was to estimate the internal state of the system despite incomplete observations, thereby addressing one of the central challenges in monitoring distributed systems. Subsequently, in [106], the same PN modeling framework was extended to develop a fault detection methodology for hybrid dynamical systems, where discrete–event dynamics are coupled with continuous evolution. Specifically, the authors in [106] tackled the problem of place/node fault detection, i.e., identifying abnormal conditions linked to the degradation or malfunctioning of certain system states.

While place–level fault detection has received significant attention, transition–level faults remain comparatively underexplored, despite their critical role in the operation of DES. In industrial applications such as automated production systems, PNs are frequently used to model the sequence of operations and interactions between machines. In such systems, transitions often correspond to events triggered by input signals, such as the activation of a robot, the start of a conveyor belt, or the opening of a valve. A failure in these transitions for example, when a transition does not fire despite the availability of resources, or when it fires unexpectedly due to an erroneous signal can cause serious problems. These may include deadlocks that block the production line, unsafe operating conditions such as the simultaneous activation of incompatible machines, or performance degradation manifested in increased cycle times and wasted resources. Detecting faults at the transition level is therefore essential, as it allows early identification of abnormal behaviors before they escalate into costly downtime or quality issues.

In this thesis, we shift the focus from faults in places to faults occurring in transitions, which correspond to abnormalities in the input channels of the system. Such faults are critical because transitions often represent events, commands, or external stimuli driving the system's dynamics. Detecting anomalies at this level requires a refined observer design. The approach proposed in this thesis aims to address this gap by developing a fault detection strategy specifically targeted at transition–level faults in POPN–modeled systems.

Building on the technical survey above, it is also valuable to emphasize how the proposed transition–level fault detection framework connects with practical application domains such as agricultural systems. PN–based modeling has been employed to represent key agricultural processes for example, the workflow of farm operations such as site selection, tilling, planting, irrigation, weeding, fertilization, and harvesting using Colored PN, as illustrated in the study [107], that formally captures the progression of discrete agricultural tasks and resource usage in crop production workflows. Similarly, generalized stochastic PNs have been used to model the dynamics of plant disease and pest propagation, capturing how environmental conditions, biological processes, and management actions interact over time. Such models have been shown to support early warning and treatment decision–making in large–scale agricultural settings [108]. These works illustrate that transitions in agricultural PN models naturally represent operational actions, environmental events, or external stimuli that directly influence system behavior, which closely aligns with the transition–focused viewpoint adopted in this thesis. While the current agricultural literature primarily concentrates on modeling and simulation rather than explicit fault diagnosis, the resulting structured PN representations form a solid foundation for the application of advanced fault detection and isolation techniques. In this sense, the methodology developed in this thesis can be seen as a complementary extension, contributing to improved reliability and robustness in automated and data–driven agricultural CPS.

The literature reviewed here demonstrates the extensive work done in control and

monitoring of DES, with specific attention to multi–agent control and coordination, attack detection and localization, and fault diagnosis and isolation. FSM–based approaches have proven effective and efficient for security analysis, particularly in addressing active and passive security threats, through attack modeling, detection conditions, and opacity analysis. Similarly, PN based frameworks, specifically POPN, offer strong modeling capabilities for fault detection in systems exhibiting concurrent and distributed behaviors. However, despite the extensive research in the respective fields, certain limitations remain intact. While numerous approaches achieve controlled coordinated behaviour of MAS, but they often assume ideal sensing, actuation, or delay–free conditions. In security, existing detection and localization techniques often rely on strong assumptions such as full observability or secure communication links. Likewise, in fault diagnosis, much of the focus has been on place–level faults, with fewer methods addressing transition–level anomalies in POPN.

When we consider agriculture, these limitations become even more significant. Agricultural environments are dynamic and uncertain, with noisy sensors, unreliable communications, and constantly changing conditions. Addressing these practical challenges is essential to ensure that MAS used for crop monitoring, irrigation management, soil analysis, coordinated field operations, etc., can operate safely, reliably, and efficiently. This underscores the importance of developing MAS methodologies that are robust, secure, and fault–tolerant, capable of handling the complexities of real–world agricultural applications.

1.3 Problem Statement

Despite extensive research on control and monitoring of MAS in the context of DES, key challenges persist in the following areas:

- **Robust Event–Triggered Consensus of MASs under Delays and Uncertainties**
  Despite substantial progress in distributed control of multi–agent or networked systems, several challenges persist. Most existing methods rely on ideal conditions, neglecting state delays, measurement errors, and actuation disturbances that commonly arise in practical implementations. The integration of quantized sampled–data and event–triggered control under such nonlinear and uncertain environments remains limited. Furthermore, ensuring consensus and stability in the presence of non–uniform sampling, communication constraints, and bounded uncertainties continues to be a key open problem requiring deeper investigation.
- **Attack Detection and localization in FSM modelled systems**:
  Current research lacks generalized frameworks for actuator attack detection and localization in single systems that avoid restrictive assumptions about attack types while ensuring precise identification of compromised channels. Likewise, decentralized detection and localization approaches for networked systems that operate without relying on physical connections, secure communication among agents, or stringent network topology requirements are still limited. Addressing these gaps is essential to develop flexible and robust security methods applicable to both single and interconnected DES.
- **Passive Attack Analysis Via Opacity**
  Opacity verification in FSM–based systems typically depends on constructing a global observer, which becomes computationally expensive and impractical for large–scale systems. This poses significant challenges for analyzing opacity in large–scale or complex DES. Despite its importance, limited progress has been made toward scalable verification methods that can manage this complexity effectively. As a result, the problem of efficiently verifying opacity in large systems remains an open challenge in the field.
- **Fault Detection in Petri Net models**
  Fault diagnosis using POPN has been extensively studied, particularly for detecting

faults at the place level. However, comparatively less attention has been given to faults occurring at the transition level. This gap is especially prominent under partial observability, where detecting such faults is critical for identifying abnormalities in input–driven behaviors. As a result, transition–level fault detection in POPN remains an underexplored area.

To address these gaps, this thesis makes the following contributions:

- Design of robust, *Quantized Sampled-data Event-triggered* (QSE) controller for consensus tracking of nonlinear MASs, addressing state delays, measurement errors and actuation disturbances.
- Design of an FSM-based framework for actuator attack detection and localization that supports a broad class of attacks and enables rigorous analysis without assuming full observability or secure links.
- Development of decentralized detection and localization conditions for active attacks in networked systems, without requiring physical coupling or putting constrained on network topology.
- Proposal of a scalable opacity verification method through observer decomposition, enabling efficient analysis of passive attacks in FSM–modeled systems.
- Formulation of a fault detection strategy for transition–level faults in POPN, enhancing reliability monitoring for distributed DES under partial observation.

While this thesis mainly focuses on the control, coordination, and monitoring of autonomous agents, agriculture is considered as one of the application domains where such methods can be relevant. As discussed in Section 1.2, precision agriculture increasingly relies on teams of autonomous agents for tasks such as field monitoring and coordinated operations. Such scenarios provide inspiration for the study of coordination, robustness, and security in MAS considered in this work.

1.4 Scope of the work

The first part of the thesis is confined to the robust control and coordination of nonlinear MASs with state delays, measurement errors, and actuation disturbances, under quantized sampled–data and event–triggered frameworks. It focuses on designing robust QSE controller to achieve reliable consensus tracking and coordinated behavior. However, this study is limited to systems with locally Lipschitz agent dynamics and bounded disturbances and measurement errors, and does not address unbounded uncertainties or highly irregular network topologies. These constraints define the practical applicability of the proposed methodologies and the scenarios where the results can be reliably implemented.

The second part of the thesis is focused on the analysis of security threats and fault detection, within the framework of DES. The work specifically considers systems modeled using FSM and POPN due to their suitability for capturing logical behavior, event–driven dynamics, and partial observability. Both single systems and multi–agent/networked systems are considered under this modeling paradigm. Specifically, it addresses problems related to attack detection, attack localization, observer decomposition for opacity analysis, and fault diagnosis, but restricts attention to discrete–event dynamics only. Continuous–time systems, hybrid system dynamics, or cryptographic security mechanisms are outside the scope of this work. Furthermore, the analysis assumes known system structure for security analysis and partial observation for fault detection, without incorporating probabilistic or learning–based models. The focus remains solely on model–based detection techniques.

Overall, the scope of this thesis is aligned with the agricultural application scenarios discussed in Section 1.2. The control, coordination, monitoring, and security problems addressed this thesis are motivated by the operational requirements of autonomous agents in agricultural environments, such as robustness to disturbances, limited communication,

security, and reliability under partial observability. While the proposed methodologies are developed in a general and application–agnostic manner, the assumptions, constraints, and problem formulations are chosen to reflect realistic conditions encountered in agricultural MASs. Consequently, the scope defined above captures both the theoretical contributions of the thesis and their relevance to autonomous agricultural systems.

1.5 Thesis Organization

This thesis is organized to provide a clear and systematic presentation of the research, carried out on the control, coordination and monitoring of autonomous agents. The thesis covers theoretical foundations, methodological developments, and provides suitable examples, to show the effectiveness and applicability of the proposed techniques. The following sections briefly summarize the purpose and scope of each chapter.

Chapter 2 establishes the foundational framework and modeling methodologies adopted in this work. It introduces the general notations used throughout the thesis. It also presents the nonlinear time–delay MAS model employed for control and coordination, and formally defines FSM and PN structures used for monitoring. This chapter provides the necessary foundation for the subsequent technical chapters.

Chapter 3 focuses on the control and coordination of autonomous agents, addressing the development of robust QSE controller for nonlinear time–delay MASs. The chapter presents in detail the theoretical foundations, key assumptions, and rigorous proofs ensuring stability and consensus for the proposed robust QSE controller, in the presence of time delays, measurement errors, and actuation disturbances. Simulation results are provided to validate the effectiveness of the proposed methodologies and to illustrate the practical performance of the control strategies.

Chapter 4 is devoted to the security analysis of autonomous agents modeled as FSMs, focusing on both active and passive attacks. This chapter develops composed FSM–based models to show/represent the behaviour of the system in the presence of attacks and provide necessary and sufficient conditions for detecting and localizing attacks on single–agent and multi–agent networks. Additionally, passive attacks are addressed through the notion of opacity, with the objective to reduce computational complexity to verify this property in large scale systems. A decomposition technique to generate sub observers is developed to achieve the stated objective. Together, these contributions offer a comprehensive methodology for monitoring and securing FSM–modeled systems against a broad range of adversarial behaviors.

Chapter 5 investigates fault detection in PN–modeled systems when only partial information is available from sensors. The chapter starts with a descriptor system formulation, to show the evolution of POPN. Furthermore, an observer–based method is developed to detect input faults from the available place and transition sensors, enabling reliable monitoring even without full system observability.

Chapter 6 concludes the thesis by providing a concise overview of the work presented throughout the study. It summarises the key contributions in the areas of control and coordination, security analysis, and fault detection of autonomous agents. The chapter highlights the significance of the methodologies developed, their theoretical foundations, and their relevance to advancing reliable and robust networked MASs. The results are also presented in the form of submitted and published articles, emphasizing the scientific impact and practical relevance of the contributions made in this research.

Chapter 2

Modeling Formalisms and Approaches

This chapter provides the necessary notations and mathematical modelling used for the control, coordination, and monitoring of autonomous agents in this study. For the control and coordination aspects, the agents are modeled as nonlinear time-delay MASs, capturing the dynamics, interconnections, errors and delays that arise in realistic networked environments. This representation provides a formal basis for the design and analysis of robust QSE controller.

As outlined in Chapter 1, this work employs FSM and PN as the primary modeling formalisms for monitoring purposes. In this chapter we also provide structured means of representing discrete event dynamics, system states, and transitions, within the framework of FSM and POPN, which are essential for effective observation and analysis of agent activities. This chapter presents a detailed discussion of the theoretical foundations of these two modelling techniques, along with their integration into the overall monitoring framework.

2.1 Motivation for Multiple Modeling Approaches

To study the behavior of autonomous agents in complex, uncertain environments, we employ three modeling frameworks that each address different aspects of the problem. Using different formalisms allows us to capture the diverse dynamics and requirements of MAS, control and coordination, security analysis, and fault detection in a way that is both rigorous and practically relevant.

First, the modeling of nonlinear MAS is chosen to address the control and coordination of agents whose dynamics may include nonlinearities, coupling effects, and practical constraints like communication delays, actuator errors or measurement noise. Nonlinear agent models allow us to describe realistic behaviors, for example autonomous vehicles or drones in a field setting and design control laws that guarantee consensus or formation despite uncertainties.

Second, we adopt the formalism of FSM for security analysis, particularly when agents or networks may face discrete–event challenges, such as cyber intrusions, communication failures or compromised channels. FSM–based approaches are effective for modeling attack scenarios, deriving detection conditions, and studying information flow or opacity properties.

Third, we use POPN to model fault detection and isolation in networked systems where only some events or states are observable. POPN are well suited to capture concurrency, distributed events, and state–transition behaviour in systems with multiple interacting agents or subsystems. The partially observable variant allows us to address situations where not all system components are visible, which is often the case in field–deployed autonomous networks.

By selecting these three complementary formalisms, nonlinear MAS for control/coordination, FSMs for security, and POPNs for fault detection, we build a comprehensive modelling toolbox. This enables us to tailor our methods to the specific demands of each task while still maintaining coherence across the overall research. It also allows a clear mapping from theoretical development to practical scenarios involving autonomous agents, such as those seen in agricultural applications, where coordination, security and reliability are all required.

2.2 Notation

We start by providing the notation used in this thesis. $\mathbb{N}$ denotes the set of nonnegative integer numbers, $\mathbb{R}$ denotes the set of real numbers, $\mathbb{R}^\star$ denotes the extended real line $[-\infty, \infty]$, $\mathbb{R}^+$ denotes the set of nonnegative reals $[0, \infty)$. The symbol $|\cdot|$ stands for the Euclidean norm of a real vector, or the induced Euclidean norm of a matrix. For a given positive integer n and a given positive real H, the symbol $\mathcal{B}_H^n$ denotes the subset $\{x \in \mathbb{R}^n : |x| \leq H\}$. For a positive integer n and for a positive real Δ (maximum involved time–delay), $\mathcal{C}^n$ denotes the space of the continuous functions mapping $[-\Delta, 0]$ into $\mathbb{R}^n$, $W_n^{1,\infty}$ denotes the space of the absolutely continuous functions, with essentially bounded derivative, mapping $[-\Delta, 0]$ into $\mathbb{R}^n$, $\mathcal{Q}^n$ denotes the space of bounded, right–continuous functions, with possibly a finite number of points with jump-type discontinuity, and with finite left-hand limit at 0, mapping $[-\Delta, 0)$ into $\mathbb{R}^n$. For $\phi \in \mathcal{C}^n$, $\phi_{[-\Delta,0)}$ is the function in $\mathcal{Q}^n$ defined, for $\tau \in [-\Delta, 0)$, as $\phi_{[-\Delta,0)}(\tau) = \phi(\tau)$. For $\phi \in \mathbb{C}^n$, we will consider $\|\phi\|_\infty = \sup_{\theta \in [-\Delta, 0]} |\phi(\theta)|$. For a positive real H, for $\phi \in \mathcal{C}^n$, $\mathbb{C}_H^n(\phi) = \{\psi \in \mathcal{C}^n : \|\psi - \phi\|_\infty \leq H\}$. The symbol $\mathcal{C}_H^n$ denotes $\mathcal{C}_H^n(0)$. For a continuous function $x \colon [-\Delta, c) \to \mathbb{R}^n$, with $0 < c \leq \infty$, for any real $t \in [0, c)$, x_t is the function in $\mathcal{C}^n$ defined as $x_t(\tau) = x(t + \tau)$, $\tau \in [-\Delta, 0]$. For a positive integer n and for $\mathbb{S} = \mathbb{R}^n$ (or $\mathbb{R}^+$), $C^1(\mathbb{S}; \mathbb{R}^+)$ denotes the space of the continuous functions from $\mathbb{S}$ to $\mathbb{R}^+$ admitting continuous (partial) derivatives, while $C_L^1(\mathbb{S}; \mathbb{R}^+)$ denotes the subset of the functions in $C^1(\mathbb{S}; \mathbb{R}^+)$ admitting locally Lipschitz (partial) derivatives. A continuous function $\gamma \colon \mathbb{R}^+ \to \mathbb{R}^+$ is of class $\mathcal{P}_0$ if $\gamma(0) = 0$, it is of class $\mathcal{N}$ if it is of class $\mathcal{P}_0$ and increasing (not necessarily strictly increasing), it is of class $\mathcal{P}$ if it is of class $\mathcal{P}_0$ and $\gamma(s) > 0$, $s > 0$, it is of class $\mathcal{K}$ if it is of class $\mathbb{P}$ and strictly increasing, it is of class $\mathcal{K}_\infty$ if it is of class $\mathcal{K}$ and unbounded. The symbol $\bar{I}_d$ denotes the identity function in $\mathbb{R}^+$. For a given positive integer n and m, the symbols $I_{n,n}$ and $0_{n,m}$ denote the identity matrix and zero matrix in $\mathbb{R}^{n \times n}$ and $\mathbb{R}^{n \times m}$, respectively. The symbol "$\circ$" denotes composition (of functions). For positive integers $\tilde{n}$, $\tilde{m}$, $\tilde{p}$, for Lipschitz on bounded subset functionals $F : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n}}$, $G : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n} \times \tilde{m}}$, and for a locally Lipschitz functional $V \colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$, the derivative in Driver's form (see, for instance, [109]) $D^+V \colon \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \times \mathbb{R}^{\tilde{m}} \to \mathbb{R}^\star$, of the functional V, is defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$, $\phi_r \in \mathcal{C}^{\tilde{p}}$ and $u \in \mathbb{R}^{\tilde{m}}$, as

$$D^+V(\phi_z, \phi_r, u) = \limsup_{h \to 0^+} \frac{V(\phi_{z_{h,u,\phi_r}}) - V(\phi_z)}{h} \tag{2.1}$$

where for $0 \leq h < \Delta$, $\phi_{z_{h,u,\phi_r}} \in \mathcal{C}^{\tilde{n}}$ is defined, for $s \in [-\Delta, 0]$, as $\phi_{z_{h,u,\phi_r}}(s) = \begin{cases} \phi_z(s + h), & s \in [-\Delta, -h) \\ \phi_z(0) + (s + h)\,(F(\phi_z, \phi_r) + G(\phi_z, \phi_r)u), & s \in [-h, 0]. \end{cases}$

For $a, b \in \mathbb{N}$, $[a, b] = \{x \in \mathbb{N} : a \leq x \leq b\}$. For a string σ, symbol $\sigma|_{[a,b]}$ denotes the string $\sigma(a)\sigma(a + 1) \ldots \sigma(b)$. For a set Q, the symbol $|Q|$ denotes its cardinality. The symbol ϵ denotes the null output. For a set $Y \subset Q$, symbol $\subset$ has to be understood as (not necessarily proper) subset and the symbol $\overline{Y}$ denotes the complement of Y in Q. For $W \subset Q \times Q$, the symbol W^s denotes the symmetric closure of W, i.e. $W^s = \{(i_1, i_2) \,|\, (i_1, i_2) \in W \text{ or } (i_2, i_1) \in W\}$. The power set of a set Q is denoted by 2^Q. For two sets Q' and Q, let $Q' \setminus Q = \{i \in Q' \,|\, i \notin Q\}$.

2.3 Nonlinear Time Delay Multi Agent Systems

To address the consensus problem, we consider a nonlinear time-delay MAS described by:

$$\begin{aligned} \dot{x}_i(t) &= f_i(x_{t,i}, \chi_{t,i}) + g_i(x_{t,i}, \chi_{t,i})(u_i(t) + d_i(t)), \\ x_i(\tau) &= x_i^0(\tau), \quad \tau \in [-\Delta, 0], \quad i = 1, \cdots, N. \end{aligned} \tag{2.2}$$

where: $x_i(t) \in \mathbb{R}^n$, $x_{t,i} \in \mathcal{C}^n$, $i = 1, \cdots, N$ denote the states of the system; $x_i^0 \in W_n^{1,\infty}$ are the initial states; $\chi_{t,i} \in \mathcal{C}^p$, $i = 1, \cdots, N$, are known disturbances, whose evolution is assumed to be known or measurable; $u_i(t) \in \mathbb{R}^m$, $i = 1, \cdots, N$, are the control input

signals; $d_i(t) \in \mathbb{R}^m$, $i = 1, \cdots, N$, are *unknown* disturbances; $f_i \colon \mathcal{C}^n \times \mathcal{C}^p \to \mathbb{R}^n$ and $g_i \colon \mathcal{C}^n \times \mathcal{C}^p \to \mathbb{R}^{n \times m}$ are functions Lipschitz on bounded subsets of $\mathcal{C}^n \times \mathcal{C}^p$; $\Delta > 0$ is the maximum involved time delay, assumed to be known; N is the number of agents. It is assumed that the known exogenous disturbances $\chi_{t,i} \in \mathcal{C}^p$, $i = 1, \cdots, N$, in (3.1) are continuously differentiable and such that there exist positive reals $\bar{\gamma}_\chi$, $\bar{\gamma}_{d\chi}$, satisfying

$$\|\chi_{t,i}\|_\infty \leq \bar{\gamma}_\chi, \ \forall t \in \mathbb{R}^+, \ \operatorname*{ess\,sup}_{\theta \in [-\Delta, 0]} \left| \tfrac{d\chi_{t,i}(\theta)}{d\theta} \right| \leq \bar{\gamma}_{d\chi}, \ \forall t \in \mathbb{R}^+. \tag{2.3}$$

The MAS presented in (2.2) and the inequality described in (2.3) will be used in the following chapter to discuss the consensus problem by designing a robust QSE controller for the given nonlinear MAS.

2.4 Finite State Machines

To support the monitoring framework proposed in this work, FSM are employed to model the behavior of autonomous agents under normal and adversarial conditions. Two distinct mathematical representations of FSM are used in this thesis, reflecting the structural and analytical differences between single–agent and multi–agent scenarios.

2.4.1 Single Agent FSM Representation

For the single–agent case, a classical six–element tuple representation is adopted. This formalism is well–suited for capturing the discrete event behavior of an individual agent, providing a clear and rigorous structure for defining states, transitions, events, and outputs. It enables precise modeling of agent–level dynamics and supports the design of monitoring algorithms for attack detection and localization at the agent level.

Formally, we consider FSM described by:

$$(X, X_0, E, Y, \Delta, H) \tag{2.4}$$

where:

- X is the finite set of states;
- $X_0 \subset X$ is the set of initial states;
- E is the finite set of events;
- Y is the finite set of outputs;
- $\Delta \subset X \times E \times X$ is the finite set of transitions;
- $H : (X \cup \Delta) \to Y$ is the output function.

To convert the FSM described above into a Moore machine, the key modification lies in the output function. In the FSM presented in (2.4), outputs depend on both states and transitions, but in a Moore machine, all output information must be associated exclusively with the states. This requires redefining the output function $H : X \to Y$, mapping each state directly to an output. Consequently the set of transitions becomes $\Delta \subset X \times X$. Thus, any information previously carried by the transitions must be encoded into the states themselves. This ensures that the system's outputs are generated solely based on the current state, allowing all relevant information to be reflected in the state, rather than being influenced by the immediate input or event.

For $x \in X$ in (2.4),

$$succ\,(x) = \{x' \in X : (x, e, x') \in \Delta\}$$

$$pre\,(x) = \{x' \in X : (x', e, x) \in \Delta\}$$

$$u\,(x) = \{e \in E : (x, e, x') \in \Delta\}$$

Similarly, for $X' \subset X$

$$succ\,(X') = \{x \in X : (x', e, x) \in \Delta \wedge x' \in X'\}$$

$$pre\,(X') = \{x \in X : (x, e, x') \in \Delta \wedge x' \in X'\}$$

FSM is in general nondeterministic, i.e. it is possible that $(x, e, x') \in \Delta$ and $(x, e, x'') \in \Delta$ with $x' \neq x''$. In our setting, the input events are available as outputs, i.e. $H((x, e, x')) = e$, and hence $E \subset Y$; $\epsilon \notin E$.

A string

$$x_1\, e_1\, x_2\, e_2\, x_3\, ... \tag{2.5}$$

with $x_i \in X$ and $e_i \in E$ is called a run of the FSM in (2.4), if $x_1 \in X_0$ and $(x_i, e_i, x_{i+1}) \in \Delta, \forall i = 1, 2, ...$. Runs may be of finite or infinite length. Given a run (2.5),

the sequence

$$r_e = e_1\, e_2\, e_3\, ... \tag{2.6}$$

is called event run, the sequence

$$r_x = x_1\, x_2\, x_3\, ... \tag{2.7}$$

is called state run and the sequence

$$r_y = H(x_1)\, e_1\, H(x_2)\, e_2\, H(x_3)\, ... \tag{2.8}$$

is called output run.

Let $\mathcal{R}$ be the set of all FSM runs, $\mathbb{E}$ be the set of all event runs, χ be the set of all state runs and and for a given $\Psi \subset X$, let χ^{Ψ} be the set of finite state runs $r_x \in \chi$ with last symbol in Ψ. Let Υ be the set of all output runs of FSM. Function $f : X_0 \times \mathbb{E} \to \mathcal{R}$ associates to an initial state and event run, the collection of all compatible runs of FSM, i.e. $f(x_1, r_e) = \{(x_1 e_1 x_2 e_2 ...), ...\}$. Function $y : \mathcal{R} \to \Upsilon$ associates to a run of FSM, the corresponding output run, i.e. for $r \in \mathcal{R}$, $y(r) = H(x_1)e_1H(x_2)e_2H(x_3)....$ For $k \geq 1$ and $k' \geq k$, the symbol $y(r)|_{[k,k']}$ denotes the string $H(x_k)e_kH(x_{k+1})e_{k+1}...H(x_{k'})$. Finally, y^{-1} denotes the inverse function of y i.e. $y^{-1}(r_y) = \{r' \in \mathcal{R} : r_y = y(r')\}$, $r \in \mathcal{R}$.

Furthermore, we adopt the notion of accessible part $Ac(.)$, of the FSM from [110], as:

$$Ac(M) = (X_{ac}, X_0, E, Y, \Delta_{ac}, H) \tag{2.9}$$

where,

- $X_{ac} = \{x \in X : \exists r_e \in \mathbb{E} \wedge x_0 \in X_0 \wedge f(x_0, r_e) = \{(x_0, e_1, ..., x)\}\}$;
- $\Delta_{ac} = \{(x, e, x') \in \Delta : x, x' \in X_{ac}\}$

Intuitively, $Ac(M)$ contains only those states that can be reached from the initial state(s) through some finite sequence of events. States that are not reachable from X_0 are considered inaccessible and are removed from the model.

Let $\boldsymbol{\Upsilon}$ be the set of strings with symbols in $\widehat{Y} = \{y \in Y : y \neq \epsilon\}$. Define $\mathbf{y} : \chi \to \boldsymbol{\Upsilon}$ as the function that associates to a state run the corresponding outputs, as $\mathbf{y}\,(r_x) = P\,(\sigma)$ where $\sigma = H\,(r_x\,(1))...H\,(r_x\,(n))$, $n = |r_x|$ if $|r_x|$ is finite and $P\,(\sigma)$ is the projection of the string σ, i.e. the string obtained from σ by erasing the symbol ϵ [111]. Otherwise if $|r_x|$ is infinite, $\mathbf{y}(r_x) = P(\sigma_\infty)$ where σ_∞ is an infinite string recursively defined as $\sigma_1 = H(r_x(1)), \sigma_{k+1} = H(r_x(k+1)), k = 1, 2, ...$. Finally, $\mathbf{y}^{-1}(\mathbf{y}(r_x)) = \{\hat{r}_x \in \chi : \mathbf{y}(\hat{r}_x) = \mathbf{y}(r_x)\}$, $r_x \in \chi$.

2.4.2 Multi–Agent FSM Representation Using Difference Equations

In contrast to single systems, the multi–agent scenario introduces additional complexity due to inter–agent interactions and network–level coordination. To address this, a difference equation–based representation of FSM is employed. This approach facilitates a more compact and scalable modeling framework for networks of agents, allowing for the analysis of system–wide behaviors and the detection of distributed anomalies.

In the networked case, the FSM behavior of each agent P_i is represented using a difference inclusion:

$$P_i = \begin{cases} x_i(t+1) \in F_i(x_i(t), y'_{3-i}(t), u_i(t)), \\ x_i(0) \in X_{i,0}, \\ y_i(t) = h_i(x_i(t)), y_{3-i}(t) = h_{3-i}(x_{3-i}(t)), \\ x_i(t) \in X_i, u_i(t) \in U_i, t \in \mathbb{N}, \end{cases} \tag{2.10}$$

with $i = 1, 2$, $x_i(t)$ is the state and $u_i(t)$ is the input at step $t \in \mathbb{N}$, and $y'_{3-i}(t)$ is the output of the agent P_{3-i} as received by agent P_i through the network, denoted by Net. $X_i, X_{i,0} \subset X_i$, Y_i and U_i are the finite sets of states, initial states, outputs and inputs, respectively. Map $F_i : X_i \times Y_{3-i} \times U_i \to 2^{X_i}$ is the state transition (possibly partial) map, and we use the symbol $F_i(x_i(t), y'_{3-i}(t), u_i(t))!$ to show that the map is defined for the given $x_i(t), y'_{3-i}(t)$ and $u_i(t)$ and $h_i : X_i \to Y_i$ is the output function. Net represents the communication network and is defined as follows:

$$Net : Y_i \times Y_A \to (Y_i \cup Y_A) \tag{2.11}$$

where $Net(y_i, y_A) = y_i$, if no attack occurs, and $Net(y_i, y_A) = y_A$, otherwise.

Next, we adopt the notion of state run as a finite sequence of states $x_i(0)x_i(1)....$ satisfying (2.10) for some finite sequence of inputs $y'_{3-i}(0)y'_{3-i}(1)...$ and $u_i(0)u_i(1)...$.

Next, we can extend the definition of *succ* and *pre* for the above set of equations as:

For a state $x \in X$:

$$succ(x) = \{x' \in X : x' \in F(x, u)\},$$
$$pre(x) = \{x' \in X : x \in F(x', u)\}.$$

Similarly, for $X' \subset X$:

$$succ(X') = \{x \in X : x \in F(x', u) \wedge x' \in X'\},$$
$$pre(X') = \{x \in X : x' \in F(x, u) \wedge x' \in X'\}.$$

Remark 2.4.1

The adoption of these two FSM modeling approaches allows the framework to adapt to the scale and complexity of the system under observation. The tuple–based model is more intuitive and directly traceable for individual agents, whereas the equation–based model provides mathematical tractability for larger, interconnected systems. Detailed implementations and applications of these models are presented in Chapter 4, where their role in attack detection and localization is fully explored. □

2.5 Petri Nets

While FSMs provide a useful framework for modeling DES, they are often limited in representing concurrent or resource–shared behaviors. To overcome these limitations, we employ PNs, which offer a more expressive modeling paradigm capable of capturing parallelism, synchronization, and causality within complex systems.

In the context of this thesis, PN serve as the foundational modeling tool for fault detection under partial observability. Specifically, we utilize a POPN structure to represent the system dynamics, where only a subset of places and transitions are observable. This facilitates monitoring and diagnosis in settings with limited sensor information.

We adopt the notion and definition of POPN from [112] as:

$$N = (P, T, Pre, Post, P_0, T_0) \tag{2.12}$$

where:

- $P = \{P_i\}, i = 1, ..., n$ is a set of n places;
- $T = \{t_j\}, j = 1, .., m$ is a set of m transitions;
- $Pre : P \times T \to N$, and $Post : P \times T \to N$ are the Pre and $Post$ incidence functions that specify the arcs;
- $P_0 \subset P$ is the set of observable places with cardinality n_1 satisfying $0 \leq n_1 \leq n$;
- $T_0 \subset T$ is the set of observable transitions with cardinality m_1 satisfying $0 \leq m_1 \leq m$.

A marking (i.e., net state) is a vector $M : P \to \mathbb{N}$ that assigns to each place of a PN or POPN a non negative integer number of tokens. We denote by $M(p)$ the marking of place p (i.e. the number of tokens in place p). We identify a set of transitions by a vector $\sigma \in \{0, 1\}^m$. A transition $t \in T$ is said enabled at marking M if $M \geq Pre(p, t)$. The enabled transition $t \in T$ can be fired reaching a new marking M_{k+1} that can be computed by [113] and [105]:

$$M_{k+1} = M_k + W\sigma_{k+1} \tag{2.13}$$

where,

- $M_k \in \mathbb{N}^n$ is the marking vector of places,
- $\sigma_k \in \mathbb{N}^m$ is the firing vector of transitions at time instant k (i.e., a vector whose $j - th$ entry denotes the number of times the transition t_j has fired), and
- W is the incidence matrix of the net, it is defined as $W(i, j) = Post(t_j, p_i) - Pre(p_i, t_j)$ if $Post(t_j, p_i)$ or $Pre(p_i, t_j)$ is not defined for a specific place p_i and transition t_j, it taken to be 0.

This section introduces the basic modeling framework of POPN, which provides the foundation for the fault detection and isolation approach developed in this thesis. The POPN formalism enables effective representation of systems with limited observability, while preserving the dynamic behavior. Further details regarding the observer design, residual generation, and fault analysis based on this model are discussed in Chapter 5.

Chapter 3

Control and coordination

The main focus of this chapter is the control and coordination of MAS, with particular attention given to practical constraints that are often encountered in real–world applications. These include the use of digitized controllers, state–delays, measurement noise, communication errors, and other uncertainties that can significantly affect the performance and reliability of the system. Under these practical constraints, ensuring that agents can work together effectively requires careful design and robust control strategies.

To address these challenges, we present the design of robust *Quantized Sampled-data Event-triggered* (QSE) controllers, which aim to achieve consensus tracking for nonlinear MAS affected by state–delays. The proposed approach leverages the concept of *Steepest Descent Consensus Feedback* (SDCF) along with the ISS redesign methodology. This combination allows the design of a QSE control term that can effectively reduce the impact of bounded actuation disturbances and suitably bounded measurement errors. In other words, even when the system is exposed to practical imperfections, the controller ensures that the agents remain coordinated and stable.

Furthermore, it is proved that there exist a sufficiently fast sampling rate and accurate quantization of the input and output channels, such that the digital implementation of robustified SDCFs (continuous or not) guarantees consensus tracking in a semiglobal practical sense. The design also handles possible discontinuities in the functions describing the control protocol, ensuring smooth operation despite irregularities. The cases of time–varying sampling intervals and of non–uniform quantization in the input/output channels are included in the theory here developed.

To illustrate the practical applicability of the proposed methodology, it is applied to a specific class of nonlinear time–delay MAS. As a numerical example, we consider the coordination control problem of a network of UAVs. This example shows how the proposed controller can keep multiple agents working together in a coordinated way, while handling actuation disturbances, and measurement errors that commonly occur in real–world situations.

Overall, the methods presented in this chapter provide a practical and robust framework for achieving effective control and coordination in complex MAS, connecting the theoretical design with real–world applications. This part of the thesis is currently being prepared for submission in [114].

3.1 Problem formulation

Let us recall the nonlinear time–delay MAS described in (2.2)

$$\begin{aligned} \dot{x}_i(t) &= f_i(x_{t,i}, \chi_{t,i}) + g_i(x_{t,i}, \chi_{t,i})(u_i(t) + d_i(t)), \\ x_i(\tau) &= x_i^0(\tau), \quad \tau \in [-\Delta, 0], \quad i = 1, \cdots, N. \end{aligned} \tag{3.1}$$

Next we formally introduce the consensus tracking problem addressed in this work.

Problem 3.1.1

For given positive reals $\bar{\gamma}_\psi$, $\bar{\gamma}_{d\psi}$, $\bar{\gamma}_{d^2\psi}$, *for a given continuously differentiable desired reference signal for coordination* $\psi_t = \begin{pmatrix} \psi_{t,1} \\ \vdots \\ \psi_{t,N} \end{pmatrix} \in \mathcal{C}^{nN}$, $\psi_{t,i} \in \mathcal{C}^n$, $i = 1, \cdots, N$, $t \in \mathbb{R}^+$, *satisfying*

$$\begin{aligned}&\|\psi_t\|_\infty \leq \bar{\gamma}_\psi,\ \forall t \in \mathbb{R}^+,\ \operatorname*{ess\,sup}_{\theta\in[-\Delta,0]}\left|\tfrac{d\psi_t(\theta)}{d\theta}\right| \leq \bar{\gamma}_{d\psi},\ \forall t \in \mathbb{R}^+,\\ &\operatorname*{ess\,sup}_{\theta\in[-\Delta,0]}\left|\tfrac{d^2\psi_t(\theta)}{d\theta^2}\right| \leq \bar{\gamma}_{d^2\psi},\ \forall t \in \mathbb{R}^+,\end{aligned} \tag{3.2}$$

the consensus control problem addressed in this paper consists of designing a robust QSE static state feedback controller for the MAS (3.1) *(see* u_i, $i = 1, \cdots, N$, *in* (3.1)*) such that the conditions*

$$\begin{aligned}&\lim_{t\to\infty} |x_1(t) - \psi_1(t)| = 0,\\ &\lim_{t\to\infty} |x_i(t) - x_{i+1}(t) - \psi_i(t)| = 0, \quad i = 1, \cdots, N-1,\end{aligned} \tag{3.3}$$

hold in a semi–global practical sense taking also into account the presence of possible unknown errors affecting the available digital state measurements. In practice, due to quantization, event–triggering, and measurement errors, the convergence in (3.3) *is interpreted in a semi–global practical sense, meaning that the errors are ultimately bounded within a small neighborhood of origin.*

Furthermore, two convergence expressions in (3.3) *reflect the leader–follower coordination structure considered in this work, where the leader agent* ($i = 1$) *tracks the desired reference trajectory, while each follower agent* ($i > 1$) *maintains a prescribed relative offset with respect to its preceding agent.* □

In the following section, the above will be solved in a semi–global practical sense. In particular, Problem 1 will be recast in a suitable robust digital stabilization problem for which a semi-global practical solution will be provided.

3.2 Design Methodology

In order to investigate Problem 3.1.1, taking into account (3.1) and (3.3), let us consider the new state variable

$$\begin{aligned}z_t(\tau) &= \begin{pmatrix} z_{t,1}(\tau) \\ z_{t,2}(\tau) \\ \vdots \\ z_{t,N}(\tau) \end{pmatrix} = \begin{pmatrix} x_{t,1}(\tau) - \psi_{t,1}(\tau) \\ x_{t,1}(\tau) - x_{t,2}(\tau) - \psi_{t,2}(\tau) \\ \vdots \\ x_{t,N-1}(\tau) - x_{t,N}(\tau) - \psi_{t,N}(\tau) \end{pmatrix}\\ &\tau \in [-\Delta, 0].\end{aligned} \tag{3.4}$$

In this formulation, the introduction of the transformed state variable $z_t(\tau)$ explicitly includes the reference signal $\psi_{t,i}(\tau)$ as part of converting the original consensus tracking problem into an equivalent convergence problem in these new coordinates. This transformation inherently involves the reference trajectory because the goal is to regulate the error between agent states and the reference or between agents themselves. Importantly, the presence of the reference signal in the formulation does not dictate a centralized control architecture. Depending on the communication and information sharing structure, the controller can be implemented in a centralized manner where a leader or central coordinator computes control inputs using global information or in a decentralized fashion where agents exchange necessary information such as local states and reference signals to compute their own controls. This assumption of reference availability is common in leader–follower and cooperative control frameworks, where the reference can be broadcast or locally generated through distributed consensus mechanisms.

Taking into account (3.4), from (3.1), we obtain the following dynamical system

$$\begin{aligned}&\dot{z}(t) = F(z_t, r_t) + G(z_t, r_t)\big(u(t) + d(t)\big),\\ &z(\tau) = z^0(\tau) = \begin{pmatrix} x_1^0(\tau) - \psi_1^0(\tau) \\ x_1^0(\tau) - x_2^0(\tau) - \psi_2^0(\tau) \\ \vdots \\ x_{N-1}^0(\tau) - x_N^0(\tau) - \psi_N^0(\tau) \end{pmatrix}, \quad \tau \in [-\Delta, 0].\end{aligned} \tag{3.5}$$

where, by calling with $\tilde{n} = nN$, $\tilde{p} = (2n+p)N$ and $\tilde{m} = mN$,

$$\begin{aligned} u(t) &= \begin{pmatrix} u_1(t)^T & \cdots & u_N(t)^T \end{pmatrix}^T \in \mathbb{R}^{\tilde{m}}, \\ d(t) &= \begin{pmatrix} d_1(t)^T & \cdots & d_N(t)^T \end{pmatrix}^T \in \mathbb{R}^{\tilde{m}}, \\ r_t(\tau) &= \begin{pmatrix} \psi_t(\tau)^T & \left[\frac{d\psi_t(\tau)}{d\tau}\right]^T & \chi_t(\tau)^T \end{pmatrix}^T \in \mathbb{R}^{\tilde{p}}, \quad \tau \in [-\Delta, 0], \\ \chi_t(\tau) &= \begin{pmatrix} \chi_{t,1}(\tau)^T & \cdots & \chi_{t,N}(\tau)^T \end{pmatrix}^T \in \mathbb{R}^{pN}, \quad \tau \in [-\Delta, 0], \end{aligned} \tag{3.6}$$

$F : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n}}$ and $G : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n} \times \tilde{m}}$ are the functions defined for any

$$\phi_z = \begin{pmatrix} \phi_{z_1} \\ \vdots \\ \phi_{z_N} \end{pmatrix} \in \mathcal{C}^{\tilde{n}}, \quad \phi_{z_i} \in \mathcal{C}^n, \ i = 1, \ldots, N,$$

and for any

$$\phi_r = \begin{pmatrix} \phi_\psi \\ \phi_{d\psi} \\ \phi_\chi \end{pmatrix} \in \mathcal{C}^{\tilde{p}}, \quad \phi_\psi = \begin{pmatrix} \phi_{\psi_1} \\ \vdots \\ \phi_{\psi_N} \end{pmatrix}, \ \phi_{d\psi} = \begin{pmatrix} \phi_{d\psi_1} \\ \vdots \\ \phi_{d\psi_N} \end{pmatrix}, \ \phi_\chi = \begin{pmatrix} \phi_{\chi_1} \\ \vdots \\ \phi_{\chi_N} \end{pmatrix},$$

where ϕ_{ψ_i}, $\phi_{d\psi_i} \in \mathcal{C}^n$ and $\phi_{\chi_i} \in \mathcal{C}^p$, $i = 1, \ldots, N$, as follows.

$$\begin{aligned} F(\phi_z, \phi_r) &= \begin{pmatrix} \tilde{f}_1^T & \cdots & \tilde{f}_N^T \end{pmatrix}^T, \\ G(\phi_z, \phi_r) &= \begin{pmatrix} \tilde{g}_1 & 0_{n,m} & 0_{n,m} & \cdots & 0_{n,m} & 0_{n,m} \\ \tilde{g}_1 & -\tilde{g}_2 & 0_{n,m} & \cdots & 0_{n,m} & 0_{n,m} \\ 0_{n,m} & \tilde{g}_2 & -\tilde{g}_3 & \cdots & 0_{n,m} & 0_{n,m} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0_{n,m} & 0_{n,m} & 0_{n,m} & \ddots & -\tilde{g}_{N-1} & 0_{n,m} \\ 0_{n,m} & 0_{n,m} & 0_{n,m} & \cdots & \tilde{g}_{N-1} & -\tilde{g}_N \end{pmatrix} \end{aligned} \tag{3.7}$$

$$\begin{aligned} \tilde{f}_1 &= f_1(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}) - \phi_{d\psi_1}(0), \\ \tilde{f}_2 &= f_1(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}) - f_2(\varsigma_2, \phi_{\chi_2}) - \phi_{d\psi_2}(0), \\ \tilde{f}_i &= f_{i-1}(\varsigma_{i-1}, \phi_{\chi_{i-1}}) - f_i(\varsigma_i, \phi_{\chi_i}) - \phi_{d\psi_i}(0), \quad i = 3, \ldots, N, \\ \tilde{g}_1 &= g_1(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}), \quad \tilde{g}_i = g_i(\varsigma_i, \phi_{\chi_i}), \\ \varsigma_i &= \phi_{z_1} + \phi_{\psi_1} - \sum_{j=2}^{i} (\phi_{z_j} + \phi_{\psi_j}), \quad i = 2, \ldots, N. \end{aligned} \tag{3.8}$$

Notice that, from (2.3), (3.2), it follows that there exist positive reals $\bar{\gamma}_r$ and $\bar{\gamma}_{dr}$ satisfying

$$\begin{aligned} \|r_{t,i}\|_\infty &\leq \bar{\gamma}_r, \quad \forall\, t \in \mathbb{R}^+, \\ \operatorname*{ess\,sup}_{\theta \in [-\Delta, 0]} \left| \frac{dr_t(\theta)}{d\theta} \right| &\leq \bar{\gamma}_{dr}, \quad \forall\, t \in \mathbb{R}^+. \end{aligned} \tag{3.9}$$

In the following, the proposed procedure for the design of robust QSE stabilizers for nonlinear time–delay MASs is presented. In particular, the proposed design methodology is based on the Artstein's approach [23] where candidate Lyapunov/Lyapunov–Krasovskii functions/functionals (see, for instance, [23], [26], [27], [22], [24], [29], [25]) are used for the design of stabilizers. According to such a procedure, as a first step, we introduce the considered set of candidate Lyapunov–Krasovskii functionals. To such an aim, the notion of smoothly separable functionals [29] and of invariantly differentiable functionals are recalled [115],[116].

