

Cyberattack Resilient Cooperative Filters for Cyber-Physical Systems

Shahram Shahkar

A Thesis

In the Department of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of
Doctor of Philosophy (PhD) at
Concordia University
Montreal, Quebec, Canada

November, 2025

© Shahram Shahkar, 2025

**CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES**

This is to certify that the thesis prepared

By: _____

Entitled: _____

and submitted in partial fulfillment of the requirements for the degree of

Doctor Of Philosophy

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____	Chair
_____	External Examiner
_____	Arm's Length Examiner
_____	Examiner
_____	Examiner
_____	Thesis Supervisor (s)

Approved by _____
Chair of Department or Graduate Program Director

_____ Date of Defence	_____ Dean,
--------------------------	----------------

Abstract

Cyberattack Resilient Cooperative Filters for Cyber-Physical Systems

Shahram Shahkar, Ph.D.

Concordia University, 2025

The present thesis proposes resilient methodologies against three different classes of security threats that are involved with Cyber-Physical Systems (CPS). The first problem involves time-delay and Denial of Service (DoS) cyberattacks inflicted on the information tele-communication signals exchanged between subsystems of the CPS. The proposed solution involves a set of equivalent interconnected filters to be located at the input channels of all transceivers at every subsystem, in such a way that the output of each filter feeds the input of its neighbouring subsystems, hence, cooperative filters. It will be shown that the cooperative filtering scheme is capable of making the CPS resilient to random time-delays that may inflict communication channels, as long as the filters make a connected graph. Theoretical results have been validated through simulation of a controversial CPS application known as the Load Frequency Control (LFC) problem in Smart Grids. The second problem involves Navigation of autonomous vehicles in GNSS denied environments. The thesis proposes a novel cooperative localization filtering scheme in which certain filters are deployed onboard the vehicles to exchange the vehicle's "perceived" geographic position obtained from onboard sensors and computational equipment, with their neighbour vehicles in a Multi-Agent System (MAS) framework, in order to compensate the estimation error associated with individual vehicles, by incorporation of the perceived positioning estimates of other vehicles in the network. Finally, the third and last problem involves authentication of navigation commands (i.e., waypoint and airspeed commands) issued from the Ground Control Stations (GCS) to a vehicle, in which the objective is to authenticate the commands received from a master ground controller at the vehicle and decide whether the commands are legitimate commands (and trustworthy to be obliged by the autopilot to follow) or have to be rejected and replaced by "trustworthy" alternatives. The vehicles use onboard filters to process waypoint commands to formulate a real-time authentication function in order to build a "trustworthy" map of the airspace, for their future navigation.

Contents

1 Introduction and Literature Review	1
1.1 Subject of the Thesis in a Glance	1
1.1.1 General Overview of the Thesis	1
1.2 Literature Review	3
1.2.1 The Load Frequency Control (LFC) Problem	9
1.2.2 The Internet of Drones (IoD)	13
1.2.3 Navigation of Autonomous Vehicles in Global Navigation Satellite Systems (GNSS) Denied Environments	18
1.2.4 Navigation of Autonomous Vehicles Subject to Actuator Attacks	23
1.3 Literature's Modelling and Control of Cyber Physical Systems (CPS) Sub- ject to Some Cyberattacks	24
1.3.1 Denial of Service (DoS) cyberattacks	25
1.3.2 Deception (or False Data Injection) cyberattacks	27
1.3.3 Static Deception Attack Detection Algorithm	28
1.3.4 Replay Attack Detection	29
1.3.5 Bayesian Attack Detection Methods	30
1.4 Switching Topologies and Delays in Multi-Agent Systems (MAS)	33
1.4.1 Weaknesses of the Solution	36
1.4.2 Strengths and Opportunities of the Solution	37
1.5 Distributed Resilient Control for MAS with Communication Delays and DoS Attacks	38
1.5.1 Strengths Weaknesses Opportunities Threats (SWOT) Analysis	39
1.6 Cooperative Control for MAS with Unknown False Data Injection and Replay Cyberattacks	41
1.6.1 SWOT Analysis	43
1.7 Summary	43
1.7.1 False Data Injection Attacks	44
1.7.2 Denial of Service Attacks	46

2 Time Delay Cyberattacks in CPS	48
2.1 Introduction	48
2.2 Resilient Control Against Time-Delay and DoS Cyberattacks in LFC	51
2.2.1 Problem Statement	51
2.2.2 Research Results for Problem 1	53
2.2.3 Simulations and Case Studies of Problem 1	58
2.2.4 Limitations of the Solution in 2.2.2	63
2.3 Time-Delay Resilient Cooperative Filters for Cyber-Physical Systems	66
2.3.1 Definitions and Assumptions	66
2.3.2 The LFC Example	68
2.3.3 Problem Statement	69
2.3.4 Research Results for Section 2.3	71
2.3.5 Simulations and Case Studies	79
2.4 Conclusion of the Chapter	84
3 Unmanned Aerial Vehicle (UAV) Navigation in GNSS Denied Environ-	
ments	87
3.1 Sensor False Data Injection (FDI) in MAS	87
3.1.1 Problem Statement of Sensor FDI in MAS	88
3.1.2 Regression Filtering Solution for Problem 2	89
3.1.3 Limitations of the Regression Filtering Solution	90
3.2 Optimization of Localization Error in MAS of UAVs through Cooperative	
Positioning: Autonomous Navigation in Partially Denied GNSS Environ-	
ments	91
3.2.1 Contributions and Assumptions of Section 3.2	92
3.2.2 Research Results for Section 3.2	93
3.2.3 Simulations and Case Studies	95
3.2.4 Conclusion	98
3.3 Cooperative Localization of Multi-Agent Unmanned Aerial Vehicle (UAV)	
Networks in Intelligent Transportation Systems	99
3.3.1 Related Works	100
3.3.2 Contributions of the Section	101
3.3.3 Problem Statement	102
3.3.4 Assumptions and Definitions	104
3.3.5 Cooperative Localization in Multi-Agent Networks	106
3.3.6 Theoretical Results	109
3.3.7 Simulations	120

3.3.8 Discussions and Clarifications	127
3.3.9 Conclusion of the Chapter and Future Works	135
4 Anti-Spoofing Aided Technology for Urban Air Mobility: Ground Com-	
mand Authentication	137
4.1 Contributions	143
4.2 Problem Statement	143
4.3 Definitions and Assumptions	145
4.4 Research Results	148
4.4.1 Static Authentication	149
4.4.2 Dynamic Authentication	151
4.5 Simulation Results	155
4.6 Chapter Conclusion and Future Works	159
5 Conclusion of the Thesis and Future Works	161
5.1 Cooperative Filters	161
5.1.1 Future Works for Improving the Efficiency of Cooperative Filters	162
5.2 Authentication of Ground Control Station Commands	162
5.2.1 Future Works in Authentication of Ground Control Station Com-	
mands	163
A List of Publications	164
Bibliography	165

List of Figures

1.1	Load frequency control and regulation in a Smart Grid where telecommu- nication channels are affected by Time-Delay Switch (TDS) cyberattack, and where instability in the CPS is a fundamental concern.	2
1.2	Chapters 3 and 4 of the Thesis	3
1.3	Block diagram of a frequency control mechanism for a generating station contributing the LFC in a multi-area power system. The solid lines are hard-wired measurements/commands that are presumably immune from cyber attacks (as they are confined within protected premises), whereas dashed lines represent telemetered data that are subject to TDS/DoS cyber attacks.	10
1.4	Two-Area power system schematic. Solid lines represent <i>hard-wired</i> con- nections and dashed lines represent communication channels. Locally mea- sured quantities are transmitted to the central control center (represented by the cloud) through <i>Remote Terminal Units</i> (RTUs). It is assumed that communication channels would be subject to TDS or DoS cyber attacks only.	12
1.5	Block diagram of Internet of Drones (IoD) as an example of a CPS, bor- rowed from [77]	14
1.6	Proposed scope of CPS control for IoD	15
1.7	Block diagram of Deception cyberattacks on system actuators and sensors	28
2.1	Frequency variations in a power system with a centralized controller (as depicted by a cloud in Figure 1.4) transmitting $\Lambda_i(t)$ and $\Lambda_j(t)$ to the generating units i and j respectively. It is assumed that the communication channels are under cyber attack causing delayed ACEs (i.e., $\Lambda_i(t - \tau_i)$ and $\Lambda_j(t - \tau_j)$) at governor inputs. The result is clearly a growing oscillation in the frequency variations of the areas yielding instability and shut down through protective relaying mechanisms.	60

2.2	Decentralized augmented controllers in equation (2.13) are active, and Λ_i , Λ_j are under delay cyber attack same as in Figure 2.1. The thick line represents ΔP_{ij} which indicates that LFC is functional despite delay cyber attack.	60
2.3	The scenario depicted in Figure 2.2 is repeated. Δf_i and Δf_j are displayed which indicates LFC is functional despite of the delay cyber attacks on Λ_i , Λ_j	61
2.4	Control commands under delay cyber attack presented in Figures 2.2 and 2.3 for reference. u_i tries to enforce the turbine power ΔP_{v_i} to track the load area ΔP_{d_i} in Figure 2.2, so that eventually $\Delta P_{ij} = 0$	61
2.5	In this scenario all communication channels are under delay cyber attack. The operating conditions are similar to Figure 2.1, however the augmented controllers in equation (2.13) have stabilized the system and largely improved LFC. Unfortunately complete LFC can not be achieved as the steady state $\Delta f_i - \Delta f_j \neq 0$	62
2.6	LFC is no longer functional despite the fact that the augmented controllers are active. The operating circumstance is the same as in Figure 2.5.	62
2.7	Most severe cyber attack circumstance where Λ_i and Λ_j are under DoS cyber attack while the telemetered measurements are randomly delayed. Black line depicts Δf_i and the grey line depicts Δf_j	63
2.8	Comparison between the Decentralized controller proposed in this work and the conventional centralized controller under DoS cyber attack scenario depicted in Figure 2.7.	63
2.9	Block diagram of a frequency control mechanism for a generating station $\mathcal{S}_i$ contributing the LFC in a multi-area power system. The solid lines are hard-wired measurements/commands that are presumably immune from cyberattacks (as they are confined in $\mathcal{S}_i$), where the dashed lines represent tele-metered data that are subject to TDS/DoS cyberattacks.	69

2.10 Schematics of a LFC power system with three area generating stations

$\mathcal{S}_i, \mathcal{S}_j, \mathcal{S}_k$ and the Centralized Control Station $\mathcal{S}_o$. The CPS $\mathcal{S}$ in this figure can be represented as $\mathcal{S} = \{\mathcal{S}_i \cup \mathcal{S}_j \cup \mathcal{S}_k \cup \mathcal{S}_o \cup \mathcal{S}_{SS_{ij}} \cup \mathcal{S}_{SS_{jk}}\}$ where $\mathcal{S}_{SS_{ij}}, \mathcal{S}_{SS_{jk}}$ denote the two substations, each also considered as a subsystem of the CPS. The tele-communication system can be further regarded as a subsystem in a more comprehensive model. However, this is not considered in this section. The CCS $\mathcal{S}_o$ and the tele-communication system comprise the cyber part of the system that is responsible for the data collection and processing, and the power system comprises the physical part of the CPS. The Front-End Processors (FEPs) are electronic apparatus inside the CCS that transmit/receive tele-communication signals and demodulate the state variables. The Remote Terminal Unit (RTU) is a micro-scale FEP with a similar function located in every substation. ΔP_{ij} is a system state whose sensor (i.e., current and voltage power transformers) is located in a substation, and whose instantaneous value is transmitted to the CCS through an RTU. The CCS receives all $\Delta P, \Delta f$, and computes Λ for individual generating stations. 70

2.11 Schematics of a MAS time-delay resilient CPS, and the schematics of the

cooperative filter $h(t)$. The agents in the MAS exchange information in order to recover a time-delayed state $x_{o(\ell)}(t) \in \mathcal{S}_o$. $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$ is the input of the filter in $\mathcal{S}_i$ (if $o \in \mathcal{N}_i$, or can be any other conjecture available to $\mathcal{S}_i$ which needs not be a correct estimate), and the output of the filter is $x_{o(\ell),i}(t + \Delta t)$, where $\Delta t > 0$ is a small response time. It will be shown that $\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t)$, where T_s is a negligible arbitrary settling time for the filter that will be controlled by the filter gain $\gamma \in \mathbb{R}^+$ 72

2.12 Spectrum of $\tilde{L}_\tau$ with reference to the Gershgorin disk theorem, is the union

of several disks where each disk corresponds to a row in $\tilde{L}_\tau$. The bigger circle represents the first N rows, referred to as the first block row, where the center of the disk is on the real axis and at $2\ell_{ii} - \sum_{i=1}^N [\Gamma_i]_{ii}$ to the right, with a radius ℓ_{ii} . The smaller disk represents the set of other block rows where each row is represented by a disk with its center on the real axis at $|[\Gamma_{ji}]_{jj}|$ and a radius a_{ij} , and a set of null disks located at the origin. 76

2.13	Performance of the time-delay resilient filter. The thin line represents Δf_i in response to a +10% load variation in ΔP_{d_i} , at 0.1sec. and back to 0 at 0.8sec., for the case where a conventional LFC is in operation. Perilous swings in the system frequency are clear when the telemetered data are attacked by sufficiently long time-delays, resulting in pervasive instability in the power system (thinner line). The same scenario is repeated when resilient cooperative filters are deployed (solid thicker line) which demonstrates stability and a satisfactory LFC control.	81
2.14	Variations in Λ_i as a result of $\Delta P_{d_i}(t)$.	82
2.15	Time-Delayed ACE signal Λ_i transmitted from $\mathcal{S}_{CCO}$ without the employment of a delay-resilient cooperative filter system, and as a result of a 10% load disturbance ΔP_{d_i} .	82
2.16	Adjustment of the servo-valve electric signal in response to the area load variations depicted in Figures 2.13.	83
2.17	Affect of the tele-communication bandwidth. Inadequate bandwidth in tele-communication channels result in marginal instability as depicted by the thin line.	84
2.18	General architecture of a CPS, subject to adversarial time-delay cyberattacks. The exogenous states of the systems (x_i, x_j, x_k) are transmitted to adjacent subsystems with unknown time-delay and the output of $h(t)$ filters in each subsystem transmits the conditioned signal back to the source, hence, cooperative filters. The architecture shown in this figure results in time-delay resiliency in the CPS as demonstrated in Figure 2.19.	85
2.19	A discrete-time network of five interconnected agents transmitting equivalent reference signals (shown by the asterisks) to adjacent subsystems. The tele-communication channels are randomly delayed and the output of the cooperative filters are shown by thinner lines for each subsystem. It is evident that the delayed signals follow the real-time reference signal in a time-duration T_s that is dependent of the filter gain and the topology of the network.	86
3.1	Sensor/Actuator False Data Injection (FDI) attack in a Multi-Agent System	88
3.2	The x-y location of a multi-agent system of UAVs with 10 agents, with their true positions with respect to an arbitrary origin. The axes are scaled in meters, and the elevation has been omitted for simplicity and better clarity of the figure.	96

3.3	Monte-Carlo simulations of cooperative sensing method (in red) in comparison with the dead-reckoning positioning estimation (in black) for a fully connected system of UAVs, as depicted in Figure 3.2. Concentration of the red samples in comparison to the black area represents the improved accuracy in localization. The position of the leader is represented by the same marker in every observation due to its deterministic nature, hence 100% accuracy. However, the variance of all other agents' positions is not zero (due to the error in range-finders) but equal (due to the fully connected topology).	97
3.4	Results of Monte-Carlo simulations for the network topology of Figure 3.2. Localization error is increased as the UAVs are distanced (communication-wise, not geographically) from the leader. This is opposed to the case in Figure 3.3, where the network error was equally distributed among the agents.	98
3.5	The LTI filter and the associated block diagram as a function of $\bar{x}^{(i)}(kT_s)$, and the onboard sensors, as well as the filter output of the neighbour UAVs. The input to the filter is the Odometry localization sample $\bar{x}^{(i)}(kT_s)$, and the onboard sensor information taken from the rangefinders, and the air-speed along the x -axis. The filter feedback gain γN_i is a parameter that will be selected later in this paper, where N_i is the number of neighbours to i , and γ is a positive scalar.	106
3.6	A distributed cooperative localization scheme for a MAS with 3 agents. Each agent i recursively transmits its self-estimated position $\hat{x}^{(i)}(kT_s + \Delta t)$ continuously to its neighbours, until a relative consensus is achieved in the network (and that is when $\hat{x}^{(i)}(kT_s + \Delta t)$ reaches a steady state).	109
3.7	A centralized Minimum-Mean-Square-Error (MMSE) based localization (referred to as regression filtering in Section 3.1.2) of a MAS with 3 agents. Every agent transmits its self-estimated position $\bar{x}(kT_s)$ at each time-step kT_s , and a centralized computation center derives H_k and transmits the corrected positions $z(kT_s) = H_k \bar{x}(kT_s)$ back to the agents.	110
3.8	Comparison of localization error in estimation of individual agents' $\bar{x}^{(i)}(kT_s)$ (in black) where conventional estimation techniques using motion models and IMU sensors are used, and cooperative localization (in red), for $N = 4$. The horizontal and vertical axis display longitudinal and lateral positions with respect to an arbitrary origin, with arbitrary scale. Ground truth position is indicated as the center of the mass of the (red) particles.	121

3.9	Localization error in a multi-agent system with $N = 4$, where low-grade sensors with higher errors are employed. It can be seen that there is little to no advantage in deploying cooperative localization in comparison with conventional (individually based) estimations. Ground truth position is indicated in the center of the mass of the (red) particles.	122
3.10	A similar case study deploying $N = 9$ agents. In comparison with Figure 3.8 it can be evident that the performance of cooperative localization takes clear advantage over odometry due to less dispersed red samples. Ground truth positions are indicated as the center of the mass of the (red) particles.	123
3.11	Localization with $N = 7$ and low-grade sensors. Ground truth positions are indicated as the center of the mass of the red particles.	124
3.12	Case study where $N = 20$, with high-grade sensors. The red to black area is further reduced to 35% indicating better cooperative localization performance as N grows.	125
3.13	Almost perfect localization is possible through cooperative localization with $N = 100$ or more agents. The performance represented by the size of the red to black areas indicate that localization can be improved by more than 15 times. The red samples are gradually converging to a single point, which shows moving toward a perfect localization as the number of agents become larger and larger.	126
3.14	Similar case study depicted in Figure 3.13 is illustrated for $N = 100$, where the connectivity of the network reduced.	127
3.15	Emulation of a fully connected network with infinite number of agents, through an anchor node. The anchor node is an agent with a ground truth position (as shown with an asterisk). It can be observed that the asterisk has zero-variance implying that the position is deterministic as opposed to a random variable. Other agents in the network attain a very accurate position through direct cooperation with the anchor.	128
3.16	The case study is the same as in Figure 3.15 with the difference that the topology of this case study associates the lowest connectivity characterized by a chain-wise connection, hence a large diameter. The agent that is immediate to the anchor has the best accuracy in the network, and as agents get farther distanced in the network from the anchor, their tendency in cooperation with the anchor becomes more and more indirect, and as a result attain more and more error.	129

3.17	Alternative resources of information in a fleet of vessels. Distance between the vessels detected by the radars are redundant to the locations observed by PNTs.	130
4.1	Simulated flight path of a vehicle from $\mathbf{x}_0 \rightarrow \mathbf{x}_k$, where $\mathbf{x}_0 \leftrightarrow 91 \in \mathcal{N}_m$, and $\mathbf{x}_k \leftrightarrow 45 \in \mathcal{N}_m$. The red path indicates the already taken path which is the most efficient route from the origin to the present position.	156
4.2	A relatively short flight path of a vehicle from $\mathbf{x}_0 \rightarrow \mathbf{x}_k$, where $\mathbf{x}_0 \leftrightarrow 1 \in \mathcal{N}_m$, and $\mathbf{x}_k \leftrightarrow 6 \in \mathcal{N}_m$. As the prior set of the prior waypoints $\{1, \dots, 6\}$ is relatively small, the authentication of the future waypoints embraces a large set of trustworthy possibilities, hence, relatively non-restricted, i.e., inaccurate.	157
4.3	A similar case study to Figure 4.2 with the exception that the set of prior waypoints in this example are $\mathcal{X}_{0,9}$ are greater in the number of elements. This entails $p(a_{10} \mathbf{x}_{10}, \cdot)$ to be evaluated based on a larger set of conditions, hence a smaller set of trustworthy options as future waypoints. Clearly the number of trustworthy points $\mathbf{x}_9$ in this figure has decreased to 24, in comparison to 39 trustworthy points in Figure 4.2, implying an increased accuracy.	158
4.4	Flight path of the aerial vehicle in Figures 4.2 and 4.3 at $k = 12$. As the prior path is increasing in size, authentication of future waypoints narrows to less waypoints, indicating the accuracy of the authentication process.	159

List of Tables

2.1	Results of the analysis of some of the more recent publications in the literature related to CPS time-delay resiliency	52
3.1	Cooperative Localization Performance Comparison	131

Chapter 1

Introduction and Literature Review

1.1 Subject of the Thesis in a Glance

Literature has defined the Cyber-Physical Systems (CPS) as multidisciplinary systems that conduct feedback control on widely distributed embedded computing systems by the combination of computation, communication and control technologies in order to achieve the performance of physical processes [1]. The focus of this thesis is mainly concentrated on the Internet of Drones (IoD) and Urban Air Mobility (UAM), as well as Smart Grids (SG) as certain CPS applications, operating in a decentralized and centralized mode of control, respectively. This research thesis intends to identify and improve some of the latest existing security challenges with regard to these applications, and specifically DoS (Denial of Service) and time-delay attacks in Smart Grids, as well as navigation attacks on data communication channels in UAM.

1.1.1 General Overview of the Thesis

The present thesis aims to investigate the cyber physical vulnerabilities of a CPS, and provide control solutions to some of the important threats, with due consideration to the state of the art methodologies provided in the literature. Particular attention will be given to UAM of UAVs as an application, where simulations and case studies have been worked out to verify the validity of theoretical results. Exceptionally, for the first chapter we have provided a different CPS example in order to study an existing real-world problem in relation with time-delay cyberattacks, where the Load Frequency Control (LFC) problem in Smart Grids has been considered to address one of the open challenges in the literature as of today.

The literature has broadly divided the problem of CPS vulnerabilities of networked

UAVs that are due to the open communication architectures of the tele-communication system, into the following main categories [3], as illustrated in Figure 1.2.

1. The communication channels between the UAVs,
2. Satellite navigation signal reception,
3. The communication between the UAVs and the Central Control Station (CCS).

Due to the above general categorization, the chapters of the thesis will be devoted to investigate the outstanding problems associated with these three items, as briefly stated below.

1. Chapter-1: Introduction and Literature Review.
2. Chapter-2: We consider the LFC problem in a Smart Grid, where separate power generating areas represent subsystems of an interconnected CPS, and where a Central Control Station (CCS) regulates the power flow among the power areas. A Time Delay Switch (TDS) cyberattack acting on the telecommunication system between the agents and the CCS causes instability in the system, and the objective is to find a methodology to stabilize the system against time delay cyberattacks. An illustration of the general system is presented in Figure 1.1.

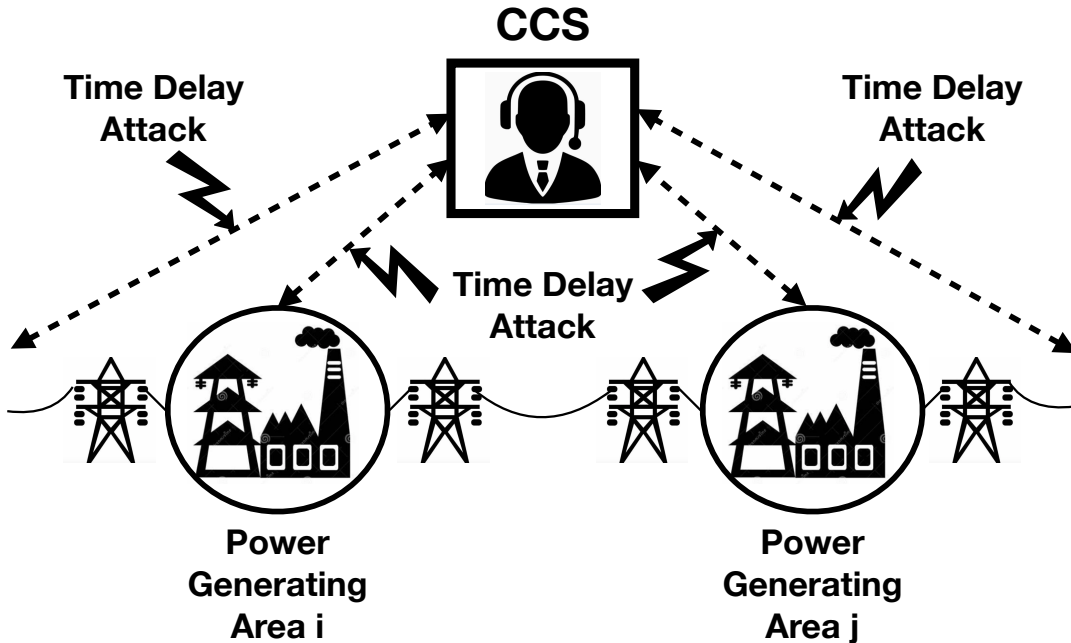


Figure 1.1: Load frequency control and regulation in a Smart Grid where telecommunication channels are affected by Time-Delay Switch (TDS) cyberattack, and where instability in the CPS is a fundamental concern.

3. Chapter-3: We assume that the true geographical position of a UAV i is compromised at the UAV radio signal receiver (e.g., Global Navigation Satellite System, GNSS) and the aim is to develop an estimation technique to recover the real-time position of the UAV through cooperation with the nearby UAVs in UAM, with the least error.
4. Chapter-4: We assume that the Ground Control Station GCS transmits a waypoint guidance command to a UAV i that is compromised by an adversary, and the objective is to retrieve a space estimation of the original command at the UAV through contemplation of the past commands and the physical properties of the UAV.

An illustrative representation of the problems for Chapters 3 and 4 is given in Figure [1.2](#).

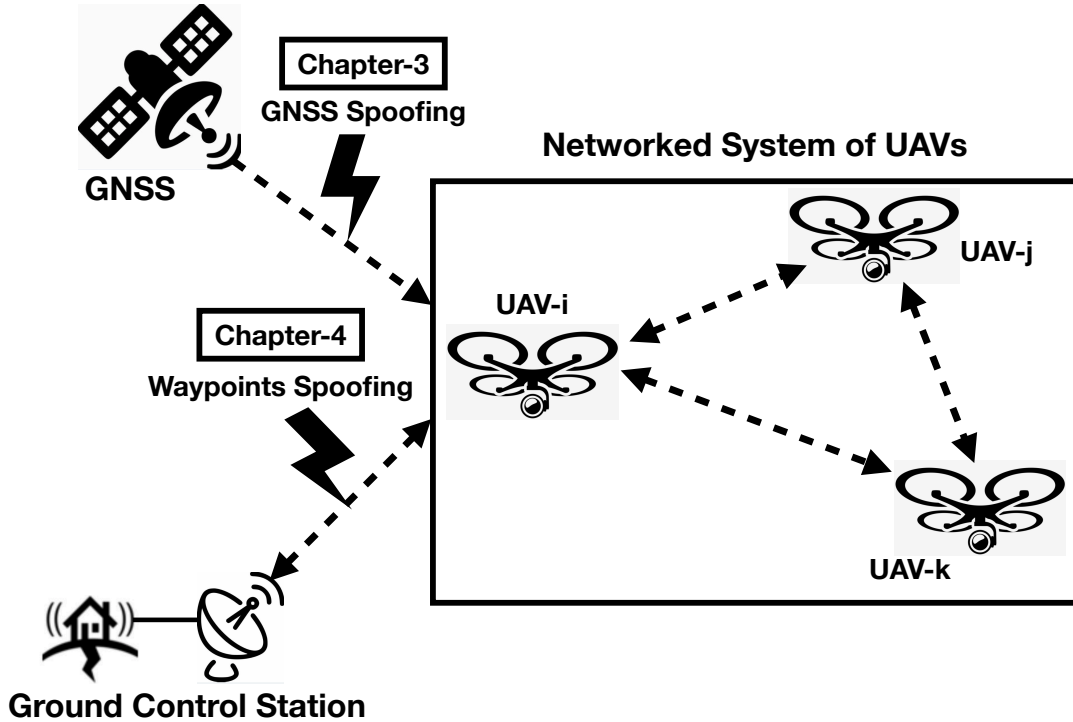


Figure 1.2: Chapters 3 and 4 of the Thesis

1.2 Literature Review

As explained before, the literature defines Cyber-Physical Systems (CPS) as multidisciplinary system of subsystems (SoS) in which a combination of tele-communication system of information, followed by a system of computation and the process of information, and

finally control technologies involve in order to achieve the desirable performance of physical processes. For example, the emerging technology of Internet of Drones (IoD) and UAM is an example of a CPS, where a number of UAVs attempt to share a common air-space to commute to their designated destinations, and where the overall objective is to effectively control the traffic and the trajectories of the aerial systems in order to achieve an overall minimal commute time for the UAVs with optimal energy efficiency. In this problem the UAVs are standalone physical systems equipped with a navigational means such as a GNSS receiver. Hence, each UAV receives a set of way-points from a ground control station (GCS) towards its destination through wireless communication. The GCS is responsible to optimize the route for each and every UAV through computational process, and the UAVs have onboard sensors to avoid collision and administer a smooth flight through the designated way-points, where the UAVs tend to share their present geographical positions with the GCS and the air traffic system as well as surrounding vehicles, hence a feedback control loop.

Therefore, data acquisition modules collect data (e.g., geographic locations in the example of the IoD presented above) by distributed field devices in CPS system and provide real-time accurate data to the information processing layers according to the demands of services and complete given tasks by information processing technologies such as data uncertainty management, statistical signal processing, data security processing and feedback control [2]. In the meantime, CPS should not be confused with the Internet of Things (IoT) or sensor networks. The authors in [2] have pointed out that wireless sensor networks (WSN), internet of things (IoT), and CPS are conceptually different in a sense that WSN only senses signals and emphasizes the perception of information and provides data support for a variety of specific applications through data collection, processing, integration and routing. IoT on the other hand, interconnects Internet information sensing devices like wireless sensor and radio frequency identification (RFID) through wireless networks, being a new type of network to realize the overall perception, reliable transmission and intelligent processing of information.

The authors in [4] have also highlighted the differences between CPS and IoT. Accordingly, the essence of the CPS is in measuring the state information and ensuring secure, efficient, and intelligent operation of the physical devices. In CPS, the sensor-actuator layer, communication layer, and application (control) layers are present. The sensor-actuator layer is used to collect real-time data and execute commands, whereas the communication layer is used to transport data between the upper and the lower layers and other subsystems, and finally, the application (control) layer is used to analyze

data and make control decisions. In contrast, IoT is a networking infrastructure that is used to interconnect smart devices (“things”) so that the devices can share data in order to achieve a specific goal. In this sense the key of IoT is in the *interconnection* across heterogeneous networks and not the control so that “data collection, resource sharing, analysis, and management can be carried out”. Therefore, according to the authors “IoT is a horizontal architecture, which should integrate communication layers of all CPS applications to achieve interconnection”.

As network systems and physical systems (occasionally) are accessible to adversaries and intruders, problems such as invasion, tampering, counterfeiting and other malicious attacks as well as delay in network transmission system are probable. Therefore, CPS must be able to deal with the problem of credibility, security, effectiveness, real-time, dynamic and predictability [2]. Accordingly, credibility refers to the authentication of the components sending information and receivers’ capabilities to exactly determine the real identity of the transmitters to prevent counterfeiting. Security refers to the encryption and decryption of sent or received information and considerations to protect the privacy of information. Validity refers to the set of preprocessing tasks to validate the integrity of information and control commands and measures in safeguarding the system operation against uncertainties, disturbances, and noise. In the meantime, real-time capability of the overall system ensures timely acquisition, transportation, data processing, and control to render stable and real-time performance of the overall system. The dynamic capability of the CPS system is responsible in restructuring and reconfiguration of the system to flawlessly adjusting control commands according to preset rules under certain circumstances. And finally, predictability pertains to CPS resource allocation strategy to reasonably allocate resources to multiple competing real-time tasks at any moment and in any case so that the real-time requirements of every real-time task can be satisfied.

The authors in [5] have broadly classified CPS security into two areas; the information (data) security and the control security. They have argued that information security involves securing information during data aggregation, processing and large-scale sharing in the network environment, especially in open and loosely coupled networks, whereas control security encompasses resolving control issues and mitigating the control system from adversarial attacks on system estimation and control algorithms. Information security focuses on data protection, for example by using encryption, whereas control security focuses on protecting the dynamics of control systems against cyber-attacks. In particular and in broad terms, the authors have represented CPS security in securing access to devices (that is similar to credibility and authentication requirements discussed before),

securing data transmission, securing applications and data storage, and finally, securing actuation that requires command signals to the actuators to be issued from authorized sources including the feedback control commands [6], the command transport systems [7] and [8] (proposing IoT research directions).

The authors in [9] have stated that CPS is more vulnerable to attacks than traditional IT systems, which are not limited to CPS, but to attacks from *network layers*, especially the Internet. Additionally, attacks may target *perception layers* including sensors and actuators, or *application layers*. Although each layer is susceptible to different attacks, some attacks could target all layers simultaneously [10,11]. Examples of these attacks have been discussed in depth in the literature:

Denial of Service (DoS): Adversaries disrupt normal transmission of data through preventing traffic flow to cause temporal unavailability in the network by, for example, flooding a transmission device with multiple requests, or taking advantage of protocol vulnerability, etc. [11,12].

Man in the Middle (MITM): The adversary intervenes the data exchange process and alters information packets in order to deliberately control the behaviour of the CPS in a particular manner. This can be realized by changing sensor information, control packets, or both simultaneously [12-14].

Eavesdropping: The adversary intercepts the transmitted data. This may include the sensor packets transmitted to the application layer in the cyber world, or the resulting control commands. The effect could be a breach of user privacy, or else [15].

Spoofing: The adversary intrudes the CPS through a false identity and emulates information provided by certain resources in order to control of the CPS. For example, attackers out-powering global positioning satellite signals on the ground level and changing ephemeris information to manipulate the decoded positioning and location of their victims [16,17,86,100].

Replay: Adversaries record and play back signals collected at a particular node and time and transmit the recorded signal to cause a malicious intent. Consider an adversary recording GPS satellite signals at a certain location on the ground and broadcasting the recorded signal at a different location to manipulate the GPS receivers being exposed to the broadcasted replayed signal [16,17].