Definition 3.2.1

A functional $V\colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ is said to be smoothly separable *if there exist:*

- *a function $V_1 \in C^1_L\big(\mathbb{R}^{\tilde{n}}; \mathbb{R}^+\big)$,*
- *a locally Lipschitz functional $V_2\colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$, and*
- *functions β_1, β_2 of class $\mathcal{K}_\infty$,*

such that, for any $\phi \in \mathcal{C}^{\tilde{n}}$, the following equality and inequalities hold:

$$V(\phi) = V_1(\phi(0)) + V_2(\phi),$$
$$\beta_1\big(|\phi(0)|\big) \leq V_1(\phi(0)) \leq \beta_2\big(|\phi(0)|\big).$$

□

As in [116], the formalism used in the classical definition of invariantly differentiable functional [115], is here suitably modified for the purpose of formalism uniformity over this work. For any given $z \in \mathbb{R}^{\tilde{n}}$, $\phi \in \mathcal{Q}^{\tilde{n}}$ and for any given continuous function $\mathcal{Y}\colon [0, \Delta] \to \mathbb{R}^{\tilde{n}}$ with $\mathcal{Y}(0) = z$, let $\psi_h^{(z,\phi,\mathcal{Y})} \in \mathcal{Q}^{\tilde{n}}$, $h \in [0, \Delta)$, be defined as $\psi_0^{(z,\phi,\mathcal{Y})} = \phi$, and, for $h > 0$,

$$\psi_h^{(z,\phi,\mathcal{Y})}(s) = \begin{cases} \phi(s+h), & s \in [-\Delta, -h) \\ \mathcal{Y}(s+h), & s \in [-h, 0). \end{cases} \tag{3.10}$$

Definition 3.2.2 ([115], [116])

A functional $V\colon \mathbb{R}^{\tilde{n}} \times \mathcal{Q}^{\tilde{n}} \to \mathbb{R}^+$ is said to be invariantly differentiable if, at any point $(z, \phi) \in \mathbb{R}^{\tilde{n}} \times \mathcal{Q}^{\tilde{n}}$:

- *For any continuous function $\mathcal{Y}\colon [0, \Delta] \to \mathbb{R}^{\tilde{n}}$ with $\mathcal{Y}(0) = z$, there exists the right–hand derivative*
$$\frac{\partial V\big(z, \psi_h^{(z,\phi,\mathcal{Y})}\big)}{\partial h}\Big|_{h=0},$$
and such derivative is invariant with respect to the function $\mathcal{Y}$;
- *There exists the derivative $\frac{\partial V(z,\phi)}{\partial z}$;*
- *For any continuous function $\mathcal{Y}\colon [0, \Delta] \to \mathbb{R}^{\tilde{n}}$ with $\mathcal{Y}(0) = z$, the following equality holds for any $\rho \in \mathbb{R}^{\tilde{n}}$ and $h \in [0, \Delta)$:*

$$V(z+\rho, \psi_h^{(z,\phi,\mathcal{Y})}) - V(z,\phi) = \frac{\partial V(z,\phi)}{\partial z}\rho + \frac{\partial V(z, \psi_l^{(z,\phi,\mathcal{Y})})}{\partial l}\Big|_{l=0} h + o\Big(\sqrt{|\rho|^2 + h^2}\Big), \tag{3.11}$$

with $\lim\limits_{s \to 0^+} \frac{o(\sqrt{s})}{\sqrt{s}} = 0$.

□

We denote here with $\mathcal{V}$ the set of Lyapunov–Krasovskii functionals $V\colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ with the following properties

P_1) there exist a locally Lipschitz function $V_1\colon \mathbb{R}^{\tilde{n}} \to \mathbb{R}^+$, a locally Lipschitz functional $V_2\colon \mathcal{Q}^{\tilde{n}} \to \mathbb{R}^+$ such that the functional $V\colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ defined, for $\phi \in \mathcal{C}^{\tilde{n}}$, as $V(\phi_z) = V_1(\phi_z(0)) + \widetilde{V}_2(\phi_z)$, where $\widetilde{V}_2\colon \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ is defined for $\phi \in \mathcal{C}^{\tilde{n}}$ as $\widetilde{V}_2(\phi_z) = V_2\left(\phi_{z_{[-\Delta,0)}}\right)$, is smoothly separable, with related functions β_1, β_2 according to Definition 3.2.1;

P_2) the function $(\phi_z, \phi_r, u) \to D^+\widetilde{V}_2(\phi_z, \phi_r, u)$, $\phi_z \in \mathcal{C}^{\tilde{n}}$, $\phi_r \in \mathcal{C}^{\tilde{p}}$ and $u \in \mathbb{R}^{\tilde{m}}$, is Lipschitz on bounded subsets of $\mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \times \mathbb{R}^{\tilde{m}}$;

P_3) the functional $\widehat{V}\colon \mathbb{R}^{\tilde{n}} \times \mathcal{Q}^{\tilde{n}} \to \mathbb{R}^+$ defined, for $z \in \mathbb{R}^{\tilde{n}}$, $\phi_z \in \mathcal{Q}^{\tilde{n}}$, as $\widehat{V}(z, \phi_z) = V_1(z) + V_2(\phi_z)$, is invariantly differentiable (see Definition 3.2.2);

P_4) there exist functions γ_1, γ_2 of class $\mathcal{K}_\infty$ such that for any $\phi_z \in \mathcal{C}^{\tilde{n}}$, the following inequalities hold

$$\gamma_1(|\phi_z(0)|) \leq V(\phi_z) \leq \gamma_2(\|\phi_z\|_\infty). \tag{3.12}$$

Remark 3.2.1

Notice that, the items P_1)-P_4) are satisfied by a very large class of Lyapunov-Krasovskii functionals, including standard complete quadratic ones (see, for instance, [116], [117], [118], [119], [120]). For instance, the following standard functional

$$V(\phi) = \phi^T(0)P\phi(0) + \int_{-\Delta}^{0} \phi^T(\tau)Q\phi(\tau)d\tau, \ \phi \in \mathcal{C}^n, \tag{3.13}$$

fulfills items P_1)-P_4) with functions $\beta_1(s) = \gamma_1(s) = \lambda_{\min}(P)s^2$, $\beta_2(s) = \lambda_{\max}(P)s^2$, $\gamma_2(s) = (\lambda_{\max}(P) + \Delta\lambda_{\max}(Q))s^2$. The invariant differentiability property, as here connected with the smooth separability one (see items P_1) and P_3)), has been proved to be very helpful in order to apply ISS redesign methodologies for the robustification of stabilizers for control-affine nonlinear time-delay systems (see [28] and the references therein). We highlight also that, in the forthcoming Section 5, it is shown how a standard functional of the form (3.13) can be easily used to apply the control design methodology proposed in this paper. □

In the following, the well–known notion of *Steepest Descent Feedback* (SDF) (see, [26], [27] for the delay–free case and [28], [30] for the delayed case) is revised in order to deal with the design of robust QSE controllers for nonlinear time–delay MASs taking simultaneously into account: (a) the presence of sampling and quantization in both input/output channels; (b) the presence of actuation disturbances and measurement errors; (c) event–triggered strategies for the updates of the control input signals; (d) the presence of known exogenous disturbances characterizing, for instance, tracking control problems. In particular, in the following the notion of *Steepest Descent Consensus Feedback* (SDCF) is introduced.

Definition 3.2.3

Let $V \in \mathcal{V}$. A locally bounded function $k : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{m}}$, continuous or not, is said to be a SDCF for the system described by (3.5) with $d(t) = 0$, induced by V, if there exist positive reals η, μ, $\bar{p}$, a function p in $C^1_L(\mathbb{R}^+;\mathbb{R}^+)$, of class $\mathcal{K}_\infty$ and satisfying $\frac{dp(s)}{ds} \leq \bar{p}$, a function $\overline{\alpha}$ of class $\mathbb{P}_0$ such that $I_d - \overline{\alpha}$ is of class $\mathcal{K}_\infty$, a real $\nu \in \{0, 1\}$, such that, for any $\phi_z \in \mathcal{C}^{\tilde{n}}$, $\phi_r \in \mathcal{C}^{\tilde{p}}$ the following conditions hold

$$\begin{aligned} &\nu D^+V(\phi_z, \phi_r, k(\phi_z, \phi_r)) + \\ &\eta \max\left\{0, D^+p \circ V_1\Big(\phi_z, \phi_r, k(\phi_z, \phi_r)\Big) + \mu p \circ V_1\big(\phi_z(0)\big)\right\} \leq \\ &\qquad\qquad \overline{\alpha}(\eta\mu e^{-\mu\Delta} p \circ \beta_1(\|\phi_z\|_\infty)), \end{aligned} \tag{3.14}$$

$$F(0, \phi_r) + G(0, \phi_r)k(0, \phi_r) = 0, \tag{3.15}$$

where: β_1 is the function of class $\mathcal{K}_\infty$ in Definition 3.2.1; where the derivatives in (2.1) is computed with $u = k(\phi_z, \phi_r)$. □

Assumption 3.2.1

There exist a functional $V \in \mathcal{V}$ and a related SDCF k for the system described by (3.5) (see Definition 3.2.3). □

Before the presentation of the proposed robust QSE control strategy, by considering the simple example provided in Section 1, we show how to practically design SDCFs.

In the following, the proposed robust QSE implementation of SDCF for nonlinear time-delay MASs is presented. Firstly, for the presentation of the proposed digital event–based controller, the notions of quantizer (see, for instance, [121]), of partition (see [26], [27], [29]) and of spline approximation (see [30]) are recalled. Such notions will be used for the characterization of the digital framework under study.

Definition 3.2.4

For a given positive integer c, a quantizer is a piece–wise constant function $q_y : \mathbb{R}^c \to Q_y^c$, with Q_y^c a suitable finite subset of $\mathbb{R}^\nu$, characterized, for some given positive real E (range of the quantizer) and μ_y (error bound of the quantizer), by the following implication holds (see, for instance, [121]):

$$|y| \leq E \quad \to \quad |q_y(y) - y| \leq \mu_y, \ y \in \mathbb{R}^c. \tag{3.16}$$

□

Definition 3.2.5

For a positive integer l, a partition $\pi = \{t_j, \ j = -l, -l+1, \ldots\}$ of $[-l\Delta, \infty)$ is a countable, strictly increasing sequence $t_j \in [-l\Delta, \infty)$, with $t_0 = 0$, such that $t_j \to \infty$ as $j \to \infty$. The diameter of π, denoted $\mathrm{diam}(\pi)$, is defined as $\sup_{j \geq -l} t_{j+1} - t_j$. The dwell time of π, denoted $\mathrm{dwell}(\pi)$, is defined as $\inf_{j \geq -l} t_{j+1} - t_j$. For a given $a \in (0, 1]$, $\delta > 0$, $\pi_{a,\delta}$ is any partition π with $a\delta \leq \mathrm{dwell}(\pi) \leq \mathrm{diam}(\pi) \leq \delta$. □

Remark 3.2.2

Notice that, Definition 3.2.5 aims at characterizing the sampled-data framework here considered by partitioning the time axis into sampling intervals $[t_j, t_{j+1})$, $j = -l, -l+1, \ldots$. We highlight that, in Definition 3.2.5, the positive real $a \in (0, 1]$ is introduced in order to consider the case of non-uniform sampling in which, for $j = -l, -l+1, \ldots$, $a\delta \leq t_{j+1} - t_j \leq \delta$, with δ representing the upper bound for the sampling period. □

For given $\delta < \Delta$ ($\Delta > 0$), $a \in (0, 1]$, let l be the smallest positive integer such that $la\delta \geq \Delta$. Let $\mathcal{T}_{l,a,\delta} \subset \mathbb{R}^{l+1}$ be the set defined as follows (see [30])

$$\begin{aligned} \mathcal{T}_{l,a,\delta} = \Big\{ & w = (w_0, \ldots, w_l) \in \mathbb{R}^{l+1}, \quad w_k \in [-l\delta, 0], \quad k = 0, 1, \ldots, l, \\ & w_0 = 0, \quad w_0 - w_l \geq \Delta, \quad \delta \geq w_k - w_{k+1} \geq a\delta, \quad k = 0, 1, \ldots, l-1 \Big\}. \end{aligned} \tag{3.17}$$

For a positive integer λ, let $P_{l,a,\delta}^{\lambda} : \mathbb{R}^{\lambda(l+1)} \times \mathcal{T}_{l,a,\delta} \to \mathcal{C}^{\lambda}$ be the function defined (see [30]), for

$$z = (z_0^T, \ldots, z_l^T)^T \in \mathbb{R}^{\lambda(l+1)}, \quad z_j \in \mathbb{R}^{\lambda}, \ j = 0, 1, \ldots, l,$$
$$w = (w_0, \ldots, w_l) \in \mathcal{T}_{l,a,\delta}, \quad \tau \in [-\Delta, 0],$$

as follows.

$$(P_{l,a,\delta}^{\lambda}(z, w))(\tau) = z_{k+1} + \frac{\tau - w_{k+1}}{w_k - w_{k+1}}(z_k - z_{k+1}), \tag{3.18}$$

where k is the smallest integer in $\{0, 1, \ldots, l-1\}$ such that $w_k \geq \tau \geq w_{k+1}$.

Remark 3.2.3

Notice that, the spline approximation methodology is here used in order to cope with problems very commons in the context of systems with state delays and mainly related to the possible non–availability in the buffer of past values of the system state required for the correct implementation of a proposed control strategy (see, for

instance, [30]). □

In the forthcoming points (i) and (ii), the actuation disturbances (see (3.1), (3.5)) and the measurement errors under investigation (see Problem 1) are described. In particular, for a given partition $\pi_{a,\delta}$ (see Definition 3.2.5), [22], [28]

(i) the actuation disturbances $d(t)$ in (3.5) (see also (3.1)):

  (i.a) are assumed to be continuous in any interval $[t_j, t_{j+1})$ with possible discontinuities in the sampling instants t_j, $j \in \mathbb{N}$;

  (i.b) satisfies $|d(t)| \leq \bar{d}$, $\forall t \in \mathbb{R}^+$, with $\bar{d}$ a known positive real;

  (i.c) are such that there exists finite $\lim_{t \to t_{j+1}^-} d(t)$, $j = 0, 1, \cdots$.

(ii) the measurement errors affecting the quantized sampled–data output channel are characterized by an unknown sequence $e : \mathbb{N} \to C^{\tilde{n}}$, satisfying $\|e_j\|_\infty \leq \bar{e}$, $j = 0, 1, \cdots$, with $\bar{e}$ a known positive real.

In order to cope with the presence of *unknown* actuation disturbances and *unknown* measurement errors (see point (i) and (ii)), in the following, an ISS redesign methodology (see, for instance, [28], [116], [122], [123], [124], [125]) is used. In particular, a new control term is designed and added to the SDCF at hand in order to arbitrarily attenuate the effects of the uncertainties considered in points (i) and (ii). To such an aim, under Assumption 3.2.1, let:

– $S : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{m}}$ be the function defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$ and $\phi_r \in \mathcal{C}^{\tilde{p}}$, as follows

$$S(\phi_z, \phi_r) = \left(\frac{\partial V_1(x)}{\partial x}\Big|_{x=\phi_z(0)} g(\phi_z, \phi_r) \right)^T, \tag{3.19}$$

  where V_1 is the function related to the SDF at hand (see Definition 3.2.3);

– $\tilde{k} : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{m}}$ be the function defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$ and $\phi_r \in \mathcal{C}^{\tilde{p}}$, as follows

$$\tilde{k}(\phi_z, \phi_r) = k(\phi_z, \phi_r) - \omega S(\phi_z, \phi_r), \tag{3.20}$$

  where: $\omega > 0$ is a control tuning parameter to be chosen (see forthcoming Theorem 3.3.1); k is the SDF in Assumption 3.2.1 (see also Definition 3.2.3).

In the following, some useful functionals are introduced for the presentation of the event–based mechanism which will be exploited for the update of the controller at hand. In particular, under Assumption 3.2.1 and taking into account the positive reals η, μ, ν and the functions p and V related to Definition 3.2.3, let:

(f.1) $V_3 : \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ be the functional defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$, as

$$V_3(\phi_z) = \sup_{\theta \in [-\Delta, 0]} e^{\mu\theta} p \circ V_1(\phi_z(\theta));$$

(f.2) $V_\infty : \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ be the functional defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$, as

$$V_\infty(\phi_z) = \nu V(\phi_z) + \eta V_3(\phi_z);$$

(f.3) $\mathcal{D}_\infty : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \times \mathbb{R}^{\tilde{m}} \to \mathbb{R}$ be the functional defined, for $\phi_z \in \mathcal{C}^{\tilde{n}}$, $\phi_r \in \mathcal{C}^{\tilde{p}}$, $u \in R^{\tilde{m}}$, as follows

$$\begin{aligned} \mathcal{D}_\infty(\phi_z, \phi_r, u) = {} & \nu D^+ V(\phi_z, \phi_r, u) - \eta\mu V_3(\phi_z) \\ & + \eta \max\Big\{0, D^+ p\big(V_1(\phi_z, \phi_r, u)\big) + \mu\, p\big(V_1(\phi_z(0))\big)\Big\}. \end{aligned} \tag{3.21}$$

In the following, the proposed QSE controller is provided.
Under Assumption 3.2.1, for given positive reals $\sigma \in (0,1)$, $\bar{\mu}$, $\tilde{\mu} \in (0,1]$, δ, E, U, ω, $L_{\mathcal{D}}$, E_1, μ_z, μ_r and μ_u, the proposed robust QSE controller for the system (3.5) when affected by measurement errors (see point (ii) above) is described by

$$\begin{aligned} u(t) = q_u(\tilde{u}_{i_j}) = q_u\Big(\tilde{k}(\mathbb{P}_{i_j}^{q_z}, \mathbb{P}_{i_j}^{q_r})\Big), \\ t \in [t_j, t_{j+1}), \quad j = 0, 1, \ldots, \quad t_j, t_{j+1} \in \pi_{a,\delta}. \end{aligned} \tag{3.22}$$

where:

- $\tilde{k}$ is the function in (3.20);
- $\pi_{a,\delta} = \{t_j,\ j = -l, -l+1, \ldots\}$ is any partition (see Definition 3.2.5) with l the smallest (nonnegative) integer such that $la\delta \geq \Delta$,$\{t_{-l}, t_{-l+1}, \ldots, 0\} \in \mathcal{T}_{l,a,\delta}$;
- the functions $q_z : \mathbb{R}^{\tilde{n}} \to Q_z^{\tilde{n}}$, $q_r : \mathbb{R}^{\tilde{p}} \to Q_r^{\tilde{p}}$ and $q_u : \mathbb{R}^{\tilde{m}} \to Q_u^{\tilde{m}}$ are quantizers with error bounds μ_z, μ_r, μ_u and ranges E_1, $\bar{\gamma}_r$, U, respectively (see (3.16));
- $\mathbb{P}_j^{q_z} = P_{l,a,\delta}^{\tilde{n}}(B_S^{q_z}(j), B_{\mathcal{T}}(j))$, $j = 0, 1, \cdots$, and $P_{l,a,\delta}^{\tilde{n}}$ is the function defined in (3.18) with $\lambda = \tilde{n}$;
- $\mathbb{P}_j^{q_r} = P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^{q_r}(j), B_{\mathcal{T}}(j))$, $j = 0, 1, \cdots$, and $P_{l,a,\delta}^{\tilde{p}}$ is the function defined in (3.18) with $\lambda = \tilde{p}$;
- $B_S^{q_z} : \mathbb{N} \to \mathbb{R}^{\tilde{n}(l+1)}$, $\bar{B}_S^{q_r} : \mathbb{N} \to \mathbb{R}^{\tilde{p}(l+1)}$ and $B_{\mathcal{T}} : \mathbb{N} \to \mathbb{R}^{l+1}$ are defined (recursively) as

$$\begin{aligned} B_S^{q_z}(0) &= \begin{pmatrix} q_z(\bar{z}^0(0) + \bar{e}_0(0)) \\ \vdots \\ q_z(\bar{z}^0(t_{-l}) + \bar{e}_0(t_{-l})) \end{pmatrix}, \\ \bar{B}_S^{q_r}(0) &= \begin{pmatrix} q_r(\bar{r}_0(0)) \\ \vdots \\ q_r(\bar{r}_0(t_{-l})) \end{pmatrix}, \\ \bar{z}^0(\tau) + \bar{e}_0(\tau) &= \begin{cases} z^0(\tau) + e_0(\tau), & \tau \in [-\Delta, 0], \\ z^0(-\Delta) + e_0(-\Delta), & \tau \in [t_{-l}, -\Delta], \end{cases} \\ \bar{r}_0(\tau) &= \begin{cases} r_0(\tau), & \tau \in [-\Delta, 0], \\ r_0(-\Delta), & \tau \in [t_{-l}, -\Delta], \end{cases} \\ B_S^{q_z}(j) &= \begin{pmatrix} q_z(z(t_j) + e_j(0)) \\ 0_{l\tilde{n}\times 1} \end{pmatrix} + \begin{pmatrix} 0_{\tilde{n}\times l\tilde{n}} & 0_{\tilde{n}\times 1} \\ I_{l\tilde{n}} & 0 \end{pmatrix} B_S^{q_z}(j-1), \\ \bar{B}_S^{q_r}(j) &= \begin{pmatrix} q_r(r(t_j)) \\ 0_{l\tilde{p}\times 1} \end{pmatrix} + \begin{pmatrix} 0_{\tilde{p}\times l\tilde{p}} & 0_{\tilde{p}\times 1} \\ I_{l\tilde{p}} & 0 \end{pmatrix} \bar{B}_S^{q_r}(j-1), \\ B_{\mathcal{T}}(0) &= \begin{pmatrix} 0 & t_{-1} & \vdots & t_{-l} \end{pmatrix}^T, \\ B_{\mathcal{T}}(j) &= \begin{pmatrix} 0_{1\times l} & 0 \\ I_l & 0 \end{pmatrix} \Big(B_{\mathcal{T}}(j-1) - (t_j - t_{j-1}) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \Big), \\ & j = 1, 2, \ldots \end{aligned} \tag{3.23}$$

- the sequence $e : \mathbb{N} \to \mathcal{C}^{\tilde{n}}$ characterizes any kind of *unknown* measurement errors as in point (ii) and satisfying

$$\sup_{\substack{\tilde{z}\in\mathcal{B}^{\tilde{n}(l+1)}_{E\sqrt{l+1}}\\ \tilde{r}\in\mathcal{B}^{\tilde{n}(l+1)}_{\bar{\gamma}_r\sqrt{l+1}}}} \Big|S\Big(P^{\tilde{n}}_{l,a,\delta}(\tilde{z}+B^e_S(j),w),P^{\tilde{p}}_{l,a,\delta}(\tilde{r},w)\Big) - S\Big(P^{\tilde{n}}_{l,a,\delta}(\tilde{z},w),P^{\tilde{p}}_{l,a,\delta}(\tilde{r},w)\Big)\Big| \le \frac{\bar{e}}{\omega}, \qquad \forall w\in\mathcal{T}_{l,a,\delta}. \tag{3.24}$$

with $\bar{\gamma}_r$ the positive real in (3.9) and the function $B^e_S:\mathbb{N}\to\mathbb{R}^{\tilde{n}(l+1)}$ defined (recursively) as:

$$B^e_S(0)=\begin{pmatrix}\bar{e}_0(0)\\ \vdots\\ \bar{e}_0(t_{-l})\end{pmatrix},\qquad \bar{e}_0(\tau)=\begin{cases}e_0(\tau), & \tau\in[-\Delta,0],\\ e_0(-\Delta), & \tau\in[t_{-l},-\Delta],\end{cases}$$
$$B^e_S(j)=\begin{pmatrix}e_j(0)\\ 0_{l\tilde{n}\times 1}\end{pmatrix}+\begin{pmatrix}0_{\tilde{n}\times l\tilde{n}} & 0_{\tilde{n}\times 1}\\ I_{l\tilde{n}} & 0\end{pmatrix}B^e_S(j-1),\qquad j=1,2,\dots \tag{3.25}$$

- the sequence i_j, $j=0,1,\dots$, is defined as $i_0=0$ and, for $j\ge 1$, $i_j=j$ in the event that (see **(f.3)**)

$$-\mathcal{D}_\infty\big(\mathcal{P}^{q_z}_j,\mathbb{P}^{q_r}_j,q_u(\tilde{u}_{i_{j-1}})\big)+\sigma\,\mathcal{D}_\infty\big(\mathbb{P}^{q_z}_j,\mathcal{P}^{q_r}_j,q_u(\tilde{u}_j)\big)\ \le\ H\big(\mathbb{P}^{q_z}_j,\mathbb{P}^{q_r}_j\big)\,. \tag{3.26}$$

  and $i_j=i_{j-1}$ otherwise;
- the function $H:\mathcal{C}^{\tilde{n}}\times\mathcal{C}^{\tilde{p}}\to\mathbb{R}^+$ is defined, for $\phi_z\in\mathcal{C}^{\tilde{n}}$, $\phi_r\in\mathcal{C}^{\tilde{p}}$ as follows

$$H(\phi_z,\phi_r)=\bar{d}\big(\nu(1-\sigma)+4\eta\bar{p}(1+\sigma)\big)\times\left(|S(\phi_z,\phi_r)|+\frac{\bar{e}+\bar{\mu}+\tilde{\mu}}{\omega}\right)+3(1+\sigma)L_{\mathcal{D}}\bar{e}, \tag{3.27}$$

- η, ν and $\bar{p}$ are the positive reals in Definition 3.2.3;
- $\bar{e}$ and $\bar{d}$ are the bounds of the involved measurement errors and actuation disturbances, respectively (see points (i) and (ii) above).

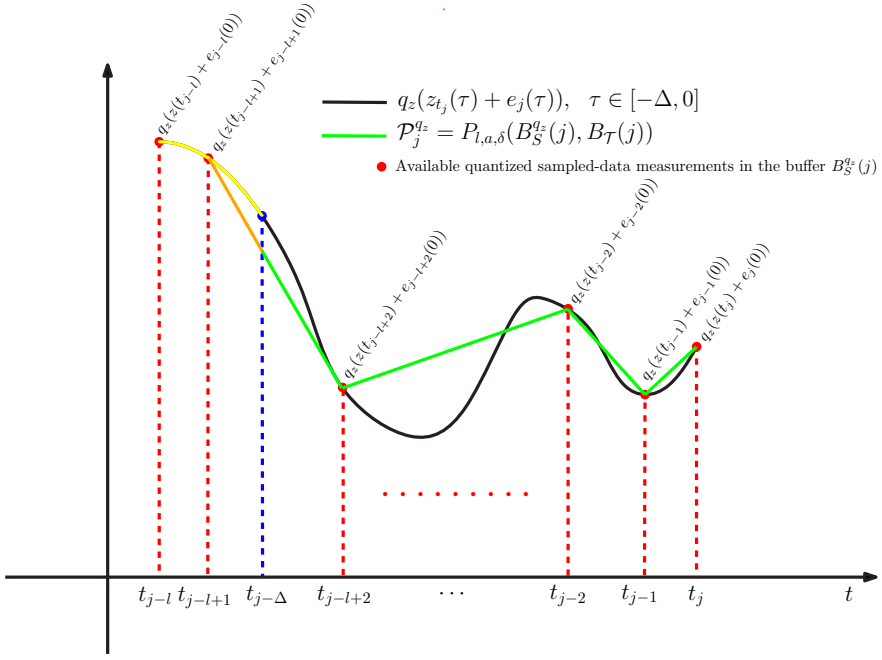


Figure 3.1: An example of the spline approximation method here used (see $\mathbb{P}^{q_z}_j$ in (3.22))

Remark 3.2.4

Notice that, the knowledge of infinite dimensional variables $q_z(z_{t_j}(\tau)+e_j(\tau))$ and $q_r(r_{t_j}(\tau))$, $\tau\in[-\Delta,0]$ is not needed for the correct implementation of the proposed robust QSE controller (3.22)*. Indeed, spline approximation methodologies (see [30]) are here used in order to obtain an approximation of the infinite dimensional variables $q_z(z_{t_j}(\tau)+e_j(\tau))$ and $q_r(r_{t_j}(\tau))$, $\tau\in[-\Delta,0]$, by interpolating the available noised quantized sampled-data state measurements $q_z(z(t_j)+e_j(0))$ and the quantized sampled-data exogenous signal $q_r(r(t_j))$ (see* (3.18) *and $\mathbb{P}_j^{q_z}$, $\mathbb{P}_j^{q_r}$ in* (3.22)*). The vectors $B_S^{q_z}$, $\bar{B}_S^{q_r}$ and $B_{\mathcal{T}}$ describe buffers of length $\tilde{n}(l+1)$, $\tilde{p}(l+1)$ and $l+1$ collecting, respectively, the quantized sampled-data state measurements affected by the noises e_j, $j=0,1,\cdots$, the known exogenous disturbances and the times elapsed between a sampling and the following which are used in the interpolation procedure to obtain the required approximations. In Fig. 3.1, an example of the interpolation method here considered is reported.* □

Remark 3.2.5

Notice that, the proposed triggering condition (3.26) *is checked just at times t_j, $j=0,1,\cdots$, guaranteeing a minimum dwell-time $a\delta$ between two consecutive sampling instants (see Definition 3.2.5). Hence, no continuous-time monitoring of the state variables is needed and possible Zeno behaviours are avoided by sampling with dwell-time.* □

3.3 Main Results

In the following, the main results are provided. In particular, we will show that, under Assumption 3.2.1, there exist suitable control tuning parameters ω and $L_{\mathcal{D}}$ (see (3.22)–(3.26)), a suitably fast sampling δ and an accurate quantization of the input/output channels (i.e., ranges and error bounds for the quantizers q_z, q_r and q_u in (3.22)) such that the semi–global practical stability property of the closed–loop system (3.5)-(3.22) is ensured regardless of the unknown actuation disturbances d (see point (i) in Section 3.2) and of the unknown measurement errors e (see point (ii) in Section 3.2) as long as (3.24) holds. In the following, we will consider functions α_i, $i=1,2$, of class $\mathcal{K}_\infty$, defined for $s\in\mathbb{R}^+$ as follows

$$\alpha_1(s)=\eta e^{-\mu\Delta}p\circ\beta_1(s),\quad \alpha_2(s)=\nu\gamma_2(s)+\eta p\circ\beta_2(s), \tag{3.28}$$

where: η, μ and ν are the positive reals in Definition 3.2.3; p is the function in Definition 3.2.3; γ_2 and β_i, $i=1,2$, are the functions related to the Lyapunov–Krasovskii functional $V\in\mathcal{V}$ (see points P_1) and P_4) in Section 3.2).

Theorem 3.3.1

Let Assumption 3.2.1 hold. Let a, $\bar{\mu}$ and $\tilde{\mu}$ be arbitrary reals in $(0,1]$. Let σ be an arbitrary real in $(0,1)$. Then, for any positive reals R_f, R_0, E, q, $\bar{d}$ and $\bar{e}$, with $0<R_f<R_0<E$ and $\alpha_1(E)>\alpha_2(R_0)$, there exist positive reals δ, T, U, ω, $L_{\mathcal{D}}$, E_1, μ_z, μ_r and μ_u, such that for any initial state $z^0\in W_{\tilde{n}}^{1,\infty}\cap\mathcal{C}_{R_0}^{\tilde{n}}$ satisfying $\operatorname*{ess\,sup}_{\theta\in[-\Delta,0]}\left|\frac{dz^0(\theta)}{d\theta}\right|\leq q$, the corresponding unique locally absolutely continuous solution of the QSE closed-loop system, described by (3.5)-(3.22)*, exists $\forall t\geq 0$ and, furthermore, satisfies:*

$$z_t\in\mathcal{C}_E^{\tilde{n}},\ \forall t\geq 0,\quad z_t\in\mathcal{C}_{R_f}^{\tilde{n}},\ \forall t\geq T, \tag{3.29}$$

i.e., Problem 1 is solved. □

Proof. The proof of Theorem 3.3.1 is reported in the Appendix. □

Remark 3.3.1

We highlight here that, the methodology provided here is a novelty also for the case of a single agent system (i.e., $N = 1$). Indeed, to the best of our knowledge, no result is available in the literature concerning robust QSE stabilizers for the class of nonlinear systems described by (3.5). In this work, inspired by the methodology proposed in [22], for the first time in the literature, results concerning the design of robust QSE stabilizers are provided for the class of systems described by (3.5). We highlight here that time–varying known exogenous disturbances are not considered in [22], thereby excluding from the developed theory several interesting practical control problems, such as the tracking one. Moreover, MASs and the related consensus problems are not considered in [22]. We highlight also that several new and not trivial developments have been here required with respect to [22] in order to correctly apply the stabilization in the sample–and–hold sense theory, here used as a tool for proving the results, to the case of nonlinear time–delay systems in presence of known exogenous disturbances introduced to characterize, for instance, tracking control problems. See, as an example, forthcoming Definition 3.2.3, (3.22)-(3.27) and steps 1)-10) in the proof of Theorem 3.3.1. □

Remark 3.3.2

Notice that, in Theorem 3.3.1, the functions d and e are unknown. More in details, the functions d and e characterize the unknown actuation disturbances and the unknown measurement errors, which affect the QSE controller when closed in the loop with system (3.5) (see (3.22)-(3.27)). The new added control term $-\omega S\left(\mathbb{P}_{ij}^{q_z}, \mathbb{P}_{ij}^{q_r}\right)$ (see (3.19)) has been introduced to arbitrarily attenuate the effects of such disturbances (see Theorem 3.3.1). It is here highlighted that, no a-priori limitation on the bounds $\bar{d}$ and $\bar{e}$ is here introduced. On the other hand, it is assumed that the measurement errors e affect marginally the new added control term S (see the inequality in (3.24)). It is highlighted also that, taking into account that discontinuities in the function describing the SDCF controller at hand are allowed (see Definition 3.2.3), even small measurement errors may turn in serious performances deterioration of the feedback control law. Then, the robustification of QSE controllers, based on the notion of SDCFs, is significant also in the case of small measurement errors. Moreover, the results here provided are valid for any actuation disturbance with arbitrarily large bound. To our best knowledge, it is the first time in the literature concerning nonlinear MASs with state delays, that a methodology for the design of robust QSE tracking protocols able to arbitrarily attenuate the effects of bounded actuation disturbances and bounded measurement errors is provided. □

Remark 3.3.3

The methodology proposed in this work aims to extend the Artstein's methodologies (see, for instance, [23], [26], [27], [24], [29], [25]) to the design of static state feedbacks protocols for nonlinear time–delay MASs. In particular, the following steps summarize the proposed methodology for the design of robust QSE protocols achieving the consensus tracking in a semiglobal practical sense, with arbitrarily small final tracking error (see (3.3)–(3.5), (3.22)-(3.27) and Theorem 3.3.1)

1) *choose a candidate Lyapunov–Krasovskii functional V belonging to $\mathcal{V}$;*
2) *by the use of the Lyapunov–Krasovskii functional V defined in Step 1, try to find a function k (continuous or not) satisfying inequality (3.14), i.e. a SDCF (see Definition 3.2.3) and, consequently, define the robustification term S as in (3.19);*
3) *implement the robust QSE controller as in (3.22)-(3.27) by using the SDCF k and the robustification term S defined in Step 2 and, apply it to the original system (3.1).*

□

3.4 Application to a Particular Class of Nonlinear MASs

To illustrate the applicability of the proposed control design, we consider in this subsection a particular class of nonlinear time–delay MASs. This class encompasses a wide range of MASs studied in the literature and allows one to explicitly demonstrate how the proposed controller can be implemented in practice. Moreover, the considered structure facilitates a transparent verification of the controller design conditions while preserving the generality of the developed approach. In this subsection, we study the case of a particular class of nonlinear time–delay MASs described by

$$\begin{aligned} \dot{x}_i(t) &= Ax_i(t) + H_i(x_{t,i}, \chi_{t,i}) + B_i(u_i(t) + d_i(t)), \\ x_i(\tau) &= x_i^0(\tau), \quad \tau \in [-\Delta, 0], \quad i = 1, \cdots, N. \end{aligned} \tag{3.30}$$

where $x_i(t) \in \mathbb{R}^{2n}$, $x_{t,i} \in \mathcal{C}^{2n}$, denote the states of the system; $x_i^0 \in W_{2n}^{1,\infty}$ are the initial states; $\chi_{t,i} \in \mathcal{C}^p$, are known disturbances continuously differentiable and satisfying (3.2); $u_i(t) \in \mathbb{R}^n$ are the control input signals; $d_i(t) \in \mathbb{R}^n$ are *unknown* disturbances; $H_i \colon \mathcal{C}^{2n} \times \mathcal{C}^p \to \mathbb{R}^{2n}$ are functions defined for any $\phi_i \in \mathcal{C}^{2n}$, $\phi_{\chi_i} \in \mathcal{C}^p$, as

$$H_i(\phi_i, \phi_{\chi_i}) = \begin{pmatrix} 0 \\ f_{i,1}(\phi_i, \phi_{\chi_i}) \\ 0 \\ f_{i,2}(\phi_i, \phi_{\chi_i}) \\ \vdots \\ 0 \\ f_{i,n}(\phi_i, \phi_{\chi_i}) \end{pmatrix} \tag{3.31}$$

with $f_{i,j} \colon \mathcal{C}^{2n} \times \mathcal{C}^p \to \mathbb{R}$, $i = 1, \cdots, N$, $j = 1, \cdots, n$, Lipschitz on bounded subsets functions; $A \in \mathbb{R}^{2n \times 2n}$ and $B_i \in \mathbb{R}^{2n \times n}$, $i = 1, \cdots, N$, are the matrices defined as:

$$\begin{aligned} A &= I_{n,n} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\ B_i &= \left(\operatorname{diag}\{b_{i,1}, b_{i,2}, \cdots, b_{i,n}\} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) \end{aligned} \tag{3.32}$$

with $b_{i,j} \in \mathbb{R}$, $i = 1, \cdots, N$, $j = 1, \cdots, n$. By exploiting the methodology proposed in this paper, in order to design a robust QSE protocol for the MAS (3.30), let

$$\psi_t = \begin{pmatrix} \psi_{t,1} \\ \vdots \\ \psi_{t,N} \end{pmatrix} \in \mathcal{C}^{2nN}, \quad \psi_{t,i}(\tau) = \begin{pmatrix} \psi_{t,i,1}(\tau) \\ \dot{\psi}_{t,i,1}(\tau) \\ \vdots \\ \psi_{t,i,n}(\tau) \\ \dot{\psi}_{t,i,n}(\tau) \end{pmatrix} \in \mathbb{R}^{2n},$$

where $i = 1, \cdots, N$, $t \in \mathbb{R}^+$, $\tau \in [-\Delta, 0]$, and $\psi_{t,i,j} \in \mathbb{R}$, $j = 1, \cdots, n$, be a desired reference signal for coordination satisfying (3.2). Notice that,

$$\dot{\psi}_{t,i}(\tau) = \begin{pmatrix} \dot{\psi}_{t,i,1}(\tau) \\ \ddot{\psi}_{t,i,1}(\tau) \\ \vdots \\ \dot{\psi}_{t,i,n}(\tau) \\ \ddot{\psi}_{t,i,n}(\tau) \end{pmatrix} \in \mathbb{R}^{2n}.$$

Taking into account (3.4), (3.5), (3.30), (3.32), and the form of the chosen reference for tracking ψ_t, the corresponding tracking error system is described by (3.5), where $\tilde{n} = 2nN$, $\tilde{p} = (4n+p)N$, and $\tilde{m} = nN$; $F : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n}}$ and $G : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{n}\times\tilde{m}}$ are the functions described for any

$$\phi_z = \begin{pmatrix} \phi_{z_1} \\ \vdots \\ \phi_{z_N} \end{pmatrix} \in \mathcal{C}^{\tilde{n}}, \quad \phi_{z_i} \in \mathcal{C}^{2n},\ i = 1, \cdots, N,$$

$$\phi_r = \begin{pmatrix} \phi_\psi \\ \phi_{d\psi} \\ \phi_\chi \end{pmatrix} \in \mathcal{C}^{\tilde{p}}, \quad \phi_\psi = \begin{pmatrix} \phi_{\psi_1} \\ \vdots \\ \phi_{\psi_N} \end{pmatrix} \in \mathcal{C}^{\tilde{n}},$$

$$\phi_{d\psi} = \begin{pmatrix} \phi_{d\psi_1} \\ \vdots \\ \phi_{d\psi_N} \end{pmatrix} \in \mathcal{C}^{\tilde{n}}, \quad \phi_\chi = \begin{pmatrix} \phi_{\chi_1} \\ \vdots \\ \phi_{\chi_N} \end{pmatrix} \in \mathcal{C}^{pN},$$

where ϕ_{ψ_i}, $\phi_{d\psi_i} \in \mathcal{C}^{2n}$ and $\phi_{\chi_i} \in \mathcal{C}^{p}$ for $i = 1, \cdots, N$, as follows,

$$\begin{aligned} F(\phi_z, \phi_r) &= \begin{pmatrix} \tilde{f}_1^T & \cdots & \tilde{f}_N^T \end{pmatrix}^T, \\ G(\phi_z, \phi_r) &= \begin{pmatrix} B_1 & 0_{n,m} & 0_{n,m} & \cdots & 0_{n,m} & 0_{n,m} \\ B_1 & -B_2 & 0_{n,m} & \cdots & 0_{n,m} & 0_{n,m} \\ 0_{n,m} & B_2 & -B_3 & \cdots & 0_{n,m} & 0_{n,m} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0_{n,m} & 0_{n,m} & 0_{n,m} & \ddots & -B_{N-1} & 0_{n,m} \\ 0_{n,m} & 0_{n,m} & 0_{n,m} & \cdots & B_{N-1} & -B_N \end{pmatrix}. \end{aligned} \tag{3.33}$$

with

$$\begin{aligned} \tilde{f}_1 &= A\big(\phi_{z_1}(0) + \phi_{\psi_1}(0)\big) + H_1\big(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}\big) - \phi_{d\psi_1}(0), \\ \tilde{f}_2 &= A\big(\phi_{z_2}(0) + \phi_{\psi_2}(0)\big) + H_1\big(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}\big) - H_2\big(\varsigma_2, \phi_{\chi_2}\big) - \phi_{d\psi_2}(0), \\ \tilde{f}_i &= A\big(\phi_{z_i}(0) + \phi_{\psi_i}(0)\big) + H_{i-1}\big(\varsigma_{i-1}, \phi_{\chi_{i-1}}\big) - H_i\big(\varsigma_i, \phi_{\chi_i}\big) - \phi_{d\psi_i}(0), \quad i = 3, \ldots, N, \\ \varsigma_i &= \phi_{z_1} + \phi_{\psi_1} - \sum_{j=2}^{i} \big(\phi_{z_j} + \phi_{\psi_j}\big), \quad i = 2, \ldots, N. \end{aligned} \tag{3.34}$$

Thus, it follows that

$$\begin{aligned} \dot{z}_1(t) &= \tilde{f}_1 + B_1\big(u_1(t) + d_1(t)\big), \\ \dot{z}_2(t) &= \tilde{f}_2 + B_1\big(u_1(t) + d_1(t)\big) - B_2\big(u_2(t) + d_2(t)\big), \\ &\vdots \\ \dot{z}_N(t) &= \tilde{f}_N + B_{N-1}\big(u_{N-1}(t) + d_{N-1}(t)\big) - B_N\big(u_N(t) + d_N(t)\big), \end{aligned} \tag{3.35}$$

$$z(\tau) = z^0(\tau) = \begin{pmatrix} x_1^0(\tau) - \psi_1^0(\tau) \\ x_1^0(\tau) - x_2^0(\tau) - \psi_2^0(\tau) \\ \vdots \\ x_{N-1}^0(\tau) - x_N^0(\tau) - \psi_N^0(\tau) \end{pmatrix}, \qquad \tau \in [-\Delta, 0].$$

According to the proposed design procedure, let $V : \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ be the function defined for any $\phi_z \in \mathcal{C}^{\tilde{n}}$ as $V(\phi_z) = V_1(\phi_z(0)) + V_2(\phi_z)$, $V_1(\phi_z(0)) = \phi_z(0)^T P \phi_z(0)$, $V_2(\phi_z) = 0$, where P is the symmetric and positive definite matrix such that

$$(\tilde{A} - \tilde{B}K)^T P + P(\tilde{A} - \tilde{B}K) = -Q, \tag{3.36}$$

with: $Q \in \mathbb{R}^{\tilde{n}\times\tilde{n}}$ an arbitrarily chosen symmetric positive definite matrix;

$$\tilde{A} = I_{N,N} \otimes A, \tilde{B} \quad = I_{\tilde{m},\tilde{m}} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.37}$$

and

$$K = \text{diag}\{K_1, \ldots, K_N\} \in \mathbb{R}^{\tilde{m}\times\tilde{n}},$$

where

$$K_i = \begin{pmatrix} K_{i,1} & K_{i,2} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & K_{i,3} & K_{i,4} & \cdots & 0 & 0 \\ \vdots & \vdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & K_{i,2n-1} & K_{i,2n} \end{pmatrix} \in \mathbb{R}^{n\times 2n}$$

is a matrix such that $(\tilde{A} - \tilde{B}K)$ is Hurwitz. Taking into account the functional V, (3.5), (3.6), (3.33), (3.34), (3.35), and considering $d = 0$, we have that for any $\phi_z \in \mathbb{C}^{\tilde{n}}$, $\phi_r \in \mathbb{C}^{\tilde{p}}$, the following conditions hold.

$$D^+V(\phi_z, \phi_r, u) = 2\phi_z(0)^T P(F(\phi_z, \phi_r) + G(\phi_z, \phi_r)u). \tag{3.38}$$

Let $k_i : \mathbb{C}^{\tilde{n}} \times \mathbb{C}^{\tilde{p}} \to \mathbb{R}^{2n}$, $i = 1, \ldots, N$, be the functions defined for any

$$\phi_z = \begin{pmatrix} \phi_{z_1} \\ \vdots \\ \phi_{z_N} \end{pmatrix} \in \mathbb{C}^{\tilde{n}}, \quad \phi_{z_i} \in \mathbb{C}^{2n},\ i = 1, \ldots, N,$$

$$\phi_r = \begin{pmatrix} \phi_\psi \\ \phi_{d\psi} \\ \phi_\chi \end{pmatrix} \in \mathbb{C}^{\tilde{p}}, \quad \phi_\psi = \begin{pmatrix} \phi_{\psi_1} \\ \vdots \\ \phi_{\psi_N} \end{pmatrix} \in \mathbb{C}^{\tilde{n}},$$

$$\phi_{d\psi} = \begin{pmatrix} \phi_{d\psi_1} \\ \vdots \\ \phi_{d\psi_N} \end{pmatrix} \in \mathbb{C}^{\tilde{n}}, \quad \phi_\chi = \begin{pmatrix} \phi_{\chi_1} \\ \vdots \\ \phi_{\chi_N} \end{pmatrix} \in \mathbb{C}^{pN},$$

with $\phi_{\psi_i}, \phi_{d\psi_i} \in \mathbb{C}^{2n}$, $\phi_{\chi_i} \in \mathbb{C}^p$, $i = 1, \ldots, N$, as follows.

$$\begin{aligned} k_1(\phi_z, \phi_r) = \text{diag}\Big\{\frac{1}{b_{0,1}}, \frac{1}{b_{0,2}}, \cdots, \frac{1}{b_{0,n}}\Big\}\Big(&- K_1\phi_{z_1}(0) - (I_{n,n} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix}) \\ &\big(H_1(\phi_{z_1} + \phi_{\psi_1}, \phi_{\chi_1}) - \phi_{d\psi_1}(0)\big)\Big), \end{aligned}$$

$$\begin{aligned} k_i(\phi_z, \phi_r) = \text{diag}\Big\{\frac{1}{b_{i,1}}, \frac{1}{b_{i,2}}, \cdots, \frac{1}{b_{i,n}}\Big\}\Big(&- (I_{n,n} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix})\Big(H_i(\varsigma_i, \phi_{\chi_i}) - \phi_{d\psi_1}(0) + \\ &\sum_{j=2}^{i} \phi_{d\psi_j}(0)\Big) - K_1\phi_{z_1}(0) + \sum_{j=2}^{i} K_j\phi_{z_j}(0)\Big), \quad i = 2, \ldots, N. \end{aligned} \tag{3.39}$$

Let $k : \mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \to \mathbb{R}^{\tilde{m}}$, be the function defined for any $\phi_z \in \mathcal{C}^{\tilde{n}}$ and for any $\phi_r \in \mathcal{C}^{\tilde{p}}$, as follows

$$k(\phi_z, \phi_r) = \begin{pmatrix} k_1(\phi_z, \phi_r) \\ \vdots \\ k_N(\phi_z, \phi_r) \end{pmatrix}. \tag{3.40}$$

From (3.38), taking into account (3.5), (3.6), (3.33), (3.34), (3.35) and by selecting $u = k(\phi_z, \phi_r)$, for any $\phi_z \in \mathcal{C}^{\tilde{n}}$ and for any $\phi_r \in \mathcal{C}^{\tilde{p}}$, the following equalities/inequality hold

$$\begin{aligned} D^+V(\phi_z, \phi_r, k(\phi_z, \phi_r)) &= 2\phi_z(0)^T P\big(F(\phi_z, \phi_r) + G(\phi_z, \phi_r)k(\phi_z, \phi_r)\big) \\ &= 2\phi_z(0)^T P(\tilde{A} - \tilde{B}K)\phi_z(0) \leq -\lambda_{\min}(Q)\,|\phi_z(0)|^2. \end{aligned} \tag{3.41}$$

It follows that, inequality (3.14) is here satisfied by choosing, for instance, $\eta = 1$, $\mu \leq \dfrac{\lambda_{\min}(Q)}{\lambda_{\max}(P)}$, $p = Id$, $\bar{\alpha} = 0$, $\nu = 1$. Thus, the function k in (3.40) is a SDCF induced by V according to Definition 3.2.3. We can apply the results in Theorem 3.3.1 implementing the SDCF (3.40) according to (3.22)-(3.27).

3.4.1 Case Study: Consensus of UAVs via Digital Controllers

In this section, we apply the results presented above to the coordination problem of a swarm of UAVs. UAVs, particularly quadrotors, have attracted remarkable attention in both research and industry due to their versatility, compact design, and vertical take–off and landing (VTOL) capabilities. Their agility and ease of control make them ideal for a wide range of applications such as search and rescue operations [126], [127], aerial delivery [128], surveillance and environmental monitoring [129], and precision agriculture [130], [131], [132], [133], [134].

In the agricultural domain, quadrotor–based UAVs have demonstrated exceptional potential in improving efficiency, reducing operational costs, and enabling sustainable farming practices. Recent studies highlight their use in tasks such as targeted pesticide spraying [131], crop health and disease detection through high–resolution multispectral imaging [132], [133], and real–time monitoring of vegetation indices and soil conditions [130], [134]. The combination of autonomous navigation, onboard sensing, and data processing allows these systems to perform precise and adaptive agricultural interventions, which are essential for modern precision farming. Furthermore, when operating in coordinated swarms, UAVs can collectively cover larger areas, share environmental information, and execute cooperative missions with enhanced robustness and fault tolerance.

In the following numerical example, by exploiting the SDCF in (3.40) and the results provided in Theorem 3.3.1, a robust QSE controller is designed for the coordination problem of a swarm of UAVs. The considered swarm of UAVs is described by [135]

$$\begin{aligned} \ddot{x} &= \frac{1}{m}(c_{\theta_3}s_{\theta_2}c_{\theta_1} + s_{\theta_3}s_{\theta_1})U_1 - \frac{k_1}{m}\dot{x} \\ \ddot{y} &= \frac{1}{m}(s_{\theta_3}s_{\theta_2}c_{\theta_1} - c_{\theta_3}s_{\theta_1})U_1 - \frac{k_2}{m}\dot{y} \\ \ddot{z} &= -g + \frac{1}{m}(c_{\theta_2}c_{\theta_1})U_1 - \frac{k_3}{m}\dot{z} \\ \ddot{\theta}_1 &= \frac{1}{I_x}(\dot{\theta}_2\dot{\theta}_3(I_y - I_z) - J_r\dot{\theta}_2\bar{w} - k_4\dot{\theta}_1^2 + dU_2) \\ \ddot{\theta}_2 &= \frac{1}{I_y}(\dot{\theta}_1\dot{\theta}_3(I_z - I_x) - J_r\dot{\theta}_1\bar{w} - k_5\dot{\theta}_2^2 + dU_3) \\ \ddot{\theta}_3 &= \frac{1}{I_z}(\dot{\theta}_1\dot{\theta}_2(I_x - I_y) - k_6\dot{\theta}_3^2 + fU_3) \end{aligned} \tag{3.42}$$

where: x, y, z represents the position of the UAV, along the $x-$, $y-$ and $z-$ axis of the UAV, respectively; $\theta_1, \theta_2, \theta_3$, represents the roll, pitch and yaw angles around $x-$, $y-$ and $z-$ axis, respectively; U_1, U_2, U_3, U_4, are the control inputs; the symbols c_y and s_y denotes the functions $cos(y)$ and $sin(y)$, respectively. The remaining parameters in the model, such as m, I_x, I_y, I_z, J_r and k_i (for $i = 1, .., 6$), represent the physical properties of the UAV, including its mass, moments of inertia, rotor dynamics, and aerodynamic coefficients (see, for instance, [135] for more details).

We consider the above model because it has been widely studied in agricultural applications, e.g., in [136], [137], where similar models were adopted to design advanced control strategies for agricultural quadrotors. In [136], an adaptive composite anti–disturbance controller was developed to enhance stability under wind, payload, and propeller failure disturbances during low–altitude operations. Likewise, [137] proposed an adaptive radial basis function neural network sliding mode controller to improve altitude stability in the presence of disturbances and propeller faults, with the effectiveness of the method verified through simulations and field experiments.

By defining the state vector

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \end{bmatrix} = \begin{bmatrix} \theta_1 \\ \dot{\theta}_1 \\ \theta_2 \\ \dot{\theta}_2 \\ \theta_3 \\ \dot{\theta}_3 \\ x \\ \dot{x} \\ y \\ \dot{y} \\ z \\ \dot{z} \end{bmatrix}$$

from (3.42), we obtain (see [135])

$$\begin{aligned}
\dot{x}_1 &= x_2 \\
\dot{x}_2 &= a_1 x_4 x_6 + a_2 x_4 + a_3 x_2^2 + b_1 U_2 \\
\dot{x}_3 &= x_4 \\
\dot{x}_4 &= a_4 x_2 x_6 + a_5 x_2 + a_6 x_4^2 + b_2 U_3 \\
\dot{x}_5 &= x_6 \\
\dot{x}_6 &= a_7 x_2 x_4 + a_8 x_6^2 + b_3 U_4 \\
\dot{x}_7 &= x_8 \\
\dot{x}_8 &= a_9 x_8 + \frac{U_1}{m}(c_{x_1} s_{x_3} c_{x_5} + s_{x_1} s_{x_5}) \\
\dot{x}_9 &= x_{10} \\
\dot{x}_{10} &= a_{10} x_{10} + \frac{U_1}{m}(c_{x_1} s_{x_3} s_{x_5} - s_{x_1} c_{x_5}) \\
\dot{x}_{11} &= x_{12} \\
\dot{x}_{12} &= a_{11} x_{12} - g + \frac{U_1}{m}(c_{x_1} c_{x_2})
\end{aligned} \tag{3.43}$$

Here $a_j \in \mathbb{R}, j = 1 \cdots 11$ and $b_j \in \mathbb{R}, j = 1 \cdots 3$ are are the involved model parameters represent the physical properties of the UAV, including its mass, moments of inertia, rotor dynamics, and aerodynamic coefficients (see, for instance, [135] for more details);

Since a quadrotor is an underactuated system, its linear motion along the $x-$ and $y-$axes depends on the roll and pitch angles, respectively. Therefore, to compute the desired roll and pitch angles needed to achieve specified x and y coordinates, we introduce three virtual control inputs as follows:

$$\begin{aligned}
v_1 &= \frac{U_1}{m}(c_{x_1} s_{x_3} c_{x_5} + s_{x_1} s_{x_5}) \\
v_2 &= \frac{U_1}{m}(c_{x_1} s_{x_3} s_{x_5} - s_{x_1} c_{x_5}) \\
v_3 &= -g + \frac{U_1}{m}(c_{x_1} c_{x_2})
\end{aligned} \tag{3.44}$$

Using (3.44), the desired roll $x_{1,\mathrm{d}}$ and pitch $x_{3,\mathrm{d}}$ angles, and the input U_1, can be formulated as:

$$\begin{aligned} U_1 &= m\sqrt{v_1^2 + v_2^2 + (v_3+g)^2} \\ x_{1,\mathrm{d}} &= arctan\Big(c_{x_3}\frac{v_1 s_{x_5} - v_2 c_{x_5}}{v_3+g}\Big) \\ x_{3,\mathrm{d}} &= arctan\Big(\frac{v_1 c_{x_5} + v_2 s_{x_5}}{v_3+g}\Big) \end{aligned} \tag{3.45}$$

Taking into account (3.43) and (3.44), the considered swarm of UAVs is here described by

$$\begin{aligned} \dot{x}_{i,1}(t) &= x_{i,2}(t) \\ \dot{x}_{i,2}(t) &= a_1 x_{i,4}(t) x_{i,6}(t) + a_2 x_{i,4}(t) + a_3 x_{i,2}(t)^2 \\ &\quad + b_1(U_{i,2}(t) + d_{i,1}(t)) \\ \dot{x}_{i,3}(t) &= x_{i,4}(t) \\ \dot{x}_{i,4}(t) &= a_4 x_{i,2}(t) x_{i,6}(t) + a_5 x_{i,2}(t) + a_6 x_{i,4}(t)^2 \\ &\quad + b_2(U_{i,3}(t) + d_{i,2}(t)) \\ \dot{x}_{i,5}(t) &= x_{i,6}(t) \\ \dot{x}_{i,6}(t) &= a_7 x_{i,2}(t) x_{i,4}(t) + a_8 x_{i,6}(t)^2 + b_3(U_{i,4}(t) + d_{i,3}(t)) \\ \dot{x}_{i,7}(t) &= x_{i,8}(t) \\ \dot{x}_{i,8}(t) &= a_9 x_{i,8}(t) + v_{i,1}(t) + d_{i,4}(t) \\ \dot{x}_{i,9}(t) &= x_{i,10}(t) \\ \dot{x}_{i,10}(t) &= a_{i,10} x_{i,10}(t) + v_{i,2}(t) + d_{i,5}(t) \\ \dot{x}_{i,11}(t) &= x_{i,12}(t) \\ \dot{x}_{i,12}(t) &= a_{11} x_{i,12}(t) + v_{i,3}(t) + d_{i,6}(t) \\ x_i(0) &= x_i^0, \quad i = 1, 2, \cdots, N, \end{aligned} \tag{3.46}$$

Here, $d_{i,j} \in \mathbb{R}$, $j = 1, \cdots, 6$ are the involved actuation disturbances;

In the following, the control problem addressed in this example is introduced. For a given reference signal

$$\psi_i(t) = \begin{pmatrix} \psi_{i,1}(t) \\ \dot{\psi}_{i,1}(t) \\ \vdots \\ \psi_{i,6}(t) \\ \dot{\psi}_{i,6}(t) \end{pmatrix} \in \mathbb{R}^{12}, \quad i = 1, \ldots, N.$$

satisfying (3.2), find a robust QSE controller ensuring that, for a swarm of UAVs composed by N agents, the leader (here denoted with index 1) follows a desired position trajectory $\psi_{1,4}(t)$, $\psi_{1,5}(t)$, $\psi_{1,6}(t)$ and a desired orientation $\psi_{1,3}(t)$ while forming a prescribed formation with the followers here characterized by the signals $\psi_i(t)$, $i = 2, \cdots, N$.

Notice that, the MAS presented in (3.46) is in the form (3.30) where:

$$H_i(\phi_i, \phi_{\chi_i}) = \begin{pmatrix} 0 \\ a_1\phi_{i,4}(0)\phi_{i,6}(0) + a_2\phi_{i,4}(0) + a_3\phi_{i,2}^2(0) \\ 0 \\ a_4\phi_{i,2}(0)\phi_{i,6}(0) + a_5\phi_{i,2}(0) + a_6\phi_{i,4}^2(0) \\ 0 \\ a_7\phi_{i,2}(0)\phi_{i,4}(0) + a_8\phi_{i,6}^2(0) \\ 0 \\ a_9\phi_{i,8}(0) \\ 0 \\ a_{10}\phi_{i,10}(0) \\ 0 \\ a_{11}\phi_{i,12}(0) \end{pmatrix}, \tag{3.47}$$

$$A = I_{6,6} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$B_i = \Big(\mathrm{diag}\{b_1, b_2, b_3, 1, 1, 1\} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\Big), \quad i = 1, \ldots, N.$$

It follows that the feedback k provided in (3.39), (3.40) is a SDCF for the system described by (3.46). Therefore, Theorem 3.3.1 can be applied. Simulations have been performed by with following settings: $N = 3$; a desired position trajectory $\psi_{1,4}(t) = 3s_{0.2t}$, $\psi_{1,5}(t) = 5s_{0.2t}$, $\psi_{1,6}(t) = 15$ and a desired orientation $\psi_{1,3}(t) = 1.57$, $\forall t \geq 0$. The desired pitch and roll are obtained from (3.45)

$$\begin{aligned} \psi_{1,1}(t) &= \arctan\Big(c_{\psi_{1,2}(t)} \frac{v_{1,1}(t)s_{\psi_{1,3}(t)} - v_{1,2}(t)c_{\psi_{1,3}(t)}}{v_{1,3}(t) + g}\Big), \\ \psi_{1,2}(t) &= \arctan\Big(\frac{v_{1,1}(t)c_{\psi_{1,3}(t)} + v_{1,2}(t)s_{\psi_{1,3}(t)}}{v_{1,3}(t) + g}\Big); \end{aligned} \tag{3.48}$$

A desired offset in the position and orientation trajectories is given by

$$\psi_{2,3}(t) = 0, \psi_{2,4}(t) = \psi_{2,5}(t) = 5, \psi_{2,6}(t) = 0,$$
$$\psi_{3,3}(t) = 0, \psi_{3,4}(t) = \psi_{3,5}(t) = 5, \psi_{3,6}(t) = 0.$$

In this formation, the Leader follows the given reference trajectory, while Follower 1 tracks the leader with a $5 - unit$ offset along both the $x-$ and $y-$axes. Follower 2, in turn, follows the same trajectory while maintaining a $5 - unit$ offset relative to Follower 1 along both axes. All agents maintain the same heading (yaw angle) and altitude throughout the motion.

The control parameters $K_{i,j}$, $i = 1, 2, 3$, $j = 1, \cdots, 12$, in (3.39), (3.40) are all set to 1; the robustification term $\omega = 10$; the uniform (i.e., $a = 1$) sampling period is $\delta = 0.0001$[s], and quantizers are based on the round–to–nearest method with

$$\begin{aligned} \mathcal{Q}_u^{18} = \{\, u \in \mathbb{R}^{18} \mid\ & u_{i,1} = u_{i,2} = u_{i,3} = \pm 0.0001j, \\ & v_{i,1} = v_{i,2} = v_{i,3} = \pm 0.1j, \\ & i = 1, 2, 3,\ j = 0, 1, \ldots, 10^3 \,\}, \end{aligned}$$

$$\begin{aligned} \mathcal{Q}_z^{36} = \{\, z \in \mathbb{R}^{36} \mid\ & z_k = z_{k+7} = z_{k+19} = \pm 0.0001j, \quad k = 1, \ldots, 6, \\ & z_k = z_{k+7} = z_{k+19} = \pm 0.1j, \quad k = 7, \ldots, 12, \\ & i = 1, 2, 3,\ j = 0, 1, \ldots, 10^5 \,\}, \end{aligned}$$

$$\begin{aligned} \mathcal{Q}_r^{72} = \{\, r \in \mathbb{R}^{72} \mid\ & r_{k+12\gamma} = \pm 0.0001j, \quad k = 1, \ldots, 6, \\ & r_{k+12\gamma} = \pm 0.1j, \quad k = 7, \ldots, 12, \\ & \gamma = 0, \ldots, 5,\ i = 1, 2, 3,\ j = 0, 1, \ldots, 10^5 \,\}. \end{aligned}$$

The initial state of the leader is defined as

$$x_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T,$$

and the initial states of the followers are

$$x_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T,$$

$$x_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T.$$

The above initial states place all agents in a straight line along the $y-$axis.

The disturbances are defined as

$$d_{i,k}(t) = 2sin(t)d_k(j), i = 1, 2, 3, k = 1, \cdots, 6, t_j \leq t < t_{j+1}, j = 0, 1, \cdots,$$

with $d_1(j)$, $d_2(j)$, $d_3(j)$ and $d_4(j)$, $d_5(j)$, $d_6(j)$ taken from the interval $[-0.05, 0.05]$ and $[-3, 3]$, respectively by emulation of the uniform probability density function.

Having defined the control parameters, quantization settings, sampling period, and initial conditions for all agents, we now proceed to evaluate the performance of the proposed control strategy through numerical simulations. The simulations consider different practical scenarios to assess the effects of sampling, quantization, event–triggered control, disturbances, and the robustification term. The control gains $K_{i,j}$ are consistently set as defined previously ($K_{i,j} = 1$) in all cases, while other mechanisms such as sampling, quantization, event–triggered updates, and robustification are selectively applied depending on the scenario.

Case 1 – **Nominal Response:** This case evaluates the system without any digitization (sampling or quantization), event–triggered mechanism, or robustification. No disturbances are introduced. This serves as a baseline to observe the nominal tracking performance with the control gains $K_{i,j} = 1$.

Fig. 3.2 depicts the evolution of the collective variable Z (as defined in (3.35)) for all three UAVs, highlighting their convergence behaviour under the baseline controller i.e. without sampling, quantization, robustness or event–triggered mechanism. Fig. 3.3 presents the trajectories of the main motion states i.e. orientation θ_3 ($x_{i,5}(t).i = 1, 2, 3$), and translational coordinates x, y, and z ($x_{i,7}(t), x_{i,9}(t)$ and $x_{i,11}(t), i = 1, 2, 3$) for the three agents, together with the corresponding desired trajectories. The plots clearly illustrate how each UAV tracks its reference while maintaining the prescribed formation offsets. Only these four states are displayed, since pitch θ_1 and roll θ_2 ($x_{i,1}(t)$and $x_{i,2}(t), i = 1, 2, 3$) are functionally dependent on the translational dynamics, as explained earlier.

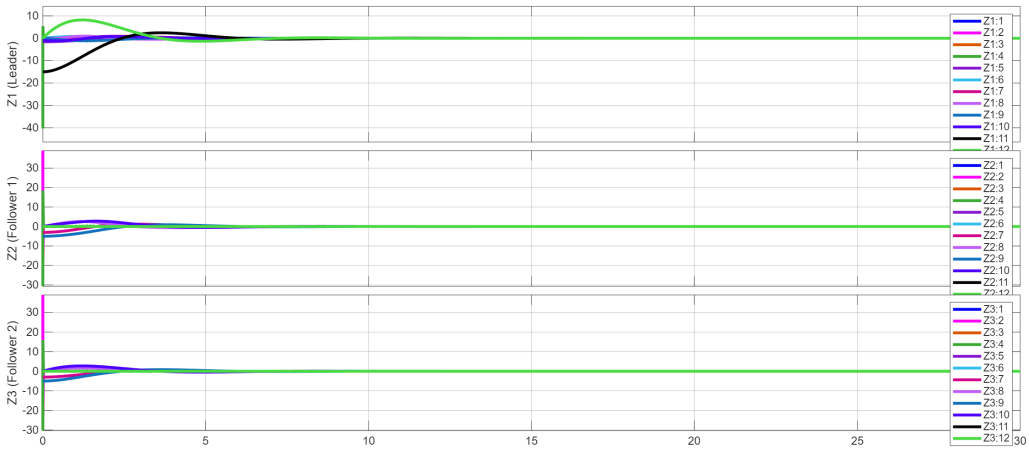


Figure 3.2: Evolution of the Z_i, for $i = 1, 2, 3$ (as defined in (3.35) for all three UAVs under the nominal case (without sampling, quantization, robustness, or event-triggering effects).

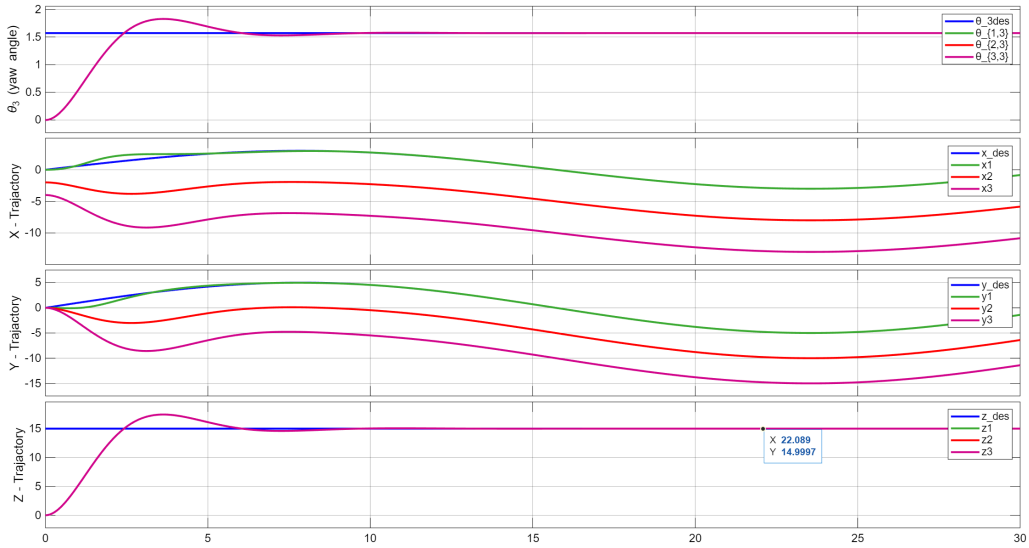


Figure 3.3: Desired and actual trajectories of θ_3 (heading) and x, y, z (position states) for the three UAVs under the nominal case (without sampling, quantization, robustness, or event-triggering effects)

Case 2 – **Sampling and Quantization:** In this case, the controllers are implemented with uniform sampling ($\delta = 0.0001$ [s]) and the quantization schemes $\mathcal{Q}_u^{18}, \mathcal{Q}_z^{36}, \mathcal{Q}_r^{72}$ as defined in the previous section. No event–triggered mechanism, disturbances, or robustification term is applied. The control gains $K_{i,j}$ remain unchanged.

The evolution of the Z variables (as defined in (3.35)) for this setup is shown in Fig. 3.4, and the corresponding trajectories of motion states $(x_{i,5}(t), x_{i,7}(t), x_{i,9}(t), x_{i,11(t)}, i = 1, 2, 3)$ of all agents are illustrated in Fig. 3.5. From these figures, it can be observed that the introduction of sampling and quantization causes small variations in the control response, particularly visible as minor oscillations or overshoot during the transient phase. These effects are expected, as quantization introduces discretization errors in the control and measurement signals, and sampling inherently limits the control update rate.

Despite these small variations, the system performs reliably overall. After a brief transient phase, all agents settle into steady state and accurately follow their desired trajectories with essentially zero steady–state error. This shows that the control design is quite robust, as it maintains stable and precise performance even when practical factors like sampling and quantization are introduced.

Case 3 – **Sampling, Quantization, and Event-Triggered Control:** Here, the system is subjected to the same sampling and quantization settings as in Case 2, but an event–triggered control mechanism is activated to reduce unnecessary control updates. Disturbances and robustification are still not applied, while the control gains remain as previously defined.

The evolution of the Z variables (as defined in (3.35)) for this configuration is shown in Fig. 3.6, and the corresponding motion trajectories $(x_{i,5}(t), x_{i,7}(t), x_{i,9}(t), x_{i,11(t)}, i = 1, 2, 3)$ of the agents are presented in Fig. 3.7. Compared to Case 2, a very small steady–state error is now observable. Although it is minimal and barely noticeable in the figures, this error arises because the event–triggered mechanism reduces the frequency of control updates, which slightly limits the system's ability to fully compensate for quantization effects. In other words, the control input is only updated when necessary, so small discrepancies can persist in steady state. Despite this, the overall performance remains highly satisfactory, with all agents closely following their desired trajectories and the tracking error remaining negligible.

Case 4 – **Sampling, Quantization, Event–Triggered Control with Disturbances:** This scenario extends Case 3 by introducing external disturbances $d_{i,k}(t)$ as defined earlier, emulating realistic noise and perturbations. Sampling, quantization, and event–triggered updates remain active, while robustification is still not applied.

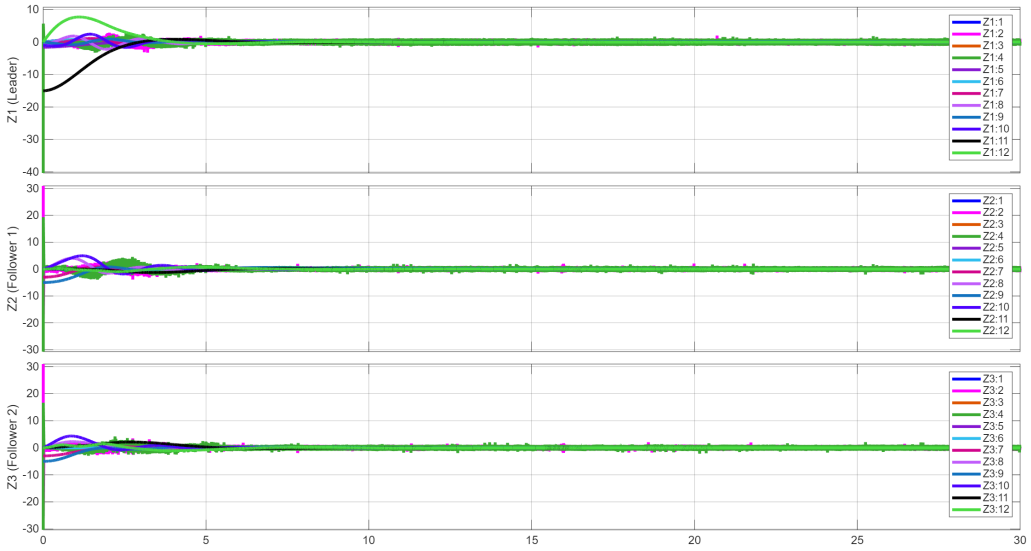


Figure 3.4: Evolution of the Z_i, for $i = 1, 2, 3$ (as defined in (3.35) for all three UAVs with sampling and quantization only.

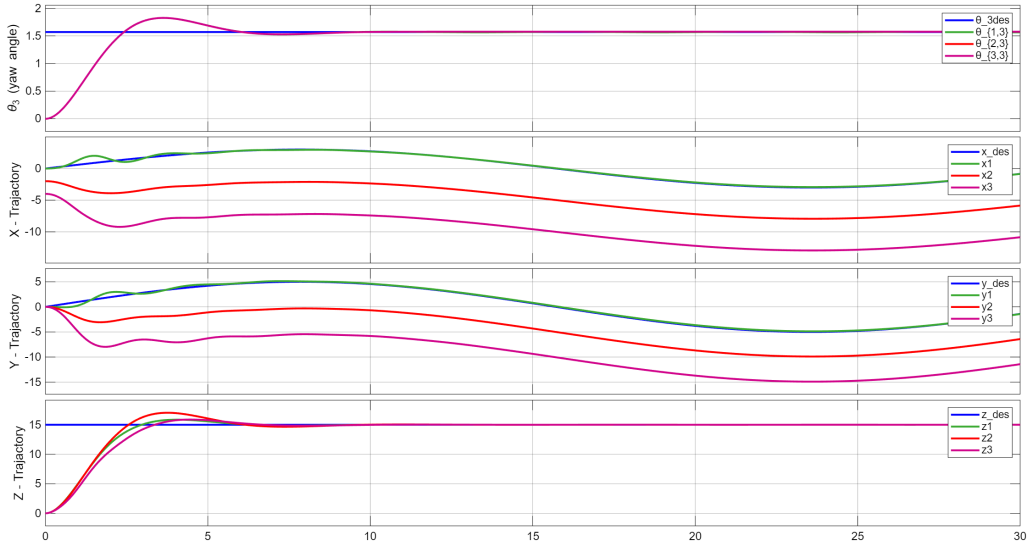


Figure 3.5: Desired and actual trajectories of θ_3 (heading) and x, y, z (position states) for the three UAVs with sampling and quantization only.

The evolution of the Z (as defined in (3.35)) variables for this configuration is shown in Fig. 3.8, and the corresponding motion trajectories $(x_{i,5}(t), x_{i,7}(t), x_{i,9}(t), x_{i,11(t)}, i = 1, 2, 3)$ of the agents are presented in Fig. 3.9. From the figures, it can be seen that the introduction of disturbances clearly affects how the system behaves. The Z variables show oscillations and noticeable overshoots, which reflect how the disturbances influence coordination between agents. In the same way, the motion trajectories slightly deviate from their intended paths, meaning the system cannot maintain perfect synchronization once noise is present.

Even with these effects, the system stays stable, and the agents continue to move in a coordinated manner. These results are important because they show how external disturbances impact performance and coordination. This case gives a good baseline for comparison, showing the system's sensitivity to noise and setting up the next case, where a robustification term is added to reduce these effects and improve the overall performance.

Case 5 – Sampling, Quantization, Event-Triggered Control with Disturbances and Robustification: Finally, the robustness of the proposed control scheme is evaluated by

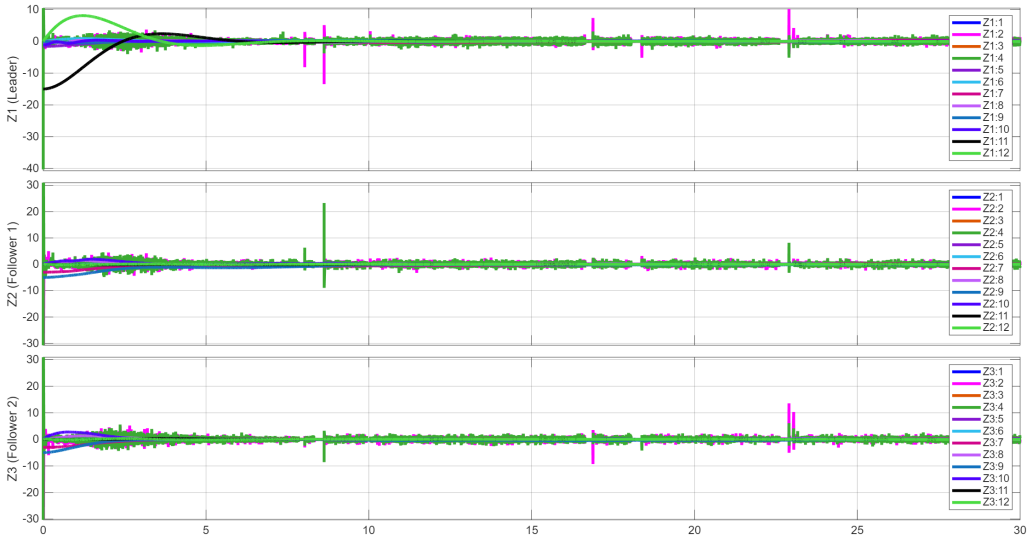


Figure 3.6: Evolution of the Z_i, for $i = 1, 2, 3$ (as defined in (3.35) for all three UAVs with sampling, quantization and event triggered control.

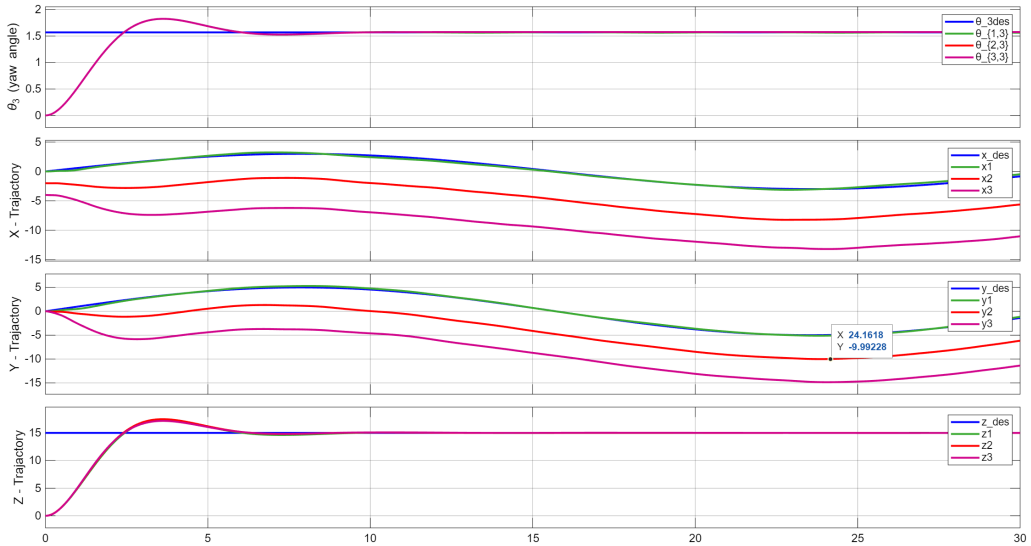


Figure 3.7: Desired and actual trajectories of θ_3 (heading) and x, y, z (position states) for the three UAVs with sampling, quantization and event triggered control.

activating the robustification term $\omega = 1$ in addition to the sampling, quantization, event-triggered control, and disturbances from Case 4. This case demonstrates the combined effect of all mechanisms on the system performance.

The evolution of the Z (as defined in (3.35)) variables and the corresponding motion trajectories $(x_{i,5}(t), x_{i,7}(t), x_{i,9}(t), x_{i,11(t)}, i = 1, 2, 3)$ are shown in Fig. 3.10 and Fig. 3.11, respectively. Compared to the previous case, the overall response shows a noticeable improvement in the motion trajectories. The agents now stay much closer to their intended paths, showing fewer deviations and smaller steady–state errors. This improvement is especially clear in the trajectory plots, where the impact of disturbances is noticeably reduced.

Overall, adding the robustification term makes the system perform better under disturbance conditions. The agents move more smoothly and accurately while staying better synchronized, demonstrating that the added robustness leads to a clear performance boost.

Looking at all five cases together really shows how the system evolves as more realistic

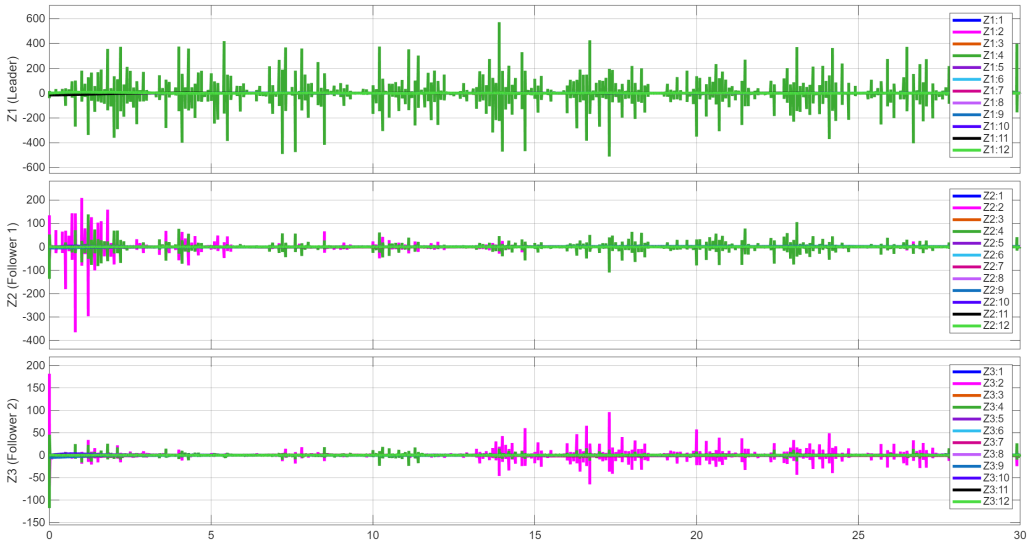


Figure 3.8: Evolution of the Z_i, for $i = 1, 2, 3$ (as defined in (3.35) for all three UAVs with sampling, quantization, event triggered control and disturbances

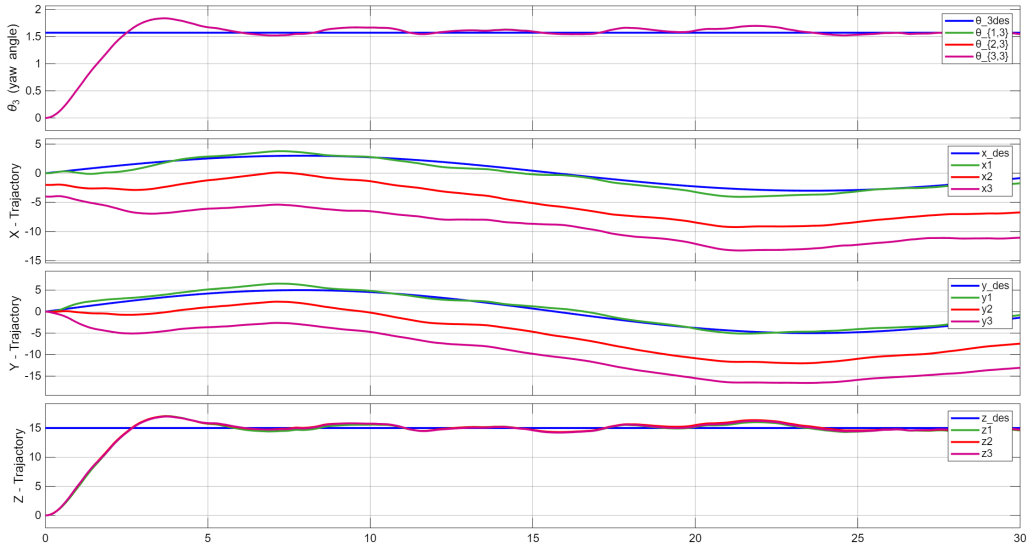


Figure 3.9: Desired and actual trajectories of θ_3 (heading) and x, y, z (position states) for the three UAVs with sampling, quantization, event triggered control and disturbances.

conditions are added. In the simplest, nominal case, without any sampling, quantization, or disturbances, the UAVs followed their desired paths almost perfectly, keeping their formation just as intended. This gives a clear picture of how well the baseline controller works under ideal conditions.

When sampling and quantization were introduced, small oscillations appeared during transients, but the UAVs still managed to settle accurately on their target paths. This shows that the control design can handle practical implementation effects without losing stability or precision. Adding the event–triggered control mechanism slightly reduced the control update frequency, which led to tiny steady–state errors. Still, the agents tracked their paths closely, showing that efficiency can be improved without sacrificing performance.