Analysis of the system vulnerabilities in response to the cyber-attacks defined above have received particular attention in the literature. For example, the authors in [22] have defined a security index for power networks as the minimum number of measurements in the system that have to be manipulated so that an attack on a particular bus remain undetectable by the monitoring system. In other words, a smaller security index in a particular point in the network signifies a high vulnerability in response to a small effort in manipulating system resources. The authors in [23] have introduced certain metrics in a general framework for CPS to quantify the security of the system against cyber-attacks. In this framework the plant has been considered to be controlled through a remote station that is connected to the plant through a communication network, and the paper introduces important concepts such as *safe systems* (in which the system states are continuously enclosed in a compact predefined set), *stealthy attacks* (where the system outputs exhibit values that are sufficiently close to the expected values for given attack vectors), and the *nominal behaviour* in the system (signifying that the system input/output is not tampered in the communication network). The authors have further defined a quantifying function indicating the impact of the CPS against cyber-security attacks as the norm of process states and tracking error estimates. As a result, concepts such as *maximum-impact attacks*, and *minimum-resource attacks* have been introduced to provide a quantitative measure of the system vulnerability and resilience in response to cyber-attacks.

Secure systems has been defined in [25] when a number of conditions are satisfied in the system: (1) The square error function defined by the residual of the plant output before and after transmission to be within a preset bound for all bounded adversarial MITM attacks. (2) The vector norm composed of the system states and the plant outputs (referred to as z) be within a preset bound, and (3) for a bounded z_0 , the mean value $\mathbb{E}(\|z_k\|^2) < \delta$, for a specified δ , and all k . However, secure systems and *security index* of a secure system has been defined differently in other publication. For example, the authors in [24] have proposed a $\mathcal{H}_2$ -norm of the transfer function from the attack vector to a subset of the system states, and claim that it is a more general characterization for studying the CPS system vulnerability to cyber-attacks, in a sense that the formulation could suggest certain entries from the attack vector for which the required effort for inflicting damage on the target states is minimized. A security index has been proposed in the paper based on the transfer function of the attack vector to system states, and the transfer function of the attack vector to the output variables. The adversarial problem is then to maximize the former (inflicting maximum damage) while minimizing the latter

(undetectability purpose).

In conclusion, the vulnerability of CPSs in the cyber parts allows injecting attacks into the system in a stealthy and unpredictable way. As an example, inserting some malware such as worms and viruses in medium access control layers or a networked components computerization could cause disruption of coordination packets. Moreover, an attacker can illegally get access to the monitoring centers while obtaining the encryption key for damaging the normal operation [1,18]. Therefore, for the reasons explained above security of CPS has attained paramount importance in the literature [18]- [21].

According to our investigations there are very limited documents available in the literature that examine simultaneous types of cyber-attacks on CPS. Among those publications, the authors in [25] have studied the security performance of systems under randomly occurring DoS attacks and randomly occurring deception (MITM) attacks simultaneously where an event based communication scheme is present in order to reduce the burden on the communication system. The reason that the authors of the paper have exclusively focused on the two specified cyber-attacks is that the authors claim network attacks to be dividable into the Denial of Service (DoS) attacks and the deception (or MITM) attacks. Furthermore, pursuing event triggered systems under DoS attacks the authors in [26,53] assume that the communication network is a packet based media and only discrete values of the plant output can be accessible to the controller. Furthermore, they have assumed that the intervals during which DoS attacks are active can be finite. The authors then propose boundaries for the maximum allowable interval of a DoS attack, as well as the number of allowable attacks, and the duration for each attack within a time period, such that the hybrid system composed by the system states and outputs is *uniformly and globally exponentially stable* (i.e., norm of the hybrid system states be bounded by a $\mathcal{K}\mathcal{L}\mathcal{L}$ function).

The authors in [28-30] analyze stability conditions for the *networked distributed systems* under DoS attacks. Networked systems are defined in the literature as interconnected subsystems where information are transmitted among the subsystems, and where the states of the subsystems are affected by each other. Networked systems are broadly classified under *centralized* and *decentralized* (or distributed), where researchers believe that the major difference between the two classes is that “in a centralized system all the states are assumed to be collected and transmitted in one attempt”, whereas in a decentralized fashion “the interconnected subsystems share one communication channel and transmission attempts of the subsystems take place asynchronously” [28]. An important

subject encompassing interconnected network controlled systems is the stabilization of such networks against DoS attacks. The authors in [28, 54] have formulated important constraints on the frequency of DoS attacks, and also the maximum duration in which transmission is allowed to be unavailable, in order that stability can be achievable. This subject will be elaborated more in the successive sections.

The problem of CPS security against DoS attacks has so far been reviewed in this thesis with respect to a system analysis approach. In particular, the literature generally assumes that a dynamic state equation of a CPS system is available, and then DoS attacks are augmented to the models by assuming that the state information can be accessible to remote controllers (and/or neighbour agents) at a later instant in time. The problem would then be formulated by examining conditions for the stability of the network in terms of communication restrictions. We will explain the modelling and the analysis later in this thesis. However, a different approach to studying CPS security has also received enormous attention, and especially in the analysis of DoS attacks in a multi-channel network where information can be distributed within the network by choosing one communication channel at a time (i.e., redundant information channels are not permitted). Assuming that the malicious attacker has a restricted budget for noise energy to jam a communication channel, and assuming that the attacker and the system defender both take rational and deliberate decisions over the channels they choose to inject attack, and transmit data, respectively, the problem would be finding the most advantageous strategies for both the players in order to disrupt and/or successfully transmit data packets to the receivers [55–57].

In the following subsections we will provide examples of Industrial CPS and examine certain security problems associated with these examples.

1.2.1 The Load Frequency Control (LFC) Problem

The electrical grid is one of the most fundamental inventions of the mankind directly affecting billions of people around the globe. The stability and uninterrupted continuity of power systems are therefore vital, and certain strategies must be incorporated to safeguard the electric grids against malicious adversaries and cyber attacks, especially with the advent of cyber space and smart grids [58, 59]. Specifically, frequency stability has been the major cause of numerous power system blackouts in the past [60] and requires particular attention. Operation of the frequency control in power systems is accomplished under three main levels [61]. The primary frequency control loop is commonly referred

to as the *Droop* control which is a simple proportional gain (D_i as shown in Figure 2.9). As evident from this figure, the droop control mechanism is part of the generating unit's controller that determines the percentage contribution of the respective unit in response to a power demand (through a gain $D_i = 1/R_i$ as defined precisely subsequently) by the network. The secondary frequency control is an integral controller that is responsible for the steady state error of the area frequency, and the power flowing through the tie-lines interconnecting the areas. Therefore, if frequency deviations of the area is denoted by Δf_i and the power flowing between area i to j is denoted by P_{ij} , the purpose of the secondary frequency control is to guarantee that $\Delta f_i = 0$ and $\Delta P_{ij} = 0$ for all variations in the load demand of the area as denoted by ΔP_{d_i} and as depicted in Figure 2.9. Consequently, the objective of the primary and secondary control mechanisms are to regulate the load and frequency, hence *Load Frequency Control (LFC)*.

The secondary frequency control command (occasionally referred to as the *Isochronous* control mode) is traditionally a telemetered signal computed and transmitted by the *centralized* controller. Automatic Generation Control (AGC) is an LFC control with the additional objective of economic dispatch (distributing the required change in generation among units to minimize costs). The basic design of the AGC is an established precedent of the 1950s [61–63].

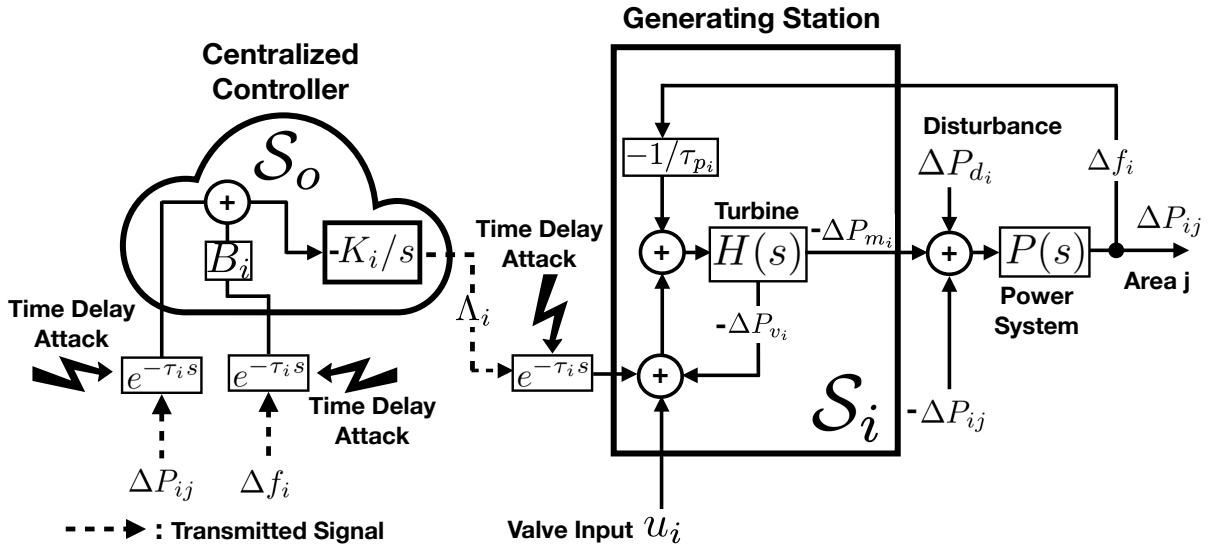


Figure 1.3: Block diagram of a frequency control mechanism for a generating station contributing the LFC in a multi-area power system. The solid lines are hard-wired measurements/commands that are presumably immune from cyber attacks (as they are confined within protected premises), whereas dashed lines represent telemetered data that are subject to TDS/DoS cyber attacks.

The third frequency control level is often managed by network operators to secure sufficient spin reserved generating units in order to cope with instantaneous demand and/or optimizing economical power dispatch. It constitutes the slowest acting control mechanism that may take up to several minutes to settle (in contrast with the primary and secondary control loops that usually settle within a fraction of a second up to a few seconds).

Wide-area measurement systems (WAMS) provide (almost) real-time feedback from network sensing devices in Phase Measurement Units (PMUs) [66]. Specifically, in a multi-area interconnected power system the power flow in the interconnecting tie-line between the area i and the adjacent area j (denoted by $\Delta P_{ij}(t)$) is a quantity that is available in the WAMS in real-time, and shall be maintained to a preset scheduled value regardless of instantaneous load fluctuations in the areas, i.e., $\int_{\tau=0}^{\infty} \Delta P_{ij}(\tau)^2 d\tau$ is to be minimized.

Additionally, frequency variations of areas should also be kept as small as possible at all times. In other words, $\int_{\tau=0}^t (\Delta f_i(\tau)^2 + \Delta f_j(\tau)^2) d\tau$ is simultaneously minimized with the tie-line power variations. Figure 2.9 illustrates the LFC control mechanism for the i^{th} generating station. It is evident from this figure that an adversary may intervene the PMUs data transmission (i.e., ΔP_{ij} and Δf_i) to the centralized controller in order to disrupt the control law [67, 68]. Cyber attacks may impede real-time transmission of the telemetered data (i.e., *Time Delay Switch (TDS)* cyber attacks) [69, 70], or jam the communication channels preventing access of the centralized controller to the telemetered measurements (i.e., *Denial of Service (DoS)* cyber attacks) [71]. A schematic diagram of a simplified two-area power system is depicted in Figure 1.4.

In Figure 1.4, G_i and G_j represent the equivalent generating stations of the areas i and j , respectively, that take part in the LFC. ΔP_{d_i} and ΔP_{d_j} denote cumulative power fluctuations in the areas representing all unknown loads and generating units, hence unmeasurable. It is assumed that the generator states including the area frequency deviations (Δf_i and Δf_j) are locally accessible to the respective generating units (hence, immune from cyber attacks), however, telemetered to the centralized controller for access by the adjacent areas. The area interconnecting tie-line power ΔP_{ij} is accessible only through telemetered packets to the areas, and subject to TDS and/or DoS cyber attacks (as shown in Figure 1.4).

After deregulation of the power industry, increasing variety of remote ancillary

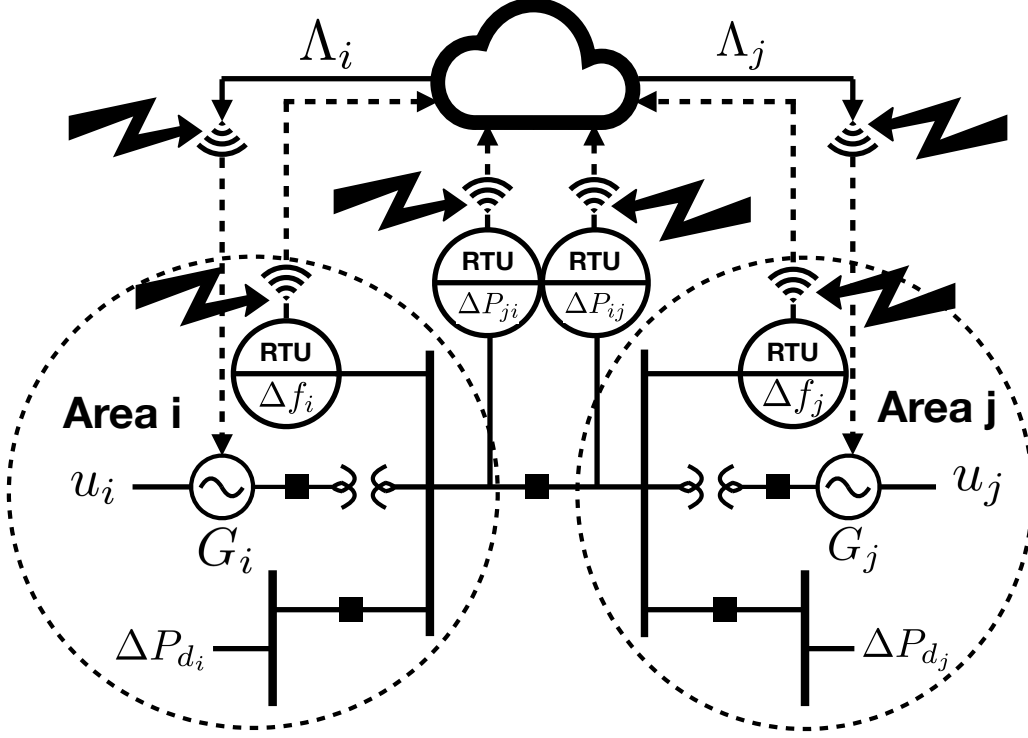


Figure 1.4: Two-Area power system schematic. Solid lines represent *hard-wired* connections and dashed lines represent communication channels. Locally measured quantities are transmitted to the central control center (represented by the cloud) through *Remote Terminal Units* (RTUs). It is assumed that communication channels would be subject to TDS or DoS cyber attacks only.

services for effective AGC gave rise to an open communication network accessible to the power generation (GENCOs) and transmission companies (TRANSCOs) [65], with the aftermath of possible significant delays on communication channels. Since then the subject of LFC with time delays has brought increasing interest and attention in the literature. The authors in [73] were among the first to address this problem in depth. The stability criterion for delayed LFC control has been broadly categorized as *delay-independent* (where asymptotic stability holds for all positive values of the delay) and *delay-dependent* (where asymptotic stability holds for some values of the delay, and system is unstable for other values) control classes [74].

In [65] the authors suggested a delay-dependent H_∞ two-term controller using linear matrix inequalities (LMIs) that could achieve stability with tolerable transients to load fluctuations. The problem associated with the proposed solution is that the state feedback controller is a function of system states of other generating stations. This makes the controller infeasible in practice since for a power system with several generating stations

system states of all contributing generators would be required, which is generic to a centralized controller design strategy. A more feasible *decentralized* sliding mode LFC was proposed in [75] that rectified the above problem although the time delay phenomenon was not addressed in the paper and system disturbances were assumed to be measurable. The authors in [72] considered time delays and reformulated the sliding mode approach to propose a robust H_∞ LFC however unfortunately, the problem was again addressed in a centralized fashion. In the sliding mode control, the system trajectories are determined through a sub-manifold in the state space named as the sliding surface, and the objective is to guide the trajectory to reach the sliding surface and stay on it.

In addition to the ongoing research concerning power system stability of delayed networks, the authors in [66] have recently addressed LFC stability under TDS cyber attacks. They introduced a time delay estimation method based on which the non-delayed system states are estimated. The condition $\tau < \tau_{max}$ has been considered to guarantee stability of estimations for some presumed τ_{max} , and that τ is a constant value. Very recently [76] discussed DoS cyber attacks on LFC and defence methods where Deep Auto-encoder Extreme Learning Machine (DAELM) methods were used to predict the missing data packets (once discovered that a data packet has been dropped due to the DoS cyber attack) in a short period of time and compute the real-time control signal according to predicted measurements based on historical database and a fast data prediction algorithm.

Despite extensive improvements in TDS and DoS resilient LFC methods available in the literature, there are several remaining concerns that are crucial to be addressed. These include a concrete, variable-delay-independent, decentralized, and integrated plan for safeguarding LFC against TDS and DoS cyber attacks on telemetered system measurements as well as transmitted control commands.

1.2.2 The Internet of Drones (IoD)

The emerging technology of Internet of Drones (IoD) is an example of a CPS, where a number of unmanned aero vehicles (UAVs) attempt to share an air-space to commute to their designated destinations, and where the overall objective is to minimize the cumulative air distance travelled by the UAVs in a given period of time. In this problem the UAVs are standalone physical systems equipped with a navigational means such as a GPS receiver. Hence, each UAV receives a set of way-points from a central control station (CCS) towards its destination through wireless communication. The CCS is responsible to optimize the route for each and every UAV through computational process, and the UAVs have onboard sensors to avoid collision and administer a smooth flight through

the designated way-points, and at each time-step the UAVs tend to share their present location to the CCS, hence a feedback control loop.

Figure 1.5 is a schematic block diagram on the IoD (borrowed from [77]) where a number of UAVs share the airspace to complete a certain mission through a cooperative control scheme. The airspace is an open space with certain obstacles (to be autonomously identified and avoided by the UAVs), divided into air-zones where each air-zone is subdivided into airways, intersections, and nodes, all controlled by a computing Zone Service Provider (ZSP), where ZSPs are further assumed to be intercommunicating through cloud and to the UAVs traversing through their respective territories (refer to [77] for further details).

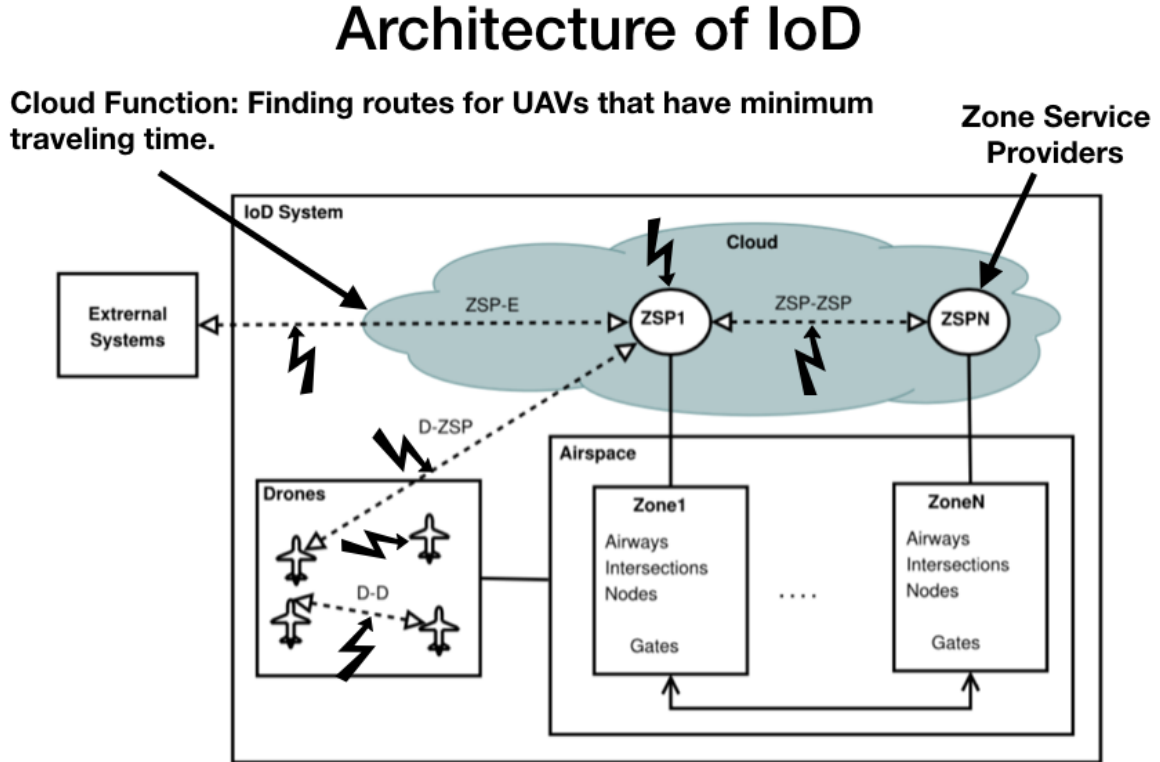


Figure 1.5: Block diagram of Internet of Drones (IoD) as an example of a CPS, borrowed from [77]

The UAVs are presumably responsible to control their own trajectory in a fully autonomous fashion, in collaboration with a set of neighbour UAVs, where respective ZSPs provide online computational service to the UAVs with regard to an optimized way-point plan to each UAV through the CCS, while secure distances among the UAVs are maintained at all times. However, detailed house-keeping operations including obstacle sensing and avoidance, path planning between way-points, task assignment (if any), navigation,

flight control, etc. are supposedly administered by the UAVs in an autonomous fashion. Responsibility of the ZSPs are mainly the airspace traffic control which is carried out by exchanging waypoints between UAVs and ZSPs through the CCS. The ZSPs and the computation center in charge of optimization of the waypoints are collectively referred to as “Cloud Service” in Figure 1.5.

This thesis suggests the control configuration for the IoD to be divided into two main layers as in Figure 1.6, where the high level control concerns the computation algorithms, in collaboration with the autonomous safety control algorithms onboard the UAV, and the low-level control that encompasses the autopilot and flight surface control that is presumably built-in the aerial vehicle by the manufacturer. The suggested scope of control responsibilities is an active topic in the literature and has not been finalized yet.

The interface between UAVs to cloud is shown in Figure 1.6. The UAVs periodically

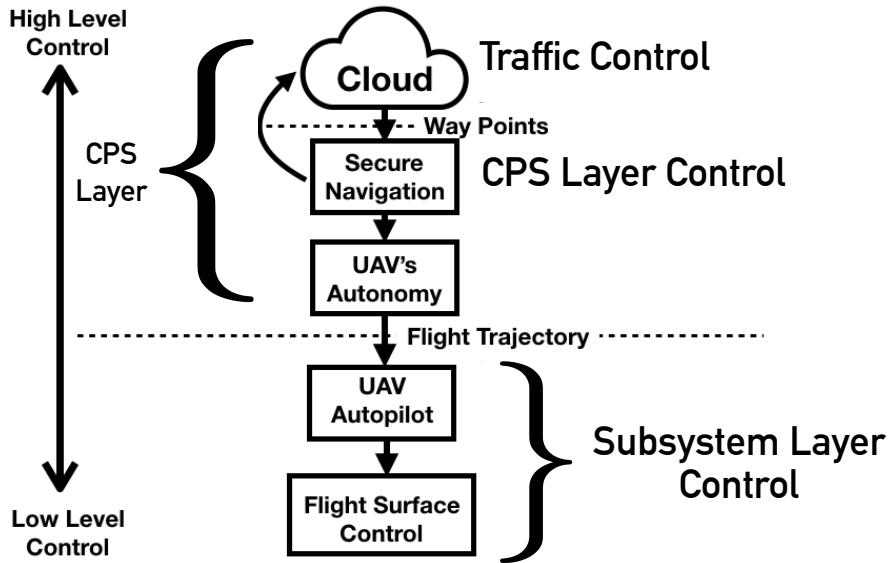


Figure 1.6: Proposed scope of CPS control for IoD

exchange their current position with the cloud service through the CCS, and the cloud computes and reverts optimal waypoints for all the UAVs in the system. Furthermore, the position of each UAV that is transmitted through radio signals can be simultaneously read and processed by neighbouring UAVs, and this provides means for the UAVs to accomplish “cooperative navigation” in a Multi-Agent System (MAS) framework as later discussed in Chapter-3. The authors in [78] have provided a detailed survey with regard to routing protocols for IoD. The authors in the literature agree that a trajectory finding

protocol is necessary for the UAVs, however, there are several challenges associated with developing the protocol. One of these challenges concerns the highly dynamic nature of UAV networks, which means that UAVs may anonymously connect and disconnect from the network. Another challenge is the range restriction between the UAVs and the base station. Therefore, “high mobility, dynamic topology, and uneven UAV distributions make the development of a routing protocol ensuring reliable communication difficult in UAV networks” [79,80]. The authors further argue that “different mobility in a multi-UAV environment requires highly accurate localization with short update intervals. GPS provides node position information at one-second intervals, which may not be satisfactory for UAV routing protocols”. In such case, an inertial measurement unit was considered, which could be calibrated by the GPS signals to provide the position of the UAV at a higher rate [81,82]. Some researchers proposed differential GPS (DGPS), or assisted GPS by using ground-based reference methods for range corrections with the accuracy of about 10m [83,84]. The limitations in UAV localization has motivated this author to propose a novel localization technique in Chapter-3 of the thesis.

However, the authors in [77] have categorized IoD cyber threats into four major categories as explained below:

- Communication Threats
 - DOS Attacks (flooding network), Jamming Attacks
 - Authentication, False Data Injection Attacks (tampering)
 - Eavesdropping, Privacy
- Mobility Threats
 - Blocking Airway/Gateway, Slow Movement
 - GPS Spoofing, False Topology
 - Traffic Analysis
- Non-Mobility Threat
 - Flooding ZSP, Deleting Metadata
 - Compromise ZSP, Modify Metadata
 - Access Confidential Metadata in ZSP
- Drones Threats
 - Physical Destruction, Depleting Resources (Power Draining)

- Malicious Drones, Compromising Drones
- Access Route Data, Access Payload Data

According to what has been discussed previously, geo-localization of UAVs (i.e., accurate estimation of vehicle’s attitude and position with respect to earth) in IoD framework seems to be a fundamental issue that has not been appropriately addressed (according to what will follow), given the fact that GPS-based navigation cannot be a promising solution due to adversarial spoofing (mobility threats listed above) as well as discussions in [78] (explained earlier).

The authors in [85] have quoted that “In GPS jamming and Spoofing, UAVs can be implicitly exploited while UAV cannot obtain legitimate GPS signals. The attacker produces a GPS jamming signal that interferes with GPS signals, causing a malfunction in the UAV of the GPS receiver. GPS spoofing is a similar attack, which is more sophisticated since the attacker sends a false message that may modify the UAV direction rather than produce distractive signals”. The authors in [86] also noted that the engineering of GNSS (Global Navigation Satellite System) signals can be in three essential forms, namely, jamming, spoofing, and meaconing. In the case of jamming, the manipulation of the GNSS signal is accomplished by overpowering the original GNSS signals by a malicious signal and in the same frequency spectrum, thus causing the geographically constrained outage of the GNSS PNT (Positioning, Navigation, Timing) service. Spoofing is a deliberate transmission of engineered (non-original) GNSS signal with the intent to cause false position estimation. “Meaconing is achieved by interception and re-broadcast of the engineered GNSS signals on the same frequency and with slightly higher power than the GNSS satellite in the malicious intent to influence position estimation process resulting in obtaining inaccurate (false) position estimate”.

Due to the threats explained above the importance of finding alternative means for navigation in GPS denied environments had been repeatedly highlighted by the industry, as well as the scientific society. For instance, the authors in [99] have recently stressed (in 2020) that “National defence forces are already in the hunt for alternate position, navigating, and timing (PNT) systems (to GPS)”. Even though military commanders prefer equipment that do not rely on GPS (due to the fact that their current systems are increasingly being jammed or spoofed), the costly GPS III program is going to be developed in the US that still relies on space signals for navigation. However, the aim is to design improved anti-jam features, including the higher-fidelity M-Code signal, exclusively for military use [87]. In the meantime, the US Air Force is looking for solutions

that could provide alternative signal sources that might even be from a non US GNSS system. Additionally, the US Department of Defence (DoD) has published an unclassified report in year 2019 [88], emphasizing that the challenge of remaining resilient in a dynamic threat environment relies on implementing new PNT capabilities rapidly and affordably in different DoD weaponry systems, and in particular providing a modernized GPS with diverse additional sources of PNT information in a modular and open system integration approach to deliver resilient PNT effects for the joint force.

Despite of significant efforts made in finding alternative means for navigation, there is no definite solution to the problem as of today. The War Zone magazine in June 2021 [89] cited latest U.S. Air Force technology for navigation in GPS denied combat environments being:

- The “VisNav” technology that involves building a database of terrain features and landmarks to be tracked by onboard sensors.
- Signals of Opportunity “SoOP”, on the other hand, leverages radio frequency (RF) emissions such as WiFi, TV signals, cellular networks, etc. and calculate the relative distance between an aircraft and those signals.
- The “MAGNAV” technology that measures variations in the Earth’s magnetic field as an aircraft travels over the surface of the planet.

1.2.3 Navigation of Autonomous Vehicles in Global Navigation Satellite Systems (GNSS) Denied Environments

In the previous subsection we reviewed the literature pertaining to structured UAV applications such as in Urban Air Mobility or the IoD. Apart from that, Unmanned Aero Vehicles (UAVs) are also increasingly used in a wide range of unstructured applications such as defence and reconnaissance, civil infrastructure inspection, agriculture, ecology, remote sensing, etc. [97,98]. The authors in [92] have explained that

in these types of applications, UAVs have to be equipped to autonomously fly a predefined path composed by a series of transmitted GPS way-points from a ground control, that are often composed of discrete commands that provide the air-speed and the time at which a particular UAV has to follow to arrive at particular point in space, given that the UAV has a clear view of the sky in order to obtain a reliable GPS positioning. In the meantime, there are challenging scenarios in which the UAV is required to fly under structures, such as bridges, within mines and buildings or below dense canopy, or in natural or urban canyons in which the GPS signal is partially or completely obstructed.

Furthermore, the relative ease by which GPS-based navigation systems can be jammed (through denial of reception by a competing signal), or spoofed (through deliberate introduction of a false signal) makes them vulnerable to cyberattacks [16, 99, 100]. The authors in [102] have concluded that the vastly growing, and nowadays complex applications of UAVs are pushing control requirements beyond human-in-the-loop capabilities and motivates research areas into UAV autonomous navigation systems. The authors further define navigation to be a “meta-capability, which includes perception, localization, motion planning and motion control methods, which include inertial, vision, radio, acoustic and radar”.

The authors in [102] further argue that localization techniques in autonomous navigation systems pose eluding estimation over long periods of time. The most common pose estimation practice is dead reckoning, where drifts over time are adjusted through other methods, of which GNSS is a common choice, but is vulnerable to spoofing, jamming, and environmental effects [103], as well as signal obscurity in urban canyons, natural canyons and forest under-stories [92, 104]. The conclusion is that such vulnerabilities call a quest for GNSS-independent navigation solutions.

The authors in [90] have introduced a MAS-UAV target finding problem in the presence of unknown obstacles and obstructions in in GPS-denied and partially observable environments, assuming that a map is initially given. In this article the location of UAV agents are assumed to be known. The author in [91] has suggested a pseudo GPS positioning system during GPS outages. According to the author the methodology consists of two parts, empirical mode decomposition threshold filtering (EMDTF) and a long short-term memory (LSTM) neural network. The EMDTF eliminates the noise in inertial sensors and provides more accurate data for subsequent calculations. The LSTM uses the current specific forces and angular rates to predict the pseudo GPS position during GPS outages. The paper suggests a Kalman filter for correction of the IMU sensors, and during a GPS outage the system predicts the motion of the vehicle by mere reliance on the IMU. A problem associated with this approach is when GPS spoofing or meaconing takes place. Additionally, when GPS signal is unavailable for prolonged durations the validity of such estimations could be highly questioned.

The authors in [92] have developed a framework that enables a drone to navigate in an unknown, unstructured and GPS-denied environment by combining the use of localization algorithms such as Simultaneous Localization and Mapping (SLAM) with Partially Observable Markov Decision Processes (POMDP) algorithms into a framework in which

the navigation and exploration tasks are modelled as sequential decision problems under uncertainty. However, SLAM methods are extremely intensive and cannot serve as a practical solution for the IoD, given the highly dynamic and extensive environment in which the system is operating. Nevertheless, it might be considerable to deploy integrated computational power of all UAVs in IoD and in a MAS framework to implement SLAM which is not the approach used in this thesis. The authors in [93] have also developed a six-dimensional localization approach based on visual odometry and Monte Carlo localization. The same approach is used in this report and is merely centred on the use of sensor data. The authors in [94] have also suggested SLAM methodologies to navigate and explore GPS denied environments by decomposing the perception task into a coarse perception layer and a fine layer, where the coarse layer would then serve navigation purposes. The author in [95] has combined IMU and landmark measurements to estimate attitude, position and linear velocity for navigation in GPS denied environments.

Finally, the authors in [96] have proposed a novel complete navigation system for autonomous flight of small unmanned aerial vehicles (UAVs) in GPS-denied environments. The hardware platform used to test the proposed algorithm is a small, custom-built UAV platform equipped with an onboard computer, RGB-D camera, 2D light detection and ranging (LiDAR), and altimeter. The error-state Kalman filter (ESKF) based on the dynamic model for low-cost IMU-driven systems is proposed, and visual odometry from the RGB-D camera and height measurement from the altimeter are fed into the measurement update process of the ESKF. The pose output of the ESKF is then integrated into the open-source simultaneous location and mapping (SLAM) algorithm for pose-graph optimization and loop closing.

Autonomous navigation has been a complex area of research due to the various involving aspects of the problem, including localization, translational velocity estimation, approach and landing, motion planning, obstacle avoidance, attitude estimation, and mapping, out of which 62% of the research work in this area has been expended on autonomous localization and positioning showing the need for a full GNSS-independent navigation solution as a primary quest [102]. The authors in [93] focus on ground-based robot localization in GPS-denied areas, relying only on information gathered by on-board sensors. They have argued that reliable long-term localization is a challenging problem that cannot be robustly solved using pure visual odometry approaches. They have therefore suggested an architecture that is mainly focused on the combination of visual odometry with additional sources of information in order to keep the localization errors bounded. [105]- [107] have also shown similar efforts in visual-inertial and visual-LiDAR

sensor fusion to conserve estimation errors, respectively. The authors in [108] have developed and integrated capabilities such as dynamic mission planning and re-planning in real-time, reactive collision avoidance navigation based on laser information, multi-sensor fusion for accurate pose estimation and altitude filtering, object recognizer component based on a Convolutional Neural Network (CNN) model, and Image-Based Visual Surveying (IBVS) algorithm using deep Reinforcement Learning (RL) for object interaction and following, in a non-supervised machine learning framework. The authors in [109] have used laser rangefinder, IMU and vision, to control drift errors. They have presented a synthesis of techniques enabling vision-based autonomous UAV systems, and computer vision processing modules to exploit visual information and simultaneously perceive obstacles in a GPS-denied environment.