Introducing disturbances in the fourth case made the challenge more noticeable. The agents' trajectories showed slight deviations, and oscillations became visible, highlighting how external noise and perturbations can affect coordination. But when the robustification term was finally included, the system's resilience became clear: the UAVs stayed much

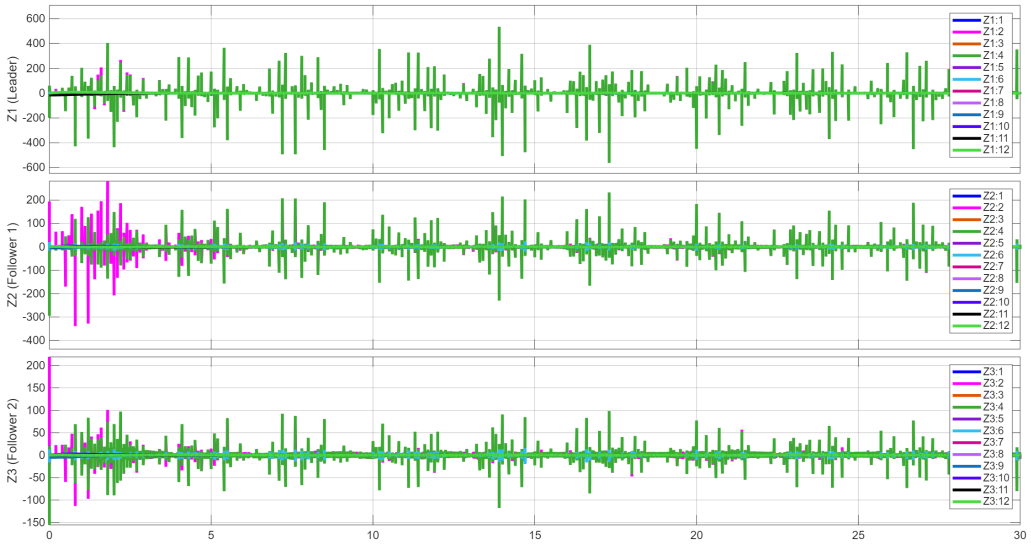


Figure 3.10: Evolution of the Z_i, for $i = 1, 2, 3$ (as defined in (3.35) for all three UAVs with sampling, quantization, event triggered control with disturbances and robustification.

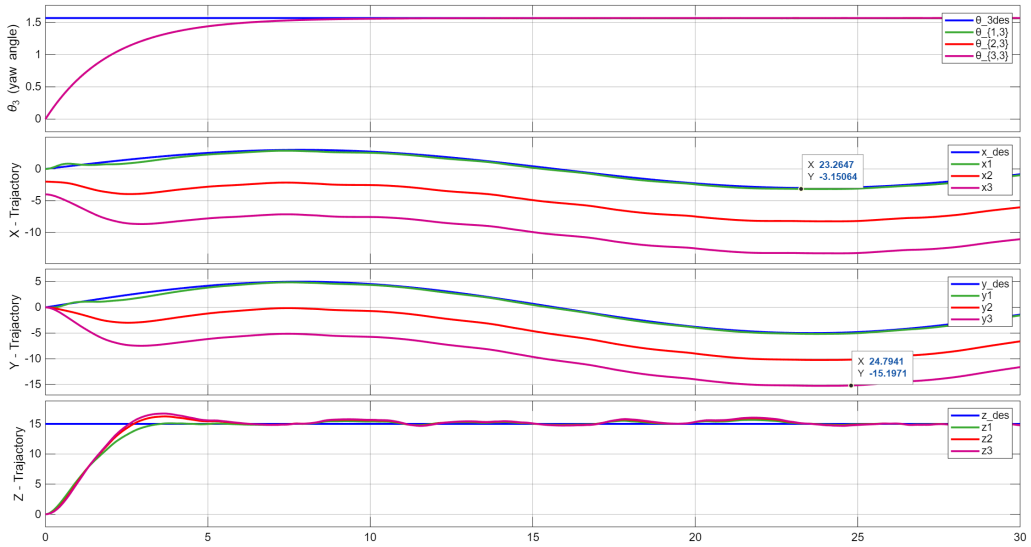


Figure 3.11: Desired and actual trajectories of θ_3 (heading) and x, y, z (position states) for the three UAVs with sampling, quantization, event triggered control with disturbances and robustification.

closer to their intended paths, moved more smoothly, and maintained synchronization even under disturbances. The robustification essentially acted as a buffer, allowing the system to cope with real–world uncertainties.

Overall, these results illustrate a clear progression: each enhancement—-sampling and quantization handling, event–triggered control, and robustification-—contributes to improved performance under increasingly realistic conditions. The study demonstrates that the proposed control framework not only achieves accurate trajectory tracking and formation maintenance but also provides resilience against disturbances, noise, and practical implementation constraints. This confirms that the approach is both reliable and practical, making it a compelling solution for real–world multi–agent coordination tasks.

Chapter 4

Security Analysis

This chapter is dedicated to the analysis of security threats in the context of FSM, which serve as a fundamental modeling framework for a wide range of DES. We investigate three main problem areas: active attacks on single–agent systems, active attacks on multi–agent networks, and passive observation–based attacks, each addressed through distinct but interconnected theoretical contributions.

We begin by examining active attacks on a single FSM, focusing on actuator attacks where an adversary interferes with the system's control channel. A formal model combining the nominal FSM and an attacker FSM is developed to study the dynamics under attack. Within this framework, we derive necessary and sufficient conditions for attack detection and localization, enabling the identification of both the presence and location of attacks. This work was presented in [59].

The analysis is then extended to a networked setting, where multiple agents each modeled as an FSM interact through shared outputs over potentially compromised communication links. In this decentralized framework, we propose a compositional model that captures the joint evolution of the agents and the attacker. The chapter provides detection and localization conditions that ensure each agent can assess the integrity of overall system, even in the presence of attacks targeting the network's inter–agent channels. The results of this study are accepted for publication in [138].

Finally, we turn to passive attacks, where an adversary attempts to infer sensitive system behavior without directly interfering with its operation. To address this, we explore the system property of opacity, which prevents an observer from confidently determining whether the system has entered a secret state. Verifying opacity often requires constructing a full observer, which can be computationally prohibitive for large–scale systems. To mitigate this, we propose a decomposition-based observer framework by introducing the concept of total indistinguishability. This approach allows for the design of efficient sub–observers that collectively preserve the observability properties needed for opacity analysis, thereby reducing the overall computational complexity. This work was published is [139].

Together, these three lines of work form a comprehensive approach to security analysis in FSM-based systems, addressing both detection and localization of attacks.

4.1 Active Attacks

4.1.1 Attack Detection for a Single Agent

For attack detection in a single agent, we consider the framework shown in Fig. 4.1. The architecture is composed of a plant M, a static function Net and an attacker M_a. The plant M is an FSM as in (2.4), i.e.

$$M = (X, X_0, E, Y, \Delta, H) \tag{4.1}$$

Similarly, the attacker M_a is represented as:

$$M_a = (X_a, X_{0a}, E_a, Y_a, \Delta_a, H_a) \tag{4.2}$$

For the attacker, $E_a = \{@_a\}$, is considered, as only the output is relevant for security analysis; the internal event has no effect on the nominal plant, and the attacker influences the system solely through its outputs that drive the plant's state evolution, and $H_a : X_a \to Y_a$.

The block $\mathcal{N}$ in Fig. 4.1 represents a communication network that is modeled as the static function:

$$\mathcal{N} : E \times Y_a \to (E \cup Y_a)$$

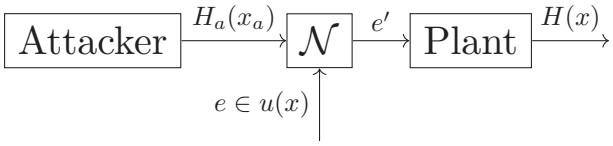


Figure 4.1: Plant under actuator attack

where $\mathcal{N}(e, H_a(x_a)) = e$, if no attack occurs, and $\mathcal{N}(e, H_a(x_a)) = H_a(x_a)$, otherwise. Here, $H_a(x_a)$ represents the output of the attacker at state x_a. The corrupted input $e' = \mathcal{N}(e, H_a(x_a))$.

We assume that M and M_a are synchronized in terms of state transitions. As it is shown in Fig. 4.1, the attacker can replace e with $e' \in Y_a$, which may or may not belong to E. If the corrupted event $e' \notin E$, then no state evolution occurs in the plant M, as such an event cannot trigger any valid transition. It is important to note that the output associated with state transition, represents the information on the actual input of the plant ($e \in E$), instead of corrupted input ($e' \in Y_a$).

Let $X_a = X_{a,off} \cup X_{a,on}$, where $X_{a,off}$ is the set of states in which the attacker is off, $X_{a,on}$ is the set in which the attacker is on and makes a replacement. We suppose that X_{0a} is a singleton x_{0a} in the set $X_{a,off}$.

For further analysis on attack detection at actuator side, we make the following assumptions:

Assumption 4.1.1

FSM M is alive, i.e., $\forall x \in X, succ\,(x) \neq \varnothing$. □

Assumption 4.1.2

Attacker is only capable of replacing the event $e \in E$ with some value e', which may or may not belong to E. Event removal is considered here as a special case of event replacement i.e. when the attacker replaces e, with e' such that $e' \notin u(x)$. However, the injection attack is not discussed in this work. □

Assumption 4.1.1 ensures that the FSM remains active at all times, meaning that from every state there is at least one possible successor. This avoids deadlock situations and allows the analysis to focus on ongoing system behavior under potential attacks. Assumption 4.1.2 restricts the attacker's capability to event replacement, which captures a broad range of realistic tampering actions while keeping the model tractable. Event removal is treated as a special case of replacement. As stated earlier, for the nominal plant M the input event is also observable as an output. Therefore, in the case of injection attacks where the attacker introduces new data instead of replacing existing events, the injected transition would immediately produce an unexpected output, making such attacks detectable as soon as they occur. For this reason, injection attacks are not considered within the current framework.

Here we analyze the security of FSM by using the notion of "indistinguishable" FSM runs.

Definition 4.1.1

Given two FSM M_1 and M_2 of the form (2.4), two runs r_1 and r_2 as indicated in (2.5) of M_1 and M_2, respectively, are indistinguishable if $y_1(r_1) = y_2(r_2)$, where y_1 and y_2 are functions associated with M_1 and M_2. □

During a state transition, starting from $x \in X$ with event $e \in u(x)$, if an attacker replaces the event e with $e' \in u(x)$, the resulting state transition will be called corrupted if $(x, e, x') \in \Delta \wedge (x, e', x'') \in \Delta \wedge x' \neq x''$. If $e' \notin u(x)$ no transition occurs in the plant, and plant M, generate ϵ as the output of the state. This may or may not lead to immediate detection of an attack, depending on the presence of silent states in the plant M. A run that includes at least one corrupted transition is called a corrupted run. For a given event

run $r_e \in \mathbb{E}$ and initial state $x_1 \in X_0$, let $\mathcal{R}^{(r_e,x_1)}$ represent the set of uncorrupted FSM runs and $\mathcal{R}_a^{(r_e,x_1)}$ the set of corrupted FSM runs.

Moreover, we make the following assumption:

Assumption 4.1.3

$pre(x_a) \subset X_{a,on}, \forall x_a \in succ(X_{a,on})$. □

Assumption 4.1.3 has been made to ensure that all the states reachable from a corrupted state transition are not reachable from uncorrupted state transitions.

Here, two different notions of security are discussed in terms of attack detectability. For a given infinite FSM run $r \in \mathcal{R}$ of the form (2.5), let $\hat{k} \in \mathbb{N}$ be the smallest value of k, such that the transition associated with (x_k, e_k, x_{k+1}) is corrupted. $k = \infty$, represents the absence of attack.

The FSM is called "Secure" if the attack is detectable immediately or after some delay.

Definition 4.1.2

(Security) FSM M is secure to attacker if there exists $d \in \mathbb{Z}$, such that for all infinite input runs $r_e \in \mathbb{E}$, starting from any initial state $x_1 \in X_0$, and for all uncorrupted runs $r \in \mathcal{R}^{(r_e,x_1)}$ and corrupted runs $r' \in \mathcal{R}_a^{(r_e,x_1)}$, the following holds

$$y(r)|_{[1,k+d+1]} \neq y(r')|_{[1,k+d+1]} \tag{4.3}$$

M is called strongly secure if $d = 0$. □

From the definition above, M is secure if there are no pairs of corrupted and uncorrupted runs with corresponding output runs coinciding.

We now introduce the notion of "Always Security", where it is possible to detect an attack, immediately or after some delay, whenever it occurs.

Definition 4.1.3

(Always Security) M is always secure if there exists $d \in \mathbb{Z}$, such that, given a run r, whenever the transition $(x_{\hat{k}}, e_{\hat{k}}, x_{\hat{k}+1})$ is corrupted, the information collected up to $\hat{k}+d+1$, (i.e. $y(r)_{[1,\hat{k}+d+1]}$), is sufficient to establish that an attack occurred at some $k \in [\hat{k}, \hat{k}+d]$. M is called always strongly secure if $d = 0$. □

The above notions of Security and Always Security are introduced directly in terms of attack detectability along system executions. At this stage, these definitions are presented independently of existing diagnosability concepts. Their connection to classical diagnosability notions in the DES literature will be developed later in this chapter, where we show that Security and Always Security can be characterized through diagnosability and critical diagnosability properties, respectively.

4.1.1.1 Composed Finite State Machine

Here we present a composed system that describes the behavior of Plant M, in the presence of attacker M_a, at the actuator side:

$$\begin{aligned} \widehat{M_a} &= \left(\widehat{X}_a, \widehat{X}_{0a}, E, Y, \widehat{\Delta}_a, \widehat{H}_a\right) \\ &= Ac\left((X \cup X^+) \times X_a, \widehat{X}_{0a}, E, Y, \widehat{\Delta}_a, \widehat{H}_a\right) \end{aligned} \tag{4.4}$$

where $Ac(.)$ represents the accessible part as mentioned in (2.9) and:

- $\widehat{X}_a$ is the finite set of states;
- X^+ is the finite set of duplicate states of M, such that:

$$((x_i^+ \in X^+) \wedge (x_i \in X) \wedge (x_i^+ = x_i))$$

- $\widehat{X}_{0a} = X_0 \times X_{0a} \subset \widehat{X}_a$ is the set of initial states;
- $\widehat{\Delta}_a \subset \widehat{X}_a \times E \times \widehat{X}_a$ is the transition relation, defined as follows: given $(x, x_a) \in \widehat{X}_a$, $\widehat{\Delta}_a$ is the set of all transitions $\widehat{\delta}_a = ((x, x_a), e, (x', x'_a)) \in \widehat{X}_a \times E \times \widehat{X}_a$ such that

$$(H_a(x_a) = \epsilon) \wedge ((x, e, x') \in \Delta) \wedge ((x_a, @_a, x'_a) \in \Delta_a) \tag{4.5}$$

or

$$(H_a(x_a) = e) \wedge ((x, e, x') \in \Delta) \wedge ((x_a, @_a, x'_a) \in \Delta_a) \tag{4.6}$$

or

$$(H_a(x_a) \notin u(x)) \wedge (e \in u(x)) \wedge (x' = x) \wedge ((x_a, @_a, x'_a) \in \Delta_a) \tag{4.7}$$

- $\widehat{H}_a : (\widehat{X}_a \cup \widehat{\Delta}_a) \to 2^Y$ is the output function where

  - if $\widehat{\delta}_a$ satisfies (4.5), then $\widehat{H}_a(\widehat{\delta}_a) = \{e\}$;
  - if $\widehat{\delta}_a$ satisfies (4.6) or (4.7), then $\widehat{H}_a(\widehat{\delta}_a) = u(x)$;
  - if $(x', x'_a) \in \widehat{X}_a$ is such that $((x, x_a), e, (x', x'_a))$ satisfies (4.7), then $\widehat{H}_a((x', x'_a)) = \{\epsilon\}$, otherwise $\widehat{H}_a((x', x'_a)) = \{H(x')\}$.

The point to set mapping $\widehat{H}_a$ above has been introduced to model the fact that, whatever the input event $e \in u(x)$ is, if $H_a(x_a) \neq \epsilon$ the attacker replaces it with the event $H_a(x_a)$, but the output information available to the monitoring system is the current value of e, i.e. the event before the attack occurs. The output for a state of $\widehat{M}_a$ which is the incoming state of the transition satisfying (4.7) has been set to ϵ to represent the fact that, whatever the input event $e \notin u(x)$ is, the plant M cannot evolve.

If attacker replaces e with e', such that $(x, e, x') \in \Delta$ and $(x, e', x'') \in \Delta$ and $x' \neq x''$, then the state (x', x'_a) of composed model $\widehat{M}_a$, is called corrupted state. The set Ω_a is the set of all corrupted states.

4.1.1.2 Main Results

Let $S^*_a \subset \widehat{X}_a \times \widehat{X}_a$ be the set of states of $\widehat{M}_a$ reached by two indistinguishable runs of $\widehat{M}_a$. Also define $\Omega^1_a \subset \Omega_a$, as the set of states reached by a state run of $\widehat{M}_a$, that never crosses Ω_a before, i.e. there exists a state run of $\widehat{M}_a$ such that $x_k \in \Omega_a \wedge x_h \notin \Omega_a, \forall h < k$ or $x_1 \in \Omega_a$. Let S^{*1}_a be the set of states of $\widehat{M}^1_a$ reached by two indistinguishable runs of $\widehat{M}^1_a$, where $\widehat{M}^1_a$ is the accessible part of the FSM obtained by $\widehat{M}_a$ by removing the transitions starting from Ω^1_a. Obviously $S^{*1}_a \subset S^*_a$.

Set S^*_a can be easily computed by first transforming FSM $\widehat{M}_a$ into a pure Moore FSM, where all output information is associated with states.

Next, we recall the recursion from [140], [141], to compute Set S^*_a. Let

$$\Pi = \{(\widehat{x}_a, \widehat{x}'_a) \in \widehat{X}_a \times \widehat{X}_a : \widehat{H}_a(\widehat{x}_a) = \widehat{H}_a(\widehat{x}'_a)\},$$

and

$$S_1 = (\widehat{X}_{0a} \times \widehat{X}_{0a}) \cap \Pi,$$

define for $i = 1, 2, 3....$

$$S_{i+1} = \{(\widehat{x}_a, \widehat{x}'_a) \in \Pi : (pre(\widehat{x}_a) \times pre(\widehat{x}'_a)) \cap S_i \neq \varnothing\} \cup S_i. \tag{4.8}$$

It is stated in [140], the least fixed point of recursion, containing $(\widehat{X}_{0a} \times \widehat{X}_{0a}) \cap \Pi$, exists, is unique, and is equal to S^*_a.

Next, we provide a proposition that uses the set S^*_a to give a formal criterion for M to be strongly secure with respect to M_a.

Proposition 4.1.1

M is strongly secure under attacker M_a if and only if:

$$S_a^{*1} \cap ((\Omega_a^1 \times \overline{\Omega_a^1}) \cup (\overline{\Omega_a^1} \times \Omega_a^1)) = \varnothing, \tag{4.9}$$

where $\overline{\Omega_a^1}$ is the complement of Ω_a^1 in $\widehat{X}_a$. □

Proof. If the current state $x_k \in \Omega_a^1 \subset \Omega_a$, then, by Assumption 4.1.3, the transition from x_{k-1} to x_k was corrupted. Condition (4.9) means that it is not possible to reach with two indistinguishable runs of $\widehat{M}_a^1$ a pair of states, one belonging to Ω_a^1 and the other not belonging to Ω_a^1. Therefore, by definition of $\widehat{M}_a^1$, the result follows. □

Proposition 4.1.2

M is always strongly secure under attacker M_a if and only if:

$$S_a^{*} \cap ((\Omega_a \times \overline{\Omega_a}) \cup (\overline{\Omega_a} \times \Omega_a)) = \varnothing \tag{4.10}$$

where $\overline{\Omega_a}$ is the complement of Ω_a in $\widehat{X}_a$. □

Proof. As in the proof of Proposition 4.1.1, if the current state $x_k \in \Omega_a$, then the transition from x_{k-1} to x_k was corrupted. Condition (4.10) means that it is not possible to reach with two indistinguishable runs of $\widehat{M}_a$ a pair of states, one belonging to Ω_a^1 and the other not belonging to Ω_a^1. Therefore, the result follows. □

By using the terminology introduced in [140] and [141], equations (4.9) and (4.10) are necessary and sufficient for $\widehat{M}_a$ to be observable with respect to Ω_a and critically observable with respect to Ω_a, respectively.

Next we recall the the notions of diagnosability and critical diagnosability from [140]. For any state run $r_x \in \chi$, as defined in (2.7), there are two possible cases, either $r_x(k) \notin \Omega, \forall k \in \mathbb{N}$, or $r_x(k) \in \Omega$, for some $k \in \mathbb{N}$. Let k_x be the minimum value associated to a state run $r_x \in \chi$, such that $r_x(k_x) \in \Omega$

Definition 4.1.4

Diagnosability: The FSM M is diagnosable with respect to a critical set $\Omega \subset X$ if there exist $\delta \in \mathbb{N}$, such that for any $r_x \in \chi$, for which $k_x \neq \infty$, it follows that for any string $r'_x \in y^{-1}(y(r_x|_{[1,k_x+\delta]}))$, $r'_x(h) \in \Omega$, for some $h \in [max\{1, k_x - \lambda_1\}, k_x + \lambda_2]$, for some $\lambda_1, \lambda_2 \in \mathbb{N}$ and $\lambda_2 \leq \delta$. □

Definition 4.1.5

Critical Diagnosability: The FSM M is critically diagnosable with respect to a critical set $\Omega \subset X$ if there exist $\delta \in \mathbb{N}$, such that for any $r_x \in \chi$, for which $k_x \neq \infty$, whenever $r_x(k) \in \Omega$, it follows that for any string $r'_x \in y^{-1}(y(r_x|_{[1,k+\delta]}))$, $r'_x(h) \in \Omega$, for some $h \in [max\{1, k - \lambda_1\}, k + \lambda_2]$, for some $\lambda_1, \lambda_2 \in \mathbb{N}$ and $\lambda_2 \leq \delta$. □

From Definition 4.1.4 and Definition 4.1.5 it is easy to prove the following result:

Proposition 4.1.3

M is secure under M_a if and only if $\widehat{M}_a$ is diagnosable with respect to Ω_a. M is always secure under M_a if and only if $\widehat{M}_a$ is critically diagnosable with respect to Ω_a. □

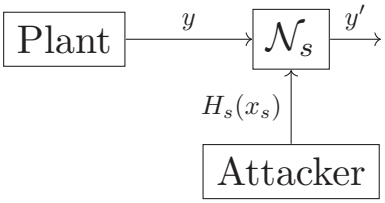


Figure 4.2: Plant under Sensor attack

4.1.2 Attack Localization for a Single Agent

The problem of attack detection at the sensor side has been discussed in [35]. Here, we extend those results, along with the results presented in the previous section, to address the problem of localization, i.e., identification of the attacked channel.

Let the FSM M_s models the dynamic for the sensor attacker shown in Fig. 4.2

$$M_s = (X_s, X_{0s}, E_s, Y_s, \Delta_s, H_s) \tag{4.11}$$

Here, $E_s = \{@_s\}$ and $H_s : X_s \to Y_s$.

Similar to the previous case of attacks at actuator side, the block $\mathcal{N}_s$ in Fig. 4.2 represents a communication network that is modeled as the static function:

$$\mathcal{N}_s : Y \times Y_s \to (Y \cup Y_s)$$

where $\mathcal{N}_s(y, H_s(x_s)) = y$, if no attack occurs, and $\mathcal{N}_s(y, H_s(x_s)) = H_s(x_s)$, otherwise. Here, $H_s(x_s)$ represents the output of the attacker at state x_s.The corrupted output $y' = \mathcal{N}(y, H_s(x_s))$.

We assume that M and M_s are synchronized and the attacker is capable of replacing any output symbol of M, which may or may not belong to the output set of plant M. We also assume that the attacker cannot remove or inject symbols in the sensor channel.

To provide conditions for security and localization we need to formalize a composed model $\widehat{M}_s$ based on the nominal plant and the attacker model of sensor attack.

$$\begin{aligned} \widehat{M}_s &= (\widehat{X}_s, \widehat{X}_{0s}, \widehat{E}_s, \widehat{Y}_s, \widehat{\Delta}_s, \widehat{H}_s) \\ &= Ac(X \times X_s, X_0 \times X_{0s}, E, Y \cup Y_s, \widehat{\Delta}_s, \widehat{H}_s) \end{aligned} \tag{4.12}$$

The composition $\widehat{M}_s$ is based on the rules formulated in [35] and [34]. In the following, we adapt these rules to our setting and present them in detail.

Set $\widehat{\Delta}_s$ contains all transitions $((x, x_s), e, (x', x'_s))$ such that,

$$\widehat{\Delta}_s = \{((x, x_s), e, (x', x'_s)) : (x, x') \in \Delta \wedge (x_s, x'_s) \in \Delta_s \wedge e \in u(x)\} \tag{4.13}$$

In our setting, the events are also available as outputs, therefore, the output map, $\widehat{H}_s : (\widehat{X}_s \cup \widehat{\Delta}_s) \to 2^{\widehat{Y}_s}$ is defined as

$$\begin{aligned} &\widehat{H}_s(x, x_s) = H_s(x) \text{ if } x_s \in X_{s,off} \\ &\widehat{H}_s(x, x_s) = H_s(x), \text{ otherwise} \\ &\widehat{H}_s((x, x_s), e, (x', x'_s)) = e \end{aligned} \tag{4.14}$$

The state (x, x_s) is called corrupted if $H(x) \neq H_s(x_s)$.

Let $\Omega_s \subset \widehat{X}_s$ be the set of all corrupted states. Also define $\Omega_s^1 \subset \Omega_s$, as the set of states reached by a state run $\widehat{M}_s$, that never crosses Ω_s before, i.e. there exists a state run of $\widehat{M}_s$ such that $x_k \in \Omega_s \wedge x_h \notin \Omega_s, \forall h < k$ or $x_1 \in \Omega_s$.

For further analysis, we make the following assumption.

Assumption 4.1.4

The attacker can replace data only at one side i.e. sensor or actuator channel, but not both. □

4.1.2.1 Main Results

To provide conditions for the detection of corrupted or attacked channel, we need to define the set $S^*_{as} \subset \widehat{X}_a \times \widehat{X}_s$, as the set of pair of states of $\widehat{M}_a$ and $\widehat{M}_s$, reachable from $\widehat{X}_{0a}$ and $\widehat{X}_{0s}$ with two runs of $\widehat{M}_a$ and $\widehat{M}_s$, respectively, which are indistinguishable. Let $S^1_{as} = \Omega^1_a \times \Omega^1_s$, and define S^{*1}_{as} as the set of pair states of $\widehat{M}^1_a$ and $\widehat{M}^1_s$ reached by two indistinguishable runs of $\widehat{M}^1_a$ and $\widehat{M}^1_s$, where $\widehat{M}^1_s$ is the accessible part of the FSM obtained from $\widehat{M}_s$ by removing transitions starting from the set Ω^1_s. Then, the following result characterizes localization.

Proposition 4.1.4

Suppose that M is strongly secure to attacker M_a and M_s. It is possible to identify the attacked channel as soon as the attack occurs if and only if:

$$S^{*1}_{as} \cap S^1_{as} = \varnothing \tag{4.15}$$

□

Proof. Suppose there is an attack in the actuator channel (or sensor channel), then under the assumption of strong security. the only condition to identify the attacked channel is that the current state $(x, x_a) \in \Omega^1_a$ (or $(x, x_s) \in \Omega^1_s$) is distinguishable from every state belonging to Ω^1_s (or Ω^1_a). Hence, the statement follows. □

Now, let us assume that M is secure under actuator attacks and it is also secure under sensor attacks, separately. Let Ψ be the subset of S^*_{as} such that for any $((x, x_a), (x', x'_s)) \in \Psi$ there are two arbitrarily long indistinguishable runs with initial states (x, x_a) and (x', x'_s), respectively.

Proposition 4.1.5

It is possible to identify the attacked channel (with some delay after the first attack) if and only if

$$(x, x_a) \notin \Omega_a \wedge (x', x'_s) \notin \Omega_s \tag{4.16}$$

$\forall((x, x_a), (x', x'_s)) \in \Psi$.

□

Proof. The sufficiency is obvious. In fact, by assumption $\widehat{M}_a$ and $\widehat{M}_s$ are alive, and condition (4.16) means that there are no two arbitrarily long corrupted indistinguishable runs of $\widehat{M}_a$ and $\widehat{M}_s$. As for necessity, suppose that (4.16) is false. Then there is an arbitrarily long actuator side (sensor side) corrupted run which is indistinguishable with a run r of $\widehat{M}_s$ ($\widehat{M}_a$, resp.). If r is not corrupted, it corresponds to a not-corrupted run of M. Since we assumed that M is secure under actuator attacks and it is also secure under sensor attacks, separately, then such a run r has to be corrupted. Hence, condition (4.16) is necessary. □

4.1.3 Example: Attack Detection and Localization for a Single Agent

4.1.3.1 Attack Detection

Consider the plant FSM M shown in Fig. 4.3 and the attacker model M_a in Fig. 4.4a. The composed model $\widehat{M}_a$ is shown in Fig. 4.5. The transitions of the composed model are based on the rules in (4.5), (4.6) and (4.7). The output associated with each state of $\widehat{M}_a$, is assigned using the output function $\widehat{H}_a$.

Next, we convert our composed model $\widehat{M}_a$ into a pure Moore Machine as shown in Fig. 4.6a. For the composed model $\widehat{M}_a$ in Fig. 4.6a, set S^{*1}_a can be computed using the algorithm presented in (4.8).

$$S^{*1}_a = \{((1, 0_a), (1, 1_a)), ((3, 0_a), (3, 1_a)), ((2, 0_a), (2, 1_a))\}$$

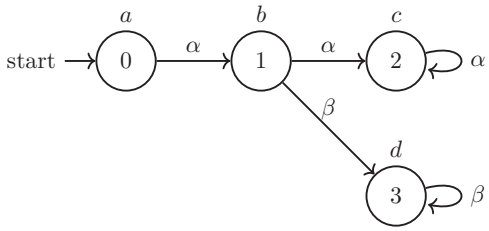
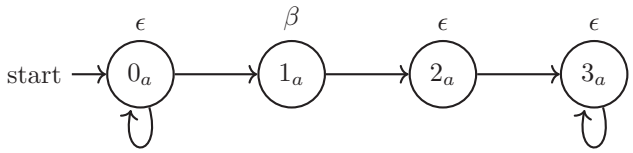
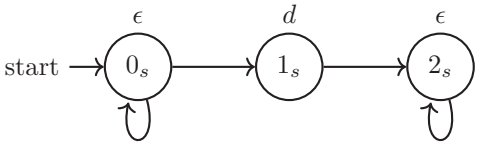


Figure 4.3: The Nominal Plant FSM model M



(a) Actuator Attacker Model



(b) Sensor Attacker Model

Figure 4.4: The Actuator and Sensor Attacker FSM

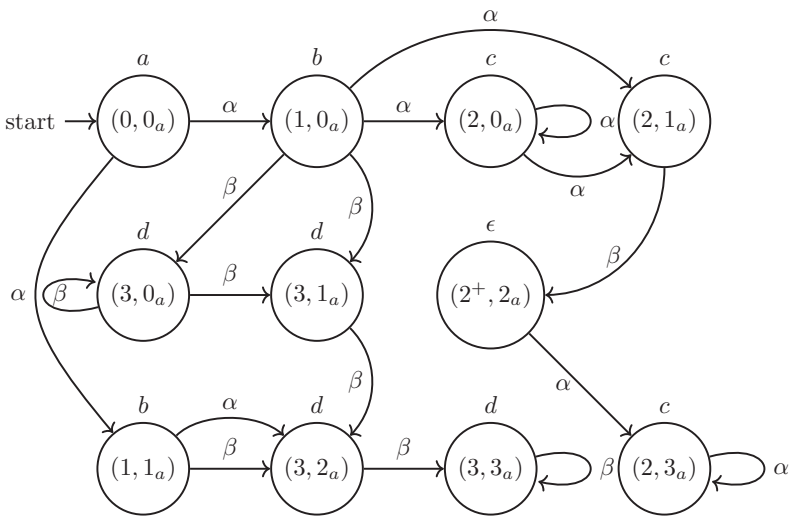
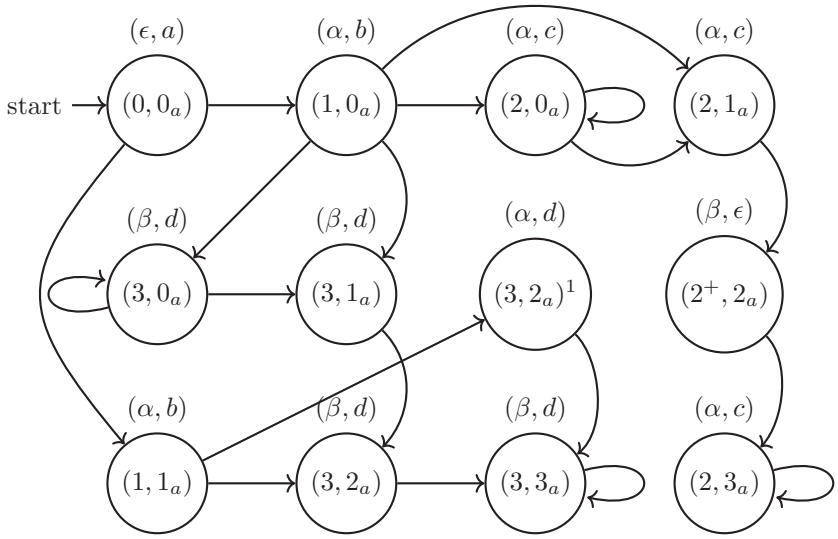
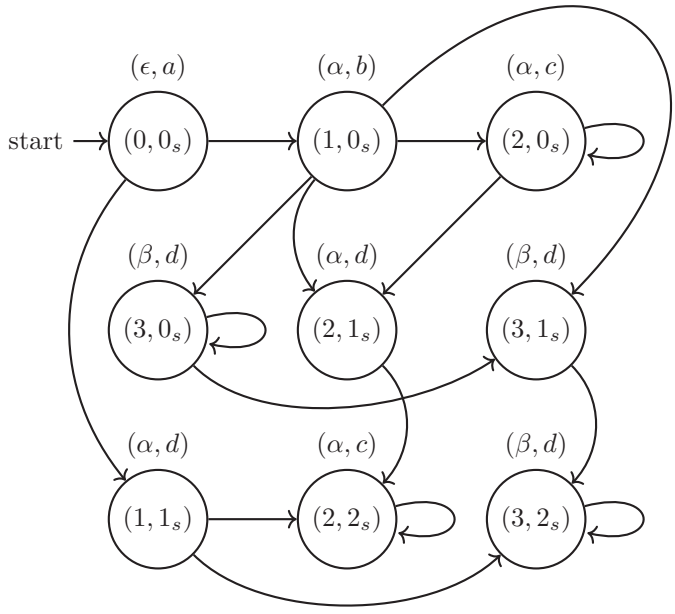


Figure 4.5: Composed FSM $\widehat{M}_a$



(a) Composed Model $\widehat{M}_a$



(b) Composed Model $\widehat{M}_s$

Figure 4.6: Composed models $\widehat{M}_a$ and $\widehat{M}_s$

Similarly the sets Ω_a^1 and Ω_a are:

$$\Omega_a^1 = \{(3, 2_a)^1, (2^+, 2_a)\},\ \Omega_a = \{(3, 2_a)^1, (2^+, 2_a)\}$$

and the sets $\overline{\Omega_a^1}$, $\overline{\Omega_a}$, are:

$$\overline{\Omega_a^1} = \overline{\Omega_a} = \{(0, 0_a), (1, 0_a), (2, 0_a), (2, 1_a), (3, 0_a), (3, 1_a), (1, 1_a), (3, 2_a), (3, 3_a), (2, 3_a)\}$$

Recalling the conditions of Proposition 4.1.1 ($S_a^{*1} \cap ((\Omega_a^1 \times \overline{\Omega_a^1}) \cup (\overline{\Omega_a^1} \times \Omega_a^1)) = \varnothing$), and Proposition 4.1.2 ($S_a^* \cap ((\Omega_a \times \overline{\Omega_a}) \cup (\overline{\Omega_a} \times \Omega_a)) = \varnothing$), we observe that both are satisfied by the computations above. As a consequence, M is strongly and always strongly secure with respect to M_a.

4.1.3.2 Localization

Consider the same nominal plant model M in Fig. 4.3 and the sensor attacker M_s in Fig. 4.4b. Based on the rules presented in (4.13) and (4.14) , the composed model is shown in Fig. 4.6b. For simplicity, we converted the composed model into a pure Moore machine.

The composed model $\widehat{M_s}$ is in Fig. 4.6b. The set S_{as}^{*1} can be computed using (4.8) as:

$$\begin{aligned} S_{as}^{*1} = \{&((0, 0_a), (0, 0_s)), ((1, 0_a), (1, 0_s)), ((1, 1_a), (1, 0_s)), \\ &((2, 0_a), (2, 0_s)), ((2, 1_a), (2, 0_s)), ((3, 0_a), (3, 0_s)), ((3, 1_a), \\ &(3, 0_s)), ((3, 0_a), (3, 1_s)), ((3, 1_a), (3, 1_s)), ((3, 2_a)^1, (2, 1_s)), \\ &((3, 2_a), (3, 0_s)), ((3, 2_a), (3, 1_s))\} \end{aligned}$$

and Ω_a^1 and Ω_s^1, are:

$$\Omega_a^1 = \{(3, 2_a)^1, (2^+, 2_a)\}, \Omega_s^1 = \{(2, 1_s), (1, 1_s)\}$$

Clearly

$$S_{as}^{*1} \cap S_{as}^1 = \{((3, 2_a)^1, (2, 1_s))\}$$

Hence, condition of Proposition 4.1.4 ($S_{as}^{*1} \cap S_{as}^1 = \varnothing$) is not satisfied, hence we can conclude it is not possible to identify the attacked channel instantly.

Finally, Ψ is given by:

$$\Psi = \{((0, 0_a), (0, 0_s)), ((1, 0_a), (1, 0_s)), ((1, 1_a), (1, 0_s))\}$$

It is clear that for all pair of states in Ψ, conditions of Proposition 4.1.5 ($(x, x_a) \notin \Omega_a \wedge (x', x_s') \notin \Omega_s$) is satisfied. Hence, in this case, it is possible to identify the attacked channel after some delay.

4.1.4 Attack Detection for a Network of Agents

We extend the results obtained in the previous sections for a single agent to a network of agents. In this setting, the agents are modeled as FSM, interconnected via output feedback composition, and share their output information through vulnerable communication channels. An attacker can act on the communication links between agents. A composed model is first developed to represent the evolution of the entire network in the presence of attacks. Based on this model, necessary and sufficient conditions are derived to ensure the detectability and localizability of the attacked channel.

Here, we consider a *Network of Agents* (NoA) composed of two systems P_1 and P_2, an attacker P_A, acting on the communication infrastructure, as shown in Fig. 4.7, where we are assuming that attacker P_A corrupts information sent by P_1 to P_2. The models of P_1, P_2 and P_A are FSM, described by difference inclusions as in (2.10).

The FSM model of attacker P_A is given by:

$$P_A = \begin{cases} x_A(t+1) \in F_A(x_A(t), u_A(t)), \\ x_A(0) \in X_{A,0}, \\ y_A(t) = h_A(x_A(t)), \\ x_A(t) \in X_A, u_A(t) \in U_A, t \in \mathbb{N}, \end{cases} \tag{4.17}$$

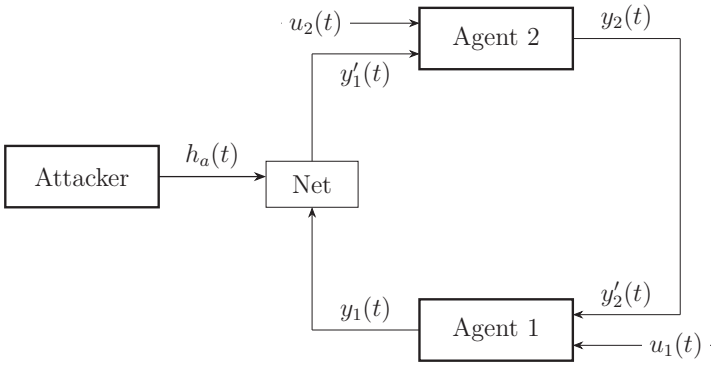


Figure 4.7: Agents interconnection in NoA.

Let $X_A = X_{A,off} \cup X_{A,on}$, where $X_{A,off}$ is the set of states in which the attacker is off, $X_{A,on}$ is the set of states in which the attacker is on and makes a replacement.

The two interconnected agents, in the presence of attack, are described using the following difference inclusion:

$$P_i = \begin{cases} x_i(t+1) \in F_i(x_i(t), y'_{3-i}(t), u_i(t)), \\ x_i(0) \in X_{i,0}, \\ y_i(t) = h_i(x_i(t)), y_{3-i}(t) = h_{3-i}(x_{3-i}(t)), \\ y'_{3-i}(t) = Net(y_{3-i}(t), y_A(t)), \\ x_i(t) \in X_i, u_i(t) \in U_i, t \in \mathbb{N}, \end{cases} \tag{4.18}$$

Net represents the communication network defined in (2.11). It can be seen in Fig. 4.7 that $y'_1(t) = Net(y_1, y_A)$ and $y'_2(t) = y_2(t)$.

To address the problem of attack detection in a network of agents within a decentralized framework, we extend the definition given in [59] and [35] to the current framework, we give the following definition:

Definition 4.1.6

The NoA is said to be secure in a decentralized setting (D−secure), whenever an attack occurs at step $\hat{t}$, at least one of the agents e.g. P_i, is able to detect the attack at most within step $\hat{t}+1$, on the base of its information $y_i(t), t \in [0, \hat{t}+1]$, $u_i(t)$, $t \in [0, \hat{t}]$ and $y'_{3-i}(t)$, $t \in [0, \hat{t}]$. □

4.1.4.1 Model Composition

Now we define a composed model P to represent the behaviour of NoA:

$$P = \begin{cases} x(t+1) = \Phi(x(t), u(t)), \\ x(0) \in X_{1,0} \times X_{2,0} \times X_{A,0}, \\ x(t) \in X_1 \times X_2 \times X_A, \\ y(t) = (h_1(x_1(t)), h_2(x_2(t))), \\ u(t) = ((u_1(t), y'_2(t)), (u_2(t), y'_1(t)), u_A(t)), \\ \in (U_1 \times Y'_2) \times (U_2 \times Y'_1) \times U_A, \\ t \in \mathbb{N}. \end{cases} \tag{4.19}$$

Here $x(t+1) = (x_1(t+1), x_2(t+1), x_A(t+1))$, $x(t) = (x_1(t), x_2(t), x_A(t))$ and $x(0) = (x_1(0), x_2(0), x_A(0))$, and

$$\Phi((x(t),u(t)) = \begin{cases} (F_1(x_1(t),y_2'(t),u_1(t)),F_2(x_2(t),y_1'(t),u_2(t)), \\ F_A(x_A(t),u_A(t))), \\ \qquad\qquad \text{if } F_i(x_i(t),y_{3-i}'(t),u_i(t))! \text{ for } i=1,2 \\ (F_1(x_1(t),y_2'(t),u_1(t)),x_2(t),F_A(x_A(t),u_A(t))), \\ \qquad\qquad \text{if } F_i(x_i(t),y_{3-i}'(t),u_i(t))! \text{ only for } i=1 \\ (x_1(t),F_2(x_2(t),y_1'(t),u_2(t)),F_A(x_A(t),u_A(t))), \\ \qquad\qquad \text{if } F_i(x_i(t),y_{3-i}'(t),u_i(t))! \text{ only for } i=2 \\ (x_1(t),x_2(t),F_A(x_A(t),u_A(t))) \qquad \text{Otherwise} \end{cases} \tag{4.20}$$

For further analysis, let us modify the composed system P such that all the available information is grouped as the output of the current state. This modification may result in multiple copies of the same states, these copies are generated using the function ϕ.

$$\hat{P} = \begin{cases} \hat{x}(t+1)^n = \phi(\hat{x}(t),\hat{u}(t)), \\ \hat{x}(0) = (x_1(0),x_2(0),x_A(0)) \in X_{1,0}\times X_{2,0}\times X_{A,0}, \\ \hat{x}(t) = (x_1(t),x_2(t),x_A(t)) \in X_1\times X_2\times X_A, \\ \hat{y}(t) = (\Psi_1(\hat{x}(t)),\Psi_2(\hat{x}(t))), \\ \hat{u}(t) = ((u_1(t),y_2'(t)),(u_2(t),y_1'(t)),(u_A(t))) \\ \qquad\qquad \in (U_1\times Y_2')\times(U_2\times Y_1')\times U_A, \\ t\in\mathbb{N}. \end{cases} \tag{4.21}$$

Here, $\Psi_i(\hat{x}(t))$ is given by:

$$\Psi_i(\hat{x}(t)) = ((u_i(t-1),y_{3-i}'(t-1)),h_i(x_i(t))), i=1,2. \tag{4.22}$$

and ϕ is defined as follows:

$$\phi(\hat{x}(t),\hat{u}(t)) = \begin{cases} (\Phi(\hat{x}(t),\hat{u}(t)))^{m+1}, & \text{if } \forall m,\exists i : \phi(\hat{x}(t),\hat{u}(t)) = \hat{x}(t+1)^m, \\ & \quad \wedge\Psi_i(\hat{x}(t+1)^m) \neq ((u_i(t),y_{3-i}'(t)), \\ & \quad h_i(x_i(t+1))); \\ (\Phi(\hat{x}(t),\hat{u}(t)))^m, & \text{if } \exists m : \phi(\hat{x}(t),\hat{u}(t)) = \hat{x}(t+1)^m \\ & \quad \wedge\Psi_i(\hat{x}(t+1)^m) = ((u_i(t),y_{3-i}'(t)), \\ & \quad h_i(x_i(t+1))),\forall i; \\ (\Phi(\hat{x}(t),\hat{u}(t)))^0, & \textit{otherwise.} \end{cases} \tag{4.23}$$

Here $\hat{x}(t+1)^n$ represents the $n-th$ copy of the state. For simplicity, let $\hat{x}(t+1)^0 = \hat{x}(t+1)$.

The first element of $\Psi_i(\hat{x}(t))$ represents the input information (i.e. $(u_i(t),y_{3-i}'(t))$), and the second element represents the output information (i.e. $(h_i(x_i(t)))$) available to the $i-th$ agent. A State-run of $\hat{P}$ is a finite sequence of states $\hat{x}(0)$, $\hat{x}(1)$, ... satisfying (4.21), and the corresponding output run is $(\Psi_1(\hat{x}(0)),\Psi_2(\hat{x}(0)),(\Psi_1(\hat{x}(1)),\Psi_2(\hat{x}(1)),\ldots$.

Let χ be the set of all state runs of the composed system $\hat{P}$ and Υ_i be the set of all output runs of Agent i. Function $f_i : \chi\to\Upsilon_i$ associates to a state run, the corresponding output run of the $i-th$ Agent, i.e. for $r_x = (\hat{x}(0)),\hat{x}(1),..$, $f_i(r_x) = \Psi_i(\hat{x}(0),\Psi_i(\hat{x}(1)),....$ The symbol $|r_x|$ represents the length of the state run.

Next, we adopt the notion of indistinguishable state run as defined in Definition 4.1.1 to the current framework.

Definition 4.1.7

Two state runs r_{x1} and r_{x2} of the composed system $\hat{P}$ are called P_i-indistinguishable

if $f_i(r_{x1}) = f_i(r_{x2})$. □

Furthermore, we define the set $f_i^{-1}(f_i(r_x))$ as:

$$f_i^{-1}(f_i(r_x)) = \{r'_x \in \chi : f_i(r_x) = f_i(r'_x)\} \tag{4.24}$$

which represents the set of all state runs which are P_i-indistinguishable from r_x.

Next, we formally define the notion of *Decentralized Critical Observability* (DCO), which captures the property that, whenever the current state of the composed system $\hat{P}$ belongs to a specified critical set, at least one agent is able to detect this belonging.

Definition 4.1.8

System in (4.21) is critically observable with respect to a set $\Omega \subset X$ *in a decentralized setting (shortly* $\Omega-$ *DCO) if whenever the current state of (4.21) at step* $\hat{t}$ *belongs to* Ω*, at least one of the agents e.g.* P_i *is able to detect the belonging on the basis of information* $y_i(t), t \in [0, \hat{t}+1]$*,* $u_i(t)$*,* $t \in [0, \hat{t}]$ *and* $y'_{3-i}(t)$*,* $t \in [0, \hat{t}]$*, corresponding to* $\Psi_i(t)$*,* $t \in [0, \hat{t}+1]$*.* □

The critical set Ω is the collection of all states $\hat{x}(t+1) \in succ(\hat{x}(t))$ of $\hat{P}$ such that:

$$\begin{aligned} &\hat{x}(t) = (x_1(t), x_2(t), x_A(t)) \wedge \\ &\quad x_A(t) \in X_{A,\text{on}} \wedge h_A(x_A(t)) \neq h_1(x_1(t)). \end{aligned} \tag{4.25}$$

4.1.4.2 Main Results

Theorem 4.1.1

The NoA is $D-$*secure if and only if* $\hat{P}$ *is* $\Omega-$ *DCO, with* Ω *as in (4.25).* □

The proof of the result above is a direct consequence of the definition of Ω.

Proposition 4.1.6

$\hat{P}$ *is* $\Omega-$ *DCO if and only if the following statement is false: there exists a state run* r_x *of* $\hat{P}$ *ending in* Ω *and for each agent* P_i*,* $i = 1, 2$*, there exists a state run* r_{xi} *ending outside* Ω*, such that* r_x *and* r_{xi} *are* P_i-*indistinguishable.* □

Proof. Necessity: Let us assume that the above statement is true, this implies that there is at least one state in Ω, for which every state run r_x leading to that state, for each agent P_i, there exists an indistinguishable state-run $r'_x \in f_i^{-1}(f_i(r_x))$ as defined in (4.24) such that r'_x leads to a state outside Ω. Hence, it is not possible to detect the belonging to the critical set Ω. *Sufficiency:* As for the sufficiency, if the above statement is false, this implies that for all the state runs r_x ending in Ω, there exists at least one agent for which all indistinguishable state runs $r'_x \in f_i^{-1}(f_i(r_x))$ defined in (4.24) also ends in Ω. Therefore the sufficiency follows. □

Let $\hat{X}_{\epsilon,i}$ be the set of $x \in \hat{X}$ such that $\Psi_i(x) = ((u_i(t), \epsilon), \epsilon)$.

Let Δ_i be the set of pairs $(\hat{x}, \hat{x}') \in \hat{X} \times \hat{X}$, such that $\Psi_i(\hat{x}) \neq ((u_i, \epsilon), \epsilon)$ and $\Psi_i(\hat{x}) = \Psi_i(\hat{x}')$.

Let us assume that $\Psi_i(\hat{x}) \neq ((u_i, \epsilon), \epsilon), \forall \hat{x} \in \hat{X}_0, \forall i = 1, 2$.

For $k = 1, 2, ...$ define the recursion,

$$S_{k+1} = S'_{k+1} \cup S_k, \tag{4.26}$$

where

$$S_1 = \{s \in \hat{X}_0^3 : (s(i), s(3)) \in \Delta_i, \text{ for } i = 1, 2\}, \tag{4.27}$$

and S'_{k+1} is the set of $s' \in \hat{X}^3$ such that for some $s \in S_k$

$$\begin{aligned}(s'(i) \in succ(s(i))) \wedge (\Psi_i(s'(i)) \neq \epsilon) \\ \wedge ((s'(i), s'(3)) \in \Delta_i) \qquad \text{for } i = 1, 2.\end{aligned} \tag{4.28}$$

Proposition 4.1.7

Consider the recursion defined in (4.26). Then

1. *S_k is the set of $s \in S^3$ such that there exist state runs r_{xi} for $i = 1, 2, 3$, ending in $s(i)$, such that the state runs r_{xi} and r_{x3} are P_i-indistinguishable and $|f_i(r_{xi})| = |f_3(r_{x3})| = k$;*
2. *the least fixed point of recursion exists, is unique and is equal to S^*;*
3. *the recursion reaches the fixed point S^* in at most $S^* < |\hat{X}|^3$ steps.*

□

Proof.

1. Suppose that S_k is the set of $s \in \hat{X}^3$ such that there exist state runs $r_{xi}, i = 1, 2, 3$ ending in $s(i)$, such that (r_{xi}, r_{x3}) are P_i-indistinguishable and $|f_i(r_{xi})| = |f_i(r_{x3})| \leq k$. Then, by construction, S_{k+1} is the set of $s \in \hat{X}^3$ such that there exist state runs $r_{xi}, i = 1, 2, 3$ ending in $s(i)$, where state runs (r_{xi}, r_{x3}) are P_i-indistinguishable and $|f_i(r_{xi})| = |f_i(r_{x3})| \leq k + 1$. Since the property holds for $k = 1$, then the result follows.
2. The sequence $S_k, k = 1, 2, ...$ non decreasing, and $s_{k+1} = S_k$ implies $S_{k+j} = S_k, \forall j = 1, 2, ...$. Since the set X is finite, the result follows.
3. Trivial.

□

Theorem 4.1.2

$\hat{P}$ is $\Omega-$ DCO if and only if the following condition is false:

$$\exists s \in S^* : s(3) \in \Omega \wedge s(i) \notin \Omega, \text{ for } i = 1, 2 \tag{4.29}$$

□

Proof. Necessity: Let's suppose that (4.29) is true. Then there exists at least one state in the critical set i.e. $\hat{x} \in \Omega$, such that for each agent there exists another state outside critical set i.e. $\hat{x}_i \notin \Omega$, such that $\hat{x}$ and $\hat{x}_i$ are reachable from P_i-indistinguishable state runs, which contradicts the definition of $\Omega-$ DCO and hence the necessity follows. *Sufficiency:* As for the sufficiency, since $s(3)$ represents the current state of $\hat{P}$, by Proposition 4.1.6, for each execution ending in Ω, at least one of the agents is able to reconstruct the belonging. Conversely, if the current state of $\hat{P}$ does not belong to Ω, since for each agent, the actual state surely belongs to the states compatible with the collected output information then no "false alert" is possible. □

4.1.5 Attack Localization for a Network of Agents

To address the problem of localization, let us consider NoA and NoA' as in Fig. 4.7 and 4.8, respectively. The term localization refers to the identification or detection of an attacked channel.

For further analysis we make the following assumption:

Assumption 4.1.5

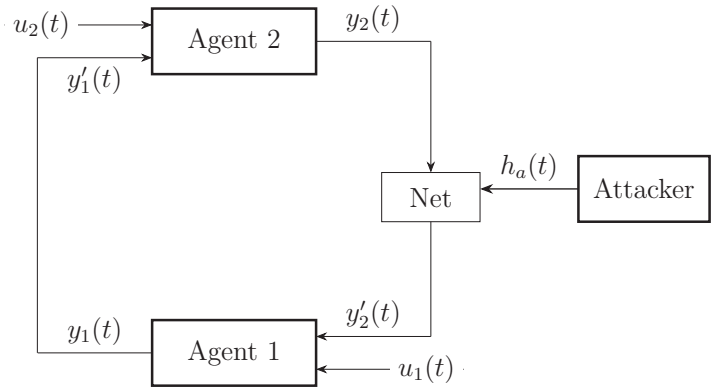


Figure 4.8: Agents interconnection in NoA'.

- *Both NoA and NoA' are $D-$secure.*
- *Attacker P_A can only corrupt one of the two channels, i.e. actual model is NoA or NoA'.*
- *No agent P_i has prior knowledge of which channel is attacked.*

□

To accommodate the possibility of attack in both channels, let us consider NoA and NoA' as shown in Fig. 4.7 and 4.8, respectively. Let $\hat{P}'$ represent the composed system, same as the one presented in eq. (4.21), such that $y_2'(t) = Net(y_2, y_A)$ and $y_1'(t) = y_1(t)$. $\hat{X}'$ represent the state of states of $\hat{P}'$ and χ' be the set of all state runs of $\hat{P}'$. Let $\Omega' \subset \hat{X}'$ represent the set of corrupted states in $\hat{P}'$.

4.1.5.1 Main Results

Proposition 4.1.8

If the attack is detected then the localization of attacked channel is possible if and only if the following statement is false: there exists a state run r_x of $\hat{P}$ ($\hat{P}'$) ending in Ω (resp. Ω') and for each agent P_i, $i = 1, 2$, there exists a state run $r_x' \in \chi'$ ($r_x' \in \chi$), such that r_x and r_x' are P_i-indistinguishable. □

Proposition above is equivalent to the following:

Proposition 4.1.9

The localization of attacked channel is possible if and only if the following statement is false

$$\exists r_x \in \chi, r_x' \in \chi' : r_x(|r_x|) \in \Omega \vee r_x'(|r_x'|) \in \Omega' \\ \wedge f_i(r_x) = f_i(r_x'), \qquad \forall i = 1, 2. \tag{4.30}$$

□

Proof. Necessity: Let us assume that the above statement is true, then it means that there exists at least one state in Ω (or Ω'), such that for all the state runs $r_x \in \chi$ ($r_x \in \chi'$, resp.), ending in that state, there exists an indistinguishable state-run $r_x' \in \chi'$ ($r_x' \in \chi$, resp.), for each agent. Therefore, if the above statement is true, locating the attacked channel is not possible. Hence, the necessity follows. *Sufficiency:* If the condition in (4.30) is false, then for every state run $r_x \in \chi$ ($r_x \in \chi'$) of the composed system $\hat{P}$ ($\hat{P}'$, resp.), that ends in Ω (Ω', resp.), there exists at least one agent such that all the indistinguishable state runs ($r_x' \in f_i^{-1}(f_i(r_x))$ in (4.24)) also belongs to χ (χ', resp.) and ends in Ω (Ω', resp.). Every time we are in the critical set of any composed system, at least one agent can detect its belonging and hence, the sufficiency follows. □

Let $W^i \subset \hat{X} \times \hat{X}'$ be the set of pair of states of $\hat{P}$ and $\hat{P}'$, reached by two P_i-indistinguishable state runs i.e.

$$W^i = \{(x, x') \in \hat{X} \times \hat{X}' : \\ \exists r_x \in \chi \wedge \exists r'_x \in \chi', f_i(r_x) = f_i(r'_x)\}. \tag{4.31}$$

The computation of W^i, can easily be derived from (4.8) to compute the set of indistinguishable states from two different FSMs.

Let $\mathbb{S} \subset S^* \times S^{*'}$ be the set of pair of strings from S^* and $S^{*'}$, where $S^{*'}$, represents the set S^* computed for the system $\hat{P}'$.

$$\mathbb{S} = \{(s, s') : s \in S^* \wedge s' \in S^{*'} \wedge (s(i), s'(i)) \in W^i, \forall i\}. \tag{4.32}$$

The set $\mathbb{S}$, can be computed as shown in Algorithm 4.1.

Algorithm 4.1 Computation of $\mathbb{S}$

1: **Input:** $S^{i*}, W^i, \forall i = 1, 2$
2: **Main:**
3: $h = 1$, $k = 1$;
4: $\mathbb{S} = \{\}$
5: **while** $h \leq |S^{1*}|$ **do**
6: $q = S^{1*}(h)$
7: **while** $k \leq |S^{2*}|$ **do**
8: $p = S^{2*}(k)$
9: **if** $(q(i), p(i)) \in W^i$ for $i = 1, 2$ **then**
10: $\mathbb{S} = \mathbb{S} \cup (q, p)$
11: **end if**
12: $k = k + 1$
13: **end while**
14: $h = h + 1$
15: **end while**
16: **Output:** $\mathbb{S}$

Theorem 4.1.3

If the attack is detected, then the localization of attack is possible if and only if the following statement is false:

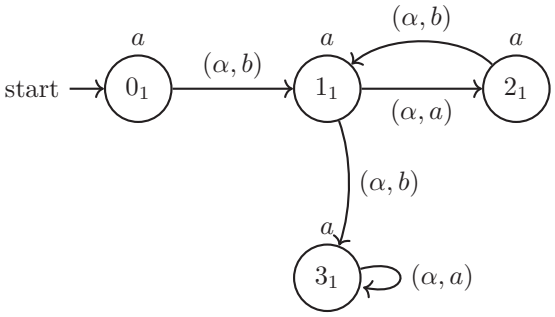
$$\exists (s, s') \in \mathbb{S} : s(3) \in \Omega \vee s'(3) \in \Omega'. \tag{4.33}$$

□

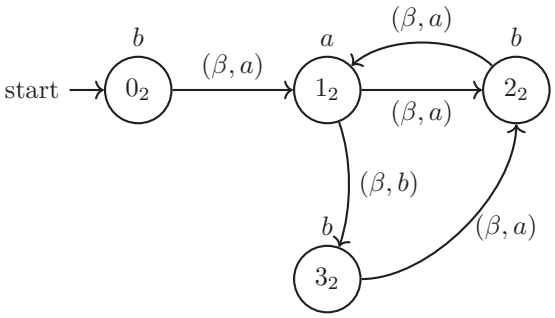
Proof. Necessity: By definition, $\mathbb{S}$ contains only those pair of tuples from S^* and $S^{*'}$, that are indistinguishable for both agents. Now if we assume that the above statement is true, then it means that there exists at least one state in Ω or Ω', such that none of the agents can reconstruct its belonging, therefore, it is not possible to localized the attack if the above statement is true and hence the necessity follows. *Sufficiency:* The sufficiency is obvious. If the above statement is false, then it means that every time the current state belongs to critical sets Ω or Ω', at least one agent can reconstruct its belonging. □

Remark 4.1.1

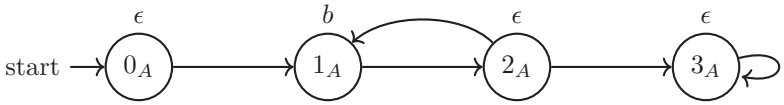
By Definition 4.1.6, if a NoA is D−secure then the attack can be detected, whenever it occurs. This requirement can be relaxed if we need to detect the attack only the first time it occurs. Similarly, another possible relaxation can be obtained by asking that the detection is possible within a finite number of steps after the attack, and not within one step, as done in this paper. We are able to solve the detection and



(a) The first Agent A_1



(b) The Second Agent A_2



(c) The Attacker

Figure 4.9: The models of Agents A_1, A_2 and Attacker

localization problems also in these different framework. Moreover it is easy to show that D−security of NoA and NoA' implies D−security of the network also when attacker has the ability of changing signals on both channels, during the same run. In the framework defined above, localization is also assured under the same conditions of Theorem 4.1.3. □

4.1.6 Example: Attack Detection and Localization for a Network of Agents

Consider interconnected Agents P_1 and P_2, with set of states $X_1 = \{0_1, 1_1, 2_1, 3_1\}$ and $X_2 = \{0_2, 1_2, 2_2, 3_2\}$, respectively. Also, $X_{1,0} = \{0_1\}$, $U_1 = \{\alpha\}$, $Y_1 = \{a, b\}$, $Y_2 = \{a, b\}$ $X_{2,0} = \{0_2\}$ and $U_2 = \{\beta\}$. The state evolution of both agents is shown in Fig. 4.9a and Fig. 4.9b, respectively. The input of each state is shown in the form of an ordered pair (i.e. $(u_i, y_{3-i}), i = 1, 2$), where the first element represents the external input and the second element represents the output of the other agent. The structure of the attacker is shown in Fig. 4.9c.

The simplified composed model $\hat{P}$ is shown in Fig. 4.10. For simplicity, a label is also assigned to each state in Fig. 4.10.

The set S^* is computed using (4.26),(4.27) and (4.28), as

$$S^* = \{(5,4,4),(4,5,4),(5,5,4),(4,4,5),(5,4,5),(7,3,3),(3,7,7),(6,7,6),(7,6,6),$$
$$(7,7,6),(6,7,7),(7,6,7)(6,6,7),(8,10,10),(10,8,8),(10,9,9),(9,10,9),(10,10,9),$$
$$(9,10,10),(10,9,10),(9,9,10),(7,9,9),(7,9,11),(7,11,9),(9,7,7),(11,7,7),(9,3,3),$$
$$(11,3,3),(3,9,9),(3,9,11),(3,11,9),(3,11,11),(3,6,6),(3,7,6),(3,6,7),(3,7,7),$$

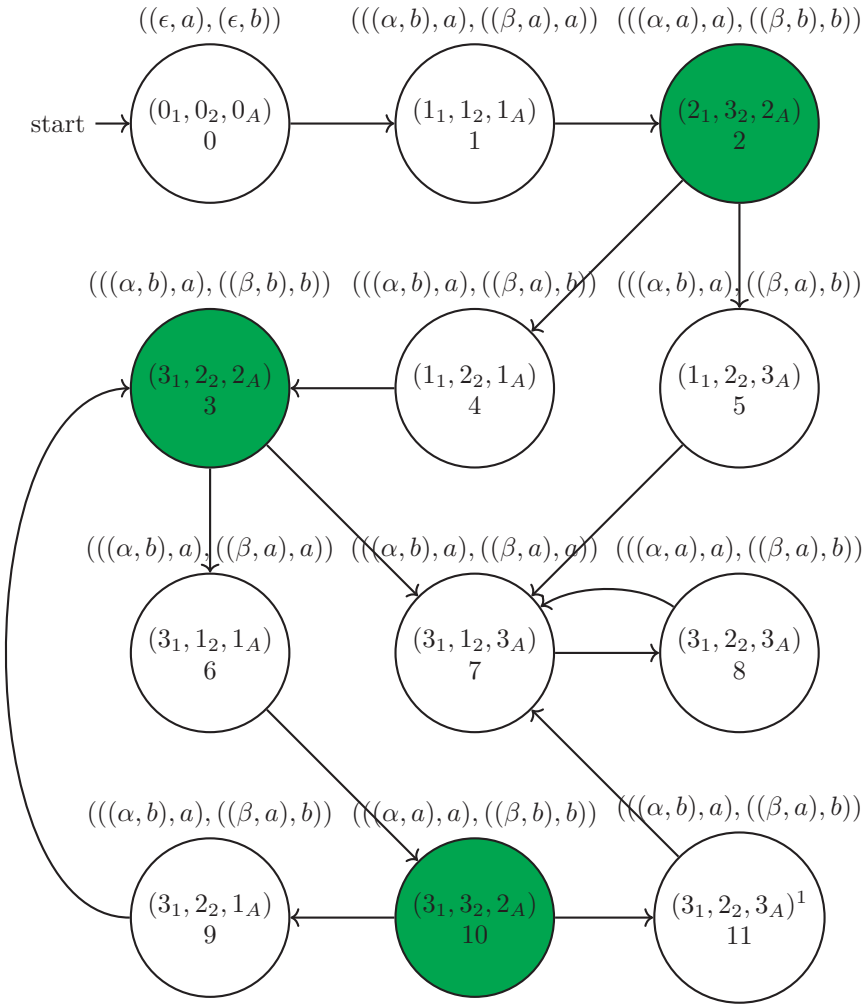


Figure 4.10: Composed System $\hat{P}$

$(6, 3, 3), ...\} \cup \Theta$

where Θ is the tuple with all equal elements and the set $\Omega = \{(2), (3), (10)\}$, as highlighted in Fig. 4.10, with green color.

4.1.6.1 Attack Detection

For the given Ω and computed S^* it can be seen that (4.29), is true for $(9, 9, 10)$, then according to Theorem 4.1.2, it can be concluded that for the given two agents and the attacker, the attack can not be detected.

Remark 4.1.2

We can also apply the same theorem to a subset of the critical set. For example, in some scenarios, it is sufficient to detect the first occurrence of an attack to generate the necessary control commands. In this case, if we define a set $\Omega_1 \in \Omega$ containing only the critical states when the attack occurred for the first time, we can verify its detectability with the help of Theorem 4.1.2. □

4.1.6.2 Localization

For the composed model $\hat{P}'$ shown in Fig. 4.11, the $S^{*'}$ can be computed as:

$$S^{*'} = \{(2', 4', 2'), (4', 2', 2'), (4', 4', 2'), (4', 2', 4'),$$

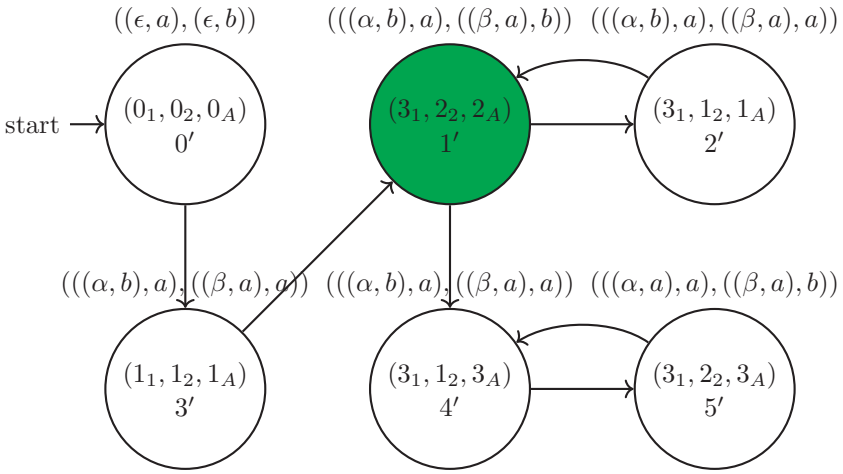


Figure 4.11: Composed System $\hat{P}'$

$$(2', 4', 4'), (2', 2', 4'), (1', 5', 1'), (5', 1', 5')\} \cup \Theta$$

Similarly, we can compute $\mathbb{S}$ using Algorithm 4.1:

$$\mathbb{S} = \{((0', 0', 0'), (0, 0, 0)), ((1', 1', 1'), (3, 3, 3))\}$$

For the computed $\mathbb{S}$, the condition in (4.33) does not hold, which means that the attack can be localized as soon as it is detected.

4.2 Passive Attacks

In the context of passive attacks, the goal of an adversary is to infer sensitive information by observing system outputs without interfering with the system's dynamics. One widely studied system property related to passive attack resistance is opacity, which ensures that certain critical (or "secret") states of a system cannot be unambiguously inferred from observations. To verify opacity and similar properties, observers are commonly used as analytical tools in the setting of FSM. However, the construction of full observers can be computationally expensive, especially for large–scale systems.

To address this challenge, we propose a decomposition–based observer design that reduces complexity by dividing the observer into a set of sub–observers. This decomposition of observer into sub-observers is based on the concept of critical observability and total indistinguishability. A switching mechanism is employed to alternate between these sub–observers, forming what we refer to as a switching observer. This framework preserves the ability to verify opacity while significantly lowering computational demands. In the following, we present this decomposition approach and illustrate its application in analyzing opacity as a security related property against passive attacks.

Here, we consider plants modelled by FSM as in (2.4). However, we assume that $E = \{e\}$ because we are only interested in the transitions events produce but not in their values. Therefore, for simplicity, the set E is not shown in the system definition and is represented by the 5-tuple:

$$M = (X, X_0, Y, H, \Delta) \tag{4.34}$$

where the transition relation $\Delta \subset X \times X$.

For further analysis, we make the following assumption:

Assumption 4.2.1

The initial states have no predecessors, i.e., $pre(x) = \emptyset$, for all $x \in X_0$. □

The assumption above can be given without loss of generality because an FSM can be always transformed into another one satisfying this condition and behaving the same as the original one, see e.g. [142].

4.2.1 Observer Decomposition

Now, we present a novel method to divide traditional observer into sub–observers for an FSM M based on the notions of "Total–indistinguishability" and "Critical observability":

We define the notion "Total–indistinguishability", by using the notion of "indistinguishable state run" define in 4.1.1

Definition 4.2.1

A pair (x, x') is called Totally-indistinguishable *(T-indistinguishable) if for any finite state run $r_x \in \mathcal{X}$ ending in x (resp. x'), there exists a finite state run $r'_x \in \mathcal{X}$ ending in x' (resp. x), with r_x and r'_x indistinguishable.* □

Total indistinguishability is a transitive property. Since it is also reflexive and symmetric, we can group the states in X into equivalence classes. Let the symbol $\sim$ denote the total indistinguishability relation on the set X. For a state $x \in X$ its equivalence class is the set $\{x' \in X : x' \sim x\}$. The set of equivalence classes induces a partition on the set of states X

$$X = X^{(1)} \cup X^{(2)} .... \cup X^{(L)} \tag{4.35}$$

with $L \leq N$ where $N = |X|$. Let $\mathcal{T} = \{X^{(1)}, X^{(2)} ..., X^{(L)}\}$.

The notion of total indistinguishability for the elements in $\mathcal{T}$ is related to the notion of equivalent states e.g. in [110] which refers to states starting from which the same marked language is obtained.

We recall hereafter the notion of critical observability [140].

Definition 4.2.2

(Critical observability) The FSM (4.34) is critically observable with respect to a set $\Omega \subset$ X (critically Ω-obs) if for any string $r_x \in \mathcal{X}$, whenever $r_x(k) \in \Omega$, it follows that for any string $\hat{r}_x \in \mathbf{y}^{-1}\left(\mathbf{y}(r_x|_{[1,k]})\right)$, $\hat{r}_x\left(|\hat{r}_x|\right) \in \Omega$. A set Ω is said to be critically observable if the FSM is critically Ω-obs. □

Let $I_c \subset \{1, 2, ...L\}$ be the set of indexes i such that M is $X^{(i)}$-critically observable, and $\mathcal{T}_C = \{X^{(i)}, i \in I_c\} \subset \mathcal{T}$.

Remark 4.2.1

By Assumption 4.2.1, $\mathcal{T}_C$ is nonempty. In fact, given X_0, each maximal subset of X_0 where the states have the same output is an element of $\mathcal{T}_C$. □

The construction of sub-observers is based on the collection $\mathcal{T}_C \subset \mathcal{T}$ where the notion of critical observability is used.

Let M' be obtained from M by removing the transitions $(x, x') \in \Delta$ with $x' \in X^{(i)}$ for all $i \in I_c$ and $M'|_i$ be the FSM M' with initial state set $X^{(i)}$. We define the FSMs M_i, $i \in I_c$ as

$$M_i = Ac(M'|_i) = (X_i, X_{0i}, E_i, Y_i, H_i, \Delta_i) \tag{4.36}$$

where $X_{0i} = X^{(i)}$ and $Ac(.)$ denotes the accessible part as defined in (2.9)

Proposition 4.2.1

Each state run of M is the concatenation of state runs of FSMs in $\{M_i, i \in I_c\}$. □

Proof. Given an initial state $x_0 \in X_0$, let $X_{0i} \in \mathcal{T}_C$ be such that $x_0 \in X_{0i}$. By Remark 4.2.1, this set exists and is unique, because $X_{0i} \cap X_{0j} = \emptyset$, $\forall i, j \in I_c$, with $i \neq j$. Therefore, until the state run of M intersects some set X_{0j}, $j \in I_c$, we will have a state run of M_i. As soon as the current state belongs to X_{0j}, we will have a state run of M_j until the state run of M intersects some set X_{0h}, $h \in I_c$, with h not necessarily different from j, etc. □

Let O be the observer for M and $\hat{X}_O$ be the set of states of the observer O, see e.g. [110].

Proposition 4.2.2

If $X^{(i)} \in \mathcal{T}_C$, then there exists $\hat{x}' \in \hat{X}_O$ such that $\hat{x}' = X^{(i)}$, and $X^{(i)} \cap \hat{x} = \emptyset$, $\forall \hat{x} \in \hat{X}_O$ with $\hat{x} \neq \hat{x}'$. □

Proof. T-indistinguishability for a set $X^{(i)}$ implies that it is not possible that a proper subset of $X^{(i)}$ is a subset of a state of the observer. Critical observability of the same set $X^{(i)}$ implies that for a state $\hat{x}$ of the observer either $\hat{x} \cap X^{(i)} = \emptyset$ or $\hat{x} \subset X^{(i)}$. □

Remark 4.2.2

By Proposition 4.2.2, $\mathcal{T}_C \subset \hat{X}_O$ but in general $\mathcal{T} \neq \hat{X}_O$. In fact, a state of the observer is the finite union of sets in $\mathcal{T}$. Therefore $\left|\hat{X}_O\right| \leq \left|2^{|\mathcal{T}|}\right|$. □

Let O_i, $i \in I_c$, be the observer for M_i, also called "sub-observer", and $\hat{X}_{O_i}$ be the set of states of O_i. Then, we have:

$$\hat{X}_O = \hat{X}_{O_1} \cup ... \cup \hat{X}_{O_L}$$

and it is possible that $\hat{X}_{O_i} \cap \hat{X}_{O_j} \neq \emptyset$. Algorithm 4.2 summarizes the procedure illustrated above.

Algorithm 4.2 Decomposition of Observer into sub-observers

1: Compute the Totally-indistinguishable sets $X^{(1)}, X^{(2)}, ..., X^{(L)}$;
2: Let $\mathcal{T}$ be the collection of $X^{(i)}$ for $i = 1, ..., L$;
3: Let $\mathcal{T}_c \subset \mathcal{T}$ be the collection of $X^{(i)} \subset \mathcal{T}$ such that $X^{(i)}$ is critically observable;
4: Define M' from M by removing the transitions $(x, x') \in \Delta$ with $x' \in X^{(i)}$ for $i \in I_c$;
5: Define $M'|_i$ as the FSM M' with initial state set $X^{(i)}$;
6: Define the FSMs M_i, $i \in I_c$ as $M_i = Ac(M'|_i)$;
7: Build the observer O_i for each subsystem M_i where $\hat{X}_{O_i}$ is the set of i-th sub-observer states.

Remark 4.2.3

Although the number of states of the traditional observer O for the FSM M, is not greater than the total number of states of all its "sub-observers", when using observers for checking some specific properties, such as opacity, the use of a sub-observer is advantageous, because it is not always necessary to build all sub-observers. This will be illustrated in the next section. □

Next, we present algorithms for the computation of $\mathcal{T}$ and $\mathcal{T}_C$. Let S^* be the maximal set of indistinguishable pairs $(x, x') \in X \times X$. The following result characterizes critical Ω-observability of an FSM by means of S^*.

Proposition 4.2.3

[143] The FSM (4.34) is critically $\Omega - obs$ if and only if

$$S^* \subset (\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega}) \tag{4.37}$$

□

Next we define

$$\Pi = \{(x, x') \in X \times X : H(x) = H(x')\}$$

Let S_T^* be the maximal set of *Totally-indistinguishable* pairs (x, x'). For simplicity, we assume in the sequel that no state is silent ($\epsilon \notin Y$), but the general case can be addressed

by appropriately defining an equivalent model without silent states, see e.g. [141]. We recall the computation of set S_T^* from [35] as follows. Define the recursion, with $k = 1, 2, ...$

$$\begin{aligned} S_T^1 &= (X_0 \times X_0) \cap \Pi \\ S_T^{k+1} &= \left\{(x, x') \in \Pi : (pre(x) \times pre(x')) \subset S_T^k\right\} \cup S_T^k \end{aligned} \tag{4.38}$$

It is obvious from the algorithm above that the sequence of sets S_T^k is increasing, i.e. $S_T^k \subset S_T^{k+1}$, $k \in \mathbb{N}$. Moreover, each set S_T^k contains totally indistinguishable pairs of states. The following preliminary result holds.

Lemma 4.2.1

The least fixed point of recursion (4.38) exists, is unique and is equal to S_T^*.

□

Proof. The set Π is a fixed point of the recursion and the intersection of fixed points is a fixed point. Therefore, the least fixed point exists and is unique. If $S_T^{k+1} = S_T^k$ for some k then $S_T^{k+i} = S_T^k$, $\forall i \geq 0$, and hence S_T^k is a fixed point. But a finite k such that $S_T^{k+1} = S_T^k$ exists because of the finite cardinality of Π. Let $\hat{k}$ be the minimum value of k such that $S_T^{k+1} = S_T^{\hat{k}}$. The fact that $S_T^{\hat{k}} = S_T^*$ comes from the maximality of S_T^*. □

Starting from S_T^*, the sets $X^{(k)} \in \mathcal{T}$ can be computed as in Algorithm 4.3.

Algorithm 4.3 Algorithm to compute sets $X^{(k)}$

1: **Input:** X, S_T^*
2: Set:
3: $\quad \Lambda = X$
4: $\quad k = 1$
5: **while** $\Lambda \neq \emptyset$ **do**
6: $\quad X^{(k)} = \{x\} \cup \{x' | (x, x') \in S_T^*\}, \; x \in \Lambda$
7: $\quad \Lambda = \Lambda \setminus X^{(k)}$
8: $\quad k = k + 1$
9: **end while**
10: **Output:** $X^{(1)}, X^{(2)}, ..., X^{(L)}$

Since all elements of a totally-indistinguishable subset are equivalent from the observability point of view, it is not necessary to check all of them to find the critical observable set. Hence, the result presented in Proposition 4.2.4 can reduce the computational cost to check this property.

Proposition 4.2.4

For $k = 1, ..., L$, let x_k be an arbitrary state belonging to $X^{(k)}$. A Totally-indistinguishable set $X^{(h)} \in \mathcal{T}$ is critically observable if and only if

$$(x_h, x_k) \notin S^*, \; \forall k = 1, ..., L, k \neq h \tag{4.39}$$

□

4.2.2 Opacity

Opacity requires that a specific behaviour of the system stays opaque to an external observer. We refer to a state-based definition of opacity as in [68], as follows:

Definition 4.2.3

The FSM M is opaque with respect to the set $\boldsymbol{\Upsilon}_S \subset X$ called secret set (shortly $\boldsymbol{\Upsilon}_S$-opaque), if for any state run r_x of M ending in $\boldsymbol{\Upsilon}_S$, there exists another state run

r'_x of M ending in $\overline{\boldsymbol{\Upsilon}_S}$, such that r_x and r'_x are indistinguishable. □

Opacity verification is based on the computation of the observer (see e.g. [84]) and its complexity has widely been investigated in the literature [85]. In this section, we use the proposed sub–observers to check opacity for DES modelled by FSMs, which may be useful for reducing computational cost.

We recall the following result, see e.g. [144], that provides a characterization of opacity.

Theorem 4.2.1

M is $\boldsymbol{\Upsilon}_S$-opaque if and only if

$$\hat{X}_O \cap 2^{\boldsymbol{\Upsilon}_S} = \emptyset$$

□

Since the set $X^{(i)}$ is critically observable, the following result holds.

Lemma 4.2.2

M is $\boldsymbol{\Upsilon}_S$-opaque only if $X^{(i)} \not\subset \boldsymbol{\Upsilon}_S$, $\forall i \in I_c$. □

4.2.3 Main Results

For $i \in I_c$, let $\boldsymbol{\Upsilon}_{S,i} = \boldsymbol{\Upsilon}_S \cap X_i$. We now show that a set $\boldsymbol{\Upsilon}_S$ is opaque for M if and only M_i is $\boldsymbol{\Upsilon}_{S,i}$-opaque, $\forall i \in I_c$ such that $\boldsymbol{\Upsilon}_{S,i} \neq \emptyset$.

Theorem 4.2.2

A set $\boldsymbol{\Upsilon}_S$ is opaque for M if and only if

$$\hat{X}_{Oi} \cap 2^{\boldsymbol{\Upsilon}_{S,i}} = \emptyset, \quad \forall i \in I_c \tag{4.40}$$

□

Proof. By Lemma 4.2.2 and definition of $X^{(i)}$, $i \in I_c$, we can assume without loss of generality that $X^{(i)} \cap \boldsymbol{\Upsilon}_S = \emptyset$, $\forall i \in I_c$. In fact, if $X^{(i)} \not\subset \boldsymbol{\Upsilon}_S$, for any state $x \in X^{(i)} \cap \boldsymbol{\Upsilon}_S$ there is a state $x' \in \overline{\boldsymbol{\Upsilon}_S}$ such that the pair (x, x') is T-indistinguishable. Therefore, in checking the property the states in $X^{(i)} \cap \boldsymbol{\Upsilon}_S$ can be skipped.
Sufficiency: if $\boldsymbol{\Upsilon}_{S,i} \cap \boldsymbol{\Upsilon}_{S,j} = \emptyset, \forall i, j \in I_c$ with $i \neq j$ (i.e. each set $\boldsymbol{\Upsilon}_{S,i}$ cannot be reached with state runs of M starting from X_{0j} with $j \neq i$), then $\boldsymbol{\Upsilon}_{S,i}$-opacity for M_i implies $\boldsymbol{\Upsilon}_{S,i}$-opacity for M. Since condition (4.40) holds $\forall i \in I_c$ then the sufficiency follows. Otherwise, suppose that for some i, j with $i \neq j$, $\boldsymbol{\Upsilon}_{S,i} \cap \boldsymbol{\Upsilon}_{S,j} \neq \emptyset$. Any two state runs $r'_x r_{xi}$ and $r''_x r_{xj}$ of M, with r_{xi} and r_{xj} state runs of M_i and M_j, respectively, are distinguishable. In fact, since X_{0i} and X_{0j} belong to $\mathcal{T}_C$, then $X_{0i} \cap X_{0j} = \emptyset$. Therefore, whenever the current state of a state run of M is in X_{0i}, such belonging can be deduced from the available output information, because of the critical observability of M with respect to each of them. The state runs r_{xi} and r_{xj} have initial states in X_{0i} and X_{0j}, respectively. Then, it is not possible that $r'_x r_{xi}$ and $r''_x r_{xj}$ are indistinguishable. Then, given a run $r'_x r_{xi}$ of M, ending in $\boldsymbol{\Upsilon}_{S,i}$, opacity holds if there exists a state run of M which is indistinguishable from $r'_x r_{xi}$ and ends in $X \setminus \boldsymbol{\Upsilon}_S$. All state runs of M which are indistinguishable from $r'_x r_{xi}$ have a run of M_i as suffix. Since M_i is $\boldsymbol{\Upsilon}_{S,i}$-opaque, then there exists a state run of M which is indistinguishable from $r'_x r_{xi}$ and ends in the $X_i \setminus \boldsymbol{\Upsilon}_{S,i}$ which is a subset of $X \setminus \boldsymbol{\Upsilon}_S$. Finally, since condition (4.40) holds $\forall i \in I_c$, the sufficiency follows.
Necessity: Straightforward by Proposition 4.2.1. □

The advantage of using the sub-observers is that it is not necessary to build all O_i to check if a set is opaque. In fact, consider the set of states X_i of M_i. It is sufficient to build the observers for the FSMs M_i if $\boldsymbol{\Upsilon}_S \cap X_i \neq \emptyset$. It is readily seen that the proposed method allows a reduction of computational cost from $2^{|X|}$ to $\sum_{i \in I} 2^{|X_i|}$.

4.2.4 Switching Observer

In this section, we propose the notion of *switching observer* by using the defined sub-observers. The purpose of the switching observer is to demonstrate how sub-observers can be used equivalently to a traditional observer by employing appropriate switching mechanisms. This suggests that the switching procedure leverages the benefits of using sub-observers while permitting the same functionality as the regular observer.

The switching observer, called $\mathcal{O}$, is constructed by appropriately switching between the observers in the family of sub-observers $\{O_i, i \in I_c\}$. Switching among observers $\{O_i, i \in I_c\}$ is triggered by the state run r_x. Roughly speaking, consider a given state run r_x of M, with $r_x(1) \in X^{(i)}$ for some $i \in I_c$. The observer at the first step is O_i and it will not change until the state run reaches a different set in the family $\mathcal{T}_C$, say $X^{(j)}, i \neq j$. At this step, called the "switching step", the current observer becomes O_j, with the current observer state equal to $X^{(j)}$ and it remains the same until the state run reaches the next different set in $\mathcal{T}_C$. Let k_h, k_{h+1} denote two consecutive switching steps, and define the intervals $I_h = [k_h, k_{h+1} - 1]$, $h = 1, 2, ..., H$, with $I_H = [k_H, |r_x| + 1)$. Let us denote with $\mathcal{O}(h) \in \{O_i, i \in I_c\}$ the observer associated to the interval I_h. Algorithm 4.4 presents the switching observer formally.

Algorithm 4.4 Evolution of Switching Observers

Input: $M = (X, X_0, Y, H, \Delta)$, $r_x \in \mathcal{X}$
Main:
  $h = 1$, $k = 2$
  i such that $r_x(1) \in X_i$
  $\mathcal{O}(h) = O_i$
while $r_x(k) \notin X_p$ for $p \in I_c \backslash \{i\} \wedge k < |r_x|$ **do**
  $k = k + 1$
  if $r_x(k) \in X_p \in \mathcal{T}_C$ **then**
    $i = p$ and $h = h + 1$
    $\mathcal{O}(h) = O_i$
  end if
end while
Output: $\mathcal{O}$: Switching observer

By construction, the traditional observer and the switching observer are synchronized with the output run of M, i.e. at each step the state of O is the same as the related state of the switching observer built following the algorithm above.