Visual data is also used to extract information regarding the drone attitude and position while exploring the environment in a Simultaneous Localization and Mapping (SLAM) fashion. The authors in [110] have identified that mapping in dynamic environments can lead to serious errors in the resulting maps such as spurious objects or misalignments due to localization errors. Nevertheless, there are several publications available in the literature where the authors have tested a prototype SLAM product in a relevant environments. For instance, the authors in [111] have introduced a vision-IMU perception algorithm where a visual-aided (Inertial Navigation System) INS is tested in a simulated known environment (software in the loop). Reference [112] deploys laser rangefinders, IMU and vision-based sensing for full GNSS-denied navigation, that is verified on a prototype in an unknown cluttered relevant environment. The authors in [113] have utilized vision, IMU, and sonar sensing for full GNSS-denied navigation and tested the prototype in a relevant environment. In addition to the above, several other research works are available in the literature that have addressed sensor-fusion UAV navigation in GNSS-denied environments [114]- [121].

The conclusion derived from the above literature review is that localization solutions combining multiple sensing and perception yield better performance than relying on IMU sensors alone. Visual Inertial Odometry (VIO), Visual Odometry and Optical Flow, LiDAR, Ultra-Wideband (UWB), and Phase Array Radio Systems (PARS) localization methods are among complementary localization techniques that are deployed in GNSS-Independent navigation. The authors in [102] have foreseen future trends in the field of UAV GNSS-independent navigation and have suggested that with the prevalence of off-the-shelf autopilots, it is safe to say that UAV flight controller and their associated structural designs have reached full technology maturity. Therefore, the focus is now

concentrated on perception, localization, motion planning, and communication.

Towards perception, future research is expected to employ more advanced sensors like “signal-of-opportunity sensors”, event cameras and miniaturized radar. With advanced sensors also comes the need for advanced algorithms. Machine learning, active vision and other adaptive AI techniques are expected to become popular solutions for addressing sensor error modelling and semantic scene understanding. Last but not least, 5G communication technology is expected to become a key enabler for on-board data-driven navigation systems with its high volume real-time data streaming capability.

The problem of multi-agent remote sensing in GPS-denied and partially observable environments has been a recent topic investigated intensively in the literature. The authors in [92] have stated that coordinating multiple UAV agents over complex environments in the presence of partially observable obstacles remains an outstanding challenge, where the paper is focused on the problem of target-finding using multiple UAV agents, in a decentralized multi-agent system framework. The authors in [91] have used empirical mode decomposition threshold filtering (EMDTF), and a long short-term memory (LSTM) neural network to provide pseudo GPS position information during GPS outages. The authors in [92] combine the use of localization algorithms such as Simultaneous Localization and Mapping (SLAM) with Partially Observable Markov Decision Processes (POMDP) algorithms into a framework in which the navigation and exploration tasks are modelled as sequential decision problems under uncertainty. In their work, the observations of the environment perceived by the UAV are represented by its onboard estimated pose measured in the local frame, internal sensors such as IMU, GPS, compass, barometric pressure, optical flow and point LiDAR are used in this estimation. In environments where no GPS is present, the estimation of the local pose can benefit from depth sensors and cameras and a SLAM algorithm that uses landmarks or texture-rich features in the scene.

So far, in spite of the major advances made in the area of GNSS-independent autonomy, the literature seems to be deficient in providing a definite solution to the localization problem in case of GNSS-denied dynamic environments, where real-time SLAM techniques seem ineffective. These scenarios include navigation of autonomous mobile robots in open spaces where local features, certain obstacles and landmarks, etc. are sensed once and never exposed again, or under complex situations where mapping is simply beyond computational power and storage of a single robot, such as navigation in a city from one geographic point to another. In these circumstances the methodologies provided so far

would fail to render any solution, if GNSS service is denied for a considerable duration in time. Deficiency of the literature under these circumstances have motivated the authors of the present research work to address this problem and suggest alternative solutions.

Therefore, this author suggests a novel approach to address localization and position finding of a group of autonomous vehicles in a MAS framework (UAVs and/or UGVs) in GPS-denied environments, and where GPS is subject to cyber-attacks. It will be assumed that at least one agent knows its position reliably, and the problem would be to suggest an optimal algorithm to estimate the position of the remaining agents through cooperation, given the erroneous nature of the ranging sensors (such as LiDARs) mounted onboard the vessels. Hence, the agents in the MAS would have to use their onboard ranging devices, such that the overall error in the estimated position of the agents in the MAS is minimized. The assumption that at least an agent has accurate access of its position can hold true in many UAV/UGV applications such as the IoD discussed earlier, since it can always be assumed that there are vehicles at known positions (such as at take-off, and landings) and vehicles adjacent to landmarks, etc. Specifically, electronic buoys may be employed to aid navigation of certain agents within the reach of transmitted radio-waves, that in-turn aid further away agents to estimate their positions accordingly. In these circumstances, cascading error of the sensing devices would results in significant error in the network, if not planned carefully. Additionally, the graph formation of the MAS would also have direct impact on the overall error due to additive effect of sensor errors. Hence, it seems to be very useful to investigate and find an optimal methodology to reduce positioning error in a MAS network given the constraints explained above. Therefore, we suggest this to stand as one problem to be discussed in the thesis.

1.2.4 Navigation of Autonomous Vehicles Subject to Actuator Attacks

In spite of the explanations provided in Subsection 1.2.3, Figure 1.6 requires secure navigation under circumstances where the Ground Control Station (GCS) commands are intruded by adversaries (as depicted in Figure 1.2) compromising the transmitted desired waypoint signals. The authors in [123] have provided a literature review with respect to the research progress addressing GCS cyberattacks. They have quoted that among the detection algorithms, excitation signals and unknown input observer (UIO) are used to detect GCS attacks [124]. Kalman filter and neural networks are combined to detect the false data injection attacks in [125]. A detection mechanism is proposed in [125] where authentication signals and the average power of the received signals are fused. In [126], a

hierarchical detection scheme which combines rules-based and anomaly detection is proposed to identify malicious anomalies. A detection countermeasure from the perspective of state estimation is proposed to recognize the dynamic injection attack [127]. In order to detect the malicious data injected in the power system state vectors, wavelet transform and deep neural network techniques are used to analyze the deviation of spatial and temporal data correlations [128]. Observer-based detection algorithms are developed in [129]- [131], where attack detection can be achieved by means of properly setting residual signals. The aforementioned studies concentrate the detection of sensor attacks, actuator attacks, and cyber attacks. However, both disturbance and attack can cause the deterioration of trajectory tracking performance. Unfortunately, despite the advances made in the literature the AFDI problem still remains an outstanding challenge as of today.

1.3 Literature’s Modelling and Control of Cyber Physical Systems (CPS) Subject to Some Cyberattacks

In the previous section we have presented two broad categories of cyber-attacks, namely the Time Delay cyberattacks under which communication and subcategories such as DoS attacks can be classified, and the man in the middle attacks (or data integrity attacks, also referred to as deception or false data injection (FDI) attacks). Traditionally, cyberattacks in the literature are also classified more or less into the same categories of DoS and FDI with some exceptions that consider replay attacks as a new category [134],[135].

The authors in [1] provide a general understanding with respect to some basic modelling techniques for representation of CPS cyberattacks, and basic control methods to circumvent cyber threats. The methodologies discussed in this article generally explains the backbone of many succeeding research work encompassing defence mechanism in CPS against cyberattacks. The notions explained in [1] are very fundamental frameworks with respect to the subject, and do not cover state of art material. More advanced topics will be discussed in subsequent sections, and will main discuss DoS attacks in CPS.

1.3.1 Denial of Service (DoS) cyberattacks

It is often beneficial to consider data transmission in the CPS (including distributed network controlled systems) under the framework of event triggered systems in order to alleviate the communication burden and therefore enhance the efficiency of the system services. In this respect, it is usual to understand the underlying concepts of system stability under the assumption that control feedback packets are transmitted only when system stability is critically affected. This understanding would help system analysts to extend the notion of DoS as factors that impede timely sampling of the control and/or sensor outputs. The following is a summary extracted from [1], and [25]- [32].

The framework of interest is a remote plant-operator setup, where the controller is physically distant from the plant and a communication network connects the plant to the control unit. The system is defined as,

$$\dot{x}(t) = Ax(t) + Bu(t) \quad (1.1)$$

where $t \in \mathbb{R}_{\geq 0}$, and $x \in \mathbb{R}^{N_x}$, $u \in \mathbb{R}^{N_u}$ are the system states and control command, A and B are real matrices of appropriate size. It is further assumed that there exists a matrix K to stabilize the system in the sense of Lyapunov, i.e. such that all the eigenvalues of $\Phi = A + BK$ have negative real part. The control action is implemented via a sample-and-hold device. Let $\{t_k\}, k \in \mathbb{N}, t_0 := 0$ represent the sequence of time instants at which it is desired to update the control action. Then, the actual control input applied to the process is given by,

$$u(t) = Kx(t_k) \quad (1.2)$$

where $x(t_k) = x(t_{k-1})$ if there exists a DoS attack at time t_k . We further define $\{h_n\}, n \in \mathbb{N}$ as the sequence of DoS triggering times, where $H_n = [h_n, h_n + \tau_n[$, $\tau_n > 0$ is the time interval of the n^{th} DoS. The objective is to determine constraints on the control command sampling times as well as the maximum allowable number and duration of the DoS attacks such that the system will remain *globally exponentially stable (GES)* (according to Definition 1 provided below).

Definition 1. Consider the control system in (1.1) with the control input in (1.2). The system is said to be *globally exponentially stable (GES)* if there exist $\alpha, \beta \in \mathbb{R}_{>0}$ such that,

$$\|x(t)\| \leq \alpha e^{-\beta t} \|x(0)\|.$$

Therefore, we are motivated on the following restriction on the admissible DoS.

Given a sequence $\{h_n\}$, let

$$\Xi(t) = \left\{ \bigcup_{n=0}^{n-1} H_n \right\} \bigcup [h_n, \min\{t, h_n + \tau_n\}]$$

denote the sum of DoS intervals up to the current time, and $|\Xi(t)|$ denote such time interval.

Assumption 1. *The DoS sequence $\{h_n\}$ is such that there exist constants $\kappa \in \mathbb{R}_{\geq 0}, \tau \in \mathbb{R}_{>0}$, such that for all $t \in \mathbb{R}_{>0}$,*

$$|\Xi(t)| \leq \kappa + \frac{t}{\tau}.$$

This signifies that (if $\kappa = 0$) the average permissible time with respect to the DoS attack is at least τ . $\kappa > 0$ allows for consideration of DoS at the process start-up which is not the case in this report. Assumption 1 together with a control update rule such as

$$\|e(t)\| \leq \sigma \|x(t)\|, \quad \forall t \notin \Xi(t) \quad (1.3)$$

(for some design parameter $\sigma \in \mathbb{R}_{>0}$ to be determined), where,

$$e(t) := x(t_k) - x(t) \quad (1.4)$$

preserves GES for the system, for an appropriate choice of σ and a sufficiently large τ as,

$$\tau > \frac{\lambda + \rho}{\lambda - \sigma\mu\|BK\|}$$

where the constants ρ , λ , and μ are parameters defining the dynamics of the open and closed loop system (with $u(t) = Kx(t)$) such that $\|e^{(A+BK)t}\| \leq \mu e^{-\lambda t}$ and $\|e^{At}\| \leq \theta e^{\rho t}$ holds for all $t \geq 0$.

The condition provided for τ above requires continuous sampling during the DoS intervals in order to succeed an updated value at the controller immediately at time $t = h_n + \tau_n$ which requires an infinite sampling rate. A more practical approach is to consider finite sampling rates at $\{t_k\}$, denoted by

$$\Delta_k := t_{k+1} - t_k > 0, \quad k \in \mathbb{N}.$$

Additionally, the set of integers associated with an attempt to update the control action during H_n is denoted by

$$\mathbb{S}_n := \{k \in \mathbb{N} | t_k \in H_n\}$$

and by defining

$$\Delta_{\mathbb{S}_n} := \sup_{k \in \mathbb{S}_n} \Delta_k$$

we have the interval $\bar{H}_n = [h_n, h_n + \tau_n + \Delta_{S_n})$ which provides an upper bound on the n^{th} time interval over which the control action is not updated. Then, a new minimum bound for τ is derived as

$$\tau > \left(\frac{\lambda + \rho}{\lambda - \sigma\mu||BK||} \right) \left(1 + \frac{\Delta_*}{\tau_*} \right)$$

where

$$\Delta_* := \sup_{n \in \mathbb{N}} \Delta_{S_n}, \quad \tau_* := \inf_{n \in \mathbb{N}} \tau_n$$

The authors in [1], [28] have used a Lyapunov based approach to derive similar conditions for τ .

1.3.2 Deception (or False Data Injection) cyberattacks

Deception attacks or False Data Injection (FDI) attacks are defined by deliberate alteration of the sensor data packets or actuator commands or both, in an attempt to compromise the performance or take control of the system. In a CPS the sensor readings are often served to make remote estimations of the system states, over which certain control commands are derived and forwarded to the actuators in order to attain a desirable response from the overall system. Some of the publications in the literature further subcategorize deception attacks in random attacks where arbitrary measurements are modified, and targeted attacks where specific system states are targeted [33], [34]. More specifically, let us consider the following discrete time system,

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k \\ y_k &= Cx_k + v_k \\ \tilde{y}_k &= Cx_k + \alpha_k \xi_k \end{aligned} \tag{1.5}$$

where $x \in \mathbb{R}^{N_x}$, $u \in \mathbb{R}^{N_u}$, $y \in \mathbb{R}^{N_y}$ represent system states, control commands, and system output, respectively, and $\tilde{y} \in \mathbb{R}^{N_y}$ denote the set of system outputs as received by the remote estimator (or controller), and w_k and v_k are randomly distributed Gaussian disturbances with distributions P and R (respectively), and appropriate dimensions, and ξ represents the vector of FDI administered by the adversary, and α_k is a (scalar) Bernoulli distributed sequence denoting the possibility of the occurrence of the deception attacks by taking values on 1 and 0 such that,

$$P[\alpha_k = 1] = \bar{\alpha}$$

$$P[\alpha_k = 0] = 1 - \bar{\alpha}$$

and $\xi_k = \eta_k - Cx_k$ where η_k is a bounded false data that the adversary intends to impersonate as the system output, where $\sum_{k=0}^{\infty} \eta_k^T \eta_k \leq \bar{\eta}^2$. Therefore, at each time-step there

is a probability of $\bar{\alpha}$ that the remote estimator would use η_k instead of y_k to estimate the system states. Additionally, assuming $\eta_k = 0$ would result in modelling random packet drops as studied in [35, 36].

Additionally, false data injection attacks can be targeting system actuator through the control input channels. In this case the adversary intervenes the remote controller output and intrudes the transmission packets u_k into $\tilde{u}_k = -u_k + \theta_k$. Hence, system [1.5] is transformed into,

$$\begin{aligned} x_{k+1} &= Ax_k + B\theta_k + w_k \\ \tilde{y}_k &= \eta_k + v_k \end{aligned} \tag{1.6}$$

under sensor and actuator deception attacks, where η_k and θ_k are adversary controlled variables through which the adversary intends to compromise the system and in the meantime modify the outputs so that the attack cannot be detected. Figure [1.7] illustrates a general framework of deception cyberattacks on system actuators and sensors.

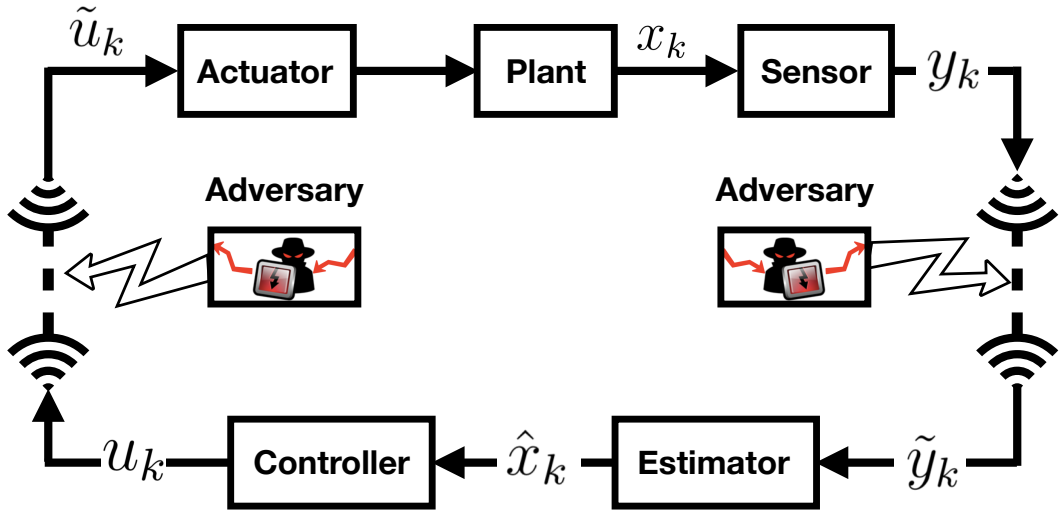


Figure 1.7: Block diagram of Deception cyberattacks on system actuators and sensors

Therefore, in the following subsections some of the elementary detection schemes will be introduced and the strength and weaknesses of the schemes will be briefly analyzed.

1.3.3 Static Deception Attack Detection Algorithm

The static deception attack detection algorithm (also referred to as the *weighted least square detector*) is the most popular method used for the detection of sensor deception attacks, especially in the power system domain [37]- [40]. The detector is simply an optimal estimator of the system states, (merely) based on the latest available sensor

measurements $\tilde{y}_k$. The system detector assumes that $\tilde{y}_k$ is a genuine (non attacked) version of the system states, i.e., $\tilde{y}_k \approx C\hat{x}_k$ and attempts to find an optimal vector $\hat{x}_k$ that best suits the actual states x_k in a least square error sense, i.e.,

$$\min_{\hat{x}_k} \mathbb{E}[(\tilde{y}_k - C\hat{x}_k)^T W (\tilde{y}_k - C\hat{x}_k)]$$

where W is a positive definite square matrix of appropriate dimension that weighs more on the most likely trusted sensors, and less on the sensors that seem to be more vulnerable. One can simply show that,

$$\hat{x}_k = (C^T W C)^{-1} C^T W \hat{y}_k \triangleq C^\dagger \hat{y}_k$$

where $C^\dagger := (C^T W C)^{-1} C^T W$ is by definition the *pseudo inverse* of C , where $C^\dagger C = I$. Thereafter, a residual indicator e_k is constructed upon each retrieval of the sensor measurements, as $e_k = \hat{y}_k - C\hat{x}_k$ that is compared to a former distribution of the random quantities $e_0, e_1, \dots, e_{k-1}$, and alarms for any unusual obtained residue.

Hence, the term *static detector* signifies the fact that the detection mechanism does not take into account the dynamic behaviour of the system states, and merely relies on the sensor readings. However, since the available set of information $\tilde{u}_0, \tilde{u}_1, \dots, \tilde{u}_{k-1}$ are not used for detecting deception cyberattacks a large fraction of intrusions (such as replay attacks) remain undetected. This is due to the fact that in a replay attack the adversary records a sequence of the system outputs in a particular time frame, such as $k \in \{k_1, k_2, \dots, k_T\}$ where $k_1 < k_T \leq k$ during which the system is at steady state (i.e., $x_{k_1} \approx x_{k_2} \approx \dots \approx x_{k_T} \approx x_k$). The adversary then replays the periodic sequence $\tilde{y}_k = y_{k_1}, \tilde{y}_{k+1} = y_{k_2}, \dots, \tilde{y}_{k+T-1} = y_{k_T}$, and again $\tilde{y}_{k+T} = y_{k_1}, \dots, \tilde{y}_{k+2T-1} = y_{k_T}$ repeatedly until a new control command is issued. As a result the residuals $e_k = e_{k_1}, e_{k+1} = e_{k_2}, \dots$ will all belong to a recognized distribution and the attack will pass the detector without triggering alarm.

In the next subsection a relatively more advanced detection mechanism will be examined that is capable of handling more complex forms of replay attacks.

1.3.4 Replay Attack Detection

The most frequently adopted mechanism provided in the literature for detection of FDI attacks is to use a χ^2 (chi-square) distribution function for the residual,

$$g_k := \sum_{i=k-\mathcal{T}+1}^k (\tilde{y}_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (\tilde{y}_i - C\hat{x}_{i|i-1})$$

where $\tilde{y}_i$ is the i^{th} sample of the output received by the remote estimator, and $\hat{x}_i$ is the system state estimated at the remote station through Kalman filtering, and $\mathcal{P}$ is the covariance matrix of the residue $\tilde{y}_i - C\hat{x}_{i|i-1}$, and $\mathcal{T}$ is an arbitrary integer denoting the window size over which χ^2 is formulated.

The authors in [41] have shown that Kalman filter residues $e_k := \tilde{y}_k - C\hat{x}_{k|i-1}$ for the above system with Kalman filter is a Gaussian independent and identically distributed (i.i.d.) variable with zero mean and covariance $\mathcal{P} = CPC^T + R$. Furthermore, g_k has a χ^2 distribution with $m\mathcal{T}$ degrees of freedom (i.e., $\mathbb{E}[g_k] = m\mathcal{T}$) during normal operation. However, g_k will be computed at each time-step at the remote estimator and checked against a given margin such as δ that can be chosen based on the samples taken in the absence of attack, and when exceeding the margin an alarm will be triggered that indicates cyber-attack.

The authors in [41] have shown that for a state feedback $u_k = L\hat{x}_k$ stabilizing $A + BL$ and a Kalman gain K , if the matrices L and K are selected such that $\mathbf{A} := (A + BL)(I - KC)$ is unstable then the replay attack can be detectable, in a sense that $g_k > \delta$ implying a non converging state estimation at the remote terminal. However, this condition requires the Kalman gain to be compromised with respect to its optimal value, and is undesirable from a practical point of view. Therefore, to rectify the problem stated above, the authors suggest a watermark Δu_k with zero mean and covariance $\mathbf{U}$, such that $u_k = L\hat{x}_k + \Delta u_k$. Then the authors in [41] show that in the absence of attack:

$$\mathbb{E}[(\tilde{y}_k - C\hat{x}_{k|k-1})^T \mathcal{P}^{-1}(\tilde{y}_k - C\hat{x}_{k|k-1})] = m$$

and under cyber-attack,

$$\mathbb{E}[(\tilde{y}_k - C\hat{x}_{k|k-1})^T \mathcal{P}^{-1}(\tilde{y}_k - C\hat{x}_{k|k-1})], k \rightarrow \infty = m + 2 \text{ Trace}(C^T \mathcal{P}^{-1} C \mathbf{U})$$

The authors in [42] have considered deception attacks in a multi-agent system event triggered framework and have designed an observer based distributed controller such that the closed loop multiagent system achieves a prescribed consensus in spite of the lossy sensors and cyberattacks.

1.3.5 Bayesian Attack Detection Methods

In the previous subsections we have seen that the cyber-attack detection methods (despite its serious shortcomings) utilized available knowledge on sensor information $\tilde{y}_k$, and

the command input vector u_k , to estimate the state states $\hat{x}_k$ at each time-step k in order to construct a residue with a predetermined probability distribution function to be able to build conjectures respecting the likelihood of a cyber-attack being present. The problem associated with these detection methods firstly lies in the estimation of the system states. The authors in [43] have shown Bias injection attacks targeting Kalman filter which implies that the estimation techniques featuring Kalman filters are not immune to cyberattacks. Secondly, the state estimation is built on the basis of u_k whereas the actual control command that is used to excite the plant can be a different vector $\tilde{u}_k \neq u_k$ as illustrated in Figure 1.7.

The Bayesian *Joint Input and State Estimation* (JISE) filter is an optimal (with respect to any criterion) remedy to the problems highlighted above [44, 45]. The objective is to determine the joint distribution function of x_k, u_k given an initial distribution $p(x_0, u_0)$, and all the past sensor information y_0 to y_k . If the joint distribution function $p(x_k, u_k | y_k)$ is available one can find the *maximum a-posteriori probability* of x_k, u_k that would be the best possible estimation of the joint system variables. Therefore, the JISE problem is to derive $p(x_k, u_k | y_k)$ based on $p(x_{k-1}, u_{k-1} | y_{k-1})$. Likewise, in the presence of cyberattacks the objective would be to address the problem of joint attack detection and state estimation, given the set of measurements up to the present time [46]. In particular, the authors in [46] introduce the following discrete-time CPS system models,

$$x_{k+1} = \begin{cases} f_k^0(x_k) + w_k, & \text{No Attack} \\ f_k^1(x_k, a_k) + w_k, & \text{Cyberattack} \end{cases}$$

where x denotes the system states as before, and $a_k \in \mathbb{R}^m$ represents an unknown attack vector affecting the system states transition, and $f_k^0(\cdot)$, $f_k^1(\cdot, \cdot)$ denoting transition functions for the system in normal operation, and under cyber-attack, respectively. The excitation vector u_k is not included in the model assuming that the system is operating under non-varying input commands. Likewise, the system measurements are modelled as,

$$y_k = \begin{cases} h_k^0(x_k) + v_k, & \text{No Attack} \\ h_k^1(x_k, a_k) + v_k, & \text{Cyberattack} \end{cases}$$

where $h_k^0(\cdot)$, $h_k^1(\cdot, \cdot)$ denote measurement functions for the system under normal operation, and cyber-attack, respectively. It is further assumed that the system measurements are actually delivered to the remote controller under a probability p_d (to account for the case where a DoS attack might be present), and also assume that the measurements y_k can be altered with a probability p_f resulting in a fake reading of the measurements $\tilde{y}_k$ at the remote terminal. Therefore, if $\mathcal{Z}_k$ denotes the set of measurements at the remote

terminal, we have,

$$\mathcal{Z}_k = \begin{cases} \emptyset, & \text{with probability } 1 - p_d \\ \{y_k\}, & \text{with probability } p_d (1 - p_f) \\ \{\tilde{y}_k\}, & \text{with probability } p_d \cdot p_f \end{cases}$$

The authors have further assumed $\mathcal{A}_k = \{a_k\}$ denoting the set of attack vectors. Additionally, a *Random Finite Set* (RFS) $\mathcal{X}$ over $\mathbb{X}$ is defined as a set of random variables taking values in a function of $\mathbb{X}$. Hence, a set density $f(\mathcal{X})$ is defined to be the density function of such random variables [52]. A Bernoulli RFS is one with can be either empty or a singleton $\{x\}$ (not to be confused with the system states, x in here denotes any arbitrary random variable) distributed over $\mathbb{X}$ according to a pdf $p(x)$ with some probability r . Hence,

$$f(\mathcal{X}) = \begin{cases} 1 - r, & \text{if } \mathcal{X} = \emptyset \\ r \cdot p(x), & \text{if } \mathcal{X} = \{x\} \end{cases}$$

A Bernoulli RFS as explained above is particularly useful in the context of cyber-attack detection in CPS since it is more important to conclude if a cyber-attack has taken place, or has not. In other words the system defender is interested to determine $p(\mathcal{A}_k, x_k | \mathcal{Z}_k)$, rather than $p(a_k, x_k | \mathcal{Z}_k)$.

Now, in case the distribution of the system states x under normal operation is represented by $p_k^0(x_k)$, and the joint distribution of the states and the attack vector by $p_k^1(a_k, x_k)$, one may observe that,

$$p(\mathcal{A}_k, x_k | \mathcal{Z}_k) = \begin{cases} (1 - r_{k|k}) p_{k|k}^0(x_k), & \text{No attack} \\ r_{k|k} \cdot p_{k|k}^1(a_k, x_k), & \text{Cyberattack} \end{cases}$$

Obviously, if $\mathcal{Z}_k = \emptyset$ (i.e., no measurement due to DoS, or else), then $r_{k|k} = r_{k|k-1}$, $p_{k|k}^0(x_k) = p_{k|k-1}^0(x_k)$, and $p_{k|k}^1(a_k, x_k) = p_{k|k-1}^1(a_k, x_k)$. However, in view of the measurement set $\mathcal{Z}_k$, the question would be to firstly update the triplets $r_{k|k}, p_{k|k}^0(x_k), p_{k|k}^1(a_k, x_k)$ based on $r_{k|k-1}, p_{k|k-1}^0(x_k), p_{k|k-1}^1(a_k, x_k)$, and secondly, to predict $p(\mathcal{A}_{k+1}, x_{k+1} | \mathcal{Z}_k)$ based on predicted triplets $r_{k+1|k}, p_{k+1|k}^0(x_{k+1}), p_{k+1|k}^1(a_{k+1}, x_{k+1})$, to be in turn estimated based on the updated triplets at time k . This work has been formulated in [46] which can assist to probabilistically detect a cyber-attack, while estimating the system states jointly. Detail derivations are not in the scope of this report.

1.4 Switching Topologies and Delays in Multi-Agent Systems (MAS)

Cooperative distributive control of multi-agent systems is a relatively new topic that has received particular attention in the literature due to its application in a variety of CPS domains. As an example, a flock of UAVs in a certain mission can be considered as a multi-agent system where the agents are aiming to estimate their geographical position in space relative to a ground based coordination system, through cooperation. The fact that each agent has its own independent positioning estimator, cooperative consensus could bring merit if the agents share information and achieve better positioning estimations through consensus. As another example, the power generation problem in an interconnected area network can be considered as a multi-agent consensus problem since each power generating unit is obliged to generate a certain amount of energy through a regulation scheme. In other words, agents have to achieve consensus over their generating capacity at each point in time in order to maintain stability of the entire power network. In this example, each area (agent) is modelled by a distinct set of dynamic equations that may be different in terms of number and nature of system states from others (in contrast with CPS systems where agents are governed by identical models, referred to as *homogenous* multi-agent system), hence, consensus of a *heterogenous multi-agent system* over certain variables of interest.

The authors in [50] and [135] have considered the *cooperative output regulation* problem for heterogeneous linear multi-agent systems in the presence of communication constraints. Cooperative output regulation is a generalization of the leader-following consensus problem of multi-agent systems. Load sharing in power systems as discussed later in Chapter 2 can also be controlled from a multi-agent systems (MAS) point of view, in which the area power systems are considered as agents, and limited information are exchanged among the agents to achieve a secondary coordinated control in a decentralized fashion. In [47] the authors have presented a distributed secondary control scheme for power allocation and voltage restoration in islanded DC micro-grids employing MAS consensus control techniques. The conditions for *consensusability* in linear homogenous MASs has been presented in [48, 49], where output feedback consensus protocols were given and the closed-loop MAS was shown to be achieving asymptotic consensus if the topology had a spanning tree. Output consensus for heterogeneous MAS with Markovian switching network topologies has been discussed in [136] and can be used as the basis for studying MAS under DoS cyberattacks assuming that DoS attacks can be represented as switching topologies. The paper however does not address cases where communication

restraints impede timely delivery of data packets. The subject of distributed consensus of heterogeneous MAS subject to switching topologies and communication time-delays has been published very recently in [137] with a focus on power systems, and is served as the core part of this section due to its relatively comprehensive approach. The paper provides a solution for stability and control of heterogeneous MAS systems considering a switching controller that alters the controller gain based on the knowledge that a time-delay attack has taken place. The condition for achieving consensus is non-infinite communication delays, which can be considered an admissible condition. However, the problem that has to be simultaneously considered is the determination of a methodology that automatically detects the onset of a time-delay attack.

The authors in [50] have investigated the *cooperative resilient output regulation* control problem with time-delay communication constraints for a specific class of heterogeneous MAS with uniform exogenous inputs (following a LTI dynamics with pure imaginary eigenvalues). Unfortunately, the work presented in [50] despite of solid theoretical results cannot be extended to general heterogeneous MAS systems. The authors in [135] have recently addressed the same subject for a class of CPS systems with non-uniform but bounded communication delays under denial-of-service (DoS) attacks, where a switching resilient control approach is proposed. However, the existence of a solution for all time-delays cannot be guaranteed, and additionally the controller is only functional for DoS attacks (where agents are assumed to understand "missing" information from neighbour agents) but not delay attacks.

Before we state the problem statement, let us introduce the basic notations and definitions of graph theory for convenience of discussion (reproduced from [136]). Let $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ be a directed graph with the vertex set $\mathcal{V} = \{1, 2, \dots, N\}$, the edge set $\mathcal{E} = \{(i, j) | i, j \in \mathcal{V}\}$ where i is the parent node and j is the child (i.e., information flow is from i to j), and the weighted adjacency matrix $\mathcal{A} = \{a_{ij}\} \in \mathbb{R}_+^{N \times N}$ if $(j, i) \in \mathcal{E}$, and $a_{ij} = 0$ otherwise. The Laplacian is denoted by $\mathcal{L}$. It is said that a directed graph has a directed spanning tree if there are directed paths from one node, called the root, to all other nodes in this graph. When the communication environment is uncertain, it is assumed that the communication topology is no longer intact and becomes a Markovian switching communication topology in $[t_k, \tilde{t}_k)$, during which an agent receives information with a time-delay. When the communication restores, the topology is switched back to its original state in $[\tilde{t}_{k+1}, t_{k+1})$.