The following result presents this property formally:

Theorem 4.2.3

For any state run of M, at each step, the state of O is equal to the state of $\mathcal{O}$. □

Proof. Whenever the current state of M is $x \in X^{(i)}$, for some $i \in I_c$, the state of O is equal to $X^{(i)}$ by Proposition 4.2.2. By construction of the switching observer, the result follows. □

4.2.5 Example

Consider the FSM shown in Fig. 4.12 where the secret set is $\mathbf{\Upsilon}_S = \{3\}$. The critical observable set of the given FSM is $\mathcal{T}_C = \{\{1\}, \{2\}, \{4, 6\}\}$. As it can be seen from Fig. 4.13, $\mathbf{\Upsilon}_S \subset X_2'$ (removing all transitions to the states of critical totally-indistinguishable set yields M_1 to be only state 1 so this is not shown in the figures). Therefore, since $X_1' \cap \mathbf{\Upsilon}_S = \emptyset$ and $X_3' \cap \mathbf{\Upsilon}_S = \emptyset$, it is only necessary to check the opacity of M_2 for the given $\mathbf{\Upsilon}_S$. Using Theorem 4.2.1,

$$\hat{X}_{O_2} \cap 2^{\mathbf{\Upsilon}_S} = \emptyset$$

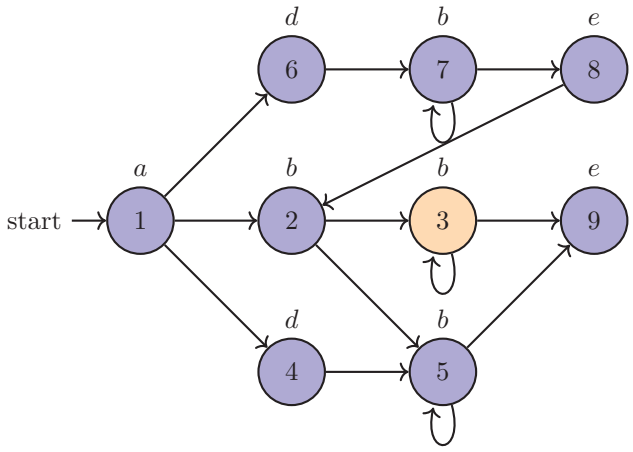
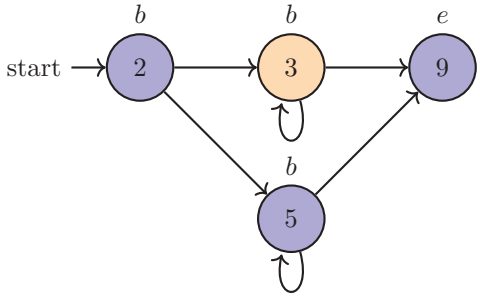
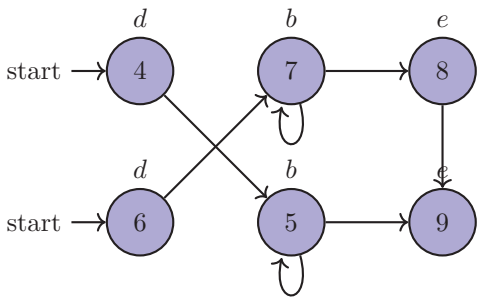


Figure 4.12: FSM Model



(a) Subsystem M_2

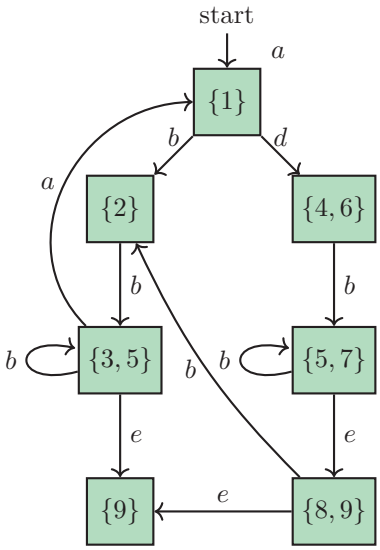


(b) Subsystem M_3

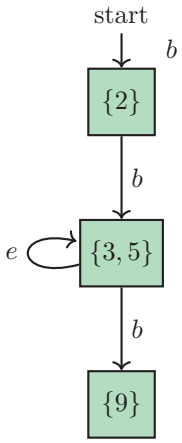
Figure 4.13: Obtained FSMs by considering $Ac(M'|_i)$

yields that the secret set is opaque to the intruder in M_2. Hence, based on Theorem 4.2.2, the defined FSM M is opaque with respect to the given secret set $\boldsymbol{\Upsilon}_S$. The observer for the overall system and the observer for M_2 are shown in Fig. 4.14. In this specific example, we need to construct an observer for a system with set of states of cardinality 4 instead of an observer for a system with set of states of cardinality 9.

In summary, this chapter has explored security in FSM–based systems from multiple perspectives: attacks on single agents, attacks across multi–agent networks, and passive observation threats. Each section tackled a specific challenge–detecting and locating actuator attacks, ensuring the integrity of interconnected agents, and protecting sensitive information from passive observers. The numerical examples included along the way helped illustrate the applicability of the proposed approaches. Altogether, these studies



(a) Traditional observer O



(b) Sub- observer O_2

Figure 4.14: Traditional observer vs sub-observer O_2

offer a clear picture of how FSM-based systems can be assessed and protected against a variety of threats, providing useful insights for both understanding and improving system security.

Chapter 5

Fault Detection

The increasing complexity of distributed and automated systems demands robust fault detection mechanisms that can operate effectively even when full observability is not guaranteed. PN, owing to their ability to model concurrent and asynchronous systems, have become a popular modeling framework in control and monitoring applications. However, in many real–world scenarios, it is often impractical or costly to observe the full state of such systems. This chapter addresses the problem of fault detection in PN under partial observation, where only a subset of the system's behavior can be measured directly.

In the context of PN, two types of sensors are typically available: place sensors, which provide information about the marking (i.e., token count) of specific places, and transition sensors, which detect the firing of transitions. Given the partial and potentially limited sensing structure, the goal of this work is to develop a methodology capable of detecting input faults i.e., faults that affect the system's inputs based on the available sensor data. To this end, the PN dynamics are reformulated using a descriptor framework, which allows for a compact representation of the marking evolution. An observer-based fault detection scheme is then designed within this framework to monitor the system and identify deviations caused by faults, despite the restricted observability.

It is worth emphasizing that this chapter focuses on fault detection for POPNs at the system level, without explicitly addressing multi–agent or cooperative control aspects. Moreover, the treatment here assumes ideal measurements and does not explicitly consider measurement noise or delays; issues of robustness are therefore not addressed in the present development. Nevertheless, POPN naturally arise in distributed and networked environments, including MASs, where limited sensing and incomplete information are common. From this perspective, the fault detection framework developed here provides a basis that can be leveraged in such settings, even though the technical development in this chapter is confined to single PN models. The results presented in this chapter are currently being prepared for submission to [145]

5.1 Petri Nets Modelling

Here we recall the model of *Partially Observed Petri Net* (POPN) as described in (2.12).

$$N = (P, T, Pre, Post, P_0, T_0) \tag{5.1}$$

Similarly, we recall the evolution of marking of POPN as described in (2.13):

$$M_{k+1} = M_k + W\sigma_{k+1}$$

For further analysis, we make the following assumptions:

Assumption 5.1.1

- *Fault represents the loss of communication between places (P)*
- *Input faults always belong to the unmeasurable space.*

□

These assumptions reflect common challenges in monitoring distributed systems. Modeling faults as communication losses allows the detection framework to focus on behavioral deviations caused by missing or delayed information, which are typical in networked environments. Moreover, restricting input faults to the unmeasurable space

introduces a realistic and nontrivial scenario, where faults cannot be detected through direct measurements alone. This necessitates the use of observer–based techniques capable of reconstructing unobservable behavior and isolating the presence of faults based on indirect evidence from the measurable part of the system.

Next, we modify (2.13), to include the effect of faults in the input channel as:

$$M_{k+1} = M_k + W\sigma_{k+1} + Ff_{k+1} \tag{5.2}$$

Here f_k is the fault function described as:

$$f_k = diag(\sigma_k) \times fault \tag{5.3}$$

and F is the fault distribution matrix.

Next, we adopt the descriptor system formulation introduced in [113], [105], and [106], and incorporate it into our framework by partitioning both the marking vector and the transition firing vector into measurable and unmeasurable components.

$$M_k = \begin{bmatrix} M_k^1 \\ M_k^2 \end{bmatrix} \text{ and } \sigma_k = \begin{bmatrix} \sigma_k^1 \\ \sigma_k^2 \end{bmatrix}$$

where,

- $M_k^1 \in \mathbb{N}^{n_1}, M_k^2 \in \mathbb{N}^{n_2}$ are respectively, the marking of measured places and unmeasured places,
- $\sigma_k^1 \in \mathbb{N}^{m_1}, \sigma_k^2 \in \mathbb{N}^{m_2}$ are respectively the firing count of the measured and unmeasured transitions at time k,
- $n = n_1 + n_2$ and $m = m_1 + m_2$

Let us also decompose the incidence matrix W based on the observable and unobservable transitions:

$$W = [W_1|W_2] = \begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{bmatrix}$$

with $W_{11} \in \mathbb{R}^{n_1 \times m_1}$, $W_{12} \in \mathbb{R}^{n_1 \times m_2}$, $W_{21} \in \mathbb{R}^{n_2 \times m_1}$ and $W_2 \in \mathbb{R}^{n_2 \times m_2}$.

Using the above decomposition of W, and (5.2), we can redefine our system as:

$$E\mathcal{M}_{k+1} = A\mathcal{M}_k + W_2\sigma_{k+1}^2 + Ff_{k+1} \tag{5.4}$$

$$y_k = C\mathcal{M}_k$$

where,

- $\mathcal{M}_k = \begin{bmatrix} M_k & \sigma_k^1 \end{bmatrix}$
- $E = \begin{bmatrix} I_n & -W_1 \end{bmatrix}$
- $A = \begin{bmatrix} I_n & 0_{n \times m_1} \end{bmatrix}$
- $C = \begin{bmatrix} I_n & 0_{n_1 \times n_2} & 0_{n_1 \times m_1} \\ 0_{m_1 \times n_1} & 0_{m_1 \times n_2} & I_{m_1} \end{bmatrix}$
- $F = -W_2$

The resulting descriptor representation of the POPN captures the evolution of the system's marking in a compact form, while also allowing for the integration of partial observations and potential fault inputs. This formulation serves as the foundation for the design of an observer that can track the system's behavior and enable fault detection, even when complete state information is not available.

5.2 Observability of Partially Observed Petri Nets

In this section, we recall notions of observability for POPN, as discussed in [105], [113]. In particular, we focus on the concepts of *Causal Observability* and *Observability* for POPN presented in (5.4).

Causal Observability of a POPN refers to the capability to uniquely infer both the marking vector M_k and the transition firing vector σ_k from the system outputs y_k, assuming that the initial marking M_0 is known. In contrast, *Observability* is defined as the ability to uniquely determine the marking vector M_k and the firing vector σ_k solely from the outputs y_k, without any prior knowledge of the initial marking M_0.

Next, we review the theorems from [105], [113], which address these concepts of *Causal observability* and *Observability* for the descriptor system defined in (5.4), and discuss their direct implications for the POPN formulation in (5.1).

Theorem 5.2.1

1. *The descriptor system in* (5.4) *is Causal Observable, if*

$$rank \begin{bmatrix} E & -W_2 \\ C & 0_{(n+m_1)\times m_2} \end{bmatrix} = n + m \tag{5.5}$$

2. *The descriptor system in* (5.4) *is Observable, if*

$$rank \begin{bmatrix} \lambda E - A & -\lambda W_2 \\ C & 0_{(n+m_1)\times m_2} \end{bmatrix} = n + m, \forall \lambda \in \mathbb{C} \tag{5.6}$$

3. *The POPN N in* (5.1) *is Causal Observable, if* $rank(W_2) = m_2$
4. *The POPN N in* (5.1) *is Observable, if* $rank(W_2) = m_2$ *and* $n = n_1$

Here λ*, represents the eigenvalues computed using* $|\lambda E - A| = 0$. □

Proof. The proof of the this theorem is presented in detail in [105], [113]. □

Building on these concepts, the next section presents the design of a faul–detecting observer.

5.3 Fault–Detecting Observer Design

We now develop an observer that enables fault detection based on the available measurements. The key idea is to ensure that the observer error, the difference between the estimated and actual system behavior, converges to zero only in the absence of faults. In the presence of input faults, this error exhibits a detectable deviation, which serves as the basis for fault identification.

Let us assume that the descriptor system presented in (5.4) is *Causal Observable*, i.e condition 1 of Theorem 5.2.1 holds. Hence,we can define a known input observer described by the following equations:

$$z_{k+1} = Nz_k + G\sigma_{k+1} + Ly_k \tag{5.7}$$

$$\hat{\mathcal{M}}_k = z_k + Hy_k$$

where $z_k \in \mathbb{N}^s$ is the state estimate at time k and y_k is the output of the POPN at time k. N, L and H are matrices of appropriate dimensions that guarantee the asymptotic convergence of the observer in the absence of faults. Thus the problem of fault detection, reduced to finding matrices N, L and H such that the estimate $\hat{\mathcal{M}}_k$ converge asymptotically to the state vector $\mathcal{M}_k$ only in the absence of faults.

The estimation error for the observer in (5.7), is defined by:

$$e_k = \mathcal{M}_k - \hat{\mathcal{M}}_k \tag{5.8}$$

$$e_k = \mathcal{M}_k - z_k - Hy_k$$

$$e_k = (I_{n+m_1} + HC)\mathcal{M}_k - z_k$$

Let $UE = (I_{n+m_1} + HC)$

$$e_k = UE\mathcal{M}_k - z_k \tag{5.9}$$

$$e_{k+1} = UE\mathcal{M}_{k+1} - z_{k+1}$$

From (5.4) and (5.7)

$$\begin{aligned} e_{k+1} &= U(A\mathcal{M}_k + W_2\sigma^2_{k+1} + Ff_{k+1}) - (Nz_k + G\sigma_{k+1} + Ly_k) \\ &= UA\mathcal{M}_k + UW_2\sigma^2_{k+1} + UFf_{k+1} - Nz_k - G\sigma_{k+1} - LC\mathcal{M}_k) \end{aligned}$$

From (5.9), we have $z_k = UE\mathcal{M}_k - e_k$

$$\begin{aligned} e_{k+1} &= UA\mathcal{M}_k + UW_2\sigma^2_{k+1} + UFf_{k+1} - N(UE\mathcal{M}_k - e_k) \\ &\quad - G^1\sigma^1_{k+1} - G^2\sigma^2_{k+1} - LC\mathcal{M}_k \\ &= Ne_k + (UA - NUE - LC)\mathcal{M}_k + (UW_2 - G_2)\sigma^2_{k+1} \\ &\quad - G^1\sigma^1_{k+1} + UFf_{k+1} \end{aligned} \tag{5.10}$$

In the absence of fault, the error will converge to zero if the following conditions hold:

(i) Matrix N is asymptotic stable

(ii) $UA - NUE - LC = 0$

(iii) $UW_2 - G_2 = 0$ and $G_1 = 0$

(iv) $UF \neq 0$

(v) $I - HC = UE$

For further analysis we make the following assumptions:

Assumption 5.3.1

- $Ff_k \notin ker(E)$
- *The matrix* CUF *is square and have full rank.*
- *Pair* (UA, C) *is detectable.*

□

These assumptions ensure the feasibility and effectiveness of fault detection and isolation using the proposed observer. The condition $Ff_k \notin ker(E)$ guarantees that faults produce a nonzero effect on the system evolution specifically, on the marking vector M_k. This is necessary for the observer to "see" the fault in the evolution of the system, a key requirement for fault detection. The assumption that CUF is square and full rank ensures that each fault induces a unique and independent effect on the output. This is essential for constructing a decoupling matrix Q in later section, allowing each residual signal to respond to only one fault, thus enabling complete fault isolation. Finally, detectability of the pair (UA, C) ensures that the observer error converges to zero in the absence of faults, even if the system is not fully observable. Together, these assumptions define the structural and dynamic properties the system must satisfy for the proposed observer–based fault detection and isolation scheme to function correctly.

In the following, we present a systematic procedure for computing the observer matrices, ensuring that the conditions outlined above are fully satisfied.

Let

$$UF = D = \begin{bmatrix} W_2 \\ \mathbf{1_{m_1 \times m_2}} \end{bmatrix} \tag{5.11}$$

Here, $\mathbf{1}_{m_1 \times m_2}$, denotes a matrix with m_1 rows and m_2 columns, with all entities equal one. This equality ensures that the effect of faults is propagated only through the components of the system that are structurally linked to the faulty transitions. In the context of POPN, this means that a fault occurring at a transition t influences only the output measurements associated with the places and transitions that are immediately connected to t, either as predecessors or successors. By limiting the propagation of fault effects to a confined part of the system, this approach enables more precise fault isolation, as will be discussed in the following section.

From (5.11) and (v), we have,

$$\begin{bmatrix} U & H \end{bmatrix} \begin{bmatrix} E & F \\ C & 0 \end{bmatrix} = \begin{bmatrix} I & D \end{bmatrix}$$

if $\begin{bmatrix} E & F \\ C & 0 \end{bmatrix}$ is full row rank matrix then we can calculate U and H using the following equation

$$\begin{bmatrix} U & H \end{bmatrix} = \begin{bmatrix} E & F \\ C & 0 \end{bmatrix}^{+} \begin{bmatrix} I & D \end{bmatrix} \tag{5.12}$$

here $()^{+} = ()^{T} \times (() \times ()^{T})^{-1}$, denotes the Moore–Penrose pseudoinverse of a matrix with full column rank.

Now, by placing (v) into (ii), we get

$$UA - N(I - HC) - LC = 0$$

$$UA - N + NHC - LC = 0$$

Let $K = L - NH$, then

$$UA - N - KC = 0$$

$$N = UA - KC \tag{5.13}$$

The gain matrix K can be adjusted to make the observer matrix N asymptotically stable, provided that the pair (UA, C) is detectable. Finally we have

$$L = K + NH \tag{5.14}$$

By using (5.11),(5.12),(5.13) and (5.14), we can compute all the required matrices for the observer.

To summarize the observer design methodology, the Algorithm 5.1 outlines the step-by-step procedure for constructing an observer that ensures fault detectability under partial observation. The effectiveness of this algorithm is guaranteed provided that Assumptions 5.3.1 are satisfied. The algorithm captures the selection of the necessary matrices and conditions required to guarantee that the observer error converges to zero only in the absence of faults.

Let

$$\upsilon_k = y_k - \hat{y}_k \tag{5.15}$$

denote the output residual, defined as the difference between the measured output and the output estimated by the observer. The proposed observer ensures that:

$$\upsilon_k(i) = 0 \quad \text{for all } i \in \mathbb{N} \quad \Longleftrightarrow \quad \text{no fault is present in the system.}$$

In other words, all components of the error signal remain identically zero over time if and only if the system operates without faults. Any deviation from zero in $\upsilon_k(i)$ indicates the presence of a fault affecting the system's unmeasurable inputs. This property forms the basis for fault detection, as the observer is sensitive to fault–induced discrepancies that cannot be explained by the system's nominal behavior alone.

Algorithm 5.1 Observer Design

1: Calculate U and H using

$$\begin{bmatrix} U & H \end{bmatrix} = \begin{bmatrix} E & F \\ C & 0 \end{bmatrix}^{+} \begin{bmatrix} I & D \end{bmatrix}$$

2: Compute $\begin{bmatrix} G_1 & G_2 \end{bmatrix}$

$$G_2 = W_2, G_1 = 0$$

3: Adjust K, so that N is stable:

$$N = UA - KC$$

4: Compute L, using

$$L = K + NH$$

5.4 Residual Design for Fault Isolation

While the detection of faults is essential, distinguishing which specific fault has occurred is equally important for enabling timely and targeted corrective actions. This process, known as fault isolation, requires the design of residual signals that not only react to the presence of faults but also provide information about their location.

In this section, we extend the residual framework introduced earlier to enable isolation by designing a structured set of residual signals, each sensitive to a specific fault or group of faults. The objective is to construct these signals such that each fault generates a distinguishable signature in the residual space, while maintaining robustness to other unmodeled disturbances or fault–free behavior.

To enable fault isolation, we build upon the observer–based residual structure introduced in the previous section. Recall that the output residual at step k is defined as:

$$\upsilon_k = y_k - \hat{y}_k$$

where y_k is the measured output and $\hat{y}_k$ is the observer's estimate. From (5.4), we have $y_k = C\mathcal{M}_k$, hence we can say:

$$\upsilon_k = C\mathcal{M}_k - C\hat{\mathcal{M}}_k$$

From (5.8), we have $e_k = \mathcal{M}_k - \hat{\mathcal{M}}_k$, hence:

$$\upsilon_k = Ce_k$$

As indicated in (5.10) and the preceding conditions from (i) to (v), the steady–state behavior of the error signal is driven solely by the fault component UFf_k. Hence we can rewrite output residual as:

$$\upsilon_k = CUFf_k$$

To isolate individual faults, we define the structured residual vector $r_k \in \mathbb{R}^{m_2}$ as:

$$r_k = Q\upsilon_k = QCUFf_k = QRf_k \tag{5.16}$$

Here $Q \in \mathbb{R}^{m_2 \times m}$ is a design matrix chosen to decouple fault effects and $R = CUF$. To ensure each component of r_k is affected by only one fault, we impose the condition

$$QR = I$$

which implies that each residual signal $r_k(i)$ responds exclusively to fault $f_k(i)$, thus enabling fault isolation.

5.4.1 Residual Compression via Signature Matrix

In practical scenarios, it may not be feasible to design as many residual signals as there are faults, due to limitations in sensing or processing capabilities. To address this, we consider a compressed residual scheme where fewer residual signals are used to distinguish between fault patterns. Let m_2 be the number of faults and p be the number of residual signals to be generated. We define a fault signature matrix $S \in \mathbb{R}^{p\times m_2}$, whose rows encode binary or structured combinations of faults. Each row of S defines how individual faults contribute to a corresponding residual.

Given that the output residual is designed as $r_k = Q\upsilon_k$, for a lower dimension residual signal $\tilde{r}_k$, we define a compression Matrix $S \in \mathbb{R}^{p\times m_2}$, here $p < m_2$ and compute:

$$\tilde{r}_k = Sr_k \tag{5.17}$$

The matrix S acts as a fault signature matrix, where each row specifies a binary or weighted combination of fault signals. This approach maintains the existing observer and isolation design, and introduces an additional post–processing layer that reduces the number of residuals without requiring any change in the original observer or Q matrix.

Remark 5.4.1

While the use of a binary–coded signature matrix S enables dimensionality reduction of the residual signal and simplifies the isolation process, it inherently limits the ability to distinguish between multiple simultaneous faults. Since the compressed residual $\tilde{r}_k = Sr_k$ is a lower–dimensional representation, different fault combinations can produce identical residual patterns, leading to ambiguity in fault interpretation. Therefore, this approach is most effective under the assumption of single–fault occurrence. The limitations of this method in the presence of multiple faults are illustrated in the example provided in the following section. □

Fig. 5.1 summarizes the overall workflow of the observer design for fault detection and isolation, and also illustrating its application during runtime.

5.5 Simulation Results

Consider the POPN shown in Fig. 5.2, it consist of six places from p_1 to p_6 and six transitions from t_1 to t_6. We assume that the places p_1, p_2, p_3 and p_4 and transitions t_1, t_2 are observable (i.e. $n_1 = 4$,$n_2 = 2$, $m_1 = 2$ and $m_2 = 4$). Additionally, transition t_4 is concurrent t_2 or t_3, meaning that the pair (t_4,t_2) or the pair (t_4,t_3) may fire in a single step.

Based on this structure, the incidence matrix W is computed as follows:

$$W = \begin{bmatrix} -1 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 & -1 \end{bmatrix}$$

Since, place p_1 initially holds a token, the initial marking M_0 is defined as:

$$M_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Recall that the evolution of the marking is described by (5.4), and the observer used for fault detection is given in (5.7). The signal compression matrix S, used for generating the reduced, is chosen as follows:

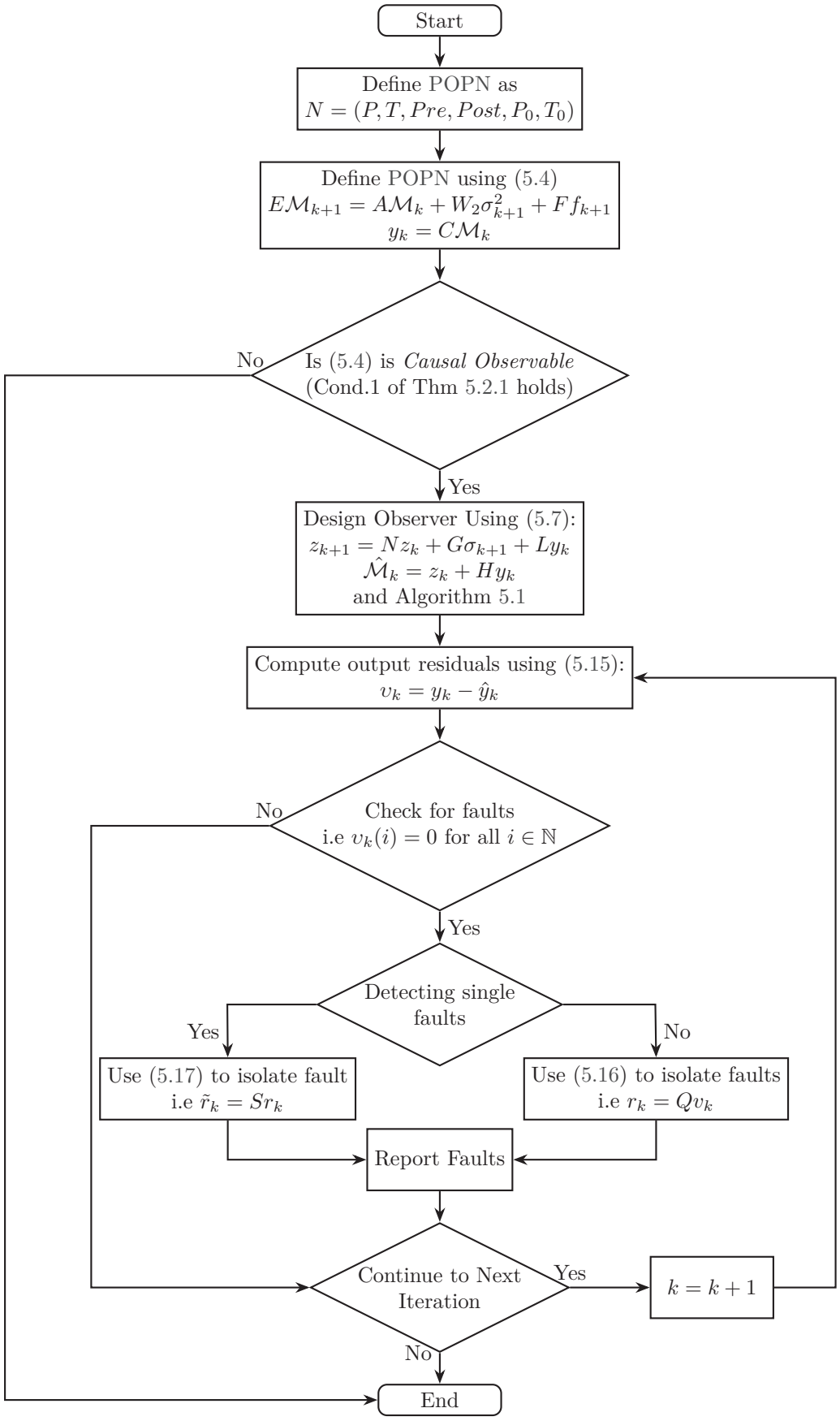


Figure 5.1: Flow Diagram of the Fault Diagnosis Framework in POPN

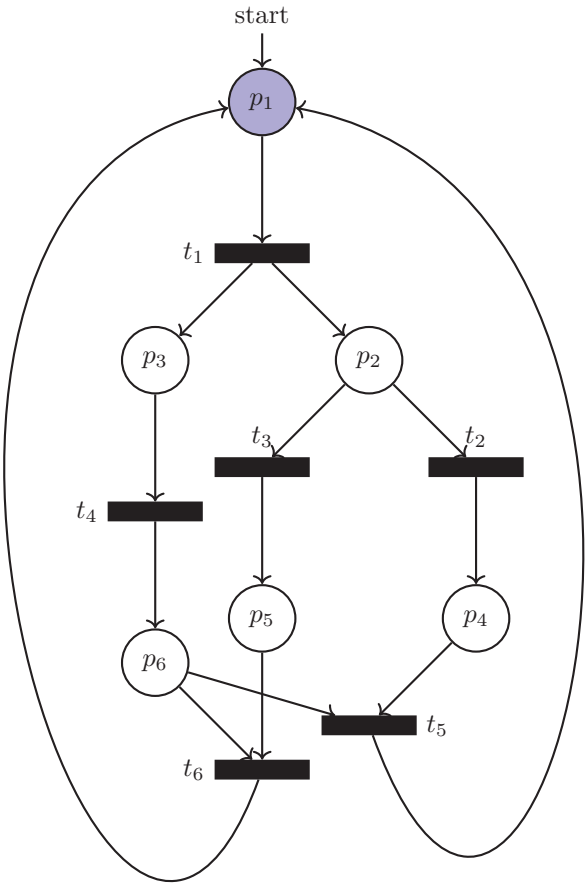


Figure 5.2: Petri Net structure

$$S = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Based on this selection, the reduced residual signal $\tilde{r}$ can be interpreted (or decoded) as:

$\tilde{r}(1)$	$\tilde{r}(2)$	$\tilde{r}(3)$	
0	0	0	no fault
1	0	0	fault in t_3
0	1	0	fault in t_4
1	1	0	fault in t_5
0	0	1	fault in t_6

The input signal σ is described as follows:

$$\sigma = \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \end{bmatrix} = \begin{bmatrix} k=1 & k=2 & k=3 & k=4 & k=5 & k=6 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

In the above matrix, each column corresponds to the input σ at a specific instant k.

In the following analysis, we examine the behavior of the given POPN structure under three distinct scenarios:

- **Case 1:** No faults
- **Case 2:** Fault in transition t_4
- **Case 3:** Fault in transition t_4 and t_5

Each case highlights different aspects of fault detection and isolation performance within the system.

5.5.1 Case 1: No Faults

In the absence of faults, as shown in Fig. 5.3, the actual output y and the estimated output $\hat{y}$ coincide perfectly. Consequently, all components of the output residual defined in (5.15) and the reduced residual signal in (5.17) remain consistently zero, as illustrated in Fig. 5.4 and Fig. 5.5, respectively.

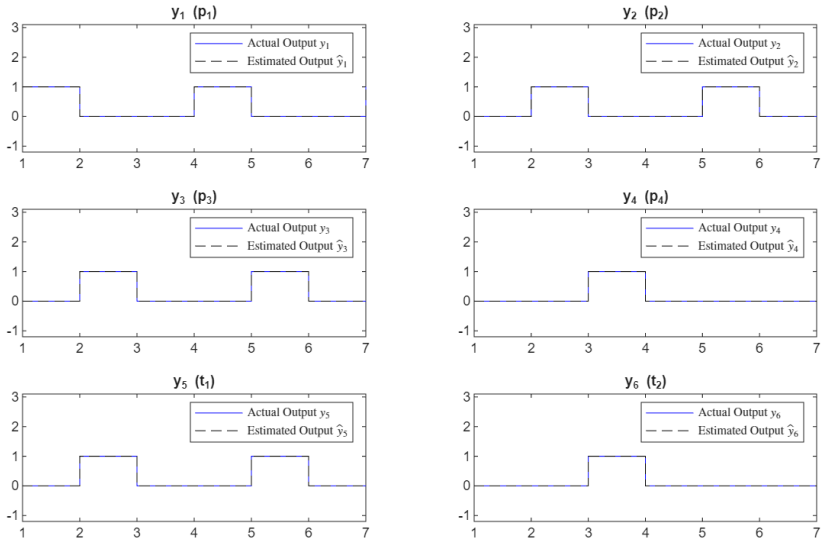


Figure 5.3: Actual y_k and Estimated output $\hat{y}_k$ in the absence of faults

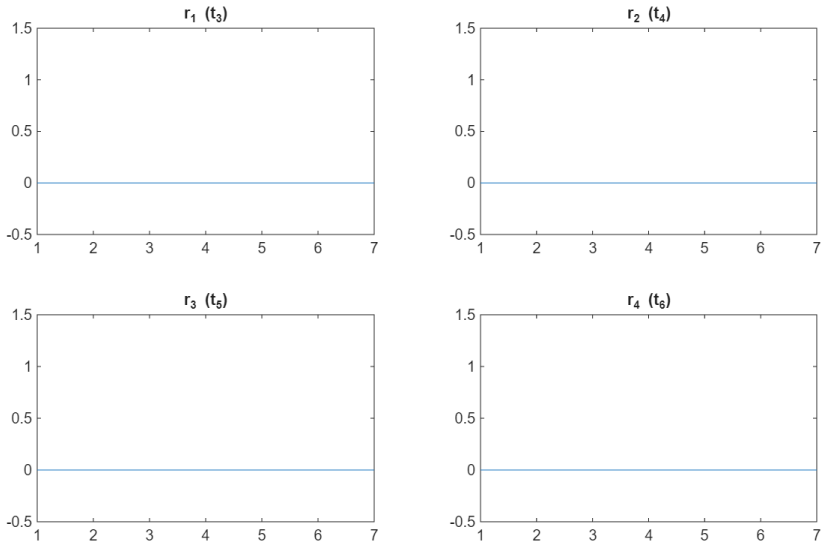


Figure 5.4: Output residual r_k in the absence of faults

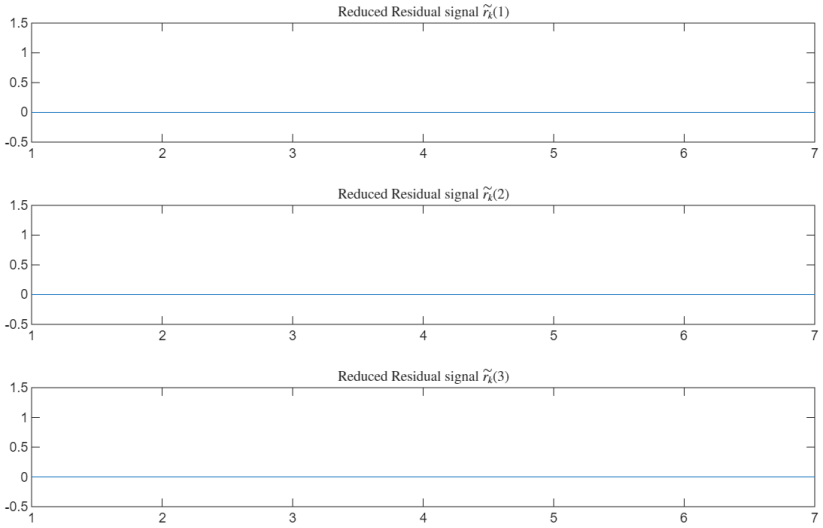


Figure 5.5: Reduced residual signal $\tilde{r}_k$ in the absence of faults

5.5.2 Case 2: Fault in transition t_4

Next, we introduce a fault in transition t_4, represented by the fault vector defined in (5.3) as:

$$\text{fault} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T.$$

The impact of this fault on transition t_4 is illustrated in Fig. 5.6. It can be observed that at each time instant k when t_4 is active (i.e., equals 1), the fault causes it to drop to 0. The resulting actual output y and estimated output $\hat{y}$ are shown in Fig. 5.7, where discrepancies appear at $k = 3$ and $k = 6$. Correspondingly, Fig. 5.8 shows that only the residual component r_2, which corresponds to t_4, deviates from zero at these time points. Similarly, the reduced residual signal $\tilde{r}(2)$ becomes active during the fault, effectively indicating the fault in t_4.

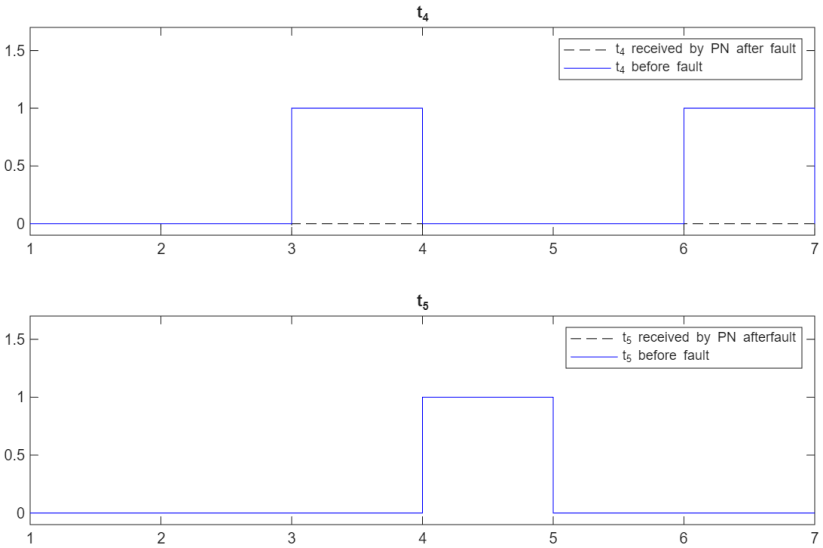


Figure 5.6: Input signal t_4 and t_5, before and after fault in t_4

5.5.3 Case 3: Fault in transitions t_4 and t_5

Finally, we examine the same structure with simultaneous faults in two channels, namely t_4 and t_5. In this case, the fault vector in (5.3) is defined as:

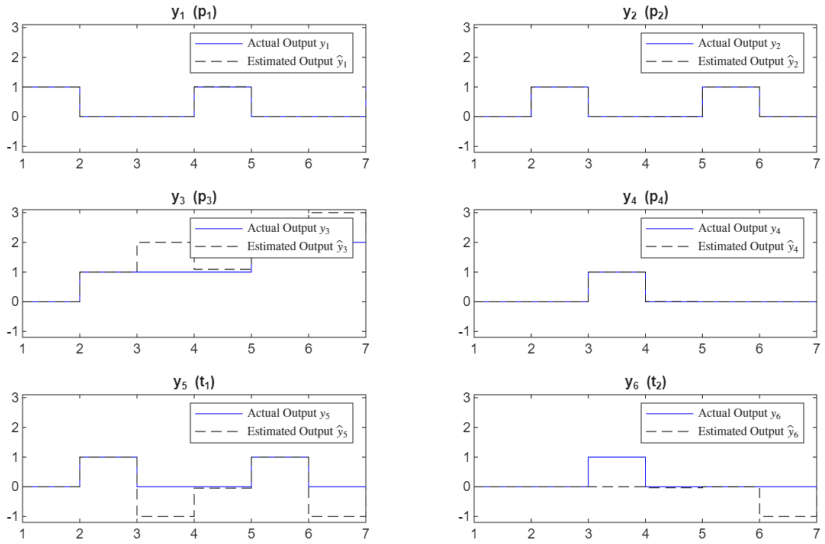


Figure 5.7: Actual y_k and Estimated output $\hat{y}_k$ in fault in channel t_4

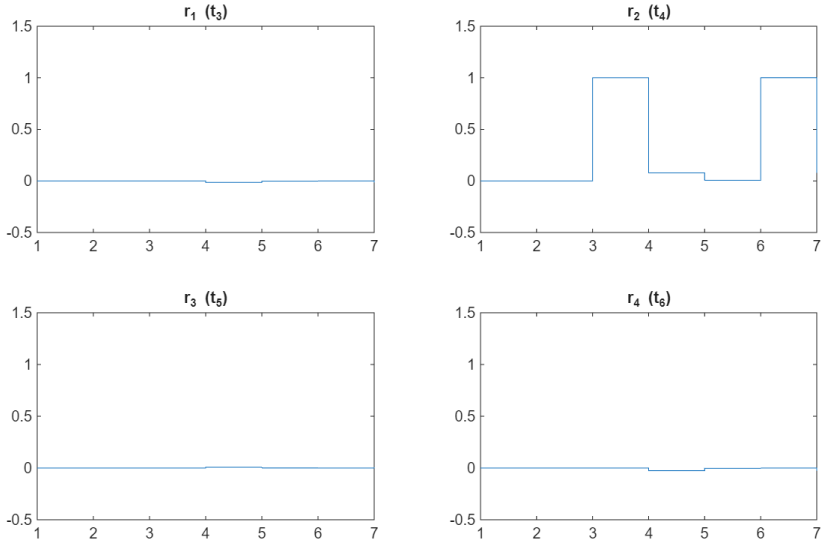


Figure 5.8: Output residual r_k in fault in channel t_4

$$\text{fault} = \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}^T.$$

The effects of these faults on t_4 and t_5 are illustrated in Fig. 5.10. As shown in Fig. 5.11, the actual output y and estimated output $\hat{y}$ deviate at fault occurrence times. Fig. 5.12 demonstrates that the residual signals r_2 and r_3 activate (equal to 1) only when their corresponding faults occur. Similarly, the reduced residual components in Fig. 5.13 distinctly indicate faults in t_4 and t_5 during the respective instances. However, as discussed in Remark 5.4.1, at time $k = 4$, both $\tilde{r}(1)$ and $\tilde{r}(2)$ are active simultaneously, which can be misinterpreted as faults in t_3 and t_4. Therefore, we conclude that the reduced residual approach remains reliable only for single-channel faults. When multiple faults occur simultaneously using the binary weighted signature matrix S, accurate fault isolation is not guaranteed.

Taken together, the three cases show how the fault detection system responds in different scenarios. In the first case, with no faults present, everything works perfectly, the actual and estimated outputs align exactly, and all residuals stay at zero, confirming that the system is reliable under normal conditions. In the second case, a single fault

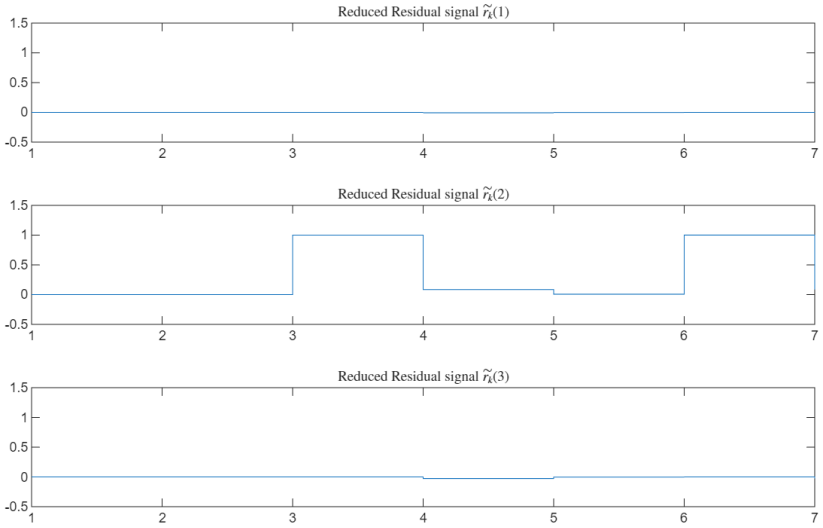


Figure 5.9: Reduced residual signal $\tilde{r}_k$ in fault in channel t_4

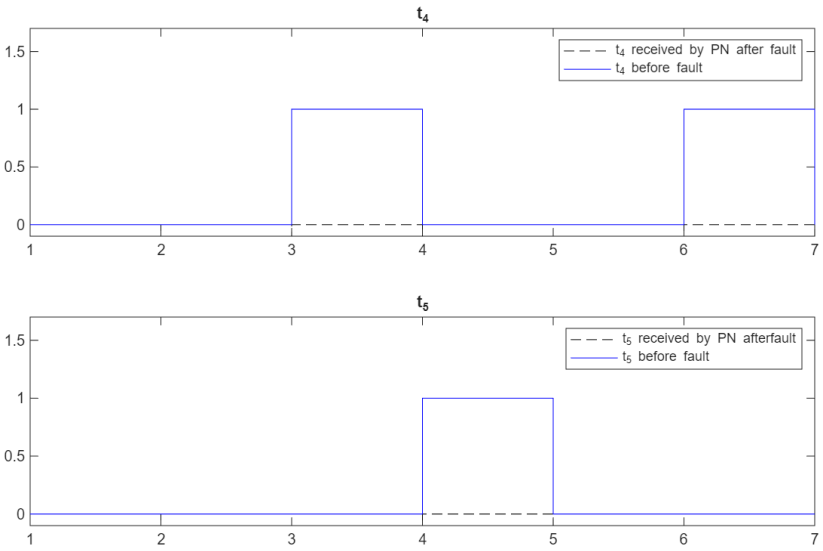


Figure 5.10: Input signal t_4 and t_5, before and after fault in t_4 and t_5

in transition t_4 is introduced, and the system detects it right away, the corresponding residual spikes precisely when the fault occurs, clearly signaling the problem. The third case introduces simultaneous faults in t_4 and t_5, which adds complexity. Here, the reduced residual approach shows its limitation, it can isolate only one fault at a time. However, when the number of residuals matches the number of faults, multiple faults can still be identified accurately. Overall, these cases demonstrate that the fault detection framework is robust and effective, performing smoothly under normal and single–fault conditions while also highlighting the strengths and boundaries of different residual strategies in handling multiple faults.