Now, a multi-agent system is considered with agents $i \in \{1, 2, \dots, N\}$, and the

dynamics,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) \\ y_i(t) &= C_i x_i(t)\end{aligned}\tag{1.7}$$

where $x_i(t) \in \mathbb{R}^{N_{x_i}}$, $u_i(t) \in \mathbb{R}^{N_{u_i}}$, and $y_i(t) \in \mathbb{R}^{N_{y_i}}$ denote the states, the control inputs, and system outputs of the i^{th} agent, respectively, and A_i, B_i, C_i are constant matrices with appropriate dimensions. It is further assumed that for each agent i , the pair (A_i, B_i) is controllable, and the pair (A_i, C_i) is detectable. The objective is to design a distributed control law to achieve output consensus in a mean square sense, i.e.,

$$\lim_{t \rightarrow \infty} \mathbb{E} [\|y_i(t) - y_j(t)\|^2] = 0, \forall i, j \in \{1, 2, \dots, N\}.\tag{1.8}$$

The article shows that the controller,

$$\begin{aligned}u_i(t) &= K_{1_i} \hat{x}_i(t) + K_{2_i} \eta_i(t) \\ \dot{\eta}_i(t) &= S \eta_i(t) + \Delta \eta_i(t) \\ \dot{\hat{x}}_i(t) &= A_i \hat{x}_i(t) + B_i u_i(t) + H_i (C_i \hat{x}_i(t) - y_i(t)) \\ \Delta \eta_i(t) &= \begin{cases} F_1 \sum_{j=1}^N a_{ij} (\eta_j(t) - \eta_i(t)), & t \in [\tilde{t}_{k-1}, t_k) \\ F_2 \sum_{j=1}^N a_{ij} (\eta_j(t - \tau) - \eta_i(t - \tau)), & t \in [t_k, \tilde{t}_k) \end{cases}\end{aligned}\tag{1.9}$$

with appropriate selection of matrices $K_{1_i}, K_{2_i}, H_i, S, F_1 = \mu_1 I$, and $F_2 = \mu_2 I$, the output consensus goal is achieved under a switching communication channel with time-delays if the intact communication topology $\mathcal{G}$ (i.e., the topology under the normal environment), has a spanning tree, where $\eta_i(t) \in \mathbb{R}^{N_{\eta_i}}$ is the controller state vector, and $\hat{x}_i(t) \in \mathbb{R}^{N_{x_i}}$ is the observer state estimation (refer to Figure 1.7, where the sensor channel is under DoS and time-delay attack, and the input channel is assumed intact). The latest solution published in the literature for output consensus problem in system (1.7) without switching communication and time-delays provides that $F_1 = FR$. The solution has certain limits and shortcoming that will be addressed later in Subsection 1.4.1.

The purpose of the control law is to designate μ_1, μ_2 such that for positive scalars ϵ_1, ϵ_2 and a Lyapunov function $V(\xi(t))$,

$$\dot{V} \leq -\epsilon_1 V, \quad t \in \Theta(t), \quad (\text{i.e., no attack})$$

$$\dot{V} \leq \epsilon_2 V, \quad t \in \Xi(t), \quad (\text{i.e., DoS attack})$$

implying that,

$$V(t) \leq V(0) e^{-\epsilon_1 |\Theta(t)| + \epsilon_2 |\Xi(t)|}$$

or,

$$\eta_i - \eta_j \rightarrow 0, \forall i, j, \text{ if } \epsilon_1 |\Theta(t)| > \epsilon_2 |\Xi(t)|,$$

ensuring consensus over the controller states of the agents, and in the meantime K_1, K_2 are selected such that output consensus in a mean sense is achievable. This methodology is the backbone of a large population of the publications dealing with output consensus of multi-agent systems in the recent years, and seem to have certain limitations that will be discussed as follows.

1.4.1 Weaknesses of the Solution

The problem associated with the method presented above lies in the fact that *consensusability* condition is tied to the possibility of finding matrices Π_i and Γ_i for each agent, such that $C_i \Pi_i = C_j \Pi_j$ for all i, j , and certain conditions hold for Γ_i . This implies that each agent requires prior arrangements with a central control station before participation in output consensus. Additionally, selection of appropriate controller parameters (and in particular, F_1, F_2) requires knowledge of the system topology. These two conditions imply that despite authors' claim stating "distributed control", the control strategy is not fully distributed and requires involvement of a central controller at all times, especially considering that the number of agents in a multi-agent system may be time-varying and not constant at all times.

Furthermore, an even more fundamental problem lies in the definition of the parameter $\varepsilon_i = x_i - \Pi_i \eta_i$, and the fact that the controllers drive $\varepsilon_i \rightarrow 0$ implying that $y_i \rightarrow C_i \Pi_i \eta_i$ for all agents i . In effect the outputs are tied to the motion of the controller states η_i and follow a predetermined motion as dictated by the system poles in S , as in the controller state motion in Equation (1.9).

However, to summarize,

1. The authors in [51, 137] have discussed output consensus for heterogenous MAS under switching topologies and time-delays. Results provide conditions under which output consensus can be attained in a mean square sense, i.e.,

$$\lim_{t \rightarrow \infty} \mathbb{E}[\|y_i(t) - y_j(t)\|^2] = 0, \forall i, j \in \mathcal{N}.$$

However, these results are valid under the condition that no disturbances are present in the system model. Additionally, in real case scenarios such as UAV networks where the consensus time is an important factor, the methodology does not seem to be very useful.

2. Cross coupling between the agents have not been included in the mathematical models presented in the literature. In certain applications with cross-coupling effects, where an agent may receive sensor measurements and/or control commands from another agent it would be required to consider the effect of these signals on the system states at the receiving end.
3. The conditions pertaining stability in this work assumes that information that is exchanged between the agents are available in real-time (i.e., no communication delays are existing) which is not practical in real world.
4. The control law requires availability of information regarding the network topology. This implies that the system is not distributed controlled and is a major drawback for practical implementation.
5. The control law requires instantaneous knowledge about the instant at which DoS takes place in a communication link. Therefore, time-delay attacks are not covered under this framework, implying the falsely claim of the authors.
6. In cases where system dynamics are time varying (or switching), the conditions for *consensusability* are non-feasible.
7. The multi-agent system is not at liberty to regulate the agents' outputs arbitrarily (i.e., according to a desirable trajectory), and is constrained to a pre-defined alternating pattern. This is the most fundamental shortcoming of the methodology proposed by the article.

1.4.2 Strengths and Opportunities of the Solution

Despite serious shortcomings and limitations, the methodology discussed in this subsection is a solid approach in dealing with output consensus in multi-agent systems. The basic idea is to alleviate the complexity of the problem by introducing simplified states in the agents' controllers, and then trying to achieve consensus among these simplified states (in contrast with actual heterogeneous plants' states). This would be considerably more attainable in comparison with the case where the plant system states are manipulated directly. Once consensus is formulated in the simplified controller states, the system will be excited such that system output follows the controller states, consequently serving consensus in the output of the agents.

The process explained above brings an opportunity to further rectify the problems stated in Subsection 1.4.1, by introducing a single integrator controller for the agents that

intend to track a desirable output path. The control law will then simply be exciting the agent states to follow a designated path through H_∞ state feedback. This will enable the control method to be designed robust to system disturbances while rectifying the problems stated above.

1.5 Distributed Resilient Control for MAS with Communication Delays and DoS Attacks

Output consensus of multi-agent systems with non-uniform delays in communication channels is a topic that has been discussed in [135]. We concluded that the methodology discussed in Section 1.4 has certain shortcomings including the fact that the control law at the controller side requires non-delayed transmission of information packets under normal conditions. Additionally, it is important to consider that the information sampled at time mh (where h is the sampling period, and $m = \{0, 1, 2, \dots\}$) and transmitted to the receivers actually receive at the receiving end at $mh + d(t)$ where $d(t)$ is a random delay for each communication link, that is depending on the traffic of the channel as well as adversarial intrusions.

The authors in [135] have formulated the problem in a slightly different way. They have assumed the system,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) + E_i v_0(t) \\ e_i(t) &= C_i x_i(t) + F_i v_0(t) \\ \dot{v}_0(t) &= S_0 v_0(t)\end{aligned}\tag{1.10}$$

where the system parameters are the same as defined before, and $v_0(t) \in \mathbb{R}^{N_v}$ is a reference signal to be tracked, or a disturbance to be rejected, and $S_0 \in \mathbb{R}^{N_v \times N_v}$ is a non-Lipschitz matrix. Furthermore, a set of controller states $v_i(t) \in \mathbb{R}^{N_v}$ are defined for all the agents to track $v_0(t)$, and controller system matrices $S_i(t) \in \mathbb{R}^{N_v \times N_v}$ for each agent to track S_0 . In other words, the authors have assumed that the agents do not have knowledge about S_0 and have tried to alleviate the dependency of the distributed controllers to a central control unit. Hence, it is assumed that distributed controllers have to estimate v_0 , S_0 through a consensus protocol defined by,

$$\begin{aligned}\dot{S}_i(t) &= -\mu_1 \sum_{j=0}^N a_{ij} (S_i(mh) - S_j(mh)) \\ \dot{v}_i(t) &= S_i(t) v_i(t) - \mu_2 \sum_{j=0}^N a_{ij} (v_i(mh) - v_j(mh))\end{aligned}\tag{1.11}$$

As explained above, the objective is to select appropriate μ_1, μ_2 and a_{ij} s such that $S_i(t) \rightarrow S_0$, and $v_i(t) \rightarrow v_0(t)$. In case this is successful then the MAS output consensus would be to choose $u_i(t)$ such that $e_i(t) \rightarrow 0$ for all i . Therefore, the focus of the paper is in the analysis of the control strategy in Equation (1.11), and the impact of time-delay in the arrival of information packets from neighbouring agents.

It can be observed that the control strategy defined in (1.11) is not very different from Equation (1.9) for $t_k \in [t_k, \tilde{t}_k)$ considering $\tau = t - mh$, and the fact that S is no longer constant. However, loosely speaking, if consensusability holds for S_i 's then when $t \rightarrow \infty$ one may assume $S_i \approx S_0, \forall i$ (i.e., constant), resulting equivalent conditions between (1.11) and (1.9). The major difference however lies in the fact that the authors in [135] have assumed that S_0 is not available to all the agents and certain mechanisms has to be in place for the agents to estimate S_0 . Therefore, the authors attempt to treat the square matrix S_i with arbitrary initial values. The columns of S_i stacked to form a vector such as $w_i \in \mathbb{R}^{N_v^2}$, and $w_i = [S_i^{(1)}, S_i^{(2)}, \dots, S_i^{(N_v)}]^T$, where $S_i^{(j)}$ denotes the j^{th} column of S_i . In a similar fashion w_0 is assumed to be the vector of S_0 columns. Hence, consensus over w_i s would be equivalent to consensus over S_i s.

Further details of [135] are beyond the scope of this report due to similarity of the results with what had been previously discussed in depth in Subsection 1.4, although methodologies differ. However, the important point that is worth discussing in this report are conceptual weaknesses associated with all the publications that are featuring an exogenous variable such as v_0 to aid output consensus. The following subsection is devoted to the comprehensive review of such weaknesses.

1.5.1 Strengths Weaknesses Opportunities Threats (SWOT) Analysis

We have highlighted certain problems associated with cooperative output consensus of MAS where controller states with predefined dynamics are used to aid consensus in the system state (refer to 1.4.1). The author of this report suggests that the problem statement be improved as follows. We consider the following model for a multi-agent system,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) + \sum_{j \in \mathcal{N}_i} B_{ij} x_j(t - \tau_j) + v_i(t) \\ y_i(t) &= C_i x_i(t) + w_i(t)\end{aligned}\tag{1.12}$$

where system parameters are as specified before, and where $v_i(t) \in \mathbb{R}^{N_{x_i}}$ and $w_i(t) \in \mathbb{R}^{N_{y_i}}$ denote some bounded random disturbances, and $\mathcal{N}_i$ denote the set of neighbouring agents

of agent $i \in \{1, 2, \dots, N\}$, and where $\tau_j \in [0, t)$ is a random delay, and $x_j(t) \in \mathbb{R}^{N_{x_j}}$ denoting system states of agent j where B_{ij} is a constant matrix with appropriate dimension.

We state that cooperative output consensus is achieved in the multi-agent system, if for all $i \in \{1, 2, \dots, N\}$ and any small arbitrary value $\delta \in \mathbb{R}_+$ and a reference output $y_0 \in \mathbb{R}^{N_{y_i}}$, there exist a finite time t_f , such that,

$$\|y_i(t) - y_0\| < \delta, \forall t \in [t_f, \infty). \quad (1.13)$$

The system model in (1.12) allows cooperative output consensus to be defined in a more realistic context where system disturbances and sensor inaccuracies are present, and also circumstances where the system states may be affected by adjacent agent states. As an example, one may consider a cooperative generation control problem in a smart grid where certain generating units attempt to regulate the exported energy to an adjacent power area when the area tie-line load is transmitted through RTUs to the generating units with certain delays or cases where communication lines are subject to DoS attack.

Additionally, the problem would be finding a control protocol for the agents so that cooperative output consensus can be achieved for an arbitrary reference signal y_0 and a time constraint t_f , under circumstances where communication lines are impaired.

In light of what has been discussed above, specific problems associated with [135] are summarized below:

1. The exogenous signal to be tracked in System (1.11) is an alternatively time varying signal that is tied to the poles of matrix S_0 . It is therefore not possible to designate a desirable path for the agents' outputs in an arbitrary fashion. Additionally, the sinusoidal behaviour of the motion is often very undesirable in certain systems. For example, one may consider the zig-zag motion of a UAV, or pulsating thermal stress on the hot path gas of a gas turbine due to alternative loading (due to sinusoidal motion of v_0).
2. A fundamental problem of the methodology in [135] lies in $S_i(t)$. Since $S_i(t)$ is time varying, agent's resources have to be allocated for continuously finding Γ_i . This is an involving practice and undesirable in MAS, and even in certain cases impossible.
3. The condition for consensusability in the MAS depends on the knowledge of the agents respecting the overall topology of the network. This condition effectively denies "distributed control" since a central station has to be present to recursively monitor the configuration of the network and report specifics to the agents.

1.6 Cooperative Control for MAS with Unknown False Data Injection and Replay Cyberattacks

Article [138] is among the solid research papers available in the literature that aims to discuss a resilient control methodology for consensus control in a leader-follower MAS framework, where the input and output communication channels of the agents are subject to FDI and replay attacks (refer to Figure 1.7). In particular, it is assumed that the dynamics of a leader (denoted by 0) is given by,

$$\dot{x}_0(t) = A_0 x_0(t) + B_0 r_0(t) \quad (1.14)$$

where $x_0 \in \mathbb{R}^{N_x}$ denotes the states of the leader and $r_0 \in \mathbb{R}^{N_r}$ is the leader control command, and A_0, B_0 are constant matrices with appropriate dimensions. On the other hand, the set of $i = \{1, \dots, N\}$ followers (denoted by $\mathcal{N}$) aim to track the states of the leader, such that $\lim_{t \rightarrow \infty} x_i(t) = x_0(t)$, $\forall i \in \mathcal{N}$. However, it is assumed that the input/output communication channels of all followers are subject to FDI such that,

$$\begin{aligned} \tilde{x}_i(t) &= x_i(t) + \delta_i^{c-a}(t) \\ \tilde{u}_i(t) &= u_i(t) + \delta_i^{s-c}(t) \end{aligned} \quad (1.15)$$

where $x_i \in \mathbb{R}^{N_x}$, $u_i \in \mathbb{R}^{N_{u_i}}$ denote the states and control commands of agent i , respectively, and $\delta_i^{c-a} \in \mathbb{R}^{N_x}$, $\delta_i^{s-c} \in \mathbb{R}^{N_{u_i}}$ denote bounded FDIs injected to the states and control commands of the agents, where,

$$\dot{x}_i(t) = A_i x_i(t) + B_i \tilde{u}_i(t). \quad (1.16)$$

Additionally, it is assumed that the neighbour agents transmit their state estimations through unsafe communication channels, such that,

$$\tilde{x}_j(t) = \hat{x}_j(t) + \delta_{j-i}^{c-a}(t)$$

where $\delta_{j-i}^{c-a} \in \mathbb{R}^{N_x}$ is the FDI inserted on the communication link between agent j to i , and $\hat{x}_j$ is the state estimation of agent j as in Figure 1.7.

The authors in [138] have further generalized the problem statement by introducing binary (unknown) parameters $\sigma_{ri}^{s-c}, \sigma_{ri}^{c-a} \in \{0, 1\}$, and generalized state, and command attack vectors, $\Delta x_i(t)$ and $\Delta u_i(t)$, respectively, where,

$$\begin{aligned} \Delta x_i(t) &= (1 - \sigma_{ri}^{s-c}) \delta_i^{s-c}(t) - \sigma_{ri}^{s-c} x_i(t) + \sigma_{ri}^{s-c} X_i(t_{ri}^{s-c}) \\ \Delta u_i(t) &= (1 - \sigma_{ri}^{c-a}) \delta_i^{c-a}(t) - \sigma_{ri}^{c-a} u_i(t) + \sigma_{ri}^{c-a} U_i(t_{ri}^{c-a}) \end{aligned} \quad (1.17)$$

to account for FDI and replay attacks, simultaneously, where $X_i(t_{r_i}^{s-c}) \in \mathbb{R}^{N_x}$ denotes sensor replay attack and $U_i(t_{r_i}^{c-a}) \in \mathbb{R}^{N_{u_i}}$ denotes the actuator command replay attack. In Equation (1.17) if $\sigma_{r_i}^{s-c} = 0$, then $\Delta x_i(t)$ represents FDI and if $\sigma_{r_i}^{s-c} = 1$, $\Delta x_i(t)$ represents replay attack. Same applies for $\sigma_{r_i}^{c-a}$, hence $\Delta x_i(t), \Delta u_i(t)$ could represent both FDI and replay attacks, that would not occur simultaneously, and finally,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + B_i(u_i(t) + \Delta u_i(t)) \\ \tilde{x}_i(t) &= x_i(t) + \Delta x_i(t).\end{aligned}\tag{1.18}$$

The vectors x_i and Δx_i as $\bar{x}_i = [x_i^T, \Delta x_i^T]^T$ are further integrated, and the observer goal is determined to find a control vector (inside the observer) $u_{\Delta u_i}$ (refer to Figure 1.7), in order to estimate $\bar{x}_i$ (denoted by $\hat{\bar{x}}_i$), such that $\lim_{t \rightarrow \infty} \hat{\bar{x}}_i(t) = \bar{x}_i(t)$, $\forall i \in \mathcal{N}$. As a result, the authors deduce Equation (8) (please see 138) as,

$$\begin{aligned}E_i \dot{\hat{\bar{x}}}_i(t) &= \bar{A}_i \bar{x}_i(t) + \bar{B}_i(u_i(t) + \Delta u_i(t)) + \bar{N}_i \Delta x_i(t) \\ \hat{\bar{x}}_i(t) &= \bar{C}_i \bar{x}_i(t)\end{aligned}\tag{1.19}$$

where details are provided in 138. Furthermore, the error signal is defined as,

$$\bar{e}_i(t) = \hat{\bar{x}}_i(t) - \bar{x}_i(t)$$

and a state equation is constructed in Equation (10) (in 138) to estimate $\hat{\bar{x}}_i(t)$ (inside the observer), as a function of excitation signals $u_{\Delta u_i}(t)$ and $u_{\delta_i}(t)$, to compensate for $\Delta u_i(t)$ and $\Delta x_i(t)$, respectively. Finally, the authors in 138 have shown that $u_{\Delta u_i}, u_{\delta_i}$ signals can be chosen such that $\bar{e}_i(t) \rightarrow 0$, as $t \rightarrow \infty$, which further implies that the system states x_i , and the associated cyber-attack vector Δx_i could be estimated under FDI and replay attacks.

Despite of minor mistakes, the article contains a relatively solid discussion for the estimation of system states of MAS agents when all communication channels are prone to FDI and replay cyber-attack. These estimates are then used in the controller in Figure 1.7 to construct a concession control signal such that agents individually track the leader state vector, and result in asymptotic state consensus in the followers. Specifically, the article suggests an observer to be constructed in the remote controller as,

$$\dot{\hat{\bar{x}}}_i(t) = f_1(\hat{\bar{x}}_i(t), \tilde{x}_i(t), u_i(t), u_{\Delta u_i}(t))\tag{1.20}$$

where $f_1(\cdot)$ is a linear time invariant function, and $u_{\Delta u_i}(t) = g_{u_{\Delta u_i}}(\bar{e}(t))$ is the observer control command (where $g_{u_{\Delta u_i}}(\cdot)$ is a time invariant linear function with parameters to be designed according to a certain set of criteria, that are discussed in the article), and is designed to ensure that $\hat{\bar{x}}_i(t) \rightarrow \bar{x}_i(t)$, as $t \rightarrow \infty$, for all $i \in \mathcal{N}$, as stated earlier. Once

$\hat{\hat{x}}_i = [\hat{x}_i^T(t), \Delta\hat{x}_i^T(t)]^T$ is estimated the observer control sequence $u_{\Delta u_i}(t)$ is no longer required in the controller, and the plant control command $u_i(t)$ can be constructed as,

$$u_i(t) = f_2(\hat{x}_i(t), \tilde{x}_i(t), r(t)) - u_{\Delta u_i}(t) \quad (1.21)$$

to ensure that $\hat{x}_i(t) \rightarrow x_0(t)$, as $t \rightarrow \infty$, for all $i \in \mathcal{N}$, where $f_2(\cdot)$ is another linear time invariant function with known parameters.

1.6.1 SWOT Analysis

1. The authors in [138] have shown remarkable results to develop local control commands to compensate FDI cyberattacks on input and output communication channels simultaneously, and estimate the plant's system states. Notwithstanding the above, it can be argued that the observer operates on the condition that all system states can be transmitted from the plant to the remote controller, which is often a questionable condition in real life applications.
2. It can be suggested to further develop the present theories in [138], so that the observers operate based on a predefined system output, rather than the entire plants' state vectors.
3. The agents' control command in (1.21) are derived based on $r(t)$ that is the leader's internal control function, and may not be accessible to all the followers (in general). Additionally, the article does not discuss the possibility of $r(t)$ being subject to FDI and/or replay cyberattacks.
4. The fact that the leaders would need to have access to $r(t)$ essentially deters the fundamental objectivity in multi-agent systems, that is distributive controllability. In particular, distributed control design philosophy in its true sole requires the control strategy of the agents to be merely a function of a limited number of neighbouring agent's sensors, that are transmitted in a discrete-time fashion. Any violation of these fundamental requirements would degrade the advantage of MAS frameworks, and have to be avoided in the control architectures (based on the viewpoint of the author of this report).

1.7 Summary

As it has been evident, the main focus of this report is on mitigation strategies with respect to FDI and DoS cyberattacks in CPS. The summary can be explained as below:

1.7.1 False Data Injection Attacks

The core objective of most FDI attack detection techniques are very similar to fault detection methods and relies on the estimation of plant's system states based on the information received from sensors, and comparing those to computational expectations of the plant motion models. In particular, the controller assuming *a priori* state of the plant at the immediately preceding time-step, and given its generated control command, estimates the present state of the plant, which is then compared to that derived from the plant output (presuming observability condition). An unjustifiable deviation the system output (read by the sensors) with respect to the observer estimated values, would trigger anomaly detectors, which then has to be analyzed further to isolate the cause (i.e., fault versus cyber-attack in a very general context). Therefore, the backbone of almost every security measure is to attain a relatively concise and validated estimation of the present system states.

In this report we have also tried to examine the evolution of elementary estimation techniques, as appeared in the literature together with a basic SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis for each. The most traditional estimation technique is the so called "static" observation that derives system states, merely on the basis of sensor information featuring a least square error derivation. This estimation method obviously cannot be validated against cyberattacks, since the dynamic characteristic of the plant has not been taken into account for comparison purposes. Despite, there has been a huge industrial and practical tendency towards application of this technique, given the redundancy in the information that is embedded in a network of sensors measuring a unique process.

We have further demonstrated that more advanced techniques not only features sensor information, but also takes advantage of the knowledge of motion models of the plant to optimize the estimation of the system states on the basis of Kalman filter. In this technique the observer is equipped with two virtually independent (in a physical context, rather than mathematical) sets of system state estimates. Kalman filter is then employed to constitute a blend that optimally represents actual system states in a least mean-square sense. The functionality of Kalman filter relies on the covariance matrices that are representations of the motion models, and the sensor models. The filtered estimate is then closer to the model that features less covariance (i.e., random data sets that exhibit less separation from a mean value). Therefore, problems arise in scenarios where adversaries replace genuine variables, with false values but small covariances. This essentially fools Kalman filter to impersonate a variable with a false value. As a result,

it has to be noted that Kalman filter although functioning favourably for fault detection purposes, may act unfavourably in a cyber-attack environment.

In summary, the counteract to these class of intrusions has been introduced in the literature, and drawn particular attention between researchers. The methodology further validates Kalman estimates through a second round of statistical filters, based on the knowledge obtained from historically generated probability density functions (pdfs) of weighted square residuals, known as chi-square detectors. This class of cyberattack detection is particularly useful against a certain class of covert attacks, including replay attacks where adversaries tend to replay a recorded stream of the system outputs under steady state conditions over and over, to mask the real variations in the system state that is under attack. An example could be an adversary that tends to record GPS radio signals at a particular location in space, and re-broadcasts the same stream with out-powered strength to surpass the genuine GPS signals at a different location in space, in order to fool the navigation system.

Notwithstanding the above, more advanced techniques have been developed in the literature that even surpass chi-square filter in spite of its profound accomplishments, and has been briefly reviewed in this report. The state-of-art in replay attack detection method (as of the knowledge of this author) is a solution referred to as water-marking. Water-marking is a technique that attaches a time-varying secret signature (designed to be invisible to the adversary, hence water-mark) to the control command transmitted to the plant, (also) designed to be decodable from sensor information under normal circumstances. A falsely injected information packet, either to the control commands or to sensor outputs, is expected to be detectable due to the fact that is not enclosed with the water-mark.

The major problem with the water-marking technique is that the watermark inevitably has to be manifested in the system states that might entail undesirable consequences. For instance, watermarking geographic locations in the navigation system would manifest unpredicted and dangerous maneuvering of the vehicle if not negligible in amplitude, and if negligible, would likely remain undecodable in the sensor outputs.

Furthermore, an advanced cyber-attack detection method has been covered in this report, which relies on joint input and state estimation (JISE), and joint attack and state estimation. These methods are certain derivations of Bayesian methods that are optimal in every respect, however, extremely involved (computationally) and difficult to

implement. The objective is to recursively construct the joint probability distribution function of attack and the state vector, based on past and present sensor measurements. The joint pdf would then be used to compute the likelihood of an attack being present and an estimation of the state vector associated with the attack.

Finally, we have tried to introduce one of the state of the art methodologies developed for state estimation and control of MAS, subject to simultaneous FDI (or replay attacks) on input/output communication channels. Limitations and strengths of the methodology has also been analyzed in this report.

1.7.2 Denial of Service Attacks

In this report we have provided a relatively in-depth review of DoS cyberattacks in MAS, aiming to cover a broad spectrum of cyber-threats. This class of cyberattacks involves jamming routers and communication channels in an attempt to cause time-delay in transmission of information, or entirely impede the delivery of information at the receiving ends. The report addressed DoS attacks in a greater depth, in comparison with FDI types of attacks. Latest research works available in the literature argue conditions under which DoS attacks may result in instability of the system. The analysis of DoS attacks on CPS pertains finding upper bounded exponential functions that bound state trajectories during time instances when latest sensor measurements do not arrive at the controller (or observer), due to communication restraints, and result in a diverging exponent due to relinquished feedback control loops. A second upper bounded exponent is also derived that bounds state trajectories when communication links are re-established and the stabilizing feedback control loop restores. These upper bounding exponents are then used to determine conditions under which the state trajectories converge to zero in a given time period.

More advanced research works have developed event triggered methods for updating sensor information in order to alleviate communicational threats by attempting to update sensor measurements only when necessary. In this approach, sensor information are transmitted only when there is a meaningful change in the sensor readings. However, exponential bounding functions (as explained above) are used to derive conditions for stability.

The analysis explained above does not provide practical means to examine conditions for stability of a CPS under DoS or time-delays, since real-world modelling of a CPS entails huge matrices with awkward dimensions. In order to control CPS in a

practical scenario researchers are tending to describe CPS in a multi-agent system framework, with distributed controllers. Information between agents are exchanged through communication links that may be subject to cyberattacks (including DoS). Therefore, the problem of CPS security against DoS has been envisaged more recently, presuming stability of agents through local controllers. However, the problem would be to achieve output consensus among agents through distributed controllers, hence, output consensus of MAS under DoS or time-delayed information. This subject has also been covered in this report in more depth, and the limitations and strengths of the latest achievements in the literature has been analyzed.

Chapter 2

Time Delay Cyberattacks in CPS

2.1 Introduction

Cyber-Physical Systems are usually networked systems composed of a number of heterogeneous systems characterized by independent system dynamics, coupled through a set of signals that are transmitted from one subsystem to other subsystems, where information is exchanged between the subsystems to enable computation of control commands, in order to regulate or track desired outputs with reference to an overall control objective in the CPS. In cases where large number of interconnecting nodes are involved it is often advantageous to administer exchange of information merely among adjacent neighbours (i.e., distributed control), rather than deploying a central control architecture that communicates with all the individual nodes. This is particularly important in order to ensure security and reliability, since in this case communication signals can be kept covert and contained locally. The dispersed nature of CPS often requires public tele-communication infrastructures to be employed for information exchange, rather than dedicated (e.g., leased) communication lines (due to cost and operating expenses). This especially poses threat to the CPS in the form of cyberattacks, and may encounter highly unwanted consequences [42,139]. Therefore, the security of the CPS has to be considered and addressed properly in the CPS design phase. A CPS with a distributed control philosophy in which the subsystems take part in a cooperative control network to achieve a common goal is referred to a Multi-Agent System (MAS), and the subsystems are referred to as the agents.

Cyberattacks are broadly categorized in the literature into deception, and time-delay or DoS attacks [140], as discussed before. In deception attacks an adversary attempts to maliciously alter the information packets that are transmitted among the agents in order to cause an intended consequence in the CPS, while time-delays and DoS

attacks are obstructive means conducted by adversaries to delay or interrupt in the normal flow of information. The authors in [140] and [50] have considered the cooperative output regulation problem for heterogeneous linear multi-agent systems in the presence of communication constraints. Cooperative output regulation is a generalization of the leader-follower consensus problem in MAS. Load sharing in power systems as discussed in Subsection 1.2.1 can be formulated from a MAS point of view, in which the area power systems are considered as agents, and limited information are exchanged among the agents to achieve a secondary coordinated control in a decentralized fashion. In [47] the authors have presented a distributed secondary control scheme for power allocation and voltage restoration in islanded DC micro-grids employing MAS consensus control techniques.

Output consensus for heterogeneous MAS with Markovian switching network topologies has been discussed in [136] and can be used as the basis for studying MAS under DoS cyberattacks assuming that DoS attacks can be represented as switching topologies. Unfortunately, [136] does not address communication time-delays and instability issues that can be caused due to information reception delays. The authors in [141] have also attempted to solve the output consensus problem in a leader-follower heterogeneous MAS under DoS attack. Unfortunately, the proposed solution in [141] can neither be applicable in real-world, since leader's dynamic is unknown to the follower agents in most scenarios (especially, in a MAS where the leader is randomly switched from time to time, such as in Advanced Air Mobility in Subsection 1.2.2 where the leader may have to be switched one agent to another due to limited battery capacity or due the robustness of the overall system with respect to the agents' internal faults and outages).

Therefore, it is not practical to assume that the dynamics of the leader is *a priori* in the design of the control law, since a replacing agent may takeover the ex-leader's role without prior notification to other agents, so that the mission can be accomplished regardless of the identity of the leader. An example in LFC of Smart Grids is the automatic switching mechanism that brings in the emergency CCS when the main CCS is faulty. In this example, switching of the CCS (i.e., the leader) is transparent to the area control centres. Moreover, in a leader-follower MAS it is important to assume that the output trajectory of the leader is unpredictable to the followers. Therefore, it is not practical to assume a pre-determined model for the trajectory of the reference signal. In conclusion, it is not reasonable to designate the consensus control law for a follower that relies on parameters of another agent. In conclusion, it is imperative that the control law is designed in such a way that is based on available and accessible information to

the agents. As a matter of example, it would be unrealistic to use network parameters (including the number of the agents in the network, or the connectivity of the network, etc.) in the design of the control law, since at any given time an agent is assumed to have “exclusive” access to the states of its neighbouring agents in a MAS (that is the main characteristic of “distributed” control systems). We refer to a control law that is designed in accordance to the above criterion are referred to as “eligible” control commands.

The subject of distributed consensus of heterogenous MAS subject to switching topologies and communication time-delays has been a recent research problem in the literature (as in [137]) with a focus on power systems. This chapter provides a comprehensive solution for stability and control of heterogenous MAS systems in the presence of information time-delays and/or DoS. The condition for achieving consensus under finite communication time-delays can be considered as an admissible condition, since malfunctions in the communication system can be considered as temporary problems. The authors of this paper believe that the determination of a methodology that automatically detects the onset of a time-delay attack is a problem that has not been addressed in [137].

The authors in [50] have investigated cooperative resilient output regulation problem with time-delay constraints for a specific class of heterogenous MAS with uniform exogenous inputs (following a LTI dynamics with pure imaginary eigenvalues). Unfortunately, the authors have assumed an exogenous signal that has predetermined characteristics, which violates the condition for the leader’s arbitrary reference signal, and this is due to the fact that the followers are in essence assuming a consensus law that is based on some predefined parameters that are beyond reasonable access to the agents. Once again, the authors of this paper believe that a complete solution for a heterogenous MAS output consensus problem is to assume an entirely unpredictable trajectory for the consensus, and not one that can be mathematically modelled prior to information exchanged in the network.

The authors in [140] have tried to address this subject for a class of CPS systems with non-uniform but bounded communication delays under denial-of-service (DoS) attacks, where a switching resilient control approach is proposed. However, the proposed controller is only functional for DoS attacks (where agents are assumed to understand “missing” information from neighbour agents) but does not address time-delay attacks. The authors in [142] have studied consensus in a homogenous MAS, where the agents are expected to follow a given reference command under intrinsic and communication time-delays and disturbances. The authors in [143] have considered consensus problem

for discrete-time homogenous multi-agent systems over an undirected, fixed network communication graph, focusing on the robustness of consensus with respect to communication delay.

The authors in [144] and [145] have discussed the problem of output synchronization in a multi-agent system subject to time-delays, with linear right-invertible agents that is subject to arbitrary time-delays. The authors in [146] have addressed adaptive consensus tracking for a class of nonlinear multi-agent systems under time varying actuator faults. Several other recent publications have also paid attention to time-delayed nonlinear MAS output regulation using data-driven consensus [147]. The authors in [148] have discussed consensus problem in a discrete-time nonlinear MAS using sliding mode control laws. The authors in [149] have investigated the consensus problem of MAS with time-varying delays subject to switching topologies with less conservative consensus conditions. The authors in [150] have very recently investigated the group consensus problem for heterogeneous MAS with time-delays via pinning control in the frequency domain. The weakness points of some of the latest research works in this area has been summarized in Table 2.1.

In the following subsections, this author tries to address time-delay and DoS cyberattacks on CPS with due considerations to the limitations and conditions explained above. Subsection 2.2 is the result of a first attempt to address time-delay attacks on information exchanged between the CCS and a power generating area in the LFC problem introduced in Subsection 1.2.1, as a special case of a CPS. The proposed methodology in Subsection 2.2 follows the standard feedback control stabilization methodology that has been discussed in the literature up to now. It will be shown in Subsection 2.2.4 that there exists fundamental shortcomings to the proposed feedback control methodology, that prevents the solution to be generalized to all CPS examples. Thereafter, this author tried to pursue a different approach to resolve these shortcomings and propose a methodology to address time-delay resiliency for a general class of CPS, as presented in Subsection 2.3.

2.2 Resilient Control Against Time-Delay and DoS Cyberattacks in LFC

2.2.1 Problem Statement

In this problem we will investigate the stability of the LFC problem in smart grids with respect to Time-Delay Switch (TDS) cyberattacks. Let us state the first problem statement as the follows:

Table 2.1: Results of the analysis of some of the more recent publications in the literature related to CPS time-delay resiliency

Reference	Year	Description of the Open Challenges
[140]	2020	The exogenous signal to be tracked is not delayed.
[137]	2020	time-delays inflict certain intervals and system is assumed intact in some other intervals.
[142]	2020	Optimal controller requires knowledge of network topology and eigenvalues of the Laplacian matrix.
[145]	2022	The goal is to track a constant reference signal that is not delayed.
[147]	2023	Cost function to be minimized is the error between the present value of the agent and the neighbour's delayed value.
[149]	2022	Identical time-delays are required between the agent and its neighbours for homogenous MAS with known system parameters.
[150]	2023	The leader information to be followed by the MAS followers is not time-delayed.
[151]	2024	Imperfections in the communication system including time-delays are estimated based on probability models that cannot assume system disturbances.

Problem 1. The generalized model for a two-area power system with delay can be represented as in [64, 65], for the i^{th} area as follows,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + A_{d_i} x_i(t - \tau_i) + A_{ij} x_j(t) + B_i u_i(t) + D_i w_i(t), \\ y_i(t) &= C_i x_i(t),\end{aligned}\tag{2.1}$$

where $x_i = \begin{bmatrix} \Delta f_i & \Delta P_{m_i} & \Delta P_{v_i} & \Delta \Lambda_i & \Delta P_{ij} \end{bmatrix}^T \in \mathbb{R}^5$, denotes the state vector of the area frequency fluctuations, the mechanical power, the governor valve position, the integrated Area Control Error (ACE) of the equivalent generating units (where $ACE = K_i B_i \Delta f_i + K_i \Delta P_{ij}$), and the tie-line power fluctuation, respectively, as implied from Figures 1.4 and 2.9, and where $\tau_i \in \mathbb{R}^+$ represents the unknown communication delay, where,

$$\Lambda_i(t) = \int_{s=0}^t K_i B_i \Delta f_i(s) + K_i \Delta P_{ij}(s - \tau_i) ds \tag{2.2}$$

with $w_i(t) = \Delta P_{d_i}$ denoting disturbances. It is assumed that Λ_i and ΔP_{ij} are the only states prone to cyber attack in the Area i (refer to Figure 1.4) since Δf_i is locally measurable in the Area i . The states (denoted by $x_i(t - \tau_i)$) are generally signals that are transmitted in the form of data packets and are subject to unknown delays due to the traffic of the communication channel, noise, adversary induced parasites, etc.

Our goal is to regulate $ACE \approx 0$ in all areas for all delays in the telemetered channels and variations in the area loads. That is primarily ensuring stability of the power system (2.3) in every circumstance (including TDS cyber attacks on ΔP_{ij} , Λ_i and Λ_j). Furthermore, it is desirable that frequency deviations as well as tie-line power fluctuations remain minimal for all variations in the system load.

2.2.2 Research Results for Problem 1

The overall system model for a two-area power system can be represented as follows,

$$\dot{x}(t) = Ax(t) + A_d x(t - \tau) + Bu(t) + Dw(t) \tag{2.3}$$

with

$$\begin{aligned}x = \begin{bmatrix} \dot{x}_i \\ \dot{x}_j \end{bmatrix} &= \begin{bmatrix} A_i & A_{ij} \\ A_{ji} & A_j \end{bmatrix} \begin{bmatrix} x_i(t) \\ x_j(t) \end{bmatrix} + \begin{bmatrix} A_{d_i} & 0 \\ 0 & A_{d_j} \end{bmatrix} \begin{bmatrix} x_i(t - \tau_i) \\ x_j(t - \tau_j) \end{bmatrix} \\ &+ \begin{bmatrix} B_i & 0 \\ 0 & B_j \end{bmatrix} \begin{bmatrix} u_i(t) \\ u_j(t) \end{bmatrix} + \begin{bmatrix} D_i & 0 \\ 0 & D_j \end{bmatrix} \begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix}.\end{aligned}\tag{2.4}$$

In view of the model in Equation (2.1), the system matrices are defined in [64, 65] as:

$$\begin{aligned}
A_i &= \begin{bmatrix} -1/\tau_{p_i} & k_{p_i}/\tau_{p_i} & 0 & 0 & -k_{p_i}/\tau_{p_i} \\ 0 & -1/\tau_{ch_i} & 1/\tau_{ch_i} & 0 & 0 \\ -1/R_i\tau_{g_i} & 0 & -1/\tau_{g_i} & 0 & 0 \\ K_i B_i & 0 & 0 & 0 & 0 \\ 2\pi T_1 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad A_{d_i} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{\tau_{g_i}} & 0 \\ 0 & 0 & 0 & 0 & K_i \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\
A_{ij} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2\pi T_1 \end{bmatrix}, \quad B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_{g_i} \\ 0 \\ 0 \end{bmatrix}, \quad D_i = \begin{bmatrix} -k_{p_i}/\tau_{p_i} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \quad (2.5)
\end{aligned}$$

The mathematical model for the j^{th} area is identical except that all the indices i should be changed to j and j to i in equations (2.1) to (2.5). For a multi-area power system with $n + 1$ areas, $A_{ij}x_j(t)$ in equation (2.1) would be replaced by $\sum_{j=1}^n A_{ij}x_j(t)$, and $A_i(5, 1) = 2n\pi T_1$ (i.e., the 1st column of the 5th row of A_i), where T_1 is the slope of the power angle curve at the initial operating angle [64].

The objective is to find K_{τ_i} and K_{τ_j} , such that $K_{\tau_i} = [k_{\tau_{i1}}, k_{\tau_{i2}}, k_{\tau_{i3}}, k_{\tau_{i4}}, 0] \in \mathbb{R}^5$ and $K_{\tau_j} = [k_{\tau_{j1}}, k_{\tau_{j2}}, k_{\tau_{j3}}, k_{\tau_{j4}}, 0] \in \mathbb{R}^5$ such that $u = K_{\tau}x$ stabilizes the system (2.4) for all τ_i and $\tau_j \in \mathbb{R}^+$, where,

$$K_{\tau} = \begin{bmatrix} K_{\tau_i} & \mathbf{0} \\ \mathbf{0} & K_{\tau_j} \end{bmatrix}. \quad (2.6)$$

Ideally, one would prefer $k_{\tau_{i4}} = 0$ and $k_{\tau_{j4}} = 0$ in order to derive a fully independent controller to telemetered measurements. However, excessive constraints on K_{τ} complicates the solution to the problem. Nevertheless, $u_i = K_{\tau_i}x_i$ and $u_j = K_{\tau_j}x_j$ will only be functions of the locally measurable states of the areas i and j , respectively. Specifically, the goal is finding K_{τ} such that $x \rightarrow 0$ as $t \rightarrow \infty$ for any initial state $x(0)$ and all $\tau \in \mathbb{R}_+^2$ where, $\dot{x}(t) = (A + BK_{\tau})x(t) + A_d x(t - \tau)$. This ensures that $\|x(t)\|$ will remain bounded for all bounded $\|w(t)\| \in \mathbb{R}^+$. Furthermore, with reference to Figure 2.9 it can be shown that,

$$\Delta f_i(s) \rightarrow \frac{s^2 \Delta P_{d_i}(s)}{2\pi T_1 K_i H(s) e^{-2\tau_i s}} \text{ as } s \rightarrow 0,$$

(details of which is omitted due to space limitations) which implies that $\Delta f_i(t) \rightarrow 0$ in response to $\Delta P_{d_i}(t)$, as long as $e^{-\tau_i s} \neq 0$ (i.e., finite delays).

Theorem 1. The controller $u = K_\tau x$ for the system (2.3) ensures that,

$$||\Delta f_i(t)||^2 + ||\Delta P_{ij}(t)||^2 + ||\Delta f_j(t)||^2 <$$

$$\gamma_\tau^2 ||x(t - \tau)||^2 + \gamma_w^2 ||w(t)||^2$$

for arbitrary small parameters γ_τ and $\gamma_w > 0$, if there exists positive definite symmetric matrices R_i and R_j and positive scalars r_i and r_j , and a matrix $F = \mathbf{Diag}(F_i, F_j)$ where $F_i = [f_{i1}, f_{i2}, f_{i3}, f_{i4}, 0]$ and $F_j = [f_{j1}, f_{j2}, f_{j3}, f_{j4}, 0]$, such that,

$$\begin{bmatrix} \Phi_1 & A_d & D & R^{-1} \\ A_d^T & -\gamma_\tau^2 I & 0 & 0 \\ D^T & 0 & -\gamma_w^2 I & 0 \\ R^{-1} & 0 & 0 & -I \end{bmatrix} < 0$$

$$\Phi_1 = AR^{-1} + BF + R^{-1}A^T + F^T B^T.$$

where $R^{-1} = \mathbf{Diag}(R_i^{-1}, r_i^{-1}, R_j^{-1}, r_j^{-1})$, and $K_\tau = FR$.

Proof. Let us assume that $V(x) = x^T R x$ is a candidate Lyapunov function of the state vector $x(t) = [x_i(t)^T \ x_j(t)^T]^T$, where $x(0) = 0$ and $R = \mathbf{Diag}(R_i, r_i, R_j, r_j)$. Substituting $u = K_\tau x$ in Equation (2.3) we have,

$$\begin{aligned} \dot{V}(x) &= x^T A^T R x + x^T R A x + x^T (t - \tau) A_d^T R x + x^T R A_d x(t - \tau) \\ &\quad + x^T K_\tau^T B^T R x + x^T R B K_\tau x + w^T D^T R x + x^T R D w. \end{aligned} \quad (2.7)$$

and through factorization,

$$\dot{V}(x) = \mathbb{X}^T \mathbf{P}_v \mathbb{X} \quad (2.8)$$

where $\mathbb{X}^T = [x^T \ x^T(t - \tau) \ w^T]$ and,

$$\mathbf{P}_v = \begin{bmatrix} A^T R + R A + K_\tau^T B^T R + R B K_\tau & R A_d & R D \\ A_d^T R & 0 & 0 \\ D^T R & 0 & 0 \end{bmatrix}$$

Our objective is to satisfy $||x(t)||^2 - \gamma_\tau^2 ||x(t - \tau)||^2 - \gamma_w^2 ||w(t)||^2 < 0$ for some arbitrary small $\gamma_\tau, \gamma_w > 0$, since $||\Delta f_i(t)||^2 + ||\Delta P_{ij}(t)||^2 + ||\Delta f_j(t)||^2 < ||x(t)||^2$. That is,

$$\mathbb{X}^T \mathbf{P}_{\text{LFC}} \mathbb{X} < 0 \quad (2.9)$$

where,

$$\mathbf{P}_{\text{LFC}} = \begin{bmatrix} I & 0 & 0 \\ 0 & -\gamma_\tau^2 I & 0 \\ 0 & 0 & -\gamma_w^2 I \end{bmatrix}.$$

Note that the condition $\mathbb{X}^T(\mathbf{P}_{\text{LFC}} + \mathbf{P}_v)\mathbb{X} < 0$ results in $\|x(t)\|^2 - \gamma_\tau^2\|x(t - \tau)\|^2 - \gamma_w^2\|w(t)\|^2 < 0$, since $\mathbb{X}^T(\mathbf{P}_{\text{LFC}} + \mathbf{P}_v)\mathbb{X} < 0$ requires $\int_0^t \mathbb{X}^T(\mathbf{P}_{\text{LFC}} + \mathbf{P}_v)\mathbb{X}dt < 0$, or $\int_0^t \dot{V}(x)dt + \int_0^t \mathbb{X}^T\mathbf{P}_{\text{LFC}}\mathbb{X}dt < 0$. That is, $V(x) - V(0) + \|x(t)\|^2 - \gamma_\tau^2\|x(t - \tau)\|^2 - \gamma_w^2\|w(t)\|^2 < 0$, or finally, $\|x(t)\|^2 - \gamma_\tau^2\|x(t - \tau)\|^2 - \gamma_w^2\|w(t)\|^2 < 0$ since $V(x) > 0$ and by assumption $V(0) = 0$.

Therefore, the objective would be finding $R > 0$ and K_τ such that $\mathbf{P}_{\text{LFC}} + \mathbf{P}_v < 0$, i.e.,

$$\mathbf{P}_{\text{LFC}} + \mathbf{P}_v = \begin{bmatrix} \Psi & RA_d & RD \\ A_d^T R & -\gamma_\tau^2 I & 0 \\ D^T R & 0 & -\gamma_w^2 I \end{bmatrix} < 0 \quad (2.10)$$

with

$$\Psi = RA + RBK_\tau + A^T R + K_\tau^T B^T R + I.$$

Unfortunately, the inequality (2.10) cannot be solved through LMI methods since for instance the term $K_\tau^T B^T R$ is a multiplication of two unknown decision matrices K_τ , and R . An equivalent criteria for the condition in (2.11) is,

$$\text{Diag}(R^{-1}, I, I)(\mathbf{P}_{\text{LFC}} + \mathbf{P}_v)\text{Diag}(R^{-1}, I, I) < 0$$

That is,

$$\begin{bmatrix} \Phi & A_d & D \\ A_d^T & -\gamma_\tau^2 I & 0 \\ D^T & 0 & -\gamma_w^2 I \end{bmatrix} < 0 \quad (2.11)$$

where $\Phi = AR^{-1} + BK_\tau R^{-1} + R^{-1}A^T + R^{-1}K_\tau^T B^T + R^{-2}$. Renaming $F = K_\tau R^{-1}$, the problem would yield to a standard LMI problem if R^{-2} could be transformed into a linear form. The following lemma allows us to resolve the problem:

Lemma 1. (Borrowed from [72]): For a given symmetric matrix,

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

the following three conditions are equivalent:

1. $S < 0$,
2. $S_{11} < 0, S_{22} < S_{12}^T S_{11}^{-1} S_{12}$,
3. $S_{22} < 0, S_{11} < S_{12} S_{22}^{-1} S_{12}^T$,

By invoking Lemma-1, the inequality (2.11) would be equivalent to,

$$\begin{bmatrix} \Phi_1 & A_d & D & R^{-1} \\ A_d^T & -\gamma_\tau^2 I & 0 & 0 \\ D^T & 0 & -\gamma_w^2 I & 0 \\ R^{-1} & 0 & 0 & -I \end{bmatrix} < 0 \quad (2.12)$$

$$\Phi_1 = AR^{-1} + BF + R^{-1}A^T + F^T B^T.$$

Therefore, the problem would be to find the decision matrices $R^{-1} = \mathbf{Diag}(R_i^{-1}, r_i^{-1}, R_j^{-1}, r_j^{-1})$ and F so that the inequality (2.12) holds for some arbitrary small positive γ_τ and γ_w , and $F = \mathbf{Diag}(F_i, F_j)$ where $F_i = [f_{i1}, f_{i2}, f_{i3}, f_{i4}, 0]$ and $F_j = [f_{j1}, f_{j2}, f_{j3}, f_{j4}, 0]$. In this case the feedback gain $K_\tau = FR$ ensures that $\|\Delta f_i(t)\|^2 + \|\Delta P_{ij}(t)\|^2 + \|\Delta f_j(t)\|^2 < \gamma_\tau^2 \|x(t - \tau)\|^2 + \gamma_w^2 \|w(t)\|^2$. Obviously, if R_i and R_j are 4×4 positive definite symmetric matrices, and r_i, r_j are positive scalars, then R is nonsingular. Additionally, the state feedbacks $u_i = K_{\tau_i} x_i$ and $u_j = K_{\tau_j} x_j$ could be derived from the locally accessible measurements $\Delta f, \Delta P_m, \Delta P_v$, and Λ . This completes the proof of the theorem. ■

The fact that Λ and P_{ij} are telemetered signals and subject to delay cyber attacks does not influence the condition $\|x(t)\|^2 < \gamma_\tau^2 \|x(t - \tau)\|^2 + \gamma_w^2 \|w(t)\|^2$ derived from Theorem 11 which is the objective of the LFC (if a sufficiently small γ_τ can be found to satisfy Theorem 11, and if $\|x(t - \tau)\|$ is bounded). Therefore, it is necessary to show that the control law in Theorem 11 also ensures boundedness of $\|x(t - \tau)\|$ for at τ , hence stability of the power system. This is shown in Theorem 2.

Theorem 2. *The control strategy $u = K_\tau x$ developed in Theorem 11 guarantees stability of the system (2.3) for all $\tau_i, \tau_j > 0$.*

Proof. Let us consider the following Lyapunov candidate function,

$$V(x) = x^T(t)Rx(t) + \int_{t-\tau}^t x^T(s)x(s)ds$$

where

$$\dot{x}(t) = (A + BK_\tau)x(t) + A_d x(t - \tau),$$

and where R is obtained as in Theorem 11. Then,

$$\dot{V}(x) = \frac{d(x^T(t)Rx(t))}{dt} + x^T(t)x(t) - x^T(t - \tau)x(t - \tau)$$

where,

$$\frac{d(x^T(t)Rx(t))}{dt} = \mathbb{X}^T \mathbf{P} \mathbb{X}, \quad \mathbb{X}^T = [x^T \quad x^T(t - \tau)] \text{ and,}$$

$$\mathbf{P} = \begin{bmatrix} A^T R + RA + K_\tau^T B^T R + RBK_\tau & RA_d \\ A_d^T R & 0 \end{bmatrix}.$$

Also,

$$x^T(t)x(t) - x^T(t-\tau)x(t-\tau) = \mathbb{X}^T \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} \mathbb{X}.$$

Therefore, $\dot{V}(x) = \mathbb{X}^T (\mathbf{P} + \mathbf{Diag}(I, -I)) \mathbb{X}$, and it follows that the sufficient condition for the stability of the power system with delayed measurements is that $\mathbf{P} + \mathbf{Diag}(I, -I) < 0$, i.e.,

$$\begin{bmatrix} A^T R + RA + K_\tau^T B^T R + RBK_\tau + I & RA_d \\ A_d^T R & -I \end{bmatrix} < 0$$

or equivalently,

$$\mathbf{Diag}(R^{-1}, I) (\mathbf{P} + \mathbf{Diag}(I, -I)) \mathbf{Diag}(R^{-1}, I) < 0, \text{ i.e.,}$$

$$\begin{bmatrix} \Phi & A_d \\ A_d^T & -I \end{bmatrix} < 0$$

where $\Phi = AR^{-1} + BK_\tau R^{-1} + R^{-1}A^T + R^{-1}K_\tau^T B^T + R^{-2}$, and finally,

$$\begin{bmatrix} \Phi_1 & A_d & R^{-1} \\ A_d^T & -I & 0 \\ R^{-1} & 0 & -I \end{bmatrix} < 0$$

where $\Phi_1 = AR^{-1} + BF + R^{-1}A^T + F^T B^T$. However, the inequality (2.12) required,

$$\begin{bmatrix} \Phi_1 & A_d & R^{-1} \\ A_d^T & -\gamma_\tau^2 I & 0 \\ R^{-1} & 0 & -I \end{bmatrix} < 0$$

implying that $\dot{V}(x) < 0$, since given $0 < \gamma_\tau < 1$,

$$\begin{bmatrix} \Phi_1 & A_d & R^{-1} \\ A_d^T & -I & 0 \\ R^{-1} & 0 & -I \end{bmatrix} < \begin{bmatrix} \Phi_1 & A_d & R^{-1} \\ A_d^T & -\gamma_\tau^2 I & 0 \\ R^{-1} & 0 & -I \end{bmatrix}$$

which completes the proof of the theorem. ■

2.2.3 Simulations and Case Studies of Problem 1

Finding a solution to the LMI of Theorem 11 when $x_i(t-\tau)^T = [0, 0, 0, \Lambda_i(t-\tau), \Delta P_{ij}(t-\tau)]$ is a complicated task and has not yet been fully resolved. We are able to find a solution for the case where $\Lambda_i(t-\tau)$ is the only delayed parameter. Therefore, the LFC cannot be

guaranteed when ΔP_{ij} is simultaneously cyber attacked. Notwithstanding the above the results obtained are still very impressive considering the simulated scenarios presented below. The system parameters used for simulations have been taken from [65] with minor changes. The power system considered in simulations is depicted in Figure 1.4. Due to space limitations parameter quantities will not be presented here but can be obtained from the reference given above. The feedback gain K_τ suggested in this work has been obtained according to Theorem 11 and presented below:

$$K_\tau = \begin{bmatrix} -123.22 & -3.65 & 0.18 & -7.54 & \mathbf{0}_{1 \times 6} \\ \mathbf{0}_{1 \times 6} & -48.7 & -4.74 & 0.75 & -1.55 \end{bmatrix}$$

The decentralized feedback control for the areas i and j are then given as follows:

$$\begin{aligned} u_i &= -123.22\Delta f_i - 3.65\Delta P_{m_i} + 0.18\Delta P_{v_i} - 7.54\Lambda_i \\ u_j &= -48.7\Delta f_j - 4.74\Delta P_{m_j} + 0.75\Delta P_{v_j} - 1.55\Lambda_j \end{aligned} \quad (2.13)$$

as it is evident the feedback control for each area only depends on the measurable states of the area and is not a function of ΔP_{ij} . This is in contrast with conventional centralized controllers where,

$$\begin{aligned} u_i &= -69.52\Delta f_i - 2.37\Delta P_{m_i} + 0.54\Delta P_{v_i} - 4.28\Lambda_i \\ &+ 0.47\Delta P_{ij} - 6.62\Delta f_j - 0.05\Delta P_{m_j} - 0.3\Delta P_{v_j} - 0.16\Lambda_j. \end{aligned} \quad (2.14)$$

It can be noted that the centralized control command for the area i is a function of the area j states, which is an undesirable characteristic. The first simulated scenario as depicted in Figure 2.1 shows the frequency variations in response to varying area load (as in Figure 2.2) in a power system with the centralized LFC when all communication channels are affected by the random delay cyber attacks. It is evident that the system is unstable.

Remark 1. *The cyber attack delay profile is often of a random nature in a sense that the telemetered state vector $x(t - \tau)$ is possessing a random (independent and) uniformly distributed τ for every telemetered state. The interested reader may refer to [58, 65, 66, 69, 70] for details.*

Figures 2.2 and 2.3 depict the performance of the augmented controllers in equation (2.13) that are proposed in this work. In this scenario the power system is under delay cyber attacks on Λ_i and Λ_j . The LFC is operative and regulates the area control error to a desirably low steady state value, while maintaining stability of the power system. Figure 2.4 depicts the control signals Λ_i , u_i and the turbine power ΔP_{v_i} for the

Delay Cyber Attack on Telemetered Measurements

Figure 2.1: Frequency variations in a power system with a centralized controller (as depicted by a cloud in Figure 1.4) transmitting $\Lambda_i(t)$ and $\Lambda_j(t)$ to the generating units i and j respectively. It is assumed that the communication channels are under cyber attack causing delayed ACEs (i.e., $\Lambda_i(t - \tau_i)$ and $\Lambda_j(t - \tau_j)$) at governor inputs. The result is clearly a growing oscillation in the frequency variations of the areas yielding instability and shut down through protective relaying mechanisms.

Delay Cyber Attack on LFC Area Command

Figure 2.2: Decentralized augmented controllers in equation (2.13) are active, and Λ_i , Λ_j are under delay cyber attack same as in Figure 2.1. The thick line represents ΔP_{ij} which indicates that LFC is functional despite delay cyber attack.

scenario considered in Figures 2.2 and 2.3. Figure 2.5 illustrates a more severe scenario where all communication channels (i.e., area commands Λ_i , Λ_j , and telemetered measurements f_i , f_j and P_{ij}) are under random delay cyber attack. The augmented controllers in equation (2.13) are active. The performance of the augmented controllers can be appreciated by comparing Figure 2.5 and Figure 2.1 (in which augmented controllers are not

Delay Cyber Attack on Area Commands



Figure 2.3: The scenario depicted in Figure 2.2 is repeated. Δf_i and Δf_j are displayed which indicates LFC is functional despite of the delay cyber attacks on Λ_i , Λ_j .

Delay Cyber Attack on Area LFC Command

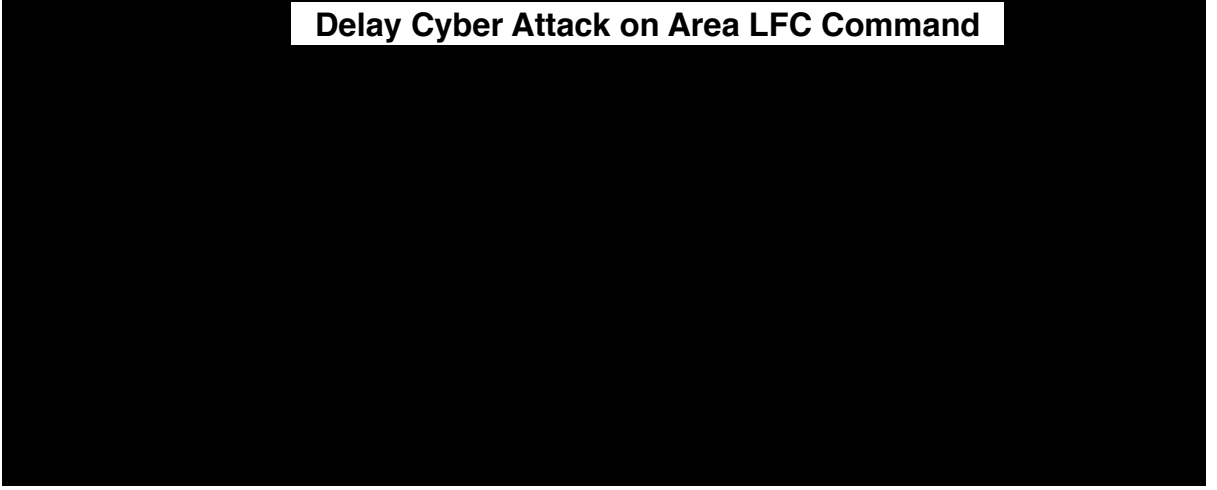


Figure 2.4: Control commands under delay cyber attack presented in Figures 2.2 and 2.3 for reference. u_i tries to enforce the turbine power ΔP_{v_i} to track the load area ΔP_{d_i} in Figure 2.2, so that eventually $\Delta P_{ij} = 0$.

deployed). Figure 2.6 shows ΔP_{ij} in the scenario captivated in Figure 2.5. The fact that the steady state $\Delta f_i - \Delta f_j \neq 0$ also results in $\Delta P_{ij} \neq 0$, which indicates that the LFC is not functional. This is due to the fact that K_τ has been computed under the condition that $x(t - \tau) = \Lambda(t - \tau)$ in Theorem T1, whereas the delay cyber attack has been plotted on all telemetered states. Unfortunately, a solution to K_τ for a general case where $x(t - \tau)$ is a vector of all delayed states cannot be simply computed, and is left as a topic for future work. Finally, Figure 2.7 illustrates the most difficult cyber attack scenario in which telemetered measurements are delayed while there is a DoS cyber attack on area control commands Λ_i and Λ_j . Accordingly, $u_i = -123.22\Delta f_i - 3.65\Delta P_{m_i} + 0.18\Delta P_{v_i}$ and $u_j = -48.7\Delta f_j - 4.74\Delta P_{m_j} + 0.75\Delta P_{v_j}$ since it has been assumed that $\Lambda_i(t) = \Lambda_j(t) = 0$.

Delay Cyber Attack on All Communication Channels

Figure 2.5: In this scenario all communication channels are under delay cyber attack. The operating conditions are similar to Figure 2.1, however the augmented controllers in equation (2.13) have stabilized the system and largely improved LFC. Unfortunately complete LFC can not be achieved as the steady state $\Delta f_i - \Delta f_j \neq 0$.

Delay Cyber Attack on All Communication Channels

Figure 2.6: LFC is no longer functional despite the fact that the augmented controllers are active. The operating circumstance is the same as in Figure 2.5.

Unfortunately the augmented controllers u_i and u_j are only capable of guaranteeing stability of the power system and have no contribution on the performance of the LFC (in comparison with Figure 2.5). However, the merit of the decentralized controller proposed in this work can be appreciated in comparison with the centralized controllers referred to in the literature. Figure 2.8 compares Δf_i with centralized and decentralized controllers in service. The centralized controller is not capable of maintaining system stability under the DoS cyber attack.

Delay Cyber Attack on Telemetered Measurements and DoS on Area Commands

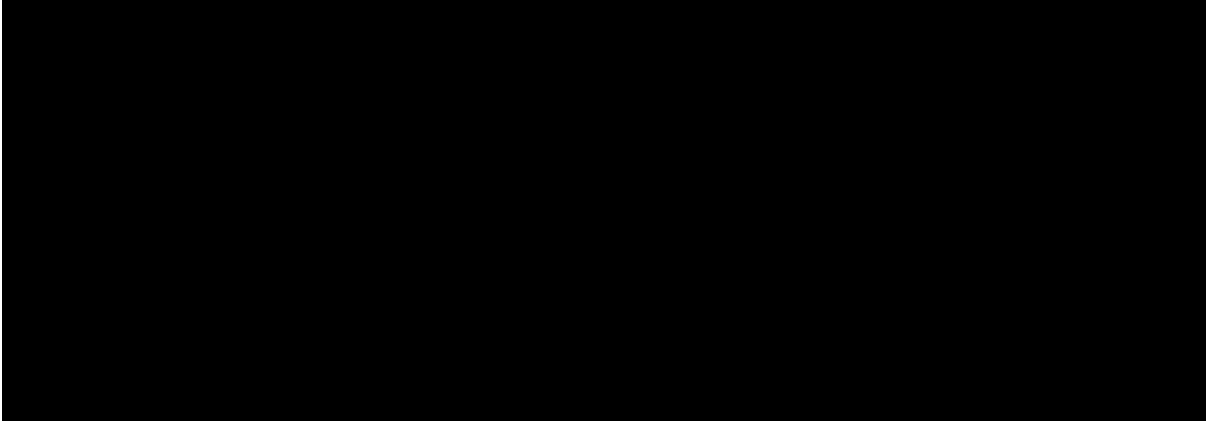


Figure 2.7: Most severe cyber attack circumstance where Λ_i and Λ_j are under DoS cyber attack while the telemetered measurements are randomly delayed. Black line depicts Δf_i and the grey line depicts Δf_j .

TDS Cyber Attack on Telemetered Measurements and DoS on Area Commands

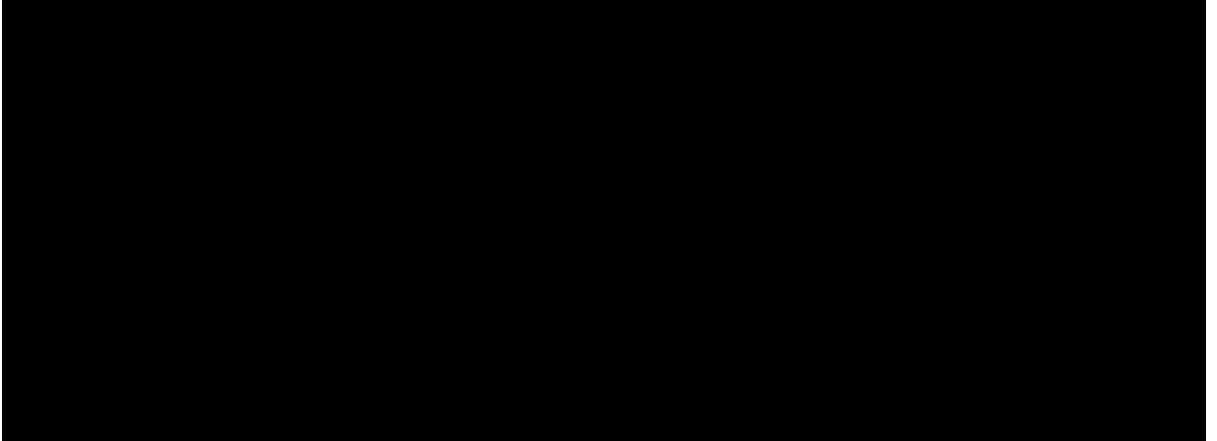


Figure 2.8: Comparison between the Decentralized controller proposed in this work and the conventional centralized controller under DoS cyber attack scenario depicted in Figure 2.7.

2.2.4 Limitations of the Solution in 2.2.2

Complete independence of the control law (i.e., to ΔP_{ij} and Λ) has not been fully implemented in this work which is its limitation although this is a subject of further investigation. The control law derived in this report alleviates the constraints with present delay resilient controllers introduced in the literature in a sense that the control command is derived from locally measurable states, therefore immune from cyber attacks to controllers. Additionally, since the control law introduced for area i does not depend on the state measurements of area j (vice versa) it enables the controllers to be implementable in practice.

Additionally, as the ultimate goal of Chapter-1 is to formulate a control law that alleviates instability problems associated with DoS and time delay attacks in a general CPS (including the IoD framework, illustrated in Figure 1.2), it is required to redefine a more general problem statement to address a scenario in which a multi-agent system of heterogeneous agents can find consensus and output regulation in a fully distributed manner.

In particular, we assume a heterogeneous linear and time-invariant multi-agent system governed by the general dynamics,

$$\begin{aligned}\dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) + D_i w_i(t) + \sum_{j \in \mathcal{N}_i} E_j x_j(t - \tau_{ij}) \\ y_i(t) &= C_i x_i(t)\end{aligned}\tag{2.15}$$

where $i \in \mathcal{N} := \{1, \dots, N\}$ and where $x_i \in \mathbb{R}^{N_{x_i}}$ denotes the state vector, $u_i \in \mathbb{R}^{N_{u_i}}$ denotes the command vector, $w_i \in \mathbb{R}^{N_{w_i}}$ denotes a vector of bounded unknown disturbances, $x_j \in \mathbb{R}^{N_{x_j}}$ is the cross-coupling state information of neighbour j , and $\tau_{ij} \in \mathbb{R}^+$ is an arbitrary time delay in transmission of information from agent j to i , and finally $y_i \in \mathbb{R}^{N_{y_i}}$ denotes the output vector of the i^{th} agent, where matrices A_i, B_i, D_i, E_j and C_i have appropriate dimensions.

The objective would be to design a control methodology for all the agents $i \in \mathcal{N}$ under the system model in (2.19) to achieve output consensus for all bounded disturbances w_i , arbitrary time delays τ_{ij} , and DoS attacks on arbitrary agents with non-constrained durations, i.e., the objective is to have

$$\lim_{t \rightarrow \infty} \|y_i(t) - y_j(t)\| = 0, \forall i, j \in \mathcal{N}.\tag{2.16}$$

Additionally, in certain applications it might be required to ensure output regulation, where the objective is to find a control action $u_i(t)$ such that,

$$\lim_{t \rightarrow \infty} y_i(t) = y_i^{(d)}, \forall i \in \mathcal{N},\tag{2.17}$$

for all bounded disturbances w_i , and arbitrary unconstrained time delays τ_{ij} and DoS attacks.