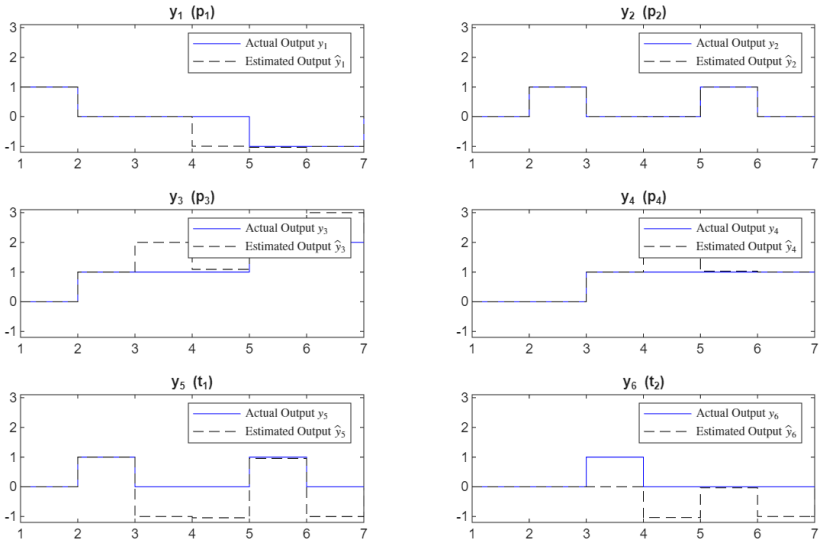


Figure 5.11: Actual y_k and Estimated output $\hat{y}_k$ in fault in channel t_4 and t_5

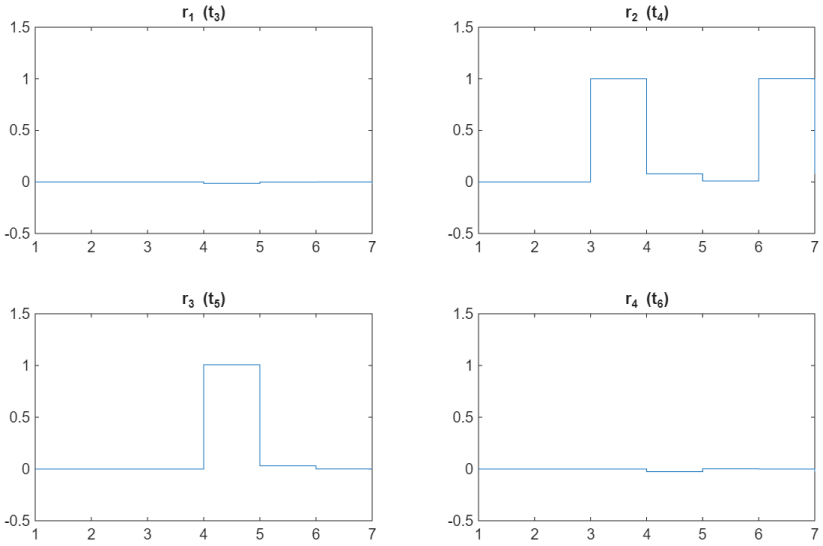


Figure 5.12: Output residual r_k in fault in channel t_4 and t_5

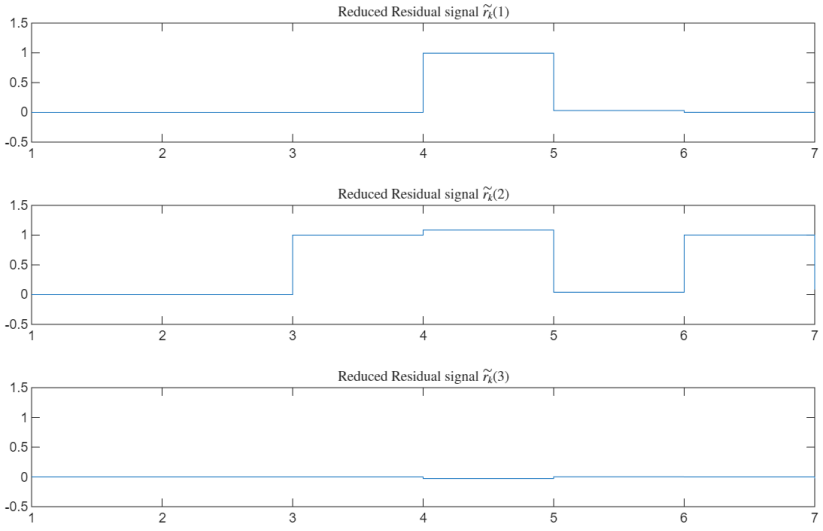


Figure 5.13: Reduced residual signal $\tilde{r}_k$ in fault in channel t_4 and t_5

Chapter 6

Conclusion

6.1 Key Findings and Contributions

The main goal of this thesis, titled *Control, Coordination, and Monitoring of Autonomous Agents in the Agri-Food Field*, was to develop and analyze robust methodologies for controlling, coordinating, and monitoring MASs in realistic, uncertain environments. These methods are particularly relevant to modern agriculture, where automation and intelligent agent collaboration can greatly improve efficiency, precision, and sustainability in tasks such as crop monitoring, irrigation management, and autonomous field operations.

The work spans three interconnected aspects, each closely tied to agricultural applications that rely on cooperation between machines and systems for safe and efficient operation: control and coordination of nonlinear MASs, security analysis of single and networked DES modeled using FSM modeling formalism, and fault detection in DES modeled as POPN. The technical details of these stated goals are presented in Chapters 3, 4, and 5, and the following provides a brief conclusion of each.

Chapter 3 presented a detailed study on the control and coordination of nonlinear MASs affected by state delays, actuation disturbances, and measurement errors. The primary objective was to develop a robust QSE control framework capable of maintaining stable and reliable consensus tracking, even under uncertain or constrained conditions.

To overcome the challenges of coordinating multiple agents, special attention was given to balancing communication efficiency, robustness, and control accuracy. The proposed control structure allows individual agents to work together smoothly while remaining stable and resilient against the disturbances and network limitations that often occur in large–scale cooperative systems.

The proposed methodology introduces a novel concept of SDCFs, derived from a general class of Lyapunov–Krasovskii functionals, which has been revisited and extended to suit the robust QSE consensus tracking of nonlinear time–delay MASs. Furthermore, by applying an ISS redesign approach, a new control law was developed to effectively attenuate the impact of bounded actuation disturbances and measurement uncertainties. The stabilization in the sample–and–hold sense was rigorously analyzed to confirm that the QSE implementation of the robustified SDCFs guarantees semiglobal practical consensus tracking, even when the system operates under time–varying sampling intervals and quantized communication channels.

To validate the theoretical results, the proposed control approach was applied to a special class of nonlinear MASs. A series of simulations were carried out for a network of UAVs modeled using the same framework. The analysis showed that the proposed controller can effectively and efficiently coordinate multiple UAVs, while maintaining reliable consensus and strong performance even under realistic conditions. The findings highlight that the proposed controller can be utilized in a wide range of agricultural applications, such as coordinating autonomous farming vehicles, optimizing precision irrigation, and managing distributed sensor networks–areas where reliable coordination and communication–aware control are crucial.

In a broader sense, this research contributes to a better understanding of how robust cooperative control and coordination can be achieved in nonlinear MASs and lays the groundwork for future practical applications, especially in situations where systems must remain reliable, flexible, and efficient under real–world conditions.

In addition to control and coordination, it is equally important to ensure the reliable operation of autonomous agents under potential security threats. Chapter 4 addresses this aspect through the security analysis of single and networked DES, providing methods to monitor and protect agents.

Chapter 4 provides a detailed analysis of different aspects of security in DES, modeled as FSM, considering both active and passive attacks, and addressing the problem at multiple levels, from a single system to networks of interacting agents.

First, the security of an individual agent/system modeled as an FSM under actuator attacks was analyzed. A composition of the nominal plant and attacker FSMs was proposed to model the system's behavior under attack. This composed model was then used to derive conditions for attack detection and attack localization under the assumption that only one channel is compromised at a time. While the case of multiple simultaneously attacked channels was not explicitly considered, the methodology is readily extendable to such scenarios. Numerical examples were provided to illustrate the applicability of the approach and validate the theoretical results.

Building on the single–agent analysis, the framework was extended to networked systems. Specifically, a network of two agents, each modeled as an FSM, was considered. For these interconnected agents, a composed model was developed to represent the joint state evolution in the presence of attacks on communication channels. By leveraging the concept of DCO, necessary and sufficient conditions for attack detectability and attack localizability were established. This analysis provides the ground work for dealing with more complex network and offers practical direction for building secure and resilient MAS in agriculture, including applications like coordinated UAVs or teams of cooperative robots.

Finally, passive attacks in the form of opacity were addressed, focusing on information flow and the system's ability to hide critical information from an intruder. To manage the computational complexity inherent in analyzing large FSMs, a sub–observer approach was proposed for checking observability properties. Notions of total indistinguishability and critical observability were used to design these sub–observers. Additionally, switching observers, constructed by appropriately switching among the set of sub–observers, were introduced. The methodology was applied to analyze opacity, with illustrative examples validating the approach.

Overall, Chapter 4 offers a systematic approach for analyzing both active and passive security threats in single and networked systems, an important aspect for the monitoring of autonomous agents.

While security analysis helps ensure that agents can withstand malicious attacks, effective monitoring also includes detecting unexpected system faults. Chapter 5, address this by focusing on fault detection and localization in POPN, providing a natural complement to the security measures presented in Chapter 4.

Chapter 5 focused on fault detection in PN–modeled systems under conditions of partial observability. The evolution of markings of POPN was modeled using a descriptor system framework. Building on this foundation, an observer–based methodology was developed to detect input faults using the information provided by available place and transition sensors.

Furthermore, fault isolation was also addressed in detail. Residual signals were constructed to isolate and identify the specific faulty channels, providing precise information about the location of the fault within the system. This capability is crucial for timely corrective actions and enhances the overall reliability and maintainability of autonomous agricultural systems, such as sensor networks or robotic machinery.

A numerical example was presented and simulation results were analyzed to show that proposed fault detection and isolation algorithm can be used effectively and efficiently in POPN. Suggesting that the combination of the observer–based framework with residual signals proves to be a reliable method for monitoring DES modeled as POPN, even when full system information is not available.

It should be noted that, although POPN naturally arise in distributed or multi–agent settings, the technical development in this chapter focuses solely on single–system fault detection and does not explicitly address multi–agent coordination or interactions. The results presented in Chapter 5 provide an effective and efficient means of addressing faults in DES.

To conclude, this thesis addresses the control, coordination, and monitoring of autonomous agents applicable to agricultural applications. Chapter 3 develops robust strategies for controlling nonlinear MAS and achieving coordinated consensus among them. Chapters 4 and 5 investigate monitoring, addressing both security issues and fault detection to ensure that these systems can operate reliably and withstand unexpected disturbances. Altogether, the results form a comprehensive framework for designing autonomous agricultural systems that are resilient, efficient, and capable of performing safely under uncertain and challenging conditions.

6.2 Research Publications

The work carried out in this thesis has led to a number of scholarly contributions, including papers that have been published, submitted, or are planned for submission. The following section provides a categorized list of these contributions, highlighting how each relates to the goals and findings of this research.

- B. Bushra, E. De Santis and G. Pola, "Security and Localization of Cyber Attacks in Finite State Machines", *IEEE 20th International Conference on Automation Science and Engineering (CASE)*, Bari, Italy, pp. 2659-2664, 2024.
- B. Bushra, E. De Santis, M. D. Di Benedetto and G. Pola, "Observer Decomposition for Finite State Machines and its Application to Opacity", *IEEE 63rd Conference on Decision and Control (CDC)*, Milan, Italy, pp. 4443-4448, 2024.
- B. Bushra, E. De Santis and G. Pola, "Decentralized Attack Detection and Localization for Finite State Machines", *IEEE 64th Conference on Decision and Control (CDC)*, 2025, accepted for publication.
- B. Bushra and M. Djemai, "Fault detection and Isolation in Partially Observed Petri Nets", to submit.
- B. Bushra, E. De Santis, M. Di Ferdinando, S. Di Gennaro and P. Pepe, "On the Consensus Problem of Nonlinear Multi-Agents Systems via Digital Controllers", *International Journal of Robust and Nonlinear Control, Special issue on Multi–Agent Systems with delays and Networked Control Systems on IJRNC*, submitted.

6.3 Future Work

Although this thesis has addressed key aspects of control, coordination, and monitoring of autonomous agents, there are still many opportunities for further research and development. Real–world challenges, such as enhancing system scalability, handling multiple simultaneous attacks, managing hybrid or partially observed systems, and integrating diverse types of agents, were only partially addressed or left for future investigation. Extending the current methods to tackle these challenges could improve the reliability, efficiency, and adaptability of autonomous systems in practice. The following paragraphs highlights these potential directions in more detail, offering a roadmap for future research that builds on the foundations established in this thesis while addressing open challenges in creating robust, resilient, and intelligent autonomous systems.

While the proposed control and coordination strategy demonstrated promising results in managing state delays, future research could extend the framework to address input–output delays, which are common in practical systems. Handling such delays would make the control design more comprehensive and applicable to a wider range of real–world multi–agent scenarios.

In the case study, the presented controller was applied to a swarm of UAVs operating under communication and actuation uncertainties. However, in many real–world applications involving autonomous coordination of UAVs or drones, it is also necessary to ensure obstacle avoidance and safe navigation in dynamic environments while still

achieving cooperative objectives. Extending the proposed approach to incorporate these aspects represents another promising research direction.

Finally, an important direction for future work is to apply the proposed control strategy to MASs where the network connections can change over time. In such systems, links between agents may be disrupted or re–established due to movement, environmental conditions, or communication limits. Exploring how the framework performs under these conditions would give a better understanding of its stability and robustness, making it more suitable for practical, large–scale cooperative systems.

Looking ahead, future research in security analysis could focus on expanding the current framework to handle multiple simultaneous attacks on actuators, sensors, or communication channels. While the present methodology focused on the case where only one channel is compromised at a time, real–world systems often face coordinated attacks targeting several components at once. Developing detection and localization strategies capable of managing such scenarios would make the approach more robust and practically relevant.

Another promising direction is to look at larger and more complex networked systems, where many agents interact and communication links can change over time. Studying how attacks might spread in these dynamic environments, and making sure that detection and localization methods continue to work effectively, could offer important insights for building more resilient autonomous systems.

Finally, future work could focus on making the analysis of large FSMs more scalable and efficient. While sub–observer and switching observer methods already help to manage complexity, further improvements like better observer designs, model reduction, or hierarchical approaches could make it possible to study even bigger networks of agents, such as swarms of UAVs or teams of cooperative robots, in real–world situations.

The findings presented in this work on fault detection in POPN–modeled systems could be expanded in several interesting directions. One possible extension is toward dynamic or reconfigurable networks, where the structure of the system can change or adapt in response to faults or evolving conditions. In this thesis, the focus was mainly on fixed network structures and on fault detection and isolation. Exploring adaptive networks and developing fault–tolerant control strategies would be a valuable next step.

It would also be worthwhile to study stochastic PN that include varying state counts or non–uniform switching times. Such models could capture more realistic scenarios, for instance when agents are activated or deactivated during operation. Handling these dynamics would improve the reliability of fault detection in complex and evolving systems.

Another important direction is to perform a robustness analysis, evaluating how sensitive the residual signals are to disturbances that are not caused by faults. This would help determine how well the method performs in uncertain or noisy environments. The approach could further be extended to detect multiple faults occurring simultaneously, for example by using non–binary signature matrices or orthogonal separation techniques.

In addition, exploring decentralized observer designs for distributed multi–agent networks could make the detection process more scalable and less dependent on centralized coordination. Finally, it would be interesting to look into hybrid systems that combine PN with continuous dynamics, which could open the door to applications in cyber–physical and real–world control systems where discrete and continuous behaviors interact.

Finally, in this thesis, control and coordination, security analysis, and fault detection for networked autonomous agents were studied separately. A promising direction for future work would be to bring these pieces together into a single, unified framework. This could allow autonomous systems to operate more reliably and robustly, coordinating their actions while staying protected against attacks and able to detect faults quickly, all within the same platform.

Appendices

Appendix A

Appendix A

A.1 Proof of Theorem 3.3.1

Firstly, two useful lemmas are provided which will be helpful for proving Theorem 3.3.1. In particular, the following lemmas are based on Lemma 13 and Lemma 14 in [28] which are here suitably revised in order to cope with nonlinear time-delay MASs affected by exogenous known disturbances r_t.

Lemma A.1.1

(See Lemma 13 in [28]) Let Assumption 3.2.1 hold. Let $\tilde{k}$ be the function defined in (3.20) with given positive real ω. Let γ be an arbitrary positive real and $D = (-\gamma, \gamma)^m \subset \mathbb{R}^{\tilde{m}}$. Let α_4 be the function of class $\mathcal{K}$ defined, for $s \in \mathbb{R}^+$, as follows

$$\alpha_4(s) = \frac{(\nu + \eta\bar{p})s^2}{4\omega},$$

where η, ν and $\bar{p}$ are the positive reals in Definition 3.2.3. Then, for any $\phi_z \in \mathcal{C}^{\tilde{n}}$, for any $\phi_r \in \mathcal{C}^{\tilde{p}}$ and for any $d \in D$ the following inequality holds:

$$\begin{aligned} &\nu D^+ V(\phi_z, \phi_r, \tilde{k}(\phi_z, \phi_r) + d) \\ &+\eta \max\{0, D^+ p \circ V_1(\phi_z, \phi_r, \tilde{k}(\phi_z, \phi_r) + d) \\ &+\mu p \circ V_1(\phi_z(0))\} \leq \bar{\alpha}(\eta\mu e^{-\mu\Delta} p \circ \beta_1(\|\phi_z\|_\infty)) + \alpha_4(|d|). \end{aligned} \tag{A.1}$$

□

Lemma A.1.2

*(See Lemma 14 in [28]) Let Assumption 3.2.1 hold. Let the functional V_3, V_∞ and $\mathcal{D}_\infty$ as defined in points **(f.1)**, **(f.2)** and **(f.3)** of Section 3.2. Let α_i, $i = 1, 2,$, be the functions of class $\mathcal{K}_\infty$ defined in (A.6). Let α_3 be a function of class $\mathcal{K}_\infty$, for $s \in \mathbb{R}^+$, as*

$$\alpha_3(s) = (I_d - \bar{\alpha})(\eta\mu e^{-\mu\Delta} p \circ \beta_1(s)),$$

where β_1 is the function of class $\mathcal{K}_\infty$ related to the smooth separability property of the functional V and $\bar{\alpha}$ is the function in Definition 3.2.3. Let γ be an arbitrary positive real and $D = (-\gamma, \gamma)^m \subset \mathbb{R}^m$. Let α_4 be the function of class $\mathcal{K}_\infty$ in Lemma A.1.1. Then, the following conditions hold:

(c.1) $\alpha_1(\|\phi_z\|_\infty) \leq V_\infty(\phi_z) \leq \alpha_2(\|\phi_z\|_\infty),\ \forall \phi_z \in \mathcal{C}^{\tilde{n}}$;

(c.2) *the function $(\phi_z, \phi_r, u) \to \mathcal{D}_\infty(\phi_z, \phi_r, u)$ is Lipschitz on bounded subsets of $\mathcal{C}^{\tilde{n}} \times \mathcal{C}^{\tilde{p}} \times \mathbb{R}^{\tilde{m}}$;*

(c.3) $D^+ V_\infty(\phi_z, \phi_r, u) \leq \mathcal{D}_\infty(\phi_z, \phi_r, u),\ \forall \phi \in \mathcal{C}^{\tilde{n}},\ \forall \phi_r \in \mathcal{C}^{\tilde{p}},\ \forall u \in \mathbb{R}^{\tilde{m}}$;

(c.4) $\mathcal{D}_\infty\big(\phi_z, \phi_r, \tilde{k}(\phi_z, \phi_r) + d\big) \leq -\alpha_3(\|\phi_z\|_\infty) + \alpha_4(|d|),\ \forall \phi \in \mathcal{C}^{\tilde{n}},\ \forall \phi_r \in \mathcal{C}^{\tilde{p}},\ \forall u \in \mathbb{R}^{\tilde{m}},\ \forall d \in D$.

□

In the following, the structure of the proof provided in [22] (see Theorem 1 in [22]) and, based on the stabilization in the sample-and-hold sense theory [26], [27], [29], will be suitably adapted to cope with the stability analysis of the QSE closed-loop system (3.5)-(3.22). Differently from [22], here known exogenous disturbances, introduced to characterize, for instance, tracking control problems, are considered. As a consequence, the proof used in [22] cannot be directly applied here and the development of a new

devoted proof is required. See, just to provide an example, steps 1)-10) in the proof of Theorem 1 in [22] and steps 1)-10) here provided. We highlight also that, as in this paper, the consideration of known exogenous disturbances turns out to be very helpful also in the context of MASs to characterize consensus problems which, in [22], are not considered at all.

Let:

1) R_f, R_0, be any positive reals, $0 < R_f < R_0$;

2) a, $\bar{\mu}$, $\tilde{\mu} \in (0, 1]$ and $\sigma \in (0, 1)$ be arbitrarily fixed;

3) the function r_t be arbitrarily chosen such that (3.9) is satisfied, q be any positive real and $z^0 \in W^{1,\infty}_{\tilde{n}} \cap \mathcal{C}^{\tilde{n}}_{R_0}$ satisfying $\operatorname*{ess\,sup}_{\theta\in[-\Delta,0]} \left|\frac{dz^0(\theta)}{d\theta}\right| \leq q$;

4) e_1, e_2, E be positive reals satisfying:

$$0 < e_2 < e_1 < R_f < R_0 < E,\ \alpha_1(E) > \alpha_2(R_0), \alpha_1(R_f) > \alpha_2(e_1); \tag{A.2}$$

5)

$$\begin{aligned}
&E_1 = E + e, \quad E_2 = E_1 + 1, \quad \tilde{\gamma}_r = \bar{\gamma}_r + 1,\\
&\tilde{L} = \sup_{\phi_1^z\in\mathcal{C}^{\tilde{n}}_{E_2},\, \phi_2^z\in\mathcal{C}^{\tilde{n}}_{E_1},\phi_1^r\in\mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r},\, \phi_2^r\in\mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r}} \left|k(\phi_1^z, \phi_1^r) - k(\phi_2^z, \phi_2^r)\right|,\\
&\bar{L} = \sup_{\phi_1^z,\phi_2^z\in\mathcal{C}^{\tilde{n}}_{E},\phi_1^r,\phi_2^r\in\mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r}} \left|k(\phi_1^z, \phi_1^r) - k(\phi_2^z, \phi_2^r)\right|,\\
&L = \sup_{\phi_1^z\in\mathcal{C}^{\tilde{n}}_{E_1},\, \phi_2^z\in\mathcal{C}^{\tilde{n}}_{E},\phi_1^r,\phi_2^r\in\mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r}} \left|k(\phi_1^z, \phi_1^r) - k(\phi_2^z, \phi_2^r)\right|,\\
&D = \bar{d} + \bar{e} + \bar{\mu} + \tilde{\mu} + \bar{L} + \tilde{L} + L,\\
&\omega \geq \bar{\omega} = \max\left\{1, \frac{(\nu + \eta\bar{p})D^2}{\sigma\alpha_3(e_2)}\right\},\\
&U = \sup_{\phi_z\in\mathcal{C}^{\tilde{n}}_{E_2},\, \phi_r\in\mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r}} \left|\tilde{k}(\phi_z, \phi_r)\right|, \quad \overline{U} = U + 1 + \bar{d}.
\end{aligned} \tag{A.3}$$

6) M, $L_{\mathcal{D}}$, L_S be positive reals such that the following inequalities hold, $\forall \phi_1^z$, $\phi_2^z \in \mathcal{C}^{\tilde{n}}_{E_2}$, $\forall \phi_1^r$, $\phi_2^r \in \mathcal{C}^{\tilde{p}}_{\tilde{\gamma}_r}$ and $\forall u_1$, $u_2 \in \mathcal{B}^{\tilde{m}}_{\overline{U}}$:

$$\begin{aligned}
&|F(\phi_1^z, \phi_1^r) + G(\phi_1^z, \phi_1^r)u_1| \leq M,\\
&|S(\phi_1^z, \phi_1^r) - S(\phi_2^z, \phi_2^r)| \leq L_S(\|\phi_1^z - \phi_2^z\|_\infty + \|\phi_1^r - \phi_2^r\|_\infty),\\
&|\mathcal{D}_\infty(\phi_1^z, \phi_1^r, u_1) - \mathcal{D}_\infty(\phi_2^z, \phi_2^r, u_2)| \leq L_{\mathcal{D}}(\|\phi_1^z - \phi_2^z\|_\infty + \|\phi_1^r - \phi_2^r\|_\infty + |u_1 - u_2|);
\end{aligned} \tag{A.4}$$

7) $\tilde{q} = \max\{q, M\}$ with M the positive real in (A.4);

8) $\beta = \omega\sigma\alpha_3(e_2) - \frac{(\nu+\eta\bar{p})D^2}{2}$;

9) δ, μ_z, μ_r, μ_u be positive reals and q_z, q_r be state quantizers with ranges E_1, $\bar{\gamma}_r$ and error bounds μ_z, μ_r such that:

$$\begin{aligned}
&\delta < \min\{1, \Delta\}, \quad 0 < \mu_x \leq 1, \quad 0 < \mu_u \leq 1, \quad e_2 + \delta M < e_1,\\
&\alpha_1(R_f) > \alpha_2(e_1) + \frac{2}{3}\frac{\beta\delta}{\omega}, \quad L_S(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta) \leq \frac{\bar{\mu}}{\omega}, R_0 + \delta M < E,\\
&\frac{\beta}{3} > 2\omega L_{\mathcal{D}}(2 + \sigma)(\mu_u + 2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + 3\mu_z + 3\mu_r),\\
&\sup_{\substack{\tilde{z}_0,\ldots,\tilde{z}_l\in\mathcal{B}^{\tilde{n}}_{E_1}\\ \tilde{r}_0,\ldots,\tilde{r}_l\in\mathcal{B}^{\tilde{p}}_{\tilde{\gamma}_r}}} \left| S\Big(P^{\tilde{n}}_{l,a,\delta}\Big(\begin{pmatrix} q_z(\tilde{z}_0)\\ \vdots\\ q_z(\tilde{z}_l)\end{pmatrix}, w\Big), P^{\tilde{p}}_{l,a,\delta}\Big(\begin{pmatrix} q_r(\tilde{r}_0)\\ \vdots\\ q_r(\tilde{r}_l)\end{pmatrix}, w\Big)\Big)\right.\\
&\qquad \left. - S\Big(P^{\tilde{n}}_{l,a,\delta}\Big(\begin{pmatrix} \tilde{z}_0\\ \vdots\\ \tilde{z}_l\end{pmatrix}, w\Big), P^{\tilde{p}}_{l,a,\delta}\Big(\begin{pmatrix} \tilde{r}_0\\ \vdots\\ \tilde{r}_l\end{pmatrix}, w\Big)\Big)\right| \leq \frac{\tilde{\mu}}{\omega}, \quad \forall w \in \mathcal{T}_{l,a,\delta}.
\end{aligned} \tag{A.5}$$

10) q_u be an input quantizer with range U and error bound μ_u.
Let us consider a partition $\pi_{a,\delta}$. Let $B_S^{z+e} : \mathbb{N} \to \mathbb{R}^{\tilde{n}(l+1)}$, $\bar{B}_S^r : \mathbb{N} \to \mathbb{R}^{\tilde{p}(l+1)}$ and $B_S^z : \mathbb{N} \to \mathbb{R}^{\tilde{n}(l+1)}$ be defined (recursively) as

$$
\begin{aligned}
B_S^{z+e}(0) &= \begin{pmatrix} \bar{z}^0(0) + \bar{e}_0(0) \\ \vdots \\ \bar{z}^0(t_{-l}) + \bar{e}_0(t_{-l}) \end{pmatrix}, \quad B_S^z(0) = \begin{pmatrix} \bar{z}^0(0) \\ \vdots \\ \bar{z}^0(t_{-l}) \end{pmatrix}, \\
\bar{B}_S^r(0) &= \begin{pmatrix} \bar{r}_0(0) \\ \vdots \\ \bar{r}_0(t_{-l}) \end{pmatrix}, \quad \bar{r}_0(\tau) = \begin{cases} r_0(\tau), & \tau \in [-\Delta, 0], \\ r_0(-\Delta), & \tau \in [t_{-l}, -\Delta] \end{cases}, \\
\bar{z}^0(\tau) + \bar{e}_0(\tau) &= \begin{cases} z^0(\tau) + e_0(\tau), & \tau \in [-\Delta, 0], \\ z^0(-\Delta) + e_0(-\Delta), & \tau \in [t_{-l}, -\Delta] \end{cases}, \\
\bar{z}^0(\tau) &= \begin{cases} z^0(\tau), & \tau \in [-\Delta, 0], \\ z^0(-\Delta), & \tau \in [t_{-l}, -\Delta] \end{cases}, \\
B_S^{z+e}(j) &= \begin{pmatrix} z(t_j) + e_j(0) \\ 0_{l\tilde{n},1} \end{pmatrix} + \begin{pmatrix} 0_{\tilde{n},l\tilde{n}} & 0_{\tilde{n},1} \\ I_{l\tilde{n},l\tilde{n}} & 0_{l\tilde{n},\tilde{n}} \end{pmatrix} B_S^{z+e}(j-1), \\
\bar{B}_S^r(j) &= \begin{pmatrix} r(t_j) \\ 0_{l\tilde{p},1} \end{pmatrix} + \begin{pmatrix} 0_{\tilde{p},l\tilde{p}} & 0_{\tilde{p},1} \\ I_{l\tilde{p},l\tilde{p}} & 0_{l\tilde{p},\tilde{p}} \end{pmatrix} \bar{B}_S^r(j-1), \\
B_S^z(j) &= \begin{pmatrix} z(t_j) \\ 0_{l\tilde{n},1} \end{pmatrix} + \begin{pmatrix} 0_{\tilde{n},l\tilde{n}} & 0_{\tilde{n},1} \\ I_{l\tilde{n},l\tilde{n}} & 0_{l\tilde{n},\tilde{n}} \end{pmatrix} B_S^z(j-1), \quad j = 1, \dots
\end{aligned}
\tag{A.6}
$$

In the following, we denote:

$$
\mathcal{P}_j^r := P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^r(j), B_{\mathcal{T}}(j)), \quad \mathcal{P}_j^z := P_{l,a,\delta}^{\tilde{n}}(B_S^z(j), B_{\mathcal{T}}(j)), \quad \mathcal{P}_j^{z+e} := P_{l,a,\delta}^{\tilde{n}}(B_S^{z+e}(j), B_{\mathcal{T}}(j)).
$$

Firstly, we notice that for any

$$
\tilde{z} = \begin{pmatrix} \tilde{z}_0 \\ \vdots \\ \tilde{z}_l \end{pmatrix}, \quad \tilde{z}_i \in \mathcal{B}_E^{\tilde{n}}, \quad i = 0, \dots, l,
$$

and for any

$$
\tilde{e} = \begin{pmatrix} \tilde{e}_0 \\ \vdots \\ \tilde{e}_l \end{pmatrix}, \quad \tilde{e}_i \in \mathcal{B}_{\tilde{e}}^{\tilde{n}}, \quad i = 0, \dots, l,
$$

we have

$$
|\tilde{z}_i + \tilde{e}_i| \le E_1, \quad i = 0, \dots, l,
$$

and consequently, for any $w \in \mathcal{T}_{l,a,\delta}$,

$$
\|P_{l,a,\delta}(\tilde{x} + \tilde{e}, w)\|_\infty \le E_1.
$$

Moreover, for any

$$
\tilde{z} = \begin{pmatrix} \tilde{z}_0 \\ \vdots \\ \tilde{z}_l \end{pmatrix}, \quad \tilde{z}_i \in \mathcal{B}_{E_1}^{\tilde{n}}, \quad i = 0, \dots, l,
$$

we have

$$
|q_z(\tilde{z}_i)| \le E_1 + 1 = E_2,
$$

and thus, for any $w \in \mathcal{T}_{l,a,\delta}$,

$$\left\| P_{l,a,\delta} \begin{pmatrix} q_z(\tilde{z}_0) \\ \vdots \\ q_z(\tilde{z}_l) \end{pmatrix}, w \right\|_\infty \leq E_2.$$

From these considerations, it follows that

$$\|\mathcal{P}_0^{z+e}\|_\infty \leq E_1, \quad \|\mathcal{P}_0^{q_z}\|_\infty \leq E_2.$$

Similarly, for any

$$\tilde{r} = \begin{pmatrix} \tilde{r}_0 \\ \vdots \\ \tilde{r}_l \end{pmatrix}, \quad \tilde{r}_i \in \mathcal{B}^{\tilde{p}}_{\bar{\gamma}_r}, \quad i = 0, \ldots, l,$$

we have, for any $w \in \mathcal{T}_{l,a,\delta}$,

$$\|P^{\tilde{p}}_{l,a,\delta}(\tilde{r}, w)\|_\infty \leq \bar{\gamma}_r,$$

and

$$|q_r(\tilde{r}_i)| \leq \bar{\gamma}_r + 1 = \tilde{\gamma}_r, \quad i = 0, \ldots, l,$$

which implies

$$\left\| P^{\tilde{p}}_{l,a,\delta} \begin{pmatrix} q_r(\tilde{r}_0) \\ \vdots \\ q_r(\tilde{r}_l) \end{pmatrix}, w \right\|_\infty \leq \tilde{\gamma}_r.$$

Hence,

$$\|\mathcal{P}_0^{r}\|_\infty \leq \bar{\gamma}_r, \quad \|\mathcal{P}_0^{q_r}\|_\infty \leq \tilde{\gamma}_r.$$

Finally, for any $d \in \mathcal{B}^{\tilde{m}}_{\tilde{d}}$, we have

$$q_u(\tilde{u}_0) + d \in \mathcal{B}^{\tilde{m}}_{\tilde{U}}.$$

Let us consider the solution of the QSE closed-loop system (3.5)-(3.22).

We show first that the solution exists in $[0, t_1]$. Otherwise, by contradiction, if the solution blows up, there exists a time $\tau \in [0, t_1)$ such that $|z(t)| < E$, $t \in [0, \tau)$, and $|z(\tau)| = E$. But, from (A.4), (A.5), for $t \in [0, \tau]$, the inequalities hold:

$$|z(t)| \leq |z^0(0)| + \int_0^t |F(z_\theta, r_\theta) + G(z_\theta, r_\theta)(q_u(\tilde{u}_0) + d(\theta))| d\theta \leq R_0 + \delta M < E. \quad \text{(A.7)}$$

Thus, taking $t = \tau$, the absurd inequality arises $E < E$. Therefore, the solution exists in $[0, t_1]$ and, by (A.7), it follows that $z_t \in \mathcal{C}^n_E$, $t \in [0, t_1]$. Let $W(t) = \omega V_\infty(z_t)$, $t \in [0, t_1]$, with $V_\infty : \mathcal{C}^{\tilde{n}} \to \mathbb{R}^+$ provided in Lemma A.1.2. Taking into account (3.9), point (c.3) in Lemma A.1.2 and Steps 6), 9), 10), for any fixed $t \in (0, t_1]$, for some $t^* \in [0, t]$, the following equalities/inequalities hold:

$$\begin{aligned}
&W(t) - W(0) = \textstyle\int_0^t \omega D^+ V_\infty(z_\tau, r_\tau, q_u(\tilde{u}_0) + d(\tau)) d\tau \leq \\
&t\left(\frac{1}{t} \textstyle\int_0^t \omega \mathcal{D}_\infty(z_\tau, r_\tau, q_u(\tilde{u}_0) + d(\tau)) d\tau \right) = \\
&t\omega \mathcal{D}_\infty(z_{t^*}, r_{t^*}, q_u(\tilde{u}_0) + \tilde{d}(t^*)) = \\
&t\omega \mathcal{D}_\infty(z_{t^*}, r_{t^*}, q_u(\tilde{u}_0) + \tilde{d}(t^*)) - t\omega \mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) + \\
&t\omega \mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) - t\omega\sigma \mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) \\
&+t\omega\sigma \mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) \leq \\
&t\omega L_{\mathcal{D}}(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + \mu_u) + t\omega(1-\sigma)\mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) \\
&+t\omega\sigma \mathcal{D}_\infty(z_0, r_0, \tilde{u}_0 + \tilde{d}(t^*)),
\end{aligned} \quad \text{(A.8)}$$

where, $\tilde{d}(t^*) = d(t^*)$ if $t^* < t_1$ and $\tilde{d}(t^*) = \lim_{t \to t_1^-} d(t)$ if $t^* = t_1$ and, by suitably repeating the reasoning in [146] (see, also, [30]), $\|z_{t^*} - z_0\|_\infty \leq 2\tilde{q}\delta$ and $\|r_{t^*} - r_0\|_\infty \leq 2\bar{\gamma}_{dr}\delta$. Now,

we notice that, $\mathbb{P}_0^z \in \mathcal{C}_E^{\tilde{n}}$, $\mathbb{P}_0^r \in \mathcal{C}_{\bar{\gamma}_r}^{\tilde{p}}$, $\mathbb{P}_0^{z+e} \in \mathcal{C}_{E_1}^{\tilde{n}}$ and $\mathbb{P}_0^{q_z} \in \mathcal{C}_{E_2}^{\tilde{n}}$, $\mathbb{P}_0^{q_r} \in \mathcal{C}_{\bar{\gamma}_r}^{\tilde{p}}$. Then, taking into account (A.4) and (A.5), the following equality/inequalities hold:

$$\begin{array}{l} |S(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) - S(\mathbb{P}_0^{z+e}, \mathbb{P}_0^r)| = \\ |S(P_{l,a,\delta}^{\tilde{n}}(B_S^{q_z}(0), B_{\mathcal{T}}(0)), P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^{q_r}(0), B_{\mathcal{T}}(0))) - \\ S(P_{l,a,\delta}^{\tilde{n}}(B_S^{z+e}(0), B_{\mathcal{T}}(0)), P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^r(0), B_{\mathcal{T}}(0)))| \leq \dfrac{\tilde{\mu}}{\omega} \\ |S(\mathbb{P}_0^z, \mathbb{P}_0^r) - S(z^0, r_0)| \leq L_S(\|\mathcal{P}_0^z - z^0\|_\infty + \|\mathcal{P}_0^r - r_0\|_\infty) \leq \\ L_S(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta) \leq \dfrac{\bar{\mu}}{\omega}, \end{array} \tag{A.9}$$

where, by a similar reasoning to the one in [146], $\|\mathcal{P}_0^z - z^0\|_\infty \leq 2\tilde{q}\delta$ and $\|\mathcal{P}_0^r - r_0\|_\infty \leq 2\bar{\gamma}_{dr}\delta$. Taking into account (A.3) and (A.9), let $v_i \in \mathcal{B}_1^m$, $i = 1, \cdots, 6$, be such that:

$$\begin{array}{l} k(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) = k(\mathbb{P}_0^{z+e}, \mathbb{P}_0^r) + \tilde{L}v_1, \\ k(\mathbb{P}_0^{z+e}, \mathbb{P}_0^r) = k(\mathbb{P}_0^z, \mathbb{P}_0^r) + Lv_2, \\ k(\mathbb{P}_0^z, \mathbb{P}_0^r) = k(z^0, r_0) + \bar{L}v_3, \\ S(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) = S(\mathbb{P}_0^{z+e}, \mathbb{P}_0^r) + \dfrac{\tilde{\mu}}{\omega}v_4, \\ S(\mathbb{P}_0^{z+e}, \mathbb{P}_0^r) = S(\mathbb{P}_0^z, \mathbb{P}_0^r) + \dfrac{\bar{e}}{\omega}v_5, \\ S(\mathbb{P}_0^z, \mathbb{P}_0^r) = S(z^0, r_0) + \dfrac{\bar{\mu}}{\omega}v_6. \end{array} \tag{A.10}$$

Then, taking into account point (c.4) in Lemma A.1.2 and (A.10), the following equalities/inequality hold:

$$\begin{array}{l} \mathcal{D}_\infty(z^0, r_0, \tilde{u}_0 + \tilde{d}(t^*)) = \\ \mathcal{D}_\infty(z^0, r_0, \tilde{k}(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) + \tilde{d}(t^*)) = \\ \mathcal{D}_\infty(z^0, r_0, k(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) - \omega S(\mathbb{P}_0^{q_z}, \mathbb{P}_0^{q_r}) + \tilde{d}(t^*)) = \\ \mathcal{D}_\infty(z^0, r_0, k(z^0, r_0) - \omega S(z^0, r_0) + \tilde{L}v_1 + Lv_2 + \bar{L}v_3 \\ \qquad -\tilde{\mu}v_4 - \mu v_5 - \bar{\mu}v_6 + \tilde{d}(t^*)) \leq \\ -\alpha_3(\|z^0\|_\infty) + \dfrac{(\nu + \eta\bar{p})D^2}{4\omega}. \end{array} \tag{A.11}$$

From (A.8), taking into account (A.5) and (A.11), for $t \in [0, t_1]$, the following inequality holds

$$\begin{array}{l} W(t) - W(0) \leq t\omega L_{\mathcal{D}}(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + \mu_u) \\ \qquad -t\omega\sigma\alpha_3(\|z^0\|_\infty) + t\dfrac{(\nu + \eta\bar{p})D^2}{4} \leq \\ \dfrac{\beta}{3}t - t\omega\sigma\alpha_3(\|z^0\|_\infty) + t\dfrac{(\nu + \eta\bar{p})D^2}{4}. \end{array} \tag{A.12}$$

Let us now consider the following two cases: 1) $\|z^0\|_\infty \leq e_2$; 2) $\|z^0\|_\infty > e_2$. As far as case (1) is concerned, by using again the first inequality in (A.7) and from (A.5), the following inequality holds, for any $t \in [0, t_1]$,

$$|z(t)| \leq e_2 + \delta M < e_1.$$

From point (c.1) in Lemma A.1.2, it follows

$$W(t) \leq \omega\alpha_2(e_1), \ t \in [0, t_1].$$

As far as case (2) is concerned, we have that

$$-\beta > -\omega\sigma\alpha_3(\|z^0\|_\infty) + \frac{(\nu + \eta\bar{p})D^2}{4}.$$

Therefore, from (A.5), we have, for any $t \in [0, t_1]$,

$$W(t) \leq W(0) + \frac{\beta}{3}t - \beta t = W(0) - \frac{2}{3}\beta t.$$

Let us introduce the following claim, which will be proved later.