The above is not an unidentified problem in the literature. There had been tremendous progress made recently to address the problem. However, the proposed methodologies and solutions each have fatal short comings. For example, the authors in [50] and [135] have considered the *cooperative output regulation* problem for heterogeneous linear multi-agent systems in the presence of communication constraints. Reference [50]

has investigated the *cooperative resilient output regulation* control problem with time-delay communication constraints for a specific class of heterogeneous MAS with uniform exogenous inputs (following a LTI dynamics with pure imaginary eigenvalues). Unfortunately, the work despite of solid theoretical results cannot be extended to general heterogeneous MAS systems.

In [47] the authors have presented a distributed secondary control scheme for power allocation and voltage restoration in islanded DC micro-grids employing MAS consensus control techniques. The conditions for “consensusability” in linear homogeneous MASs has been presented in [48, 49], where output feedback consensus protocols were given, and the closed-loop MAS was shown to be achieving asymptotic consensus if the topology had a spanning tree. Output consensus for heterogeneous MAS with Markovian switching network topologies has been discussed in [136], and can be used as the basis for studying MAS under DoS cyberattacks assuming that DoS attacks can be represented as switching topologies. The paper however does not address cases where communication restraints impede timely delivery of data packets. The subject of distributed consensus of heterogeneous MAS subject to switching topologies and communication time-delays has been published very recently in [137] with a focus on power systems, and serves as a novel approach due to its relatively comprehensive coverage. The paper provides a solution for stability and control of heterogeneous MAS systems considering a switching controller that alters the controller gain based on the knowledge that a time-delay attack has taken place. The condition for achieving consensus is non-infinite communication delays, which can be considered an admissible condition. However, the problem that has to be simultaneously considered is the determination of a methodology that automatically detects the onset of a time-delay attack. The authors in [135] have very recently addressed the same subject for a class of CPS systems with non-uniform but bounded communication delays under denial-of-service (DoS) attacks, where a switching resilient control approach is proposed. However, the existence of a solution for all time-delays cannot be guaranteed, and additionally the controller is only functional for DoS attacks (where agents are assumed to understand “missing” information from neighbour agents) but not delay attacks.

Due to the limitations addressed above, it seems that the objectives in (2.16) and (2.17) require more serious effort, in order to be able to securely operate CPS under telecommunication time-delays and DoS. The next section provides a more general solution for this problem.

2.3 Time-Delay Resilient Cooperative Filters for Cyber-Physical Systems

2.3.1 Definitions and Assumptions

Let us consider an interconnected CPS $\mathcal{S}$, and its N constituent subsystems $\mathcal{S}_i \subset \mathcal{S}$, $i \in \{1, 2, \dots, N\}$, hereinafter referred to as “subsystems”. Generally, subsystems in a CPS may (or may) not involve states that are shared with other subsystems.

Definition 2. We define an “exogenous state” as a shared state between dynamically coupled subsystems whose value is transmitted from one subsystem to another subsystem through a tele-communication channel. On the other hand “endogenous states” are defined as subsystem states when the coupling between the subsystems are removed. Therefore, one may assume that exogenous states are prone to cyberattacks, and endogenous states are immune against cyberattacks.

Exogenous states are distinct from exogenous signals in a sense that time-delays in exogenous states can cause instability in the systems. The dynamic couplings between the subsystems can be physical (such as in interconnected power systems) or non-physical (such as in automated air traffic systems in advanced air mobility).

Definition 3. Let $x_{j(\ell)} \in \mathbb{R}$ denote the ℓ^{th} state of $\mathcal{S}_j$, and $x_{j(\ell),i} \in \mathbb{R}$ denote the value of $x_{j(\ell)}$ after transmission to $\mathcal{S}_i$, and $x_{j,i}$ denote the exogenous state vector of $\mathcal{S}_i$ that is transmitted from $\mathcal{S}_j$ to $\mathcal{S}_i$. In a delayed communication system $x_{j(\ell),i}(t) = x_{j(\ell)}(t - \tau_{j,i})$ and $x_{j,i}(t) = x_j(t - \tau_{j,i})$, where $\tau_{j,i} \in \mathbb{R}^+$ is a random time-delay of the communication link from $\mathcal{S}_j \rightarrow \mathcal{S}_i$. Therefore, $x_i + \sum_{\mathcal{S}_j} x_{j,i}$ represents the full state vector of $\mathcal{S}_i$ which is the sum of the endogenous (i.e., x_i) and exogenous states $\sum_{\mathcal{S}_j} x_{j,i}$.

When the subsystems in a CPS are dynamically coupled, in order to model subsystem dynamics the state of other subsystems involve. One can imagine a very heavy load that is chained and transported by multiple helicopters, or a power system that involves interconnected power areas, which are examples of physically and dynamically coupled subsystems. Autonomous air traffic control in urban air mobility is another example where the coupling between subsystems are non-physical.

Remark 2. It is generally problematic to model a dynamically coupled CPS in which randomly time-delayed exogenous states are involved, and where the dynamic model of the subsystems are unavailable to other subsystems.

In this article we consider a multi-agent system framework in order to facilitate time-delay recovery in the CPS. Therefore, we consider an undirected graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{A})$

where $\mathcal{N}$ is the set of nodes representing N number of subsystems (or agents), $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$ as the set of edges (or communication links between the subsystems), and $\mathcal{A} = [a_{ij}]_{N \times N}$, $a_{ij} \in \{0, 1\}$, representing the adjacency matrix. The elements of $\mathcal{A}$ are defined such that $a_{ij} = 1$, if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$, if $(i, j) \notin \mathcal{E}$. Let $\mathcal{N}_i$ denote the neighbour set of agent i (where, $a_{ij} = 1$). The Laplacian matrix $L := \mathcal{D} - \mathcal{A} = [\ell_{ij}] \in \mathbb{R}^{n \times n}$, associated to $\mathcal{G}$ is defined such that,

$$\ell_{ii} = \sum_{j=1}^n a_{ij}, \quad \ell_{ij} = -a_{ij}, \quad \text{for } i \neq j, \quad (2.18)$$

where $\mathcal{D} = [\ell_{ii}]$ is the diagonal in-degree matrix. Generally, a heterogeneous linear subsystem $\mathcal{S}_i \subset \mathcal{S}$ with a time-delay tele-communication system can be defined by the equations,

$$\begin{aligned} \dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t) + D_i w_i(t) + \sum_{j \in \mathcal{N}_i} E_{j,i} x_{j,i}(t), \\ y_i(t) &= C_i x_i(t) + \sum_{j \in \mathcal{N}_i} C_{j,i} x_{j,i}(t), \end{aligned} \quad (2.19)$$

where $x_{j,i}(t) \in \mathbb{R}^{N_{x_i}}$ denotes the exogenous states of $\mathcal{S}_i$ according to Definition 3. Furthermore, $x_i \in \mathbb{R}^{N_{x_i}}$ denotes the endogenous state vector of $\mathcal{S}_i$, $u_i \in \mathbb{R}^{N_{u_i}}$ denotes the local control command vector, and $w_i \in \mathbb{R}^{N_{w_i}}$ denotes a vector of bounded unknown disturbances, and finally $y_i \in \mathbb{R}^{N_{y_i}}$ denotes the output vector of $\mathcal{S}_i$, where matrices $A_i, B_i, D_i, E_{j,i}$ and $C_{j,i}$ have appropriate dimensions. System matrices are such that when there is no time-delay present in the tele-communication system Equation (2.19) could be represented as,

$$\dot{x}_i(t) = (A_i + \sum_{j \in \mathcal{N}_i} E_{j,i})(x_i(t) + x_{j,i}(t)) + B_i u_i(t) + D_i w_i(t),$$

as later exemplified in Remark 7 (in Section 3.3.7).

Definition 4. *Time-delay resiliency in a CPS is defined as a condition where $|x_{j(\ell),i}(t) - x_{j(\ell)}(t)| < \epsilon$, $\forall i, j \in \mathcal{N}$, $\forall \ell \in \{1, 2, \dots, N_{x_i}\}$, and for all $t > \tau_{j,i} > 0$, where $\epsilon \in \mathbb{R}^+$ is an arbitrarily small number, where from Definition 3 we had $x_{j(\ell),i}(t) = x_{j(\ell)}(t - \tau_{j,i})$.*

Assumption 2. *We assume that the network $\mathcal{G}$ is a connected network with N agents, where all subsystems are stable when there is no time-delay in the tele-communication channels. In other words, the endogenous states $x_{i(\ell)}$ are continuous Lipchitz functions of time, and there exists a small $\epsilon \in \mathbb{R}^+$, such that $|x_{i(\ell)}(t) - x_{i(\ell)}(t - T_s)| < \epsilon$, for an arbitrarily small $T_s \in \mathbb{R}^+$.*

Assumption 3. *Let us assume that $(A_i + \sum_{j \in \mathcal{N}_i} E_{j,i}, B_i)$ constitute a controllable pair, and $(A_i + \sum_{j \in \mathcal{N}_i} E_{j,i}, C_i + \sum_{j \in \mathcal{N}_i} C_{j,i})$ constitute an observable pair, for all $\mathcal{S}_i \subset \mathcal{S}$.*

Assumption 4. We assume that a Denial of Service (DoS) attack on agent i from j is equivalent to the condition $a_{ij} = 0, j \in \mathcal{N}_i$ in a finite duration in time. This is due to the fact that $a_{ij} = 0$ is equivalent to the edge (i, j) being removed from $\mathcal{E}$, implying no communication service from j to i , hence DoS on i from j .

2.3.2 The LFC Example

The LFC example clarifies the definitions introduced in the previous section, and explains the complexities behind modelling of a general CPS. We use the model explained in Problem 2.2.1 for the states in a generating station $\mathcal{S}_i$ as $x_i = [\Delta f_i, \Delta P_{m_i}, \Delta P_{v_i}, \Lambda_i, \Delta P_{ij}]^T \in \mathbb{R}^5$, where $\text{ACE} = K_i B_i \Delta f_i + K_i \Delta P_{ij}$, and the interconnecting tie-line power, respectively, as in Figure 2.9, where,

$$\Lambda_i(t) = \int_{s=0}^t K_i B_i \Delta f_i(s) + K_i \Delta P_{ij}(s) ds, \quad (2.20)$$

$$\Delta P_{ij}(t) = 2\pi T_{ij} \int_{s=0}^t [\Delta f_i(s) - \Delta f_j(s)] ds, \quad (2.21)$$

The objective of the LFC as the name implies is to control the area frequency with respect to changes in ΔP_{d_i} , while maintaining the preset amount of energy exchange between the areas (i.e., P_{ij}). In other words, the objective of the LFC is that,

$$\lim_{t \rightarrow \infty} |\Delta f_i(t)|^2 + |\Delta P_{ij}(t)|^2 \approx 0, \quad \forall \Delta P_{d_i}(t). \quad (2.22)$$

This is due to the fact that $P_{ij}(t)$ is often a time-varying contracted variable between two areas and is set by the main input $u_i(t)$ in Figure 2.9, where one area commits to supply a regulated amount of energy to the other area, irrespective of the variations in area load. Λ_i and ΔP_{ij} are exogenous states for $\mathcal{S}_i$, and the first three entries of x_i are endogenous states for $\mathcal{S}_i$. A time-delay cyberattack on the tele-communication channels of $\mathcal{S}_i$ causes the actual $\Lambda_i(t)$ to be observed by the controller in $\mathcal{S}_i$ as $\Lambda_i(t - \tau_{\Lambda_i})$, where $\tau_{\Lambda_i} \in \mathbb{R}^+$ is an unknown random time-delay. Similarly, let P_{ij} denote the desirable power to be traded between $\mathcal{S}_i$ and its adjacent power area $\mathcal{S}_j$. The sensor collecting the instantaneous power $P_{ij} + \Delta P_{ij}(t)$ is often remote from the controller in $\mathcal{S}_i$. Therefore, the practice is to install Remote Terminal Units (RTUs) inside the power substations (controlling circuit breakers, disconnecter switches, and other electric apparatus associated with transmission lines) to continuously read $P_{ij} + \Delta P_{ij}(t)$ and transmit the value to the CCS through a tele-communication line for the computation of $\Lambda_i(t)$. However, the tele-communication time-delays result in $P_{ij} + \Delta P_{ij}(t - \tau_{P_{ij}})$, and $f_i + \Delta f_i(t - \tau_{f_i})$ being observed in the CCS. Therefore, time-delays $\tau_{P_{ij}}, \tau_{f_i} \in \mathbb{R}^+$ affect the computed value $\Lambda_i(t)$, and $\Lambda_i(t)$ is further delayed by τ_{Λ_i} to finally affect $x_i(t)$. In the LFC example of Figure 2.10, Λ 's

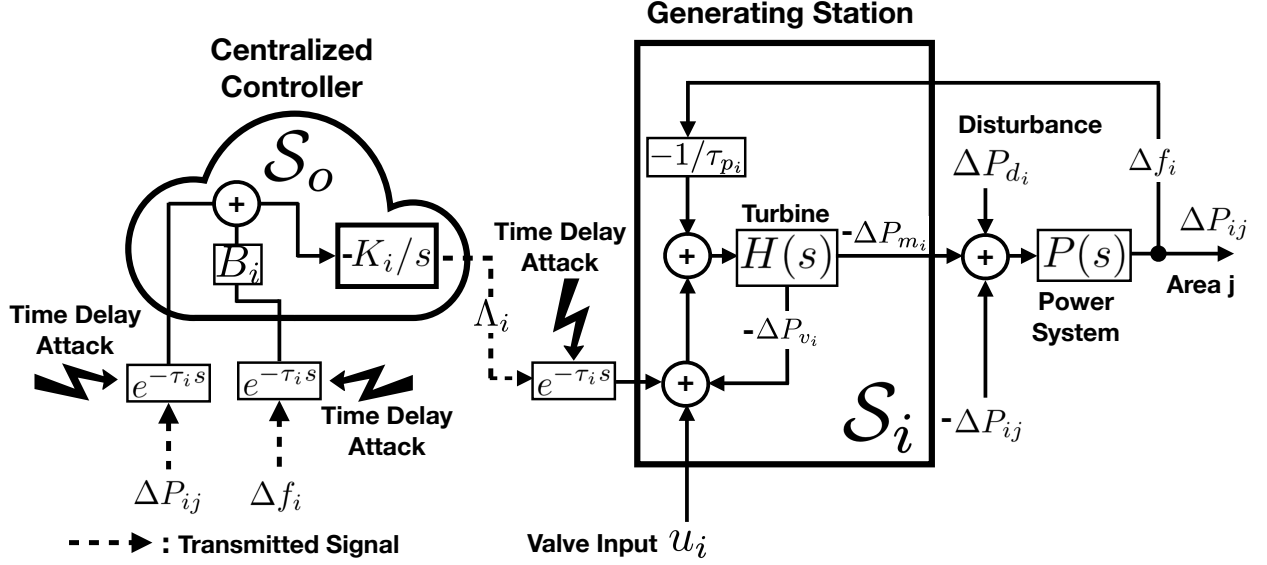


Figure 2.9: Block diagram of a frequency control mechanism for a generating station S_i contributing the LFC in a multi-area power system. The solid lines are hard-wired measurements/commands that are presumably immune from cyberattacks (as they are confined in S_i), where the dashed lines represent tele-metered data that are subject to TDS/DoS cyberattacks.

are the only exogenous states that are actually required by the generating areas for the operation. However, the CCS requires the tie-line power values (i.e., ΔP_{ij} 's) and the area frequencies Δf 's to compute the Λ 's. Figure 2.10 depicts the interconnection of the area generating stations in an LFC through power transmission lines and the flow of information, as an example of a CPS.

2.3.3 Problem Statement

Before we formally state the problem, let us note from the definitions and the assumptions that $x_{j(\ell)}(t) - \epsilon \leq x_{j(\ell),i}(t) \leq x_{j(\ell)}(t) + \epsilon$, $\forall j, \ell$, resulting $x_j(t) - \epsilon \vec{1}_{N_{x_i}} \leq x_{j,i}(t) \leq x_j(t) + \epsilon \vec{1}_{N_{x_i}}$, $\forall j$, where $\vec{1}_{N_{x_i}} \in \mathbb{R}^{N_{x_i}}$ is a vector of ones. Through substitution in Equation (2.19) it follows that,

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + \sum_{j \in N_i} E_{j,i} x_j(t) \pm \sum_{j \in N_i} E_{j,i} \mu \vec{1}_{N_{x_i}} + D_i w_i(t),$$

where $\mu \in \mathbb{R}^+$, $\mu \leq \epsilon$, and due to the controllability condition in Assumption 3 one would be able to design a feedback control law such as $u_i(t) = K_i x_i(t) + \sum_{j \in N_i} K_{j,i} x_{j,i}(t)$ using H_∞ methods, so that $\lim_{t \rightarrow \infty} \|y_i(t)\|^2 < \epsilon_{y_i}^2$, $\forall i$, and for an arbitrarily small $\epsilon_{y_i}^2 > 0$, ensuring stability of the CPS in a Lyapunov sense. This would be always possible since $\sum_{j \in N_i} E_{j,i} \mu \vec{1}_{N_{x_i}}$ could be considered as a small disturbance similar to $D_i w_i(t)$ and rejected through an appropriate state feedback. Therefore,

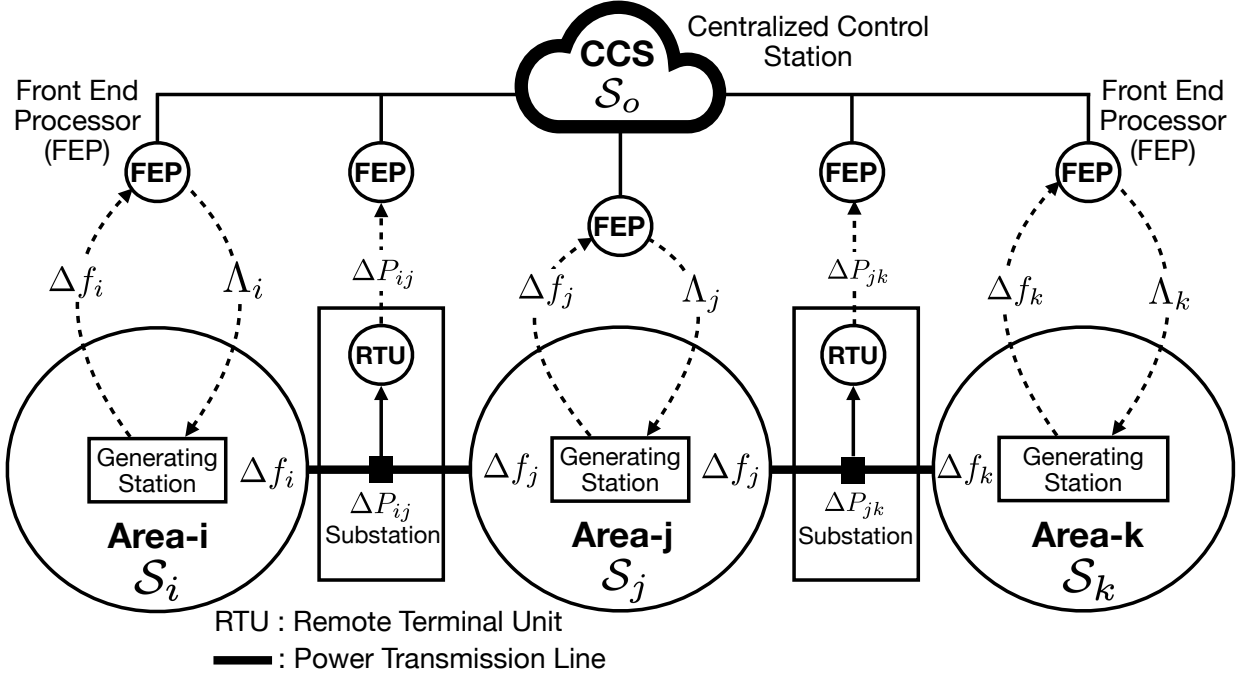


Figure 2.10: Schematics of a LFC power system with three area generating stations $\mathcal{S}_i, \mathcal{S}_j, \mathcal{S}_k$ and the Centralized Control Station $\mathcal{S}_o$. The CPS $\mathcal{S}$ in this figure can be represented as $\mathcal{S} = \{\mathcal{S}_i \cup \mathcal{S}_j \cup \mathcal{S}_k \cup \mathcal{S}_o \cup \mathcal{S}_{SS_{ij}} \cup \mathcal{S}_{SS_{jk}}\}$ where $\mathcal{S}_{SS_{ij}}, \mathcal{S}_{SS_{jk}}$ denote the two substations, each also considered as a subsystem of the CPS. The tele-communication system can be further regarded as a subsystem in a more comprehensive model. However, this is not considered in this section. The CCS $\mathcal{S}_o$ and the tele-communication system comprise the cyber part of the system that is responsible for the data collection and processing, and the power system comprises the physical part of the CPS. The Front-End Processors (FEPs) are electronic apparatus inside the CCS that transmit/receive tele-communication signals and demodulate the state variables. The Remote Terminal Unit (RTU) is a micro-scale FEP with a similar function located in every substation. ΔP_{ij} is a system state whose sensor (i.e., current and voltage power transformers) is located in a substation, and whose instantaneous value is transmitted to the CCS through an RTU. The CCS receives all $\Delta P, \Delta f$, and computes Λ for individual generating stations.

Remark 3. A time-delay resilient CPS as in Definition 4 guarantees stability of the CPS under all random time-delays $t > \tau_{j,i} > 0$, including the objective in Equation (2.22).

Let $\mathcal{G}$ denote a connected graph of a CPS $\mathcal{S} = \mathcal{S}_o \cup \mathcal{S}_i \cup \mathcal{S}_j \cup \dots$ with random communication delays between the constituent subsystems $o, i, j, \dots$. Let $x_{o(\ell)}(t) \in \mathcal{S}_o \subset \mathcal{S}$ be an endogenous state of $\mathcal{S}_o$ to be transmitted to all other subsystems $\mathcal{S}_i, \mathcal{S}_j, \dots$, and let $x_{o(\ell),i}(t), x_{o(\ell),j}(t), \dots$ denote the delayed value of $x_{o(\ell)}(t)$ at $\mathcal{S}_i, \mathcal{S}_j, \dots$, respectively, where $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i}), x_{o(\ell),j}(t) = x_{o(\ell)}(t - \tau_{o,j}), \dots$

The problem is to recover the real-time value of $x_{o(\ell)}(t)$ at all recipient subsystems $\mathcal{S}_i, \mathcal{S}_j, \dots$, with an arbitrarily negligible time-delay T_s , by cooperatively filtering of the delayed signals. In particular, the objective is to find an LTI filter with impulse response $h(t)$ so that,

$$x_{o(\ell)}(t - T_s) = (\alpha_i x_{o(\ell),i}(t) + \sum_{j \in \mathcal{N}_i} \alpha_j x_{o(\ell),j}(t - \tau_{j,i})) * h(t), \quad (2.23)$$

for all $\mathcal{S}_i \subset \mathcal{S}$, where α 's are real constant coefficients, $T_s > 0$ is an arbitrarily small transient time for the filter $h(t)$, and where $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$ is the input of the filter, and $x_{o(\ell),j}(t) = x_{o(\ell),j}(t - \tau_{o,j})$, $\forall j \in \mathcal{N}_i$ are auxiliary inputs from the neighbouring subsystems of $\mathcal{S}_i$.

Definition 5. A CPS that incorporates the exchange of information among constituent subsystems in order to achieve a common goal (i.e., time-delay resiliency) in a distributed system framework is referred to as a Multi Agent System (MAS), and the processing component (e.g., the filter) in each subsystem that involves the exchange of information is referred to as an "agent". Therefore, the cooperative filter proposed in Equation (2.23) is a MAS.

2.3.4 Research Results for Section 2.3

The multi-agent filtering structure in Figure 3.5 guarantees time-delay resiliency in the CPS despite of the random time-delay cyberattacks on the communication channels, and the objective is to attain the real-time value of a state $x_{o(\ell)}(t) \in \mathcal{S}_o$ in agent $\mathcal{S}_i$. The filters $h(t)$ are identical in all agents and are located immediately after the data receivers. The internal block diagram of the filter $h(t)$ is as shown in the box for $\mathcal{S}_i$ where the input $x_{o(\ell),i}(t)$ can be $x_{o(\ell)}(t - \tau_{o,i})$ if there is a direct communication link between $\mathcal{S}_o \rightarrow \mathcal{S}_i$, or any arbitrary conjecture available to $\mathcal{S}_i$. The output of the filter is $x_{o(\ell),i}(t + \Delta t)$ where Δt is a controllable transient time for the filter that can be arbitrarily adjusted through the filter gain γ , and is fed to the internal controller in $\mathcal{S}_i$ and simultaneously shared with the neighbouring agents. The interesting and important characteristic of the multi-agent filtering scheme is that the outputs of all filters will become identical after lapse of the filter transients and within a negligible settling time $T_s > 0$. In particular, for any arbitrary set of inputs $x_{o(\ell),1}(t), x_{o(\ell),2}(t), \dots, x_{o(\ell),N}(t)$ one will have,

$$\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell),j}(t + \Delta t), \quad \forall i, j \in \{1, \dots, N\},$$

regardless of the time delays in the tele-communication channels. Consequently, if any single agent such as $\mathcal{S}_o$ temporarily maintains its output at $x_{o(\ell)}(t + \Delta t) = x_{o(\ell)}(t)$, $T_s \geq \Delta t \geq 0$, then it follows that,

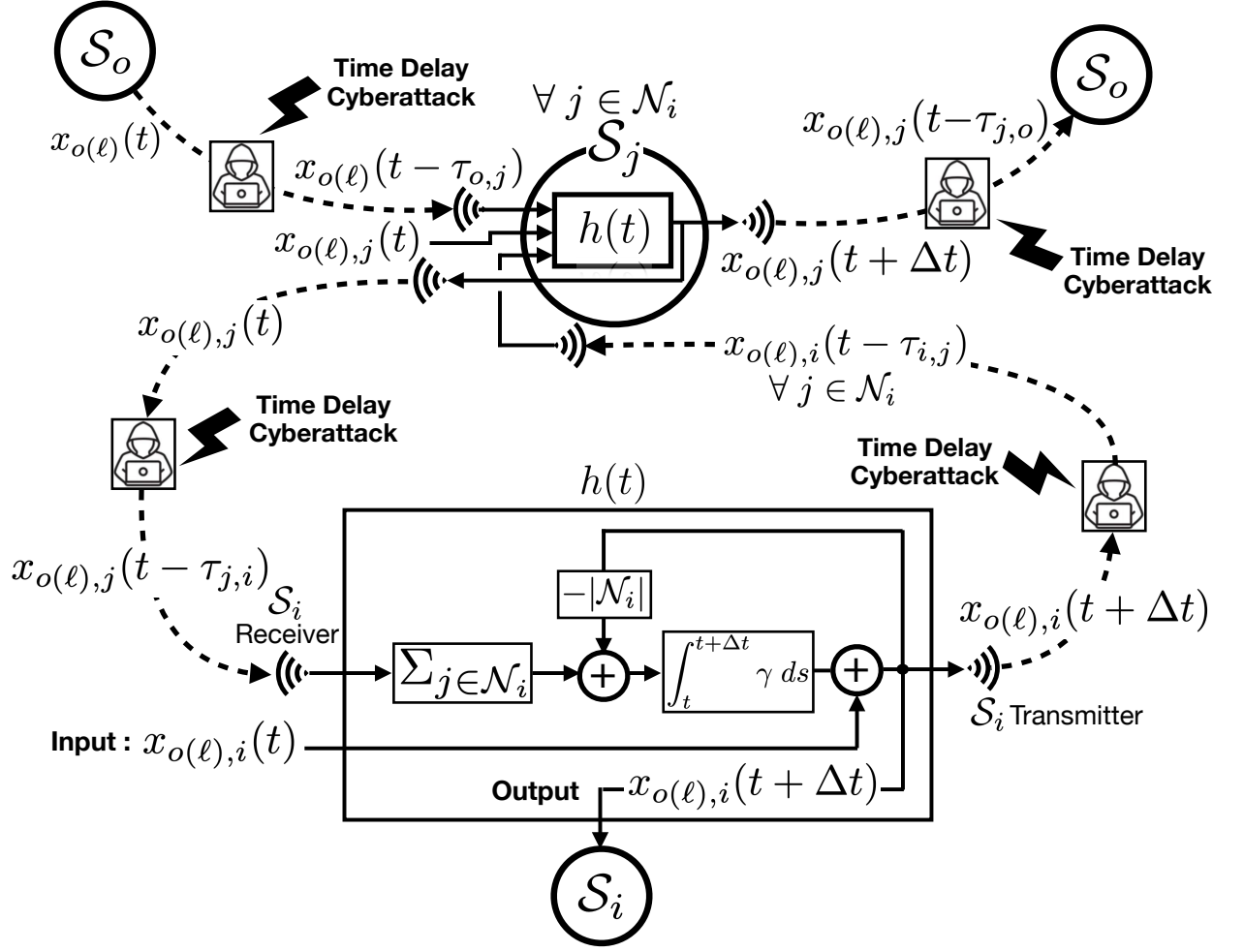


Figure 2.11: Schematics of a MAS time-delay resilient CPS, and the schematics of the cooperative filter $h(t)$. The agents in the MAS exchange information in order to recover a time-delayed state $x_{o(\ell)}(t) \in \mathcal{S}_o$. $x_{o(\ell),i}(t) = x_{o(\ell)}(t - \tau_{o,i})$ is the input of the filter in $\mathcal{S}_i$ (if $o \in \mathcal{N}_i$, or can be any other conjecture available to $\mathcal{S}_i$ which needs not be a correct estimate), and the output of the filter is $x_{o(\ell),i}(t + \Delta t)$, where $\Delta t > 0$ is a small response time. It will be shown that $\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t)$, where T_s is a negligible arbitrary settling time for the filter that will be controlled by the filter gain $\gamma \in \mathbb{R}^+$.

$$\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t), \forall i \in \mathcal{N}, \quad (2.24)$$

which satisfies the objective in Equation (2.23). This implies that any single agent in the MAS such as $\mathcal{S}_o$ where its output follows its input for a time period $T_s \geq \Delta t \geq 0$ will act as the leader in the MAS and all other agents in $\mathcal{S}$ will follow and track the output $x_{o(\ell)}(t)$. More specifically,

Remark 4. The connected MAS shown in Figure 2.11 will achieve consensus as in Equation (2.24) regardless of the time-delays in the tele-communication links, and the consensus value will be equal to the output of the leader only if there is a single leader

such as $\mathcal{S}_o$ available in the MAS, and where the leader is characterized by the equation $\dot{x}_{o(\ell)}(t + \Delta t) = 0, \forall T_s \geq \Delta t \geq 0$.

Remark 5. Clearly, realization of time-delay resiliency through the cooperative filters $h(t)$ does not involve dynamic models of the subsystems (as it is evident from Figure 2.11). Furthermore, T_s can be arbitrarily reduced to improve the error ϵ in Definition 4 by increasing the filter gain γ (the relationship between γ and T_s is later formulated in Section 3.3.6). Finally, cooperative filters are components that can be added to existing communication systems without necessary modifications to the existing subsystems. These characteristics are unique advantages that would make the presented technique an ideal solution for CPS time-delay security.

In case there are multiple leaders in the MAS the consensus output will be the centroid of the leaders outputs. In what follows the statement in Remark 4 will be justified mathematically, which constitutes firstly, proof of the stability of the MAS filter scheme in the presence of time-delays, and secondly, the output consensus of the MAS under all random time-delays. The following equations can be derived from the schematics of $h(t)$ in Figure 2.11.

$$x_{o(\ell),i}(t + \Delta t) = x_{o(\ell),i}(t) + \gamma \int_t^{t+\Delta t} \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(s - \tau_{j,i}) - x_{o(\ell),i}(s)) ds,$$

or,

$$\begin{aligned} \dot{x}_{o(\ell),i}(t + \Delta t) - \dot{x}_{o(\ell),i}(t) = & \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t + \Delta t - \tau_{j,i}) - x_{o(\ell),i}(t + \Delta t)) \\ & - \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t - \tau_{j,i}) - x_{o(\ell),i}(t)) \end{aligned}$$

which follows that,

$$\dot{x}_{o(\ell),i}(t) = \gamma \sum_{j \in \mathcal{N}_i} (x_{o(\ell),j}(t - \tau_{j,i}) - x_{o(\ell),i}(t)), \forall t > 0, i \in \mathcal{N}, \quad (2.25)$$

In order to simplify the notations let $\eta_i \triangleq x_{o(\ell),i}, \forall i \neq o \in \mathcal{N}$ and $\eta_o \triangleq x_{o(\ell)}$. With this simplification, the input/output equation of the MAS in Figure 2.11 reduces in a compact form to,

$$\dot{\eta}(t) = -\gamma \mathcal{D} \eta(t) + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji} \eta(t - \tau_{j,i}), \quad (2.26)$$

where $\mathcal{D}$ is the diagonal in-degree matrix as defined earlier, $\eta = [\eta_1, \dots, \eta_N]^T$, and $\mathcal{A}_{ji}$ is the adjacency matrix of the nodes with time delay $\tau_{j,i}$, where $\mathcal{A} = \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji}$. Note that in case of no time delay, the input-output relation of Figure 2.11 could be simply represented as $\dot{\eta}(t) = -\gamma L \eta(t)$, where the Laplacian matrix would be $L = \mathcal{D} - \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \mathcal{A}_{ji}$.

Lemma 2. For a connected MAS $\mathcal{S}$ with no time-delays, the cooperative filter in Figure 2.11 with a sufficiently large gain $\gamma > 0$ ensures that $|\eta_i - \eta_o| < \epsilon$, as $\Delta t \rightarrow T_s$, $\forall \mathcal{S}_i \subset \mathcal{S}$, if $x_{o(\ell)} \in \mathcal{S}_o \subset \mathcal{S}$ is not filtered, while all other agents $\mathcal{S}_i, \mathcal{S}_j, \dots \subset \mathcal{S}$ use $h(t)$ to filter their inputs as depicted in the figure.

The proof is straightforward and can be found in standard MAS textbooks. The implication of Lemma 2 is that the schematics in Figure 2.11 guarantees that the agents filter outputs simultaneously converges to $x_{o(\ell)}(t)$ if all the agents except $\mathcal{S}_o$ use $h(t)$ to filter their inputs, and if the output of $\mathcal{S}_o$ is simply connected to the input of $\mathcal{S}_o$, when there is no time-delay in the system. Theorem 3 and Theorem 5 below will prove that this would be the case even if there is a time-delay in the communication channels, and this would prove time-delay resiliency of the MAS in Figure 2.11. The condition $\|\lim_{\Delta t \rightarrow T_s} \eta(t + \Delta t) - \eta(t)\| < N\epsilon$ would be equivalent to $\|\lim_{t \rightarrow \infty} \eta(t) - \eta(0)\| < N\epsilon$ for an arbitrarily small T_s and a sufficiently large γ .

Theorem 3. Given the connected MAS $\mathcal{S}$ in Figure 2.11, the time-delayed system in Equation (2.26) is marginally stable (i.e., $\|\eta(t)\|^2$ remains bounded) for all finite time-delays, and all $\gamma > 0$.

Proof. Assume the Lyapunov candidate function,

$$V(\eta) = \|\eta(t)\|^2 + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \int_{t-\tau_{ji}}^t \|\eta(\xi)\|^2 d\xi. \quad (2.27)$$

In order to prove the theorem it would be sufficient to show that $\dot{V}(\eta) \leq 0$, since in this case $V(t) \leq V(0)$, $\forall t > 0$, or $\|\eta(t)\|^2 \leq \|\eta(0)\|^2$, $\forall t > 0$, or $\sum_{i=1}^N \eta_i^2(t) \leq \|\eta(0)\|^2$, $\forall t > 0$, implying boundedness of $\eta_i(t)$, $\forall i \in \mathcal{N}$. However, from Equation (2.27) it follows that,

$$\begin{aligned} \dot{V}(\eta) &= -2\gamma \eta^T(t) \mathcal{D} \eta(t) + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \eta^T(t) \mathcal{A}_{ji} \eta(t - \tau_{j,i}) \\ &\quad + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \eta^T(t - \tau_{j,i}) \mathcal{A}_{ji}^T \eta(t) \\ &\quad + \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \|\eta(t)\|^2 - \gamma \sum_{i=1}^N \sum_{j \in \mathcal{N}_i} \|\eta(t - \tau_{j,i})\|^2, \end{aligned}$$

which can be written in a compact form as,

$$\dot{V}(\eta) = -\gamma [\eta^T(t) \eta^T(t - \tau_1) \cdots \eta^T(t - \tau_N)]$$

$$\begin{bmatrix} 2\mathcal{D} - \sum_{i=1}^N \Gamma_i & -\mathcal{A}_1 & \cdots & -\mathcal{A}_N \\ -\mathcal{A}_1^T & +\Gamma_1 & \cdots & 0_{N \times N} \\ \vdots & \vdots & \ddots & \vdots \\ -\mathcal{A}_N^T & 0_{N \times N} & \cdots & +\Gamma_N \end{bmatrix} \begin{bmatrix} \eta(t) \\ \eta(t - \tau_1) \\ \vdots \\ \eta(t - \tau_N) \end{bmatrix}$$

where, $\eta(t - \tau_i) = [\eta^T(t - \tau_{1,i}), \dots, \eta^T(t - \tau_{N,i})]^T$, excluding $\eta^T(t - \tau_{i,i})$, and $\mathcal{A}_i = [\mathcal{A}_{1i}, \dots, \mathcal{A}_{Ni}]$, excluding $\mathcal{A}_{ii}$, and $\Gamma_i = \mathbf{Diag}(\Gamma_{1i}, \dots, \Gamma_{Ni})$, excluding Γ_{ii} , where $\Gamma_{ji} = \mathbf{Diag}(0, \dots, a_{ij}, \dots, 0)$ is a diagonal matrix with all entries being zeros except $[\Gamma_{ji}]_{jj} = a_{ij}$. Therefore, one can write,

$$\begin{aligned} \dot{V}(\eta) &= -\gamma [\eta^T(t) \eta^T(t - \tau_1) \cdots \eta^T(t - \tau_N)] \\ \check{L}_\tau [\eta^T(t) \eta^T(t - \tau_1) \cdots \eta^T(t - \tau_N)]^T \end{aligned} \quad (2.28)$$

where it is denoted that,

$$\check{L}_\tau \triangleq \begin{bmatrix} 2\mathcal{D} - \sum_{i=1}^N \Gamma_i & -\mathcal{A}_1 & \cdots & -\mathcal{A}_N \\ -\mathcal{A}_1^T & +\Gamma_1 & \cdots & 0_{N \times N} \\ \vdots & \vdots & \ddots & \vdots \\ -\mathcal{A}_N^T & 0_{N \times N} & \cdots & +\Gamma_N \end{bmatrix}$$

and the sufficient condition for marginal stability is to have $\check{L}_\tau \geq 0$. We use the Gershgorin disk theorem to evaluate the eigenvalues of $\check{L}_\tau$, which states that “if $M = [m_{ij}]$ is an $m \times m$ real matrix, then all the eigenvalues of M are located in the union of the following sets”,

$$\cup_i \{z \in \mathbb{C} \mid |z - m_{ii}| \leq \sum_{j=1, \dots, m}^{j \neq i} |m_{ij}|\}.$$

Figure 2.12 is an illustration of the spectrum of $\check{L}_\tau$ according to the Gershgorin disk theorem, where each disk corresponds to one row in $\check{L}_\tau$, and encloses an eigenvalue of $\check{L}_\tau$. Therefore, the eigenvalues of $\check{L}_\tau$ are encapsulated by the union of the disks illustrated in Figure 2.12.

Consequently, the condition $\check{L}_\tau \geq 0$ is equivalent to satisfying the following conditions simultaneously,

$$\begin{cases} 1) & 2|\ell_{ii}| - \sum_{i=1}^N [\Gamma_i]_{ii} \geq |\ell_{ii}|, \quad \forall i \in \mathcal{N}, \\ 2) & |[\Gamma_{ji}]_{jj}| \geq a_{ij}, \quad \forall i \neq j \in \mathcal{N}, \end{cases}$$

or,

$$\begin{aligned} \check{L}_\tau \geq 0 &\equiv \\ \begin{cases} 1) & |\ell_{ii}| \geq \sum_{i=1}^N [\Gamma_i]_{ii}, \quad \forall i \in \mathcal{N}, \\ 2) & |[\Gamma_{ji}]_{jj}| \geq a_{ij}, \quad \forall i \neq j \in \mathcal{N}, \end{cases} \end{aligned}$$

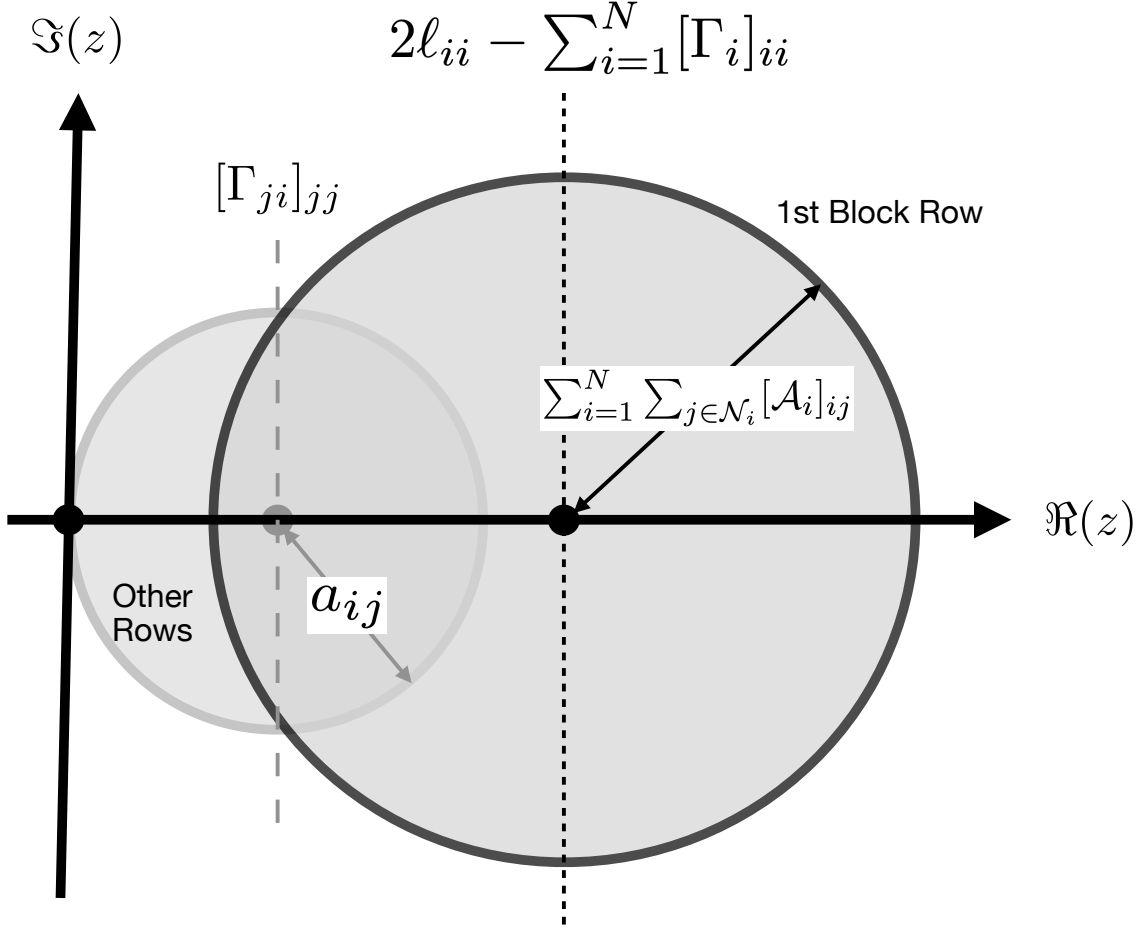


Figure 2.12: Spectrum of $\check{L}_\tau$ with reference to the Gershgorin disk theorem, is the union of several disks where each disk corresponds to a row in $\check{L}_\tau$. The bigger circle represents the first N rows, referred to as the first block row, where the center of the disk is on the real axis and at $2\ell_{ii} - \sum_{i=1}^N [\Gamma_i]_{ii}$ to the right, with a radius ℓ_{ii} . The smaller disk represents the set of other block rows where each row is represented by a disk with its center on the real axis at $|\Gamma_{ji}|_{jj}$ and a radius a_{ij} , and a set of null disks located at the origin.

where the second condition always hold since $|\Gamma_{ji}|_{jj} = a_{ij}$. On the other hand $\sum_{i=1}^N [\Gamma_i]_{ii} = \sum_{i=1}^N [\mathbf{Diag}(\Gamma_{1i}, \Gamma_{2i}, \dots, \Gamma_{Ni})]_{ii} = \sum_{j \in \mathcal{N}_i} a_{ij}$, where $\sum_{j \in \mathcal{N}_i} a_{ij} = \ell_{ii}$, validating the first condition for all i . In conclusion, for all finite $t > \tau_{ji} > 0$ one may assume $\check{L}_\tau \geq 0$, which completes the proof of the theorem. $\blacksquare$

Theorem 4 below will examine consensus in a delayed cyber-system that is governed by the control protocol in Theorem 3.

Theorem 4. *The connected MAS with finite time-delays in Theorem 3 achieves consensus. In other words, there exists some $\kappa \in \mathbb{R}$, such that $\eta(t - \tau) \rightarrow \kappa \vec{\mathbf{1}}$, $\forall t > \tau > 0$, as $t \rightarrow \infty$, where $\vec{\mathbf{1}}$ is a column vector with all unit entries.*

Proof. One can prove consensus if firstly, $\eta = [\eta^T(t) \ \eta^T(t - \tau_1) \ \dots \ \eta^T(t - \tau_N)]^T = \kappa \vec{\mathbf{1}}$ at

$\dot{V} = 0$ (i.e., the equilibrium), and secondly, if the equilibrium point is only at the point $\eta = \kappa \vec{\mathbf{1}}$. Therefore, consensusability would be equivalent to the condition, where firstly, the sum of all the entries in every row of $\check{L}_\tau$ is zero, and secondly, if $\eta \neq \kappa \vec{\mathbf{1}} \Rightarrow \dot{V} \neq 0$.

In Theorem 3, it was specified that $\mathcal{A}_i = [\mathcal{A}_{1i}, \mathcal{A}_{2i}, \dots, \mathcal{A}_{Ni}]$, and $\Gamma_i = \mathbf{Diag}(\Gamma_{1i}, \Gamma_{2i}, \dots, \Gamma_{Ni})$, $[\Gamma_{ji}]_{jj} = a_{ij}$ (with every other entry being zero), and $[\mathcal{A}_{ji}]_{ji} = a_{ij}$ (with every other entry being zero). This implies that $\vec{\mathbf{1}}^T(\Gamma_{ji} - \mathcal{A}_{ji}) = 0$ and $(\Gamma_{ji} - \mathcal{A}_{ji})\vec{\mathbf{1}} = 0$, or $\vec{\mathbf{1}}^T(\Gamma_i - \mathcal{A}_i) = 0$, and $(\Gamma_i - \mathcal{A}_i)\vec{\mathbf{1}} = 0$, $\forall i \in \mathcal{N}$. On the other hand, since $(\mathcal{D} - \sum_{i=1}^N \mathcal{A}_i)\vec{\mathbf{1}} = \vec{\mathbf{0}}$, and $\mathcal{D} = \sum_{i=1}^N \Gamma_i$, it follows that, $(2\mathcal{D} - \sum_{i=1}^N \Gamma_i - \sum_{i=1}^N \mathcal{A}_i)\vec{\mathbf{1}} = \vec{\mathbf{0}}$, and finally, $\vec{\mathbf{1}}^T \check{L}_\tau = 0$ and $\check{L}_\tau \vec{\mathbf{1}} = 0$, which proves that $\kappa \vec{\mathbf{1}}$ is an equilibrium for V . On the other hand, since $\eta = \kappa \vec{\mathbf{1}}$ is the only solution for $(2\mathcal{D} - \sum_{i=1}^N \Gamma_i - \sum_{i=1}^N \mathcal{A}_i)\eta = \vec{\mathbf{0}}$, it follows that $\kappa \vec{\mathbf{1}}$ is the only equilibrium for the system, which completes the proof of the theorem. ■

Theorem 5. *A time-delayed connected MAS with the cooperative filter scheme in Figure 2.11 is time-delay resilient with respect to $x_{o(\ell)}(t) \in \mathcal{S}_o \subset \mathcal{S}$ against all bounded time-delay attacks, if $x_{o(\ell)}(t)$ is the output of $\mathcal{S}_o$. In other words $\lim_{\Delta t \rightarrow T_s} x_{o(\ell),i}(t + \Delta t) = x_{o(\ell)}(t)$, $\forall i \in \mathcal{N}$.*

Proof. The proof of this theorem results from the fact that consensus in any connected MAS with one and only one agent (such as Agent-0) having unchanged output, implies all filter outputs to approach the output of the unchanged filter, as expressed in the following remark.

Remark 6. *For a connected MAS network with no time-delays, the control law $\dot{\eta}_i = \sum_{j=0}^N a_{ij}(\eta_j - \eta_i)$, and $\dot{\eta}_0 = 0$, ensures that $\eta_i \rightarrow \eta_0$, as $t \rightarrow \infty$, $\forall i \in \mathcal{N}$. Obviously, the same applies for the case where η_i is a vector except that the control law has to be repeated for each entry in the vector. For the sake of simplicity in the notation, and without losing generality let us consider that the internal controller states η_i are scalars, and $\eta = [\eta_1, \dots, \eta_N]^T$.*

Proof. The controller state equations can be written in a compact form as,

$$\begin{bmatrix} \dot{\eta}_0 \\ \dot{\eta} \end{bmatrix} = - \begin{bmatrix} 0 & \vec{\mathbf{0}}^T \\ -\vec{D}_0 & L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0) \end{bmatrix} \begin{bmatrix} \eta_0 \\ \eta \end{bmatrix}$$

where $\vec{D}_0$ is a $N \times 1$ vector with entries 1 (if the corresponding agent is a neighbour of the leader), and 0 otherwise, and $L_{\mathcal{N}}$ is the Laplacian matrix associated with the nodes in $\mathcal{N}$. Let us also define $\delta_i = \eta_i - \eta_0$, and $\delta = [\delta_1, \dots, \delta_N]^T$. Then, one can write,

$$\dot{\delta} = \vec{D}_0 \eta_0 - (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0))\eta$$

$$\begin{aligned}
&= \vec{D}_0 \eta_0 - (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \vec{1} \eta_0 \\
&\quad - (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \eta + (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \vec{1} \eta_0 \\
&= \vec{D}_0 \eta_0 - (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \vec{1} \eta_0 - (L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \delta
\end{aligned}$$

where $\vec{D}_0 \eta_0 = \mathbf{Diag}(\vec{D}_0) \vec{1} \eta_0$ (since $\vec{D}_0 = \mathbf{Diag}(\vec{D}_0) \vec{1}$), and $L_{\mathcal{N}} \vec{1} \eta_0 = 0$ (since $L_{\mathcal{N}} \vec{1} = 0$), resulting that,

$$\dot{\delta} = -(L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0)) \delta.$$

However, $\mathbf{Diag}(\vec{D}_0) > 0$ if D_0 at least has one nonzero element (i.e., one or more agents connected to the leader). Therefore, $L_{\mathcal{N}} + \mathbf{Diag}(\vec{D}_0) > 0$, signifying that $\delta_i \rightarrow 0$ as $t \rightarrow \infty$, $\forall i \in \mathcal{N}$, or $\eta_i \rightarrow \eta_0$, $\forall i \in \mathcal{N}$. ■

Since cooperative filters with time-delayed inputs achieve consensus, where $\dot{x}_{o(\ell)}(t) = 0$, it follows that the output of every other filter in the MAS would follow $x_{o(\ell)}(t) = 0$. Specifically, the output of all the agents in Figure 2.11 at $t + T_s$ is necessarily equivalent regardless of the inputs at time t , and since the output of $\mathcal{S}_o$ is $x_{o(\ell)}(t) = x_{o(\ell)}(t + T_s)$, it follows that the output of all the filters at $t + T_s$ is $x_{o(\ell)}(t)$, which is a proof to the theorem. ■

As discussed in the Assumptions, a DoS cyberattack from agent i to j can be represented by the assumption $a_{ij} = 0$. Therefore, a DoS cyberattack on a random set of edges $\tilde{\mathcal{E}}_k \subset \mathcal{E}$ (where $\tilde{\mathcal{E}}_k$ represents the k^{th} attack on some edges) in the time duration $\tilde{T}_k$ would result a random subgraph $\tilde{\mathcal{G}}_k \subset \mathcal{G}$ and a new Laplacian matrix $\tilde{L}_k$ where, $\mathbf{eig}(\tilde{L}_k) \geq 0$.

Theorem 6. *The cooperative filter scheme in Figure 2.11 achieves asymptotic consensus under arbitrarily random DoS cyberattacks, if there is no infinite DoS attack that disconnects the graph.*

Proof. Let us denote that $\delta_i = \eta_i - \eta_o$, and $\delta = [\delta_1, \dots, \delta_N]^T$. Let us also denote the Laplacian matrix of the MAS comprising the leader $\mathcal{S}_o$ and the followers $\mathcal{S}_i$, $i \in \mathcal{N}$ as $\tilde{L}$. We have seen that for a non switching topology δ_i is asymptotically stable for all $i \in \mathcal{N}$. However, in case of random DoS attacks (refer to [152]) we assume that there are N_σ possible topologies that an adversary may inflict in the network as a result of DoS attack on one or more communication channels, including disconnections in the grid among the followers as well as the leader. Let us consider N_σ Laplacian matrices corresponding to each scenario, denoted by $\tilde{L}_1, \tilde{L}_2, \dots, \tilde{L}_{N_\sigma}$ where $\tilde{L}_i \geq 0$ (where $\mathbf{Rank}(\tilde{L}_i) = 0$ implies

disconnections in the network). Corresponding to each scenario $\tilde{L}_i$ let us consider a symmetric positive definite matrix P_i with the same dimension (i.e., $N \times N$), and let us additionally consider a Lyapunov function $V(\delta(t)) = \delta^T(t)P_i\delta(t)$.

We will further assume that a random switching scenario σ_k takes place for $t \in [t_k, t_{k+1})$ where $T_k = t_{k+1} - t_k$ is finite for all σ_k . In order to prove Theorem 6 it would be sufficient to prove that for an arbitrary σ_k and an arbitrary topology (denoted by $\tilde{L}_i$ and P_i), one could find a P_j up to the next switching scenario σ_{k+1} (with topology $\tilde{L}_j$) such that $V(\delta(t_{k+2})) < V(\delta(t_{k+1}))$. For this, one could simply derive $V(\delta(t_{k+1}))$ and $V(\delta(t_{k+2}))$ as,

$$V(\delta(t_{k+1})) = \delta^T(t_k)e^{-\tilde{L}_i^T T_k} P_i e^{-\tilde{L}_i T_k} \delta(t_k) \quad (2.29)$$

and,

$$V(\delta(t_{k+2})) = \delta^T(t_{k+1})e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} \delta(t_{k+1}). \quad (2.30)$$

Substituting $\delta(t_{k+1}) = e^{-\tilde{L}_i T_k} \delta(t_k)$ in Equation (2.30), one could obtain,

$$\begin{aligned} V(\delta(t_{k+2})) &= \\ \delta^T(t_k) e^{-\tilde{L}_i^T T_k} e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} e^{-\tilde{L}_i T_k} \delta(t_k). \end{aligned} \quad (2.31)$$

However, if

$$e^{-\tilde{L}_j^T T_{k+1}} P_j e^{-\tilde{L}_j T_{k+1}} < P_i$$

or equivalently,

$$P_j < e^{\tilde{L}_j^T T_{k+1}} P_i e^{\tilde{L}_j T_{k+1}} \quad (2.32)$$

then $V(\delta(t_{k+2})) < V(\delta(t_{k+1}))$, or simply $V(t_{k+2}) < V(t_{k+1})$, for all $t_{k+2} > t_{k+1}$, implying that $\dot{V}(t) < 0$, $\forall t > 0$, which further implies that $\delta(t) \rightarrow 0$, as $t \rightarrow \infty$, or $\eta_i(t) \rightarrow \eta_0$, $\forall i \in \mathcal{N}$, as $t \rightarrow \infty$.

This could always be possible even if $\tilde{L}_i = 0$ or $\tilde{L}_j = 0$, which proves that there always exists positive symmetric matrices $P_1, P_2, \dots$ for all $T_1, T_2, \dots$ such that the Lyapunov function uniformly decays for all scenarios σ_k , under the condition that a disconnection does not last infinitely, which completes the proof of the theorem. ■

2.3.5 Simulations and Case Studies

The results derived in Section 2.3.4 can be validated by examining the LFC problem discussed in Figure 2.10, when the CPS is under time-delay attacks and multiple tele-metered variables such as $\Delta P_{ij}, \Lambda_i, \Delta f_j$ are simultaneously attacked by different random

time-delays, and when ΔP_{d_i} is a random non-predictable bounded disturbance in the area load. To the best of the knowledge of this authors the above problem is yet a state-of-the-art open problem constituting an open challenge in the literature. The objective is to guarantee that $|\Delta P_{ij}|^2 + |\Delta f_i|^2 \rightarrow 0$ for all bounded load variations ΔP_{d_i} , regardless of the time-delay cyberattacks. The time-delayed LFC equation for area $\mathcal{S}_i$ can be represented by,

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + E_{CCS,i} x_{CCS,i}(t - \tau_{CCS,i}) + D_i w_i(t) \quad (2.33)$$

where,

$$x_i = [\Delta f_i, \Delta P_{m_i}, \Delta P_{v_i}, 0, \Delta P_{ij}]^T$$

is the state vector of the endogenous states in $\mathcal{S}_i$,

$$x_{CCS,i} = [0, 0, 0, \Lambda_i, 0]^T$$

is the vector of the exogenous states in $\mathcal{S}_i$ from $\mathcal{S}_{CCS}$ (i.e., the central control station CCS) as in Figure 2.9, and where,

$$A_i = \begin{bmatrix} -1/\tau_{p_i} & k_{p_i}/\tau_{p_i} & 0 & 0 & -k_{p_i}/\tau_{p_i} \\ 0 & -1/\tau_{ch_i} & 1/\tau_{ch_i} & 0 & 0 \\ -1/R_i \tau_{g_i} & 0 & -1/\tau_{g_i} & 0 & 0 \\ K_i B_i & 0 & 0 & 0 & K_i \\ 2\pi T_1 & 0 & 0 & 0 & -2\pi T_1 \end{bmatrix},$$

$$E_{CCS,i} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{\tau_{g_i}} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$B_i = \begin{bmatrix} 0 \\ 0 \\ 1/\tau_{g_i} \\ 0 \\ 0 \end{bmatrix}, \quad D_i = \begin{bmatrix} -k_{p_i}/\tau_{p_i} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad (2.34)$$

and where $w_i = \Delta P_{d_i}$ is a disturbance in the LFC representing the variations in the area load, and the renewable energies that contribute to the area power generation.

Remark 7. Clearly, in a real-time LFC without time-delays $x_i + x_{CCS,i}$ is the state vector for $\mathcal{S}_i$ as explained in outset of Section 2.3.2, and $A_i + E_{CCS,i}$ is the state matrix of the LTI system.

Refer to the explanations provided prior to Definition 4 for details.

In the simulation results below, a relatively significant and sudden load change in ΔP_{d_i} ($\pm 10\%$ of the nominal area load at time 0.1sec. and 0.8sec. , as per the dashed line Figure 2.14) that triggers swings in the power system which has to be contained automatically. Time-delay attacks (if present) are capable of inducing severe instability in the power system if not appropriately circumvented as shown by the thinner line in Figure 2.13, which depicts the variations in the area frequency Δf_i when resilient filters are not present. The solid curve in Figure 2.13 illustrates the simulation results in the

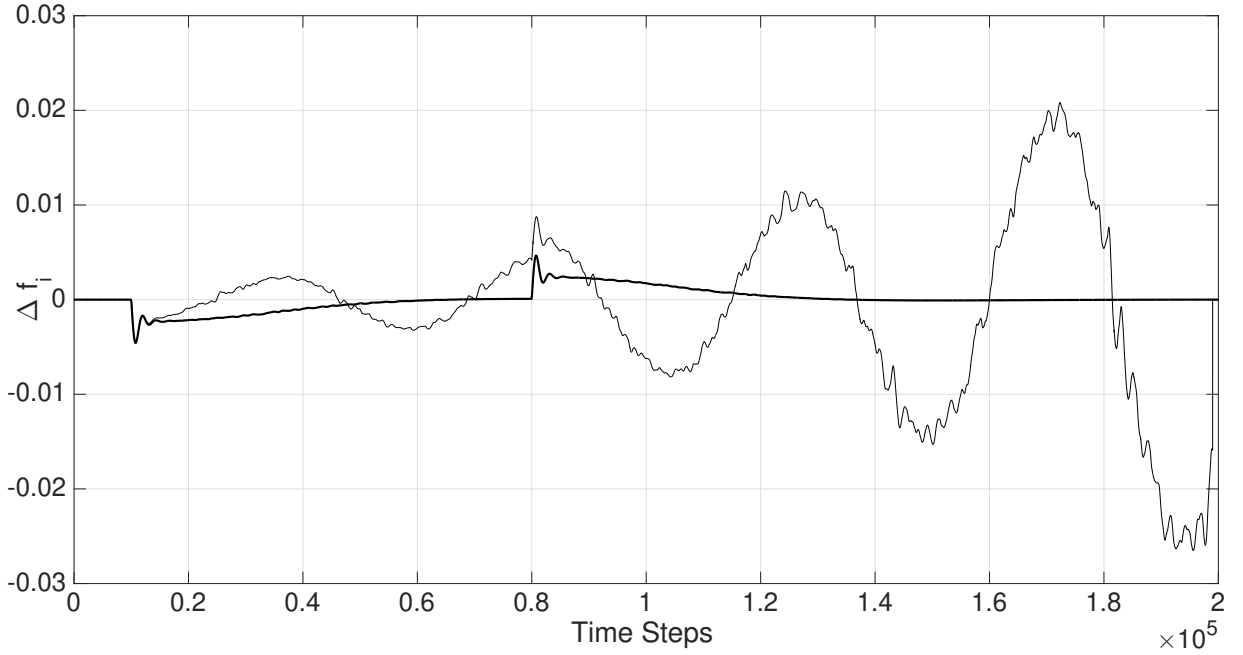


Figure 2.13: Performance of the time-delay resilient filter. The thin line represents Δf_i in response to a $+10\%$ load variation in ΔP_{d_i} , at 0.1sec. and back to 0 at 0.8sec. , for the case where a conventional LFC is in operation. Perilous swings in the system frequency are clear when the telemetered data are attacked by sufficiently long time-delays, resulting in pervasive instability in the power system (thinner line). The same scenario is repeated when resilient cooperative filters are deployed (solid thicker line) which demonstrates stability and a satisfactory LFC control.

presence of cooperative filters (outlined in Figure 2.11), where all tele-metered signals were conditioned by $h(t)$ before they were applied to the agents $\mathcal{S}_o, \mathcal{S}_i$. Corresponding to each exogenous state variable (i.e., $\Delta f_i, \Delta f_j, \Delta P_{ij}$, and Λ_i) a cooperative filter is deployed to recover time-delays in the signals. As a result, the instability in the power system can be maintained and the swings in the frequency in result to load variations are rapidly contained. The thick line in Figure 2.14 depicts the ACE Λ_i in response to a 10% load variations $\Delta P_{d_i}(t)$ (the dashed line). The ACE is the control parameter telemetered by

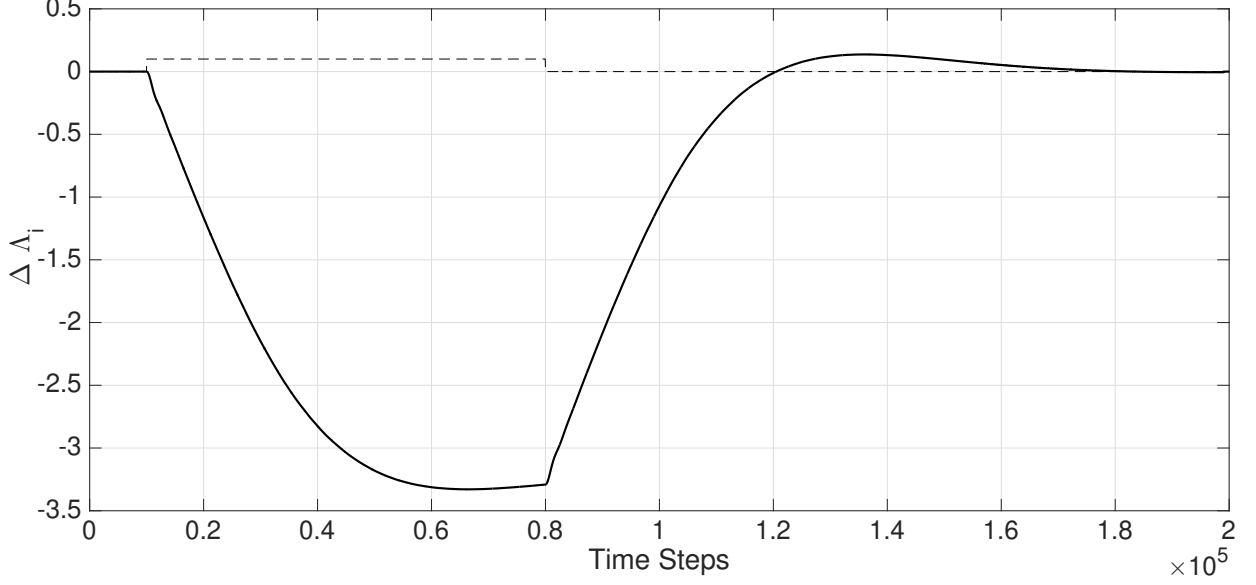


Figure 2.14: Variations in Λ_i as a result of $\Delta P_{d_i}(t)$.

the CCS $\mathcal{S}_o$ to all individual power generating units participating in the LFC. In the absence of a resilient filter mechanism, time-delay attacks on tele-communication links cause delayed inputs to CCS and delayed commands transmitted to the generating units. This inflicts uncontrollable swings in the area power system that disseminates to the

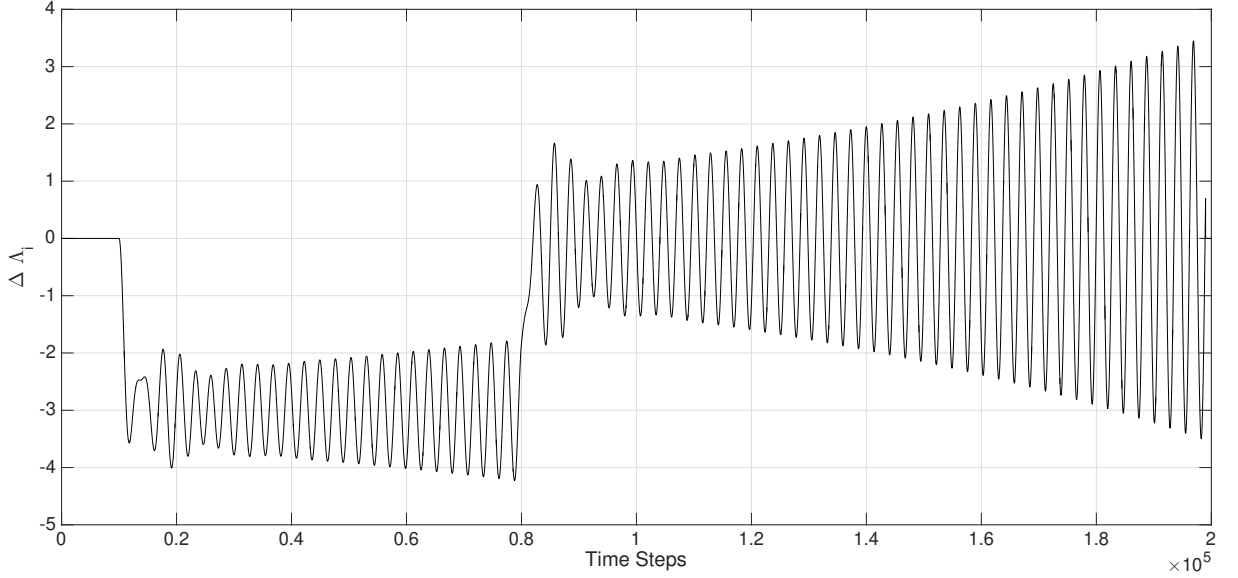


Figure 2.15: Time-Delayed ACE signal Λ_i transmitted from $\mathcal{S}_{CCO}$ without the employment of a delay-resilient cooperative filter system, and as a result of a 10% load disturbance ΔP_{d_i} .

entire power system $\mathcal{S}$ as exemplified in [2.13](#). For the purpose of comparison, the time-delayed ACE signal $\Lambda_i(t - \tau_{\Lambda_i})$ without deploying delay-resilient cooperative filters would be as in Figure [2.15](#). It is important to note that the CCS requires ΔP_{ij} to be transmitted

from $\mathcal{S}_{\text{RTU}} \rightarrow \mathcal{S}_{\text{CCS}}$ (as explained in Figure 2.10), as well as Δf_i to be transmitted from $\mathcal{S}_i \rightarrow \mathcal{S}_{\text{CCS}}$, in order to compute Λ_i according to Equation (2.20). Without employment of a time-delay resilient methodology, the delayed information $\Delta P_{ij}(t - \tau_{\text{RTU,CCS}})$ and $\Delta f_i(t - \tau_{f_i,\text{CCS}})$ would cause instability in the CCS controlled which will be disseminated to $\mathcal{S}_i$, which indeed is the phenomenon taking place in our case studies. Clearly, being at $\mathcal{S}_i$ it appears to be heuristically impossible to recover the real-time signal $\Lambda_i(t)$ from $\Lambda_i(t - \tau_{\Lambda_i})$, since the instability observed in $\mathcal{S}_i$ stems from a delayed signal transmitted from $\mathcal{S}_{\text{RTU}} \rightarrow \mathcal{S}_{\text{CCS}}$. Consequently, recovery of $\Lambda_i(t - \tau_{\Lambda_i})$ (while being at $\mathcal{S}_i$) requires information that is clearly beyond the reach of $\mathcal{S}_i$. The significance of the proposed methodology in this section would now become clear, as it has been possible to restore normality in the entire CPS without requirement of subsystem's information, and only through the filtering of available signals at the subsystems.

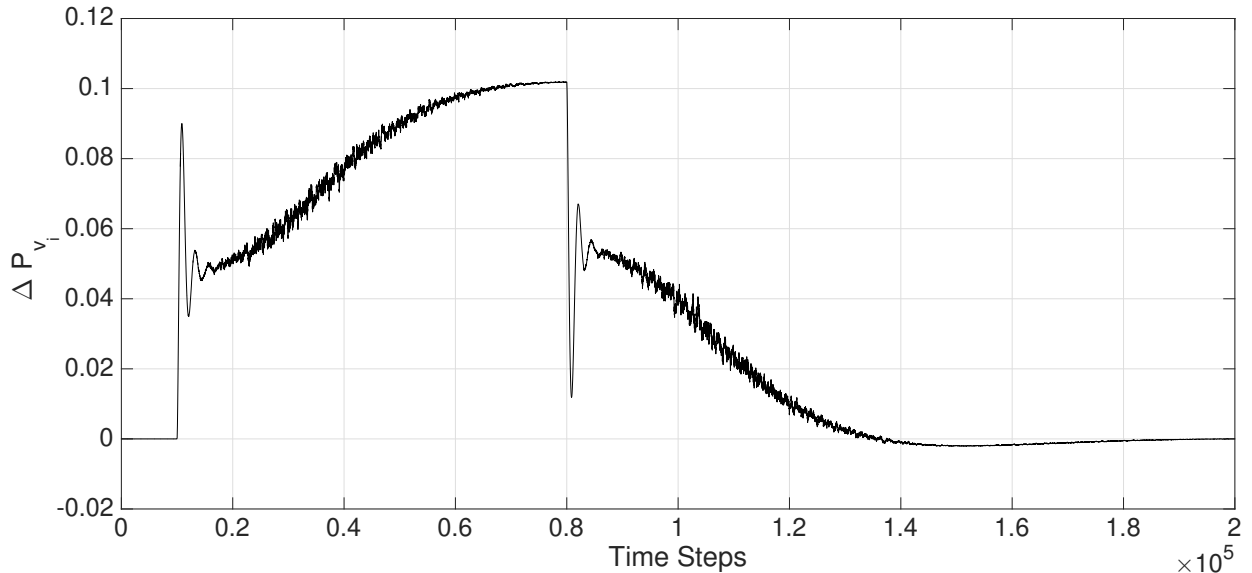


Figure 2.16: Adjustment of the servo-valve electric signal in response to the area load variations depicted in Figures 2.13.

Figure 2.16 depicts the electric signal to the governor servo-valve of the generator in $\mathcal{S}_i$ in response to the disturbance ΔP_{d_i} in the area load. It is evident that the $\pm 10\%$ load change triggers a $\pm 10\%$ command to the servo-valve in order to compensate for the load, ensuring complete balance in the supply-demand, which expectedly guarantees that $\Delta f_i \rightarrow 0$ and $\Delta P_{ij} \rightarrow 0$. However, satisfactory functioning of the time-delay resilient LFC control scheme proposed in this section strictly depends on the bandwidth of the tele-communication system and the speed of data transported between the system controllers, in comparison to the natural frequency of the system states. Figure 2.17 illustrates the importance of the tele-communication system bandwidth by comparing two

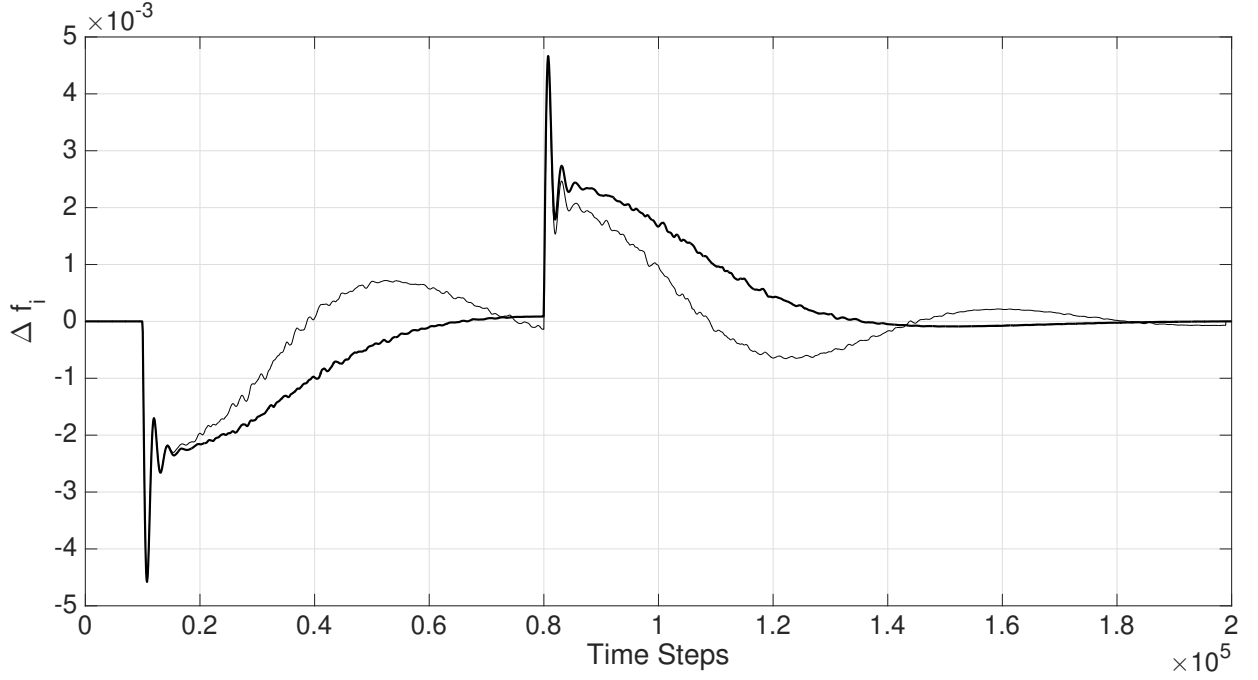


Figure 2.17: Affect of the tele-communication bandwidth. Inadequate bandwidth in tele-communication channels result in marginal instability as depicted by the thin line.

scenarios. In the first scenario (thick line) a high bandwidth system is deployed, and in another attempt low bandwidth communication channels were being used. It is evident that inadequate bandwidth gives rise to instability in the power system (as depicted by the thin line in Figure 2.17).

Finally, Figure 2.18 is a general schematic of a part of an interconnected CPS with a random topology. It is assumed that the subsystems are transmitting equivalent reference signals to others, where each signal is subject to a random time-delay. Figure 2.19 is the simulation result of the cooperative filters for five interconnected subsystems in a discrete-time framework. It is evident that the filters can track the real-time reference signal despite of the unknown time-delays within a time-duration T_s .

2.4 Conclusion of the Chapter

Resiliency against time-delay and DoS cyberattacks on CPS, and in particular, the LFC problem in smart grids have been investigated in this section. It has been shown that augmentation of the tele-communication receivers with certain cooperative filters that exchange their outputs with neighbouring filters (in a multi-agent system framework) can circumvent time-delay sabotage, without any modification to the systems internal controllers. In essence, the cooperative filters receive the time-delayed outputs of their

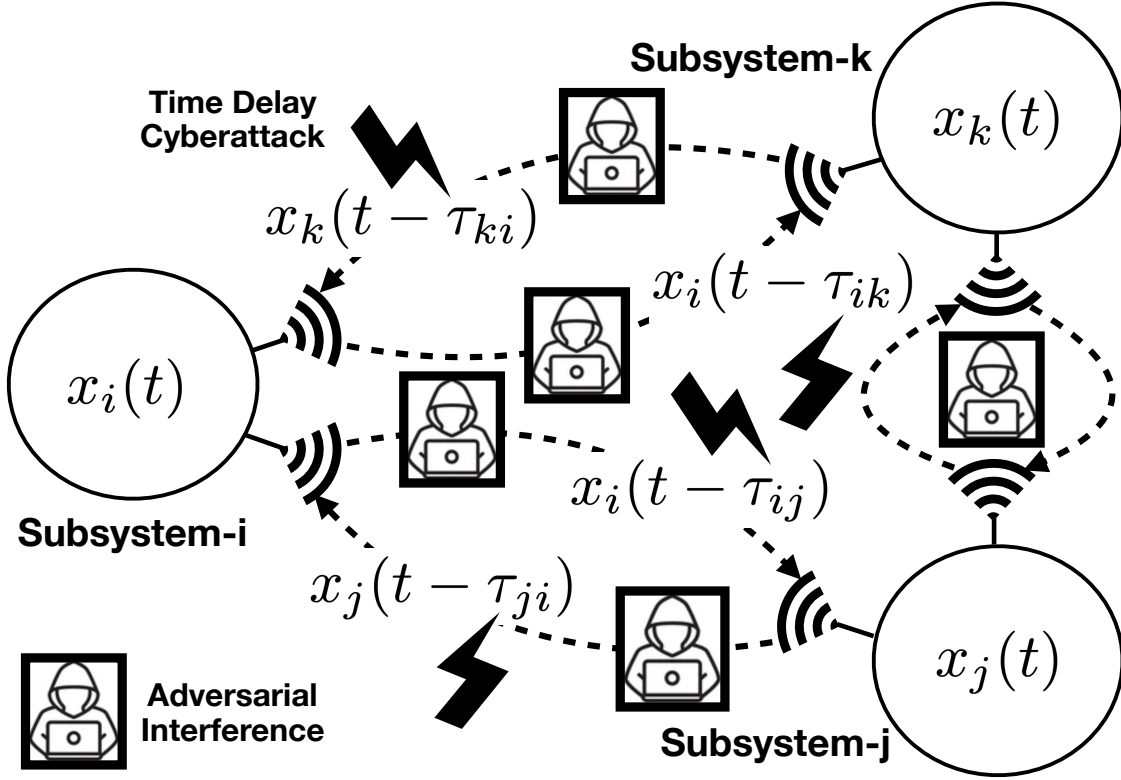


Figure 2.18: General architecture of a CPS, subject to adversarial time-delay cyberattacks. The exogenous states of the systems (x_i, x_j, x_k) are transmitted to adjacent subsystems with unknown time-delay and the output of $h(t)$ filters in each subsystem transmits the conditioned signal back to the source, hence, cooperative filters. The architecture shown in this figure results in time-delay resiliency in the CPS as demonstrated in Figure 2.19

neighbouring filters and augment this information with a locally derived conjecture of the real-time value of some exogenous state that is under time-delay cyberattack, to derive the true real-time value of the attacked state under question. The section has also shown that finite-time denial of service (DoS) cyberattacks cannot distract the convergence of the cooperative filters and invalidate the results. Theoretical results of the proposed methodology has been examined through a case study in a simulation platform that involves a load frequency control problem in a multi-area power system. Complicated control problems such as random time-delays in the transportation of data packets in the LFC that normally elevate instability issues and severe frequency swings had been successfully contained through the proposed cooperative filtering scheme as a result of the simulation.

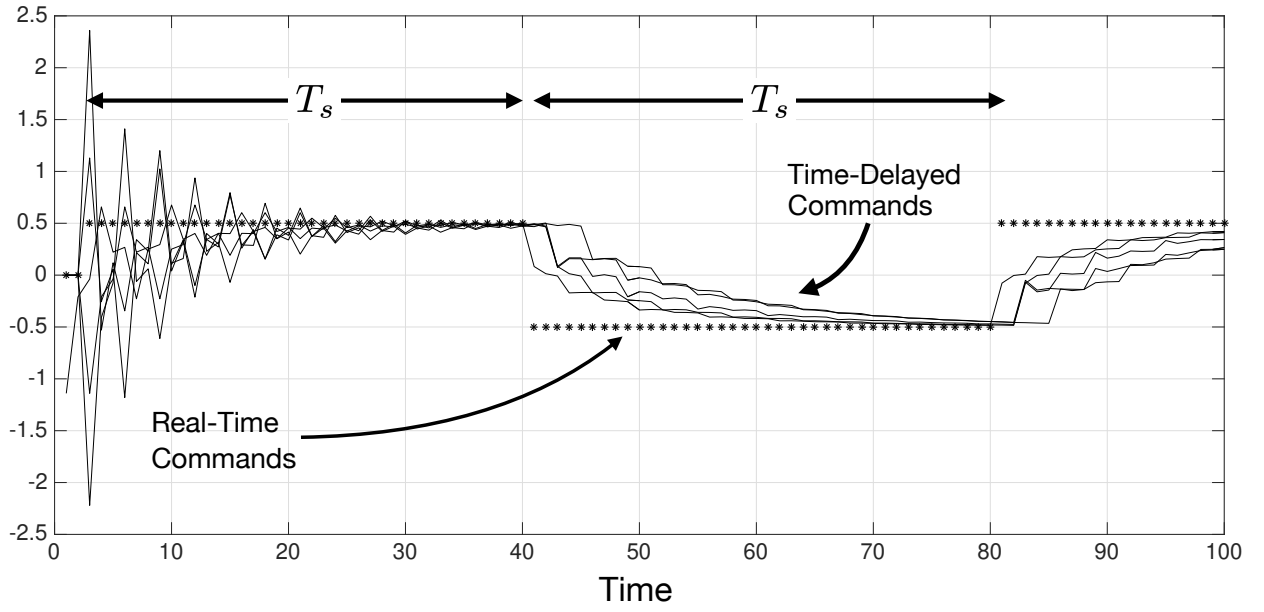


Figure 2.19: A discrete-time network of five interconnected agents transmitting equivalent reference signals (shown by the asterisks) to adjacent subsystems. The tele-communication channels are randomly delayed and the output of the cooperative filters are shown by thinner lines for each subsystem. It is evident that the delayed signals follow the real-time reference signal in a time-duration T_s that is dependent of the filter gain and the topology of the network.

Chapter 3

Unmanned Aerial Vehicle (UAV) Navigation in GNSS Denied Environments

GNSS denied service can be a result of natural signal obscurity, or adversarial signal jamming, and under extreme cases spoofing cyberattacks. Generally, a broad range of cyberattacks can be categorized under the class of sensor and/or actuator “False Data Injection” (FDI) attacks. As a special case, GNSS receivers onboard aerial (or ground) vehicles could be considered as positioning sensors, and GNSS denied service could then be regarded as a FDI cyberattack. The block diagram of a sensor and actuator False Data Injection (FDI) cyberattack in a general MAS is illustrated in Figure 3.1. Vectors $\tilde{x}_k^{(i)}$, and $\tilde{x}_k^{(j)}$ are assumed to be state vectors of agents i and j , respectively, at time-step k , that are under cyberattack by an adversary, where $x_k^{(i)}$ and $x_k^{(j)}$ denote the actual intact sensor output of Agents i, j at time-step k , respectively, and where $\bar{x}_k^{(i)}$ denotes the measured state vector of $x_k^{(i)}$ by means of onboard sensors. In this section we assume that there is no attack of the telecommunication channels between the agents in the MAS, and that control commands to the agents are also intact against cyberattacks, i.e., $\tilde{u}_k^{(i)} = u_k^{(i)}$, for all k . Therefore, the only variable in the system that is subject to cyberattacks will be the sensor outputs of the agents, hence “Sensor FDI”.

3.1 Sensor False Data Injection (FDI) in MAS

Sensor FDI in MAS as outlined above, has received enormous attention in the area of navigational cybersecurity of autonomous vehicles, including aerial UAVs and ground UGVs, as well as the defence industry and in particular in naval vessels. Specifically, if

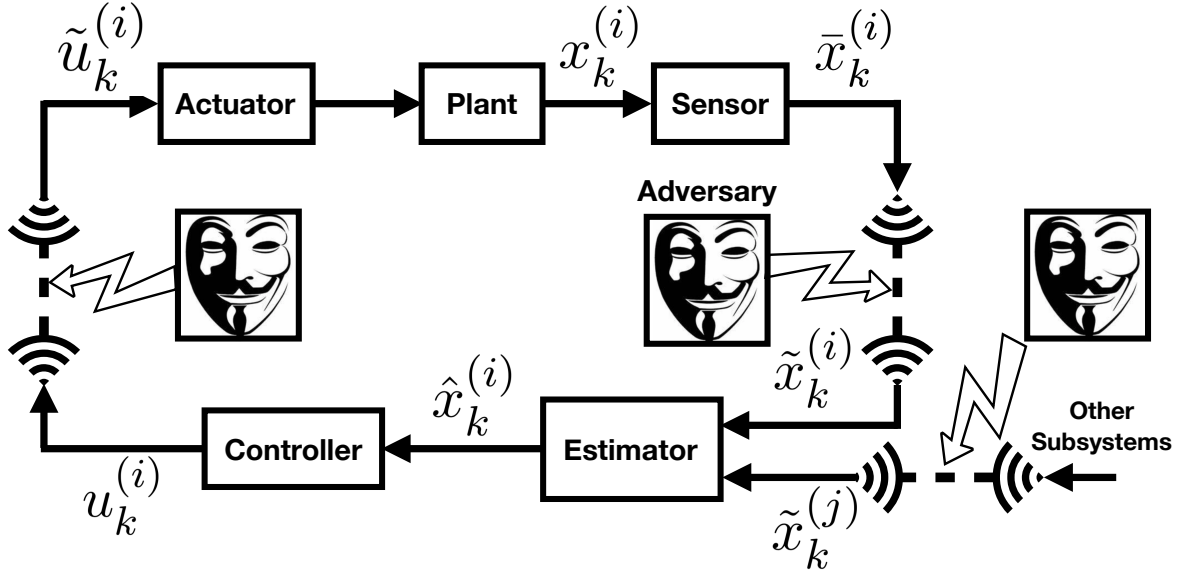


Figure 3.1: Sensor/Actuator False Data Injection (FDI) attack in a Multi-Agent System

the Sensor block in Figure 3.1 is assumed to be the Global Navigation Satellite System (GNSS), the problem of Sensor FDI outlined above reduces to the “localization problem of autonomous vehicles” in GNSS denied environments, that has allocated 62% of the researchers’ attention in the domain of autonomous aerial systems cybersecurity, according to the authors in [102]- [104], i.e., the most prominent research problem in autonomous systems. Accordingly, the second problem of our thesis will be dedicated to this problem and formally stated as in Subsection 3.1.1 below. In Section 3.2 we will be merely concerned with the estimation of $x_k^{(i)}$ from $\hat{x}_k^{(i)}$, and the neighbour information of subsystem i , denoted by $\hat{x}_k^{(j)}$ (as illustrated in Figure 3.1). Therefore, the analysis will be in a discrete time-domain, as the process of information is often carried out by digital computers. However, in Section 3.3 the estimation problem will be involved in conjunction with the physical systems. Therefore, the author would prefer to pursue the discussions of Section 3.3 in a continuous time-domain.

3.1.1 Problem Statement of Sensor FDI in MAS

Let us assume a MAS with a network graph denoted by $\mathcal{G}$ with N agents, where the agents have to navigate in a GNSS denied environment. If the actual position of an agent i at the time-step k along the x -axis is denoted by $x_k^{(i)} \in \mathbb{R}$, and its estimated position is denoted by $\hat{x}_k^{(i)} \in \mathbb{R}$, we have $\hat{x}_k^{(i)} = x_k^{(i)} + \Delta x_k^{(i)}$ for all $i \in \{1, \dots, N\}$, where $\Delta x_k^{(i)} \in \mathbb{R}$ is the longitudinal estimation error. Same concept applies to the position of the agents along y and z axis. Therefore, let us concentrate our discussions on the variables along the x -axis.

Let us also consider an undirected connected graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{A})$, where $\mathcal{N}$ is the set of nodes representing N number of agents, $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$ represents the set of edges, and $\mathcal{A} = [a_{ij}]_{N \times N}$, $a_{ij} \in \{0, 1\}$ the adjacency matrix, where $i \in \{1, \dots, N\}$ denotes the number of agents. The elements of $\mathcal{A}$ are defined such that $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$ if $(i, j) \notin \mathcal{E}$. Let $\mathcal{N}_i$ denote the neighbours of the agent i (i.e., agents whose elements in the Adjacency is $a_{ij} = 1$). The Laplacian matrix $L := [\ell_{ij}] \in \mathbb{R}^{n \times n}$ associated to $\mathcal{G}$ is finally defined as $\ell_{ii} = \sum_{j=1}^N a_{ij} = \sum_{i=1}^N a_{ij}$, and $\ell_{ij} = -a_{ij}$, $\forall i \neq j$, where for the Laplacian matrix of the graph $\mathcal{G}$, we have $L(\mathcal{G}) = \Delta(\mathcal{G}) - D(\mathcal{G})$, where $\Delta(\mathcal{G}) = \mathbf{Diag}(\ell_{11}, \ell_{22}, \dots, \ell_{NN})$, and $D(\mathcal{G})$ is the incidence matrix.

Problem 2. The problem is to estimate $\hat{x}_k^{(i)}$ based on $\tilde{x}_k^{(i)}$, and $\tilde{x}_k^{(j)}$, $j \in \mathcal{N}_i$, such that the total network error in $\mathcal{G}$, that is defined by

$$E(\mathcal{G}) := \sum_{i=1}^N \mathbb{E}[(\hat{x}_k^{(i)} - x_k^{(i)})^2], \quad (3.1)$$

is minimized.

Refer to Figure [3.1](#) for a visual imagination of the variables $x_k^{(i)}$, $\tilde{x}_k^{(i)}$, and $\hat{x}_k^{(i)}$.

3.1.2 Regression Filtering Solution for Problem [2](#)

Let $x_k = [x_k^{(1)}, \dots, x_k^{(N)}]^T$, and $\tilde{x}_k = [\tilde{x}_k^{(1)}, \dots, \tilde{x}_k^{(N)}]^T$. Let us also assume that the Estimator in Figure [3.1](#) is a linear time-varying system, with an impulse response $h_k^{(i)}$, such that,

$$\hat{x}_k^{(i)} = \sum_{j=1:N} h_k^{(i)}(j) \cdot \tilde{x}_k^{(j)} = (h_k^{(i)})^T \tilde{x}_k. \quad (3.2)$$

The objective is to minimize $\mathbb{E}[(\hat{x}_k^{(i)} - x_k^{(i)})^2]$ with respect to $h^{(i)}$, given Equation [\(3.18\)](#). For this one must have,

$$\frac{\partial \mathbb{E}[(x_k^{(i)} - \hat{x}_k^{(i)})^2]}{\partial [h_k^{(i)}(1), \dots, h_k^{(i)}(N)]} = 0,$$

where,

$$\frac{\partial \mathbb{E}[(x_k^{(i)} - \hat{x}_k^{(i)})^2]}{\partial [h_k^{(i)}(1), \dots, h_k^{(i)}(N)]} = \frac{\partial \mathbb{E}[(x_k^{(i)} - \hat{x}_k^{(i)})^2]}{\partial \hat{x}_k^{(i)}} \cdot \frac{\partial \hat{x}_k^{(i)}}{\partial [h_k^{(i)}(1), \dots, h_k^{(i)}(N)]}$$

Therefore, one must have,

$$\mathbb{E}[x_k^{(i)} - \hat{x}_k^{(i)}] \cdot \frac{\partial \hat{x}_k^{(i)}}{\partial [h_k^{(i)}(1), \dots, h_k^{(i)}(N)]} = 0,$$

where, from Equation [\(3.18\)](#),

$$\frac{\partial \hat{x}_k^{(i)}}{\partial [h_k^{(i)}(1), \dots, h_k^{(i)}(N)]} = \tilde{x}_k,$$

resulting,

$$\mathbb{E}[x_k^{(i)} \tilde{x}_k^{(j)}] = \mathbb{E}[\hat{x}_k^{(i)} \tilde{x}_k^{(j)}], \quad \forall i, j,$$

or simply,

$$\mathbb{E}[x_k \cdot \tilde{x}_k^T] = \mathbb{E}[\hat{x}_k \cdot \tilde{x}_k^T] \quad (3.3)$$

Equation (3.3) implies that $\mathbb{E}[\Delta x_k \cdot \tilde{x}_k^T] = 0$, which further implies that the vectors Δx_k and $\tilde{x}_k$ shall be “orthogonal” for all k . As a result, Equation (3.3) shall be hereinafter referred to as the “Orthogonality Principle”. However, from Equation (3.18) one may write $\hat{x}_k = H_k \tilde{x}_k$, if H is denoted by,

$$H_k = \begin{bmatrix} h_k^{(1)}(1) & \cdots & h_k^{(1)}(N) \\ h_k^{(2)}(1) & \cdots & h_k^{(2)}(N) \\ \vdots & \ddots & \vdots \\ h_k^{(N)}(1) & \cdots & h_k^{(N)}(N) \end{bmatrix}.$$

Substituting $H_k \cdot \tilde{x}_k$ for $\hat{x}$ in Equation (3.3), would result in $\mathbb{E}[x_k \cdot \tilde{x}_k^T] = H_k \cdot \mathbb{E}[\tilde{x}_k \cdot \tilde{x}_k^T]$, or,

$$H_k = \mathbb{E}[x_k \cdot \tilde{x}_k^T] \cdot \mathbb{E}[\tilde{x}_k \cdot \tilde{x}_k^T]^{-1} \quad (3.4)$$

that is,

$$H_k = \begin{bmatrix} \mathbb{E}[x_k^{(1)} \tilde{x}_k^{(1)}] & \cdots & \mathbb{E}[x_k^{(1)} \tilde{x}_k^{(N)}] \\ \vdots & \ddots & \vdots \\ \mathbb{E}[x_k^{(N)} \tilde{x}_k^{(1)}] & \cdots & \mathbb{E}[x_k^{(N)} \tilde{x}_k^{(N)}] \end{bmatrix} \begin{bmatrix} \mathbb{E}[\tilde{x}_k^{(1)} \tilde{x}_k^{(1)}] & \cdots & \mathbb{E}[\tilde{x}_k^{(1)} \tilde{x}_k^{(N)}] \\ \vdots & \ddots & \vdots \\ \mathbb{E}[\tilde{x}_k^{(N)} \tilde{x}_k^{(1)}] & \cdots & \mathbb{E}[\tilde{x}_k^{(N)} \tilde{x}_k^{(N)}] \end{bmatrix}^{-1}.$$

As a consequence, Equation (3.42) will be the optimal filter that solves Problem 2, in a sense that $H_k \cdot \tilde{x}_k$ would be an optimal representation for x_k that minimizes the estimation error Δx_k in a “Mean Square Sense”. We refer to this solution as the “Regression Filtering” solution.

3.1.3 Limitations of the Regression Filtering Solution

There are two main limitations in using Equation (3.42) as a solution for Problem 2. The first problem is that deriving H_k requires that one to approximate $\mathbb{E}[x_k \cdot \tilde{x}_k^T]$, and requires a knowledge of $p(x_k)$, i.e., the probability distribution function (pdf) of x_k that is generally unavailable. Secondly, it requires a central controller that can receive x_k and $\tilde{x}_k$ from the agents at each time-step, and then transmit $h_k^{(i)}$ back to the local controller of the agents, so that the local controllers can estimate $\hat{x}_k^{(i)}$, as in Equation (3.18). Centralized control architectures in CPS are often associated with numerous problems. For example, in IoD one of the greatest constraints associated with the UAVs is the energy

conservation, and the energy required to transmit information to a central controller can become unaffordable as the distance between the UAV and the controller grows. In a distributed control architecture, the agents tend to transmit information to their surrounding neighbours in a relatively closer proximity, therefore, the energy conservation constraints makes distributed control architectures a preferable choice. In view of the limitations explained above an alternative solution had to be considered for the problem.

3.2 Optimization of Localization Error in MAS of UAVs through Cooperative Positioning: Autonomous Navigation in Partially Denied GNSS Environments

It has been stated previously that Unmanned Aerial Vehicles (UAVs) are increasingly being used in a wide range of applications such as surveillance and reconnaissance, civil infrastructure inspection, agriculture, ecology, remote sensing, among others [97,98,103]. The authors in [92] have stated that “for these types of applications, a UAV can be programmed to autonomously fly a predefined path composed by a series of GNSS waypoints, provided the UAV has a clear view of the sky in order to obtain a reliable GNSS positioning. However, there exist challenging scenarios in which the UAV is required to fly under structures, such as bridges, within mines and buildings or below dense canopy, or in natural or urban canyons in which the GNSS signal is partially obstructed”. Therefore, autonomous navigation (including localization, translational velocity estimation, approach and landing, motion planning, obstacle avoidance, attitude estimation, and mapping) in partially denied GNSS spaces has been a major subject of ongoing research in autonomous control. The authors in [102] have performed a survey concluding that among this vastly growing research area 62% of the work has been expended on autonomous localization and positioning, showing the need for a GNSS-independent navigation solution as a primary quest. The authors further define navigation to be a “meta-capability, which includes perception, localization, motion planning and motion control methods, which include inertial, vision, radio, acoustic and radar”.

The work in the literature suggests alternative ways of navigation in GNSS denied environments. The authors in [153] suggest signals of opportunity such as electromagnetic radio wave signals for localization. Other works discuss utilization of IMU sensors onboard vehicles to initially estimate positions and then to alleviate the error through

filtering [154], or machine learning approaches as in [155], and camera and LiDAR (Light Detection and Ranging) solutions as in [156].

In this section a novel solution is proposed with better localization accuracy for partially denied GNSS environments, where it is assumed that we have multi-agent autonomous vehicles with at least an agent having access to its precise location (namely, the leader), while others exchange their perceived locations (as discussed in [153]- [156]) and their onboard ranging devices (such as LiDARs and RADARs) to attain a relatively accurate localization with reference to the network leader.

3.2.1 Contributions and Assumptions of Section 3.2

The contributions of this section can be summarized as follows:

1. Improvement of positioning estimation in a multi-agent system of vehicles by fusion of data from onboard IMU sensors and ranging devices through consensus.
2. Determination of an optimal topological formation in a given network of agents to reduce the overall network error in the positioning estimation in partially denied GNSS environments.

We firstly introduce a small relaxation for Problem 2 based on the assumption that an adversary cannot simultaneously attack all the agents in a given MAS, due to the presumed energy restraints in adversarial resources. In other words, since practical multi-agent systems (such as IoD) generally span a vast geographic space, we could assume that an unaffordable energy would be required by the adversaries to simultaneously attack all the agents. Specifically, we are proposing the following assumptions for the problem.

Assumptions: The assumptions that are made for our solution are as follows:

1. There exists at least one agent (referred to as the “leader”, and named as Agent 1, i.e., $i = 1$) in the connected graph $\mathcal{G}$ with a deterministic position, where $\Delta x_k^{(1)} = 0$, $\forall k \in \mathbb{N} \cup \{0\}$.
2. For all $i \in \{2, \dots, N\}$, it is noted that $\Delta x_k^{(i)}$ is a random variable with some unknown distribution.
3. We assume that the agents are equipped with range-finding sensors (such as LiDAR, RADARs, etc.) that can measure their relative distances (referred to as $\omega_k^{(i,j)}$ with

respect to their neighbours). Therefore, $\omega_k^{(i,j)} = x_k^{(i)} - x_k^{(j)}$ is available for all $i \in \mathcal{N}$, and for all $j \in \mathcal{N}_i$, where $\mathcal{N}_i$ is the set of agents having radio communication with agent i (referred to as neighbours of i) and vice-versa.

4. We further assume that the time-steps k are selected such that $x_k^{(i)}$ is a stationary process at each time-step for all $i \in \mathcal{N}$. The UAV motion models have been linearized according to the dynamic equations that are provided in [122], [123].

3.2.2 Research Results for Section 3.2

Let the agents one by one exchange their estimated locations with their neighbours at each time-step k , and let the agents update their estimations after each round of exchanges, until the estimations converge to a consensus value, through iteratively updating $\hat{x}_k^{(i)}$ for all $i \in \mathcal{N} \setminus \{1\}$ (in each and every time-step k), where the $(n+1)^{th}$ update is performed by the following protocol,

$$\begin{aligned} \hat{x}_k^{(i)}(n+1) &= \hat{x}_k^{(i)}(n) + \\ \Delta t_n \sum_{j \in \mathcal{N}_i} (\hat{x}_k^{(j)}(n) - \hat{x}_k^{(i)}(n) + \omega_k^{(i,j)}), \quad \forall i \neq 1, i \in \mathcal{N}, \\ \hat{x}_k^{(1)}(n+1) &= \hat{x}_k^{(1)}(n), \quad (\text{i.e., no update for the leader}), \end{aligned} \quad (3.5)$$

where $\hat{x}_k^{(i)}(0) = \hat{x}_k^{(i)}$ is the initial estimation derived for each agent and for each time-step, based on the motion models and IMU sensor information, and Δt_n is the time for one round of information exchange among all the agents in the network. In other words, if $\hat{x}_k^{(i)}(n)$ in the discrete-time domain is corresponding to $\hat{x}^{(i)}(t)$ in the continuous-time domain, then $\hat{x}_k^{(i)}(n+1)$ would also correspond to $\hat{x}^{(i)}(t + \Delta t_n)$. Since we have assumed that $x_k^{(i)}$ is stationary for each k , it follows that $\omega_k^{(i,j)}$ is constant, and can be read only once in each time-step k . Equation (3.5) has to be sufficiently iterated in each time-step, until the estimations converge. At each round of exchange the neighbours exchange their latest