Claim A.1.1

The solution $z(t)$ of (3.5)-(3.22), exists in $[0,+\infty)$ and, furthermore, $z_t \in \mathcal{C}_E^{\tilde{n}}$, $\forall t \geq 0$. □

Notice that, taking into account the control input in (3.22), Claim A.1.1 and the same reasoning used in the first interval $[0,t_1]$, for any $d \in \mathcal{B}_d^{\tilde{m}}$, $q_u(\tilde{u}_{i_j}) + d \in \mathcal{B}_U^{\tilde{m}}$, $j = 1, \cdots$. Let $W(t) = \omega V_\infty(z_t)$, $t \in \mathbb{R}^+$. Taking into account the reasoning used in the interval $[0,t_1]$, points (c.3) in Lemma A.1.2 and Steps 6), 9), 10), for any fixed $t \in (t_j, t_{j+1}]$, $j \geq 1$, for some $t^* \in [t_j, t]$, the following inequalities hold:

$$\begin{array}{l} W(t) - W(t_j) \leq \omega(t-t_j)\mathcal{D}_\infty(z_{t^*}, r_{t^*}, q_u(\tilde{u}_{i_j}) + \tilde{d}(t^*)) \\ \leq \omega(t-t_j)\Big(\mathcal{D}_\infty(z_{t^*}, r_{t^*}, q_u(\tilde{u}_{i_j}) + \tilde{d}(t^*)) \\ -\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_j} + \tilde{d}(t^*)) + \mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_j} + \tilde{d}(t^*)) \\ -\sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) + \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) \leq \\ \omega(t-t_j)L_{\mathcal{D}}(2\tilde{q}\delta + 2\bar{\gamma}_{dr} + \mu_u) \\ +\omega(t-t_j)\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_j} + \tilde{d}(t^*)) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) \\ +\sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big), \end{array} \tag{A.13}$$

where, $\tilde{d}(t^*) = d(t^*)$ if $t^* < t_j$ and $\tilde{d}(t^*) = \lim_{t \to t_j^-} d(t)$ if $t^* = t_j$ and, by suitably repeating the reasoning in [146] (see, also, [30]), $\|z_{t^*} - z_{t_j}\|_\infty \leq 2\tilde{q}\delta$ and $\|r_{t^*} - r_0\|_\infty \leq 2\bar{\gamma}_{dr}\delta$. Taking into account (3.9) and Claim A.1.1, we notice that, $\mathbb{P}_j^z \in \mathcal{C}_E^{\tilde{n}}$, $\mathbb{P}_j^r \in \mathcal{C}_{\tilde{\gamma}_r}^{\tilde{p}}$, $\mathbb{P}_j^{z+e} \in \mathcal{C}_{E_1}^{\tilde{n}}$ and $\mathbb{P}_j^{q_z} \in \mathcal{C}_{E_2}^{\tilde{n}}$, $\mathbb{P}_j^{q_r} \in \mathcal{C}_{\tilde{\gamma}_r}^{\tilde{p}}$, $j = 0, 1, \cdots$. Then, taking into account (A.4) and (A.5), the following equality/inequalities hold:

$$\begin{array}{l} |S(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}) - S(\mathbb{P}_j^{z+e}, \mathbb{P}_j^r)| = \\ |S(P_{l,a,\delta}^{\tilde{n}}(B_S^{q_z}(j), B_{\mathcal{T}}(j)), P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^{q_r}(j), B_{\mathcal{T}}(j))) - \\ S(P_{l,a,\delta}^{\tilde{n}}(B_S^{z+e}(j), B_{\mathcal{T}}(j)), P_{l,a,\delta}^{\tilde{p}}(\bar{B}_S^r(j), B_{\mathcal{T}}(j)))| \leq \dfrac{\tilde{\mu}}{\omega} \\ |S(\mathbb{P}_j^z, \mathbb{P}_j^r) - S(z_{t_j}, r_{t_j})| \leq L_S(\|\mathcal{P}_j^z - z_{t_j}\|_\infty + \|\mathcal{P}_{t_j}^r - r_{t_j}\|_\infty) \leq \\ L_S(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta) \leq \dfrac{\bar{\mu}}{\omega}, \end{array} \tag{A.14}$$

where, by a similar reasoning to the one in [146], $\|\mathcal{P}_j^z - z_{t_j}\|_\infty \leq 2\tilde{q}\delta$ and $\|P_{t_j}^r - r_{t_j}\|_\infty \leq 2\bar{\gamma}_{dr}\delta$. Taking into account (A.3) and (A.14), let $v_i \in \mathcal{B}_1^m$, $i = 1, \cdots, 6$, be such that:

$$\begin{array}{rl} k(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}) &= k(\mathbb{P}_j^{z+e}, \mathbb{P}_j^r) + \tilde{L}v_1, \\ k(\mathbb{P}_j^{z+e}, \mathbb{P}_j^r) &= k(\mathbb{P}_j^z, \mathbb{P}_j^r) + Lv_2, \\ k(\mathbb{P}_j^z, \mathbb{P}_j^r) &= k(z_{t_j}, r_{t_j}) + \bar{L}v_3, \\ S(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}) &= S(\mathbb{P}_j^{z+e}, \mathbb{P}_j^r) + \dfrac{\tilde{\mu}}{\omega}v_4, \\ S(\mathbb{P}_j^{z+e}, \mathbb{P}_j^r) &= S(\mathbb{P}_j^z, \mathbb{P}_j^r) + \dfrac{\bar{e}}{\omega}v_5, \\ S(\mathbb{P}_j^z, \mathbb{P}_j^r) &= S(z_{t_j}, r_{t_j}) + \dfrac{\bar{\mu}}{\omega}v_6. \end{array} \tag{A.15}$$

Then, taking into account point (c.4) in Lemma A.1.2 and (A.15), the following equalities/inequality hold:

$$\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) \leq -\alpha_3(\|z_{t_j}\|_\infty) + \frac{(\nu + \eta\bar{p})D^2}{4\omega}. \tag{A.16}$$

Moreover, taking into account (3.22), (3.26) and (A.13), we have that

$$\begin{aligned}&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_j} + \tilde{d}(t^*)) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big)\\ &= \begin{cases}\omega(1-\sigma)\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) & i_j = j,\\ \omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*))\\ \qquad -\sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) & i_j = i_{j-1}.\end{cases}\end{aligned} \tag{A.17}$$

Taking into account (A.16), if $i_j = j$ (trigger), the following inequality holds:

$$\begin{aligned}&\omega(1-\sigma)\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) \leq\\ &\quad -\omega(1-\sigma)\alpha_3(\|z_{t_j}\|_\infty) + (1-\sigma)\frac{(\nu+\eta\bar{p})D^2}{4}.\end{aligned} \tag{A.18}$$

In the case that $i_j = i_{j-1}$ (no trigger), the triggering condition (3.26) is false and, consequently, the following inequality holds:

$$\begin{aligned}&\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_{i_{j-1}}))\\ &-\sigma\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_j)) \leq -H(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}).\end{aligned} \tag{A.19}$$

For simplicity in the notation, in the following we will call with: $\Psi_1(\phi_z, \phi_r, u)$ the function $D^+p \circ V_1(\phi_z, \phi_r, u) + \mu p \circ V_1(\phi_z(0))$ and with $\Psi_2(\phi_z, \phi_r, d)$ the function $\left.\frac{dp}{ds}\right|_{s=V_1(\phi_z(0))} \left.\frac{\partial V_1}{\partial z}\right|_{z=\phi_z(0)} G(\phi_z, \phi_r)\, d$. Taking into account (3.21), the following equalities hold

$$\begin{aligned}&\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*)) =\\ &\nu D^+V(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*)) - \eta\mu V_3(z_{t_j})\\ &\quad +\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*))\} =\\ &\nu D^+V(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) + \nu \left.\frac{\partial V_1}{\partial z}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\tilde{d}(t^*)\\ &\quad -\eta\mu V_3(z_{t_j}) + \eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*))\}\\ &+\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}})\} - \eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}})\}\\ &= \mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) + \nu \left.\frac{\partial V_1}{\partial z}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\tilde{d}(t^*)\\ &\quad +\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) + \Psi_2(z_{t_j}, r_{t_j}, \tilde{d}(t^*))\}\\ &-\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}})\}.\end{aligned} \tag{A.20}$$

Moreover, by exploiting the same reasoning used in (A.20), we have that

$$\begin{aligned}&\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*)) =\\ &\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j) + \nu \left.\frac{\partial V_1}{\partial z}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\tilde{d}(t^*)\\ &+\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_j) + \Psi_2(z_{t_j}, r_{t_j}, \tilde{d}(t^*))\}\\ &-\eta\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_j)\}.\end{aligned} \tag{A.21}$$

Then, taking into account (A.20) and (A.21), the following equality/inequality hold:

$$\begin{aligned}
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*)) \\
&\qquad -\sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) = \\
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j)\Big) \\
&+\omega\nu(1-\sigma)\left.\frac{\partial V_1}{\partial x}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\tilde{d}(t^*) \\
&+\omega\eta\Big(\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) + \Psi_2(z_{t_j}, r_{t_j}, \tilde{d}(t^*))\} \\
&-\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}})\}\Big) \\
&+\omega\sigma\eta\Big(\max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_j)\} - \max\{0, \Psi_1(z_{t_j}, r_{t_j}, \tilde{u}_j) \\
&+\Psi_2(z_{t_j}, r_{t_j}, \tilde{d}(t^*))\}\Big) \leq \\
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j)\Big) \\
&+\omega\nu(1-\sigma)\left.\frac{\partial V_1}{\partial z}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\tilde{d}(t^*) \\
&+4\omega(1+\sigma)\eta\bar{p}\bar{d}\left|\left.\frac{\partial V_1}{\partial z}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right)\right|.
\end{aligned} \tag{A.22}$$

From (A.15) and (3.19), we notice that

$$\begin{aligned}
&\left.\frac{\partial V_1}{\partial x}\right|_{z=z(t_j)} G\left(z_{t_j}, r_{t_j}\right) = S(z_{t_j}, r_{t_j})^T = \\
&S(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r})^T - \frac{\tilde{\mu}v_4^T + \bar{e}v_5^T + \bar{\mu}v_6^T}{\omega}.
\end{aligned} \tag{A.23}$$

Taking into account (A.23), from (A.22), the following inequality holds:

$$\begin{aligned}
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*)) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) \leq \\
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j)\Big) + \\
&\omega\Big(\bar{d}\big(\nu(1-\sigma) + 4\eta\bar{p}(1+\sigma)\big)\Big(|S(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r})| + \frac{\tilde{\mu} + \bar{e} + \bar{\mu}}{\omega}\Big)\Big).
\end{aligned} \tag{A.24}$$

Then, taking into account (3.27), (A.4) and (A.24), the following inequalities hold:

$$\begin{aligned}
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}} + \tilde{d}(t^*)) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) \leq \\
&\quad\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j)\Big) + \\
&\quad\omega\Big(\bar{d}\big(\nu(1-\sigma) + 4\eta\bar{p}(1+\sigma)\big)\Big(|S(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r})| + \frac{\tilde{\mu} + \bar{e} + \bar{\mu}}{\omega}\Big)\Big) \\
&\quad+\omega\Big(\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_{i_{j-1}})) - \sigma\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_j)) \\
&\quad-\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_{i_{j-1}})) + \sigma\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_j))\Big) \leq \\
&\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_{j-1}}) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j)\Big) - 3\omega(1+\sigma)L_{\mathcal{D}}\bar{e} \\
&\quad+\omega\Big(-\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_{i_{j-1}})) + \sigma\mathcal{D}_\infty(\mathbb{P}_j^{q_z}, \mathbb{P}_j^{q_r}, q_u(\tilde{u}_j))\Big) \leq \\
&-3\omega(1+\sigma)L_{\mathcal{D}}\bar{e} + \omega(1+\sigma)L_{\mathcal{D}}\mu_u \\
&\quad+\omega(1+\sigma)L_{\mathcal{D}}(\|\mathbb{P}_j^{q_z} - z_{t_j}\|_\infty + \|\mathbb{P}_j^{q_r} - r_{t_j}\|_\infty) \leq \\
&\omega(1+\sigma)L_{\mathcal{D}}(\|\mathbb{P}_j^{q_z} - \mathbb{P}_j^{z+e} + \mathbb{P}_j^{z+e} - \mathbb{P}_j^z + \mathbb{P}_j^z - z_{t_j}\|_\infty \\
&\quad+\|\mathbb{P}_j^{q_r} - \mathbb{P}_j^r + \mathbb{P}_j^r - r_{t_j}\|_\infty) \\
&\quad-3\omega(1+\sigma)L_{\mathcal{D}}\bar{e} + \omega(1+\sigma)L_{\mathcal{D}}\mu_u \leq \\
&-3\omega(1+\sigma)L_{\mathcal{D}}\bar{e} + \omega(1+\sigma)L_{\mathcal{D}}\mu_u \\
&\quad+\omega(1+\sigma)L_{\mathcal{D}}(2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + 3\mu_z + 3\mu_r + 3\bar{e}) \leq \\
&\omega(1+\sigma)L_{\mathcal{D}}(\mu_u + 2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + 3\mu_z + 3\mu_r).
\end{aligned} \tag{A.25}$$

Then, taking into account (A.19), (A.25), from (A.17), we have that, for $j \geq 1$, the following inequality holds:

$$\begin{aligned}\omega\Big(\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_{i_j} + \tilde{d}(t^*)) - \sigma\mathcal{D}_\infty(z_{t_j}, r_{t_j}, \tilde{u}_j + \tilde{d}(t^*))\Big) \leq \\ \omega(1+\sigma)L_{\mathcal{D}}(\mu_u + 2\tilde{q}\delta + 2\bar{\gamma}_{dr}\delta + 3\mu_z + 3\mu_r) \\ +(1-\sigma)\frac{(\nu+\eta\bar{p})D^2}{4}.\end{aligned} \tag{A.26}$$

From (A.13), and taking into account (A.5), (A.26), for $t \in [t_j, t_{j+1}]$, $j \geq 1$, the following inequality holds

$$\begin{aligned}W(t) \leq W(t_j) + (t-t_j)\frac{\beta}{3} - (t-t_j)\sigma\omega\alpha_3(\|z_{t_j}\|_\infty) \\ + (t-t_j)\frac{(\nu+\eta\bar{p})D^2}{4}.\end{aligned} \tag{A.27}$$

Then, taking into account of both cases $\|z_{t_j}\|_\infty \leq e_2$ and $\|z_{t_j}\|_\infty > e_2$ (see cases (1) and (2) in $[0, t_1]$), for any $t \in [t_j,\, t_{j+1}]$, $j = 0, 1, \ldots$, we obtain:

$$\begin{aligned}W(t) \leq (W(t_j) - \frac{2}{3}\beta(t-t_j))H(\|z_{t_j}\|_\infty - e_2) \\ +\omega\alpha_2(e_1)H_0(e_2 - \|z_{t_j}\|_\infty).\end{aligned} \tag{A.28}$$

The symbols H_0 and H denote Heaviside functions defined, for $s \in \mathbb{R}$, as follows: $H_0(s) = 1$ if $s \geq 0$, $H_0(s) = 0$ if $s < 0$; $H(s) = 1$ if $s > 0$, $H(s) = 0$ if $s \leq 0$.
Notice that, by induction reasoning with (A.28), for any integer $j \geq 0$, the inequality holds $W(t_j) \leq \omega\alpha_2(R_0)$. From here on, by suitably exploiting (A.28), the same steps used in the proof of Theorem 5.3 in [29] can be properly repeated, in order to prove that the solution $z(t)$ of the closed-loop system (3.5)-(3.22), exists for all $t \in \mathbb{R}^+$ and, furthermore, satisfies $z_t \in \mathcal{C}_E^{\tilde{n}}$, $\forall t \in \mathbb{R}^+$ (Claim A.1.1 holds true) and $z_t \in \mathcal{C}_{R_f}^{\tilde{n}}$, $\forall t \geq T$, with

$$T = \frac{3\omega\alpha_2(R_0)}{\beta a} + 1. \tag{A.29}$$

The reader can refer to steps from (5.15) to (5.23) in [29] with $k_2 = [\frac{3\omega\alpha_2(R_0)}{\beta a\delta}] + 1$. The proof of the theorem is complete.

References

[1] Conesa-Muñoz, J., Gonzalez-de-Soto, M., Gonzalez-de-Santos, P., and Ribeiro, A., "Distributed multi-level supervision to effectively monitor the operations of a fleet of autonomous vehicles in agricultural tasks," *Sensors*, vol. 15, no. 3, pp. 5402–5428, 2015.

[2] Wang, Z., Zhang, F., Ma, S., Wang, H., Zhang, S., and Gao, X., "Research on collaborative scheduling strategies of multi-agent agricultural machinery groups," *Scientific Reports*, vol. 15, no. 1, p. 9045, 2025.

[3] Elmokadem, T., "Distributed coverage control of quadrotor multi-UAV systems for precision agriculture," *IFAC-PapersOnLine*, vol. 52, no. 30, pp. 251–256, 2019.

[4] Villarrubia, G., De Paz, J. F., De La Iglesia, D. H., and Bajo, J., "Combining multi-agent systems and wireless sensor networks for monitoring crop irrigation," *Sensors*, vol. 17, no. 8, p. 1775, 2017.

[5] Catalano, C., Paiano, L., Calabrese, F., Cataldo, M., Mancarella, L., and Tommasi, F., "Anomaly detection in smart agriculture systems," *Computers in Industry*, vol. 143, p. 103 750, 2022.

[6] Mponela, P., Le, Q. B., Snapp, S., Villamor, G. B., Tamene, L., and Borgemeister, C., "Massai: Multi-agent system for simulating sustainable agricultural intensification of smallholder farms in africa," *MethodsX*, vol. 11, p. 102 467, 2023.

[7] Chen, F., Ren, W., et al., "On the control of multi-agent systems: A survey," *Foundations and Trends® in Systems and Control*, vol. 6, no. 4, pp. 339–499, 2019.

[8] Al Asif, M. R., Hasan, K. F., Islam, M. Z., and Khondoker, R., "Stride-based cyber security threat modeling for IoT-enabled precision agriculture systems," in *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, IEEE, 2021, pp. 1–6.

[9] Mustafa, A. and Panagou, D., "Adversary detection and resilient control for multiagent systems," *IEEE Transactions on Control of Network Systems*, vol. 10, no. 1, pp. 355–367, 2022.

[10] Albarakati, A. J. et al., "Multi-agent-based fault location and cyber-attack detection in distribution system," *Energies*, vol. 16, no. 1, 2023.

[11] Hua, C.-C., Li, K., and Guan, X.-P., "Semi-global/global output consensus for nonlinear multiagent systems with time delays," *Automatica*, vol. 103, pp. 480–489, 2019.

[12] Huang, R., Ding, Z., and Cao, Z., "Distributed output feedback consensus control of networked homogeneous systems with large unknown actuator and sensor delays," *Automatica*, vol. 122, p. 109 249, 2020.

[13] Ploennigs, J., Vasyutynskyy, V., and Kabitzsch, K., "Comparative study of energy-efficient sampling approaches for wireless control networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 3, pp. 416–424, 2010.

[14] Cesarone, F. and Pepe, P., "Sample-and-hold solution of a consensus problem with nonlinear dynamics and input/output disturbances," *European Journal of Control*, vol. 59, pp. 227–237, 2021.

[15] Menard, T., Ajwad, S. A., Moulay, E., Coirault, P., and Defoort, M., "Leader-following consensus for multi-agent systems with nonlinear dynamics subject to additive bounded disturbances and asynchronously sampled outputs," *Automatica*, vol. 121, p. 109 176, 2020.

[16] Wei, J., Yi, X., Sandberg, H., and Johansson, K. H., "Nonlinear consensus protocols with applications to quantized communication and actuation," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 598–608, 2018.

[17] Di Ferdinando, M., Bianchi, D., Di Gennaro, S., and Pepe, P., "Robustification of digital tracking protocols for nonlinear multi-agent systems with state delays," *IFAC-PapersOnLine*, vol. 59, no. 13, pp. 183–188, 2025.

[18] Li, Z., Xu, C., Liu, C., and Xu, H., "Robust consensus for nonlinear multiagent systems with uncertainty and disturbance," *Mathematical Problems in Engineering*, vol. 2018, no. 1, p. 8 509 306, 2018.

[19] Liu, J., Yu, Y., Sun, J., and Sun, C., "Distributed event-triggered fixed-time consensus for leader-follower multiagent systems with nonlinear dynamics and uncertain disturbances," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 11, pp. 3543–3559, 2018.

[20] Stanković, S. S., Beko, M., and Stanković, M. S., "Nonlinear robustified stochastic consensus seeking," *Systems & Control Letters*, vol. 139, p. 104 667, 2020.

[21] Syed Ali, M., Agalya, R., Saroha, S., and Saeed, T., "Leaderless consensus of non-linear mixed delay multi-agent systems with random packet losses via sampled-data control," *International Journal of Control, Automation and Systems*, vol. 18, no. 7, pp. 1885–1893, 2020.

[22] Di Ferdinando, M., Di Gennaro, S., Borri, A., Pola, G., and Pepe, P., "On the robustification of digital event-based stabilizers for nonlinear time-delay systems," *Nonlinear Analysis: Hybrid Systems*, vol. 52, p. 101 463, 2024.

[23] Artstein, Z., "Stabilization with relaxed controls," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 7, no. 11, pp. 1163–1173, 1983.

[24] Di Ferdinando, M., Pepe, P., and Di Gennaro, S., "A new approach to the design of sampled-data dynamic output feedback stabilizers," *IEEE Transactions on Automatic Control*, vol. 67, no. 2, pp. 1038–1045, 2021.

[25] Sontag, E. D., "A universal construction of Artstein's theorem on nonlinear stabilization," *Systems & control letters*, vol. 13, no. 2, pp. 117–123, 1989.

[26] Clarke, F., "Discontinuous feedback and nonlinear systems," *IFAC Proceedings Volumes*, vol. 43, no. 14, pp. 1–29, 2010.

[27] Clarke, F. H., Ledyaev, Y. S., Sontag, E. D., and Subbotin, A. I., "Asymptotic controllability implies feedback stabilization," *IEEE Transactions on Automatic Control*, vol. 42, no. 10, pp. 1394–1407, 1997.

[28] Di Ferdinando, M. and Pepe, P., "Robustification of sample-and-hold stabilizers for control-affine time-delay systems," *Automatica*, vol. 83, pp. 141–154, 2017.

[29] Pepe, P., "Stabilization in the sample-and-hold sense of nonlinear retarded systems," *SIAM Journal on Control and Optimization*, vol. 52, no. 5, pp. 3053–3077, 2014.

[30] Pepe, P., "On stability preservation under sampling and approximation of feedbacks for retarded systems," *SIAM Journal on Control and Optimization*, vol. 54, no. 4, pp. 1895–1918, 2016.

[31] Mammarella, M. and Capello, E., "A Tube-based robust MPC for a fixed-wing UAV: An Application for Precision Farming," *arXiv preprint arXiv:1805.04295*, 2018.

[32] Seo, S. and Lee, K., "Density-driven multi-agent coordination for efficient farm coverage and management in smart agriculture," *arXiv preprint arXiv:2511.12492*, 2025.

[33] Valenzuela-Garcia, J. R. et al., "Precision farming drones: Advances and future directions," *Agri Res and Tech: Open Access J.*, 2024.

[34] Pola, G., De Santis, E., and Di Benedetto, M. D., "Approximate current state observability of discrete-time nonlinear systems under cyber-attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 50, p. 101 403, 2023.

[35] Shamloo, N. F., De Santis, E., and Di Benedetto, M. D., "Security and diagnosability of finite state machines under cyber-attacks," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 5108–5116, 2024.

[36] N. Ahmed, M., Abdullah, A. H., and Kaiwartya, O., "FSM-F: Finite state machine based framework for denial of service and intrusion detection in manet," *Plos one*, vol. 11, no. 6, e0156885, 2016.

[37] Gao, C., Seatzu, C., Li, Z., and Giua, A., "Multiple attacks detection on discrete event systems," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, IEEE, 2019, pp. 2352–2357.

[38] Abd Alrahman, Y. and Piterman, N., "Modelling and verification of reconfigurable multi-agent systems," *Autonomous Agents and Multi-Agent Systems*, vol. 35, no. 2, p. 47, 2021.

[39] Basilio, J. C., Hadjicostis, C. N., Su, R., et al., "Analysis and control for resilience of discrete event systems: Fault diagnosis, opacity and cyber security," *Foundations and Trends® in Systems and Control*, vol. 8, no. 4, pp. 285–443, 2021.

[40] Oliveira, S., Leal, A. B., Teixeira, M., and Lopes, Y. K., "A classification of cybersecurity strategies in the context of discrete event systems," *Annual reviews in Control*, vol. 56, p. 100 907, 2023.

[41] Carvalho, L. K., Wu, Y.-C., Kwong, R., and Lafortune, S., "Detection and prevention of actuator enablement attacks in supervisory control systems," in *2016 13th International workshop on discrete event systems (WODES)*, IEEE, 2016, pp. 298–305.

[42] Li, Y., Tong, Y., and Giua, A., "Detection and prevention of cyber-attacks in networked control systems," *IFAC-PapersOnLine*, vol. 53, no. 4, pp. 7–13, 2020.

[43] Lin, L., Thuijsman, S., Zhu, Y., Ware, S., Su, R., and Reniers, M., "Synthesis of supremal successful normal actuator attackers on normal supervisors," in *2019 American control conference (ACC)*, IEEE, 2019, pp. 5614–5619.

[44] Zhu, Y., Lin, L., and Su, R., "Supervisor obfuscation against actuator enablement attack," in *2019 18th European Control Conference (ECC)*, IEEE, 2019, pp. 1760–1765.

[45] Ma, Z. and Cai, K., "On resilient supervisory control against indefinite actuator attacks in discrete-event systems," *IEEE Control Systems Letters*, vol. 6, pp. 2942–2947, 2022.

[46] Yao, J., Yin, X., and Li, S., "On attack mitigation in supervisory control systems: A tolerant control approach," in *2020 59th IEEE Conference on Decision and Control (CDC)*, IEEE, 2020, pp. 4504–4510.

[47] Wang, Y. and Pajic, M., "Supervisory control of discrete event systems in the presence of sensor and actuator attacks," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, IEEE, 2019, pp. 5350–5355.

[48] Carvalho, L. K., Wu, Y.-C., Kwong, R., and Lafortune, S., "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, 2018.

[49] Fritz, R. and Zhang, P., "Modeling and detection of cyber attacks on discrete event systems," *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 285–290, 2018.

[50] Yu, Z., Duan, X., Cong, X., Li, X., and Zheng, L., "Detection of actuator enablement attacks by petri nets in supervisory control systems," *Mathematics*, vol. 11, no. 4, p. 943, 2023.

[51] Oliveira, S., Leal, A. B., Teixeira, M., and Lopes, Y. K., "Security of cyber-physical systems against actuator attacks through cryptography," in *2023 International Conference on Information Technology (ICIT)*, IEEE, 2023, pp. 758–764.

[52] Fritz, R. and Zhang, P., "Detection and localization of stealthy cyberattacks in cyber-physical discrete event systems," *IEEE Transactions on Automatic Control*, vol. 68, no. 12, pp. 7895–7902, 2023.

[53] Barboni, A., Rezaee, H., Boem, F., and Parisini, T., "Distributed detection of covert attacks for interconnected systems," in *2019 18th European Control Conference (ECC)*, IEEE, 2019, pp. 2240–2245.

[54] Al-Dabbagh, A. W., Barboni, A., and Parisini, T., "Distributed detection and isolation of covert cyber attacks for a class of interconnected systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 772–777, 2020.

[55] Barboni, A., Rezaee, H., Boem, F., and Parisini, T., "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3728–3741, 2020.

[56] Gallo, A. J., Barboni, A., and Parisini, T., "On detectability of cyber-attacks for large-scale interconnected systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 3521–3526, 2020.

[57] Taheri, M., Khorasani, K., Shames, I., and Meskin, N., "Undetectable cyber attacks on communication links in multi-agent cyber-physical systems," in *2020 59th IEEE Conference on Decision and Control (CDC)*, IEEE, 2020, pp. 3764–3771.

[58] Alves, M. V., Barcelos, R. J., Carvalho, L. K., and Basilio, J. C., "Robust decentralized diagnosability of networked discrete event systems against dos and deception attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 44, p. 101 162, 2022.

[59] Bushra, B., De Santis, E., and Pola, G., "Security and localization of cyber attacks in finite state machines," in *2024 IEEE 20th International Conference on Automation Science and Engineering (CASE)*, IEEE, 2024, pp. 2659–2664.

[60] Anguluri, R., Katewa, V., and Pasqualetti, F., "Centralized versus decentralized detection of attacks in stochastic interconnected systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3903–3910, 2019.

[61] Gallo, A. J., Boem, F., and Parisini, T., "Distributed cyber-attack isolation for large-scale interconnected systems," in *2021 European Control Conference (ECC)*, IEEE, 2021, pp. 48–53.

[62] Gu, Z., Park, J. H., Yue, D., Wu, Z.-G., and Xie, X., "Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 10, pp. 6197–6206, 2020.

[63] Wang, Y., Bozkurt, A. K., Smith, N., and Pajic, M., "Attack-resilient supervisory control of discrete-event systems: A finite-state transducer approach," *IEEE Open Journal of Control Systems*, vol. 2, pp. 208–220, 2023.

[64] Jiang, X., Mu, X., and Hu, Z., "Decentralized adaptive fuzzy tracking control for a class of nonlinear uncertain interconnected systems with multiple faults and denial-of-service attack," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 10, pp. 3130–3141, 2020.

[65] Tan, S., Guerrero, J. M., Xie, P., Han, R., and Vasquez, J. C., "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.

[66] He, W., Xu, W., Ge, X., Han, Q.-L., Du, W., and Qian, F., "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3595–3608, 2021.

[67] Zhang, D., Feng, G., Shi, Y., and Srinivasan, D., "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[68] Lafortune, S., Lin, F., and Hadjicostis, C. N., "On the history of diagnosability and opacity in discrete event systems," *Annual Reviews in Control*, vol. 45, pp. 257–266, 2018.

[69] Guo, Y., Jiang, X., Guo, C., Wang, S., and Karoui, O., "Overview of opacity in discrete event systems," *IEEE Access*, vol. 8, pp. 48 731–48 741, 2020.

[70] Tong, Y., Li, Z., Seatzu, C., and Giua, A., "Verification of state-based opacity using Petri Nets," *IEEE Transactions on Automatic Control*, vol. 62, no. 6, pp. 2823–2837, 2016.

[71] Jacob, R., Lesage, J.-J., and Faure, J.-M., "Overview of discrete event systems opacity: Models, validation, and quantification," *Annual reviews in control*, vol. 41, pp. 135–146, 2016.

[72] Badouel, E., Bednarczyk, M., Borzyszkowski, A., Caillaud, B., and Darondeau, P., "Concurrent secrets," *Discrete Event Dynamic Systems*, vol. 17, no. 4, pp. 425–446, 2007.

[73] Lin, F., "Opacity of discrete event systems and its applications," *Automatica*, vol. 47, no. 3, pp. 496–503, 2011.

[74] Saboori, A. and Hadjicostis, C. N., "Verification of initial-state opacity in security applications of discrete event systems," *Information Sciences*, vol. 246, pp. 115–132, 2013.

[75] Balun, J. and Masopust, T., "Comparing the notions of opacity for discrete-event systems," *Discrete Event Dynamic Systems*, vol. 31, no. 4, pp. 553–582, 2021.

[76] Wintenberg, A., Blischke, M., Lafortune, S., and Ozay, N., "A general language-based framework for specifying and verifying notions of opacity," *Discrete Event Dynamic Systems*, vol. 32, no. 2, pp. 253–289, 2022.

[77] Han, X., Zhang, K., Zhang, J., Li, Z., and Chen, Z., "Strong current-state and initial-state opacity of discrete-event systems," *Automatica*, vol. 148, p. 110 756, 2023.

[78] Dong, Y., Li, Z., and Wu, N., "Symbolic verification of current-state opacity of discrete event systems using Petri Nets," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 12, pp. 7628–7641, 2022.

[79] Zhou, S., Yin, L., and Li, Z., "Quantifying opacity of discrete event systems modeled with probabilistic Petri Nets," *Information Sciences*, vol. 666, p. 120 434, 2024.

[80] Dulce-Galindo, J. A., Alves, L. V., Raffo, G. V., and Pena, P. N., "Enforcing state-based opacity using synchronizing automata," in *2021 60th IEEE Conference on Decision and Control (CDC)*, IEEE, 2021, pp. 7009–7014.

[81] Tong, Y., Li, Z., Seatzu, C., and Giua, A., "Current-state opacity enforcement in discrete event systems under incomparable observations," *Discrete Event Dynamic Systems*, vol. 28, no. 2, pp. 161–182, 2018.

[82] Colelli, R., Foglietta, C., Panzieri, S., and Pascucci, F., "An opacity approach for security exposure of iot components in critical infrastructures," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, IEEE, 2019, pp. 427–432.

[83] Xie, Y., Yin, X., and Li, S., "Opacity enforcing supervisory control using nondeterministic supervisors," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6567–6582, 2021.

[84] Cassez, F., Dubreil, J., and Marchand, H., "Dynamic observers for the synthesis of opaque systems," in *International Symposium on Automated Technology for Verification and Analysis*, Springer, 2009, pp. 352–367.

[85] Balun, J. and Masopust, T., "On opacity verification for discrete-event systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2075–2080, 2020.

[86] Ju, C. and Son, H. I., "Discrete event systems based modeling for agricultural multiple unmanned aerial vehicles: Automata theory approach," in *2018 18th International Conference on Control, Automation and Systems (ICCAS)*, IEEE, 2018, pp. 258–260.

[87] Tychola, K. A. and Rantos, K., "Cyberthreats and security measures in drone-assisted agriculture," *Electronics*, vol. 14, no. 1, p. 149, 2025.

[88] Ferrag, M. A., Shu, L., Friha, O., and Yang, X., "Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 407–436, 2021.

[89] Brentarolli, E., "Towards a digital twin for agriculture: Modeling of complex processes for monitoring, prediction and control in greenhouse farming," Available at: https://iris.univr.it/handle/11562/1165528, Ph.D. dissertation, Università degli Studi di Verona, Verona, Italy, 2025.

[90] Taji, K., Elkhalyly, B., Ahmad, Y. T., Ghanimi, I., and Ghanimi, F., "Securing smart agriculture: Proposed hybrid meta-model and certificate-based cyber security approaches," *Data and Metadata*, vol. 2, pp. 155–155, 2023.

[91] Li, X. and Hadjicostis, C. N., "Synthesis of State-Attack strategies for anonymity and opacity violation in discrete event systems," *arXiv preprint arXiv:2510.22657*, 2025.

[92] Al Asif, M. R., Hasan, K. F., Islam, M. Z., and Khondoker, R., "STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems," in *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, IEEE, 2021, pp. 1–6.

[93] Liu, J., Mvungi, E. S., Zhang, X., and Dias, A., "Fault diagnosis in Partially Observable Petri Nets with quantum bayesian learning," *Applied Sciences*, vol. 14, no. 1, p. 52, 2023.

[94] Giua, A., "Petri net state estimators based on event observation," in *Proceedings of the 36th IEEE Conference on Decision and Control*, IEEE, vol. 4, 1997, pp. 4086–4091.

[95] Giua, A. and Seatzu, C., "Observability of place/transition nets," *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1424–1437, 2002.

[96] Giua, A., Seatzu, C., and Corona, D., "Marking estimation of Petri Nets with silent transitions," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1695–1699, 2007.

[97] Bourij, A. and Koenig, D., "An original petri net state estimation by a reduced luenberger observer," in *Proceedings of the 1999 American Control Conference (Cat. No. 99CH36251)*, IEEE, vol. 3, 1999, pp. 1986–1989.

[98] Arichi, F., Cherki, B., and Djemai, M., "Active mode detection in hybrid mechatronic systems," in *In Proc. of International conference on Automatics and Mechatronics, Oran, Algeria*, 2011.

[99] Arichi, F., Cherki, B., and Djemai, M., "Discrete state estimation in hybrid photovoltaic systems," in *2012 2nd International Symposium On Environment Friendly Energies And Applications*, IEEE, 2012, pp. 256–261.

[100] Ramírez-Treviño, A., Rivera-Rangel, I., and López-Mellado, E., "Observability of discrete event systems modeled by interpreted Petri Nets," *IEEE Transactions on Robotics and Automation*, vol. 19, no. 4, pp. 557–565, 2003.

[101] Aguirre-Salas, L., Begovich, O., and Ramírez-Treviño, A., "State estimation in des modeled by a class of interpreted Petri Nets," in *Proceedings of the IEEE Internatinal Symposium on Intelligent Control*, IEEE, 2002, pp. 574–579.

[102] Ru, Y. and Hadjicostis, C. N., "State estimation in discrete event systems modeled by labeled Petri Nets," in *Proceedings of the 45th IEEE Conference on Decision and Control*, IEEE, 2006, pp. 6022–6027.

[103] Li, L. and Hadjicostis, C. N., "Least-cost transition firing sequence estimation in labeled Petri Nets with unobservable transitions," *IEEE Transactions on Automation Science and Engineering*, vol. 8, no. 2, pp. 394–403, 2010.

[104] Taleb, M., Leclercq, E., and Lefebvre, D., "Control design of timed Petri Nets via model predictive control with continuous petri nets," *IFAC Proceedings Volumes*, vol. 47, no. 2, pp. 149–154, 2014.

[105] Arichi, F., Petreczky, M., Djemai, M., and Cherki, B., "Observability and observer design of Partially Observed Petri Nets," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 27–32, 2015.

[106] Arichi, F., Cherki, B., Djemai, M., and Engin, S. N., "Discrete modes faults diagnosis for hybrid dynamical systems using Petri Nets," in *2022 IEEE 21st international Ccnference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, IEEE, 2022, pp. 165–170.

[107] Kile, A., Eneh, A., and Tumenayu, O., "Farm processes workflow management using Colored Petri Nets," 2023.

[108] Ran, W. and Tang, Q., "Research on plant disease and pest diagnosis model based on generalized Stochastic Petri Net," *Applied Sciences*, vol. 15, no. 12, p. 6656, 2025.

[109] Pepe, P., "On Liapunov–Krasovskii functionals under caratheodory conditions," *Automatica*, vol. 43, no. 4, pp. 701–706, 2007.

[110] Cassandras, C. G. and Lafortune, S., *Introduction to discrete event systems*. Springer, 2007.

[111] Ramadge, P. J. and Wonham, W. M., "The control of discrete event systems," *Proceedings of the IEEE*, vol. 77, no. 1, pp. 81–98, 2002.

[112] Ru, Y. and Hadjicostis, C. N., "Fault diagnosis in discrete event systems modeled by Partially Observed Petri Nets," *Discrete Event Dynamic Systems*, vol. 19, no. 4, pp. 551–575, 2009.

[113] Arichi, F., Cherki, B., Djemai, M., and Djouadi, S. M., "Fault diagnosis for discrete events systems described by Partially Observed Petri Nets," *ISA transactions*, vol. 128, pp. 220–228, 2022.

[114] Bushra, B., De Santis, E., Di Ferdinando, M., Di Gennaro, S., and Pepe, P., "On the consensus problem of nonlinear multi-agents systems via digital controllers," *International Journal of Robust and Nonlinear Control, Special issue on Multi-Agent Systems with delays and Networked Control Systems on IJRNC*, submitted.

[115] Kim, A., "On the Lyapunov's functionals method for systems with delays," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 28, no. 4, pp. 673–687, 1997.

[116] Pepe, P. and Ito, H., "On saturation, discontinuities, and delays, in iiss and iss feedback control redesign," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1125–1140, 2011.

[117] Mahboobi Esfanjani, R. and Nikravesh, S., "Stabilising predictive control of nonlinear time-delay systems using control Lyapunov–Krasovskii functionals," *IET control theory & applications*, vol. 3, no. 10, pp. 1395–1400, 2009.

[118] Gu, K., Chen, J., and Kharitonov, V. L., *Stability of time-delay systems*. Springer Science & Business Media, 2003.

[119] Kharitonov, V., *Time-delay systems: Lyapunov functionals and matrices*. Springer Science & Business Media, 2012.

[120] Niculescu, S.-I., *Delay effects on stability: a robust control approach*. Springer, 2002.

[121] Liberzon, D., *Switching in systems and control*. Springer, 2003, vol. 190.

[122] Ledyaev, Y. S. and Sontag, E. D., "A Lyapunov characterization of robust stabilization," *Nonlinear Analysis-Series A Theory and Methods and Series B Real World Applications*, vol. 37, no. 7, pp. 813–840, 1999.

[123] Malisoff, M. and Sontag, E., "Asymptotic controllability and input-to-state stabilization: The effect of actuator errors," in *Optimal control, stabilization and nonsmooth analysis*, Springer, 2004, pp. 155–171.

[124] Pepe, P., "Robustification of nonlinear stabilizers in the sample-and-hold sense," *Journal of The Franklin Institute*, vol. 352, no. 10, pp. 4107–4128, 2015.

[125] Sontag, E. D. et al., "Smooth stabilization implies coprime factorization," *IEEE transactions on automatic control*, vol. 34, no. 4, pp. 435–443, 1989.

[126] Lyu, M., Zhao, Y., Huang, C., and Huang, H., "Unmanned aerial vehicles for search and rescue: A survey," *Remote Sensing*, vol. 15, no. 13, p. 3266, 2023.

[127] Cui, J. et al., *Search and rescue using multiple drones in post-disaster situation*, 2016.

[128] Pappalardo, C. M., Del Giudice, M., Oliva, E. B., Stieven, L., and Naddeo, A., "Computer-aided design, multibody dynamic modeling, and motion control analysis of a quadcopter system for delivery applications," *Machines*, vol. 11, no. 4, p. 464, 2023.

[129] Zenkin, A., Berman, I., Pachkouski, K., Pantiukhin, I., and Rzhevskiy, V., "Quadcopter simulation model for research of monitoring tasks," in *2020 26th Conference of Open Innovations Association (FRUCT)*, IEEE, 2020, pp. 449–457.

[130] Karam, K., Mansour, A., Khaldi, M., Clement, B., and Ammad-Uddin, M., "Quadcopters in smart agriculture: Applications and modelling," *Applied Sciences*, vol. 14, no. 19, p. 9132, 2024.

[131] Yousfi, A. E. and Alawi, Y., "Development and evaluation of drone based spraying system for precision agriculture application.," *Mathematical Modelling of Engineering Problems*, vol. 12, no. 1, 2025.

[132] Mazzia, V., Comba, L., Khaliq, A., Chiaberge, M., and Gay, P., "Uav and machine learning based refinement of a satellite-driven vegetation index for precision agriculture," *Sensors*, vol. 20, no. 9, p. 2530, 2020.

[133] Chin, R., Catal, C., and Kassahun, A., "Plant disease detection using drones in precision agriculture," *Precision Agriculture*, vol. 24, no. 5, pp. 1663–1682, 2023.

[134] Shirwal, S., Abishek, A., Murali, M., et al., "Application of drones in precision agriculture: A review on benefits and challenges," *Journal of Experimental Agriculture International*, vol. 47, no. 7, pp. 516–531, 2025.

[135] Labbadi, M. and Cherkaoui, M., "Novel robust super twisting integral sliding mode controller for a quadrotor under external disturbances," *International Journal of Dynamics and Control*, vol. 8, no. 3, pp. 805–815, 2020.

[136] Wang, S., Chen, J., and He, X., "An adaptive composite disturbance rejection for attitude control of the agricultural quadrotor uav," *ISA transactions*, vol. 129, pp. 564–579, 2022.

[137] Le, W., Xie, P., and Chen, J., "Disturbance rejection control of the agricultural quadrotor based on adaptive neural network," *Information Processing in Agriculture*, 2024.

[138] Bushra, B., De Santis, E., and Pola, G., "Decentralized attack detection and localization for finite state machines," in *2025 IEEE 64th Conference on Decision and Control (CDC)*, Accepted for publication, IEEE, 2025.

[139] Bushra, B., De Santis, E., Di Benedetto, M. D., and Pola, G., "Observer decomposition for finite state machines and its application to opacity," in *2024 IEEE 63rd Conference on Decision and Control (CDC)*, IEEE, 2024, pp. 4443–4448.

[140] De Santis, E. and Di Benedetto, M. D., "Observability and diagnosability of finite state systems: A unifying framework," *Automatica*, vol. 81, pp. 115–122, 2017.

[141] De Santis, E. and Di Benedetto, M. D., *H-Systems*. Springer International Publishing, 2023.

[142] Fiore, G., De Santis, E., and Di Benedetto, M. D., "Secure diagnosability of hybrid dynamical systems," in *Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems*, Springer, 2018, pp. 175–200.

[143] Pola, G., De Santis, E., Di Benedetto, M. D., and Pezzuti, D., "Design of decentralized critical observers for networks of finite state machines: A formal method approach," *Automatica*, vol. 86, pp. 174–182, 2017.

[144] Saboori, A. and Hadjicostis, C. N., "Notions of security and opacity in discrete event systems," in *2007 46th IEEE Conference on Decision and Control*, IEEE, 2007, pp. 5056–5061.

[145] Bushra, B. and Djemai, M., "Fault detection and isolation in partially observed petri nets," to submit.

[146] Di Ferdinando, M., Pepe, P., and Borri, A., "On practical stability preservation under fast sampling and accurate quantization of feedbacks for nonlinear time-delay systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 314–321, 2020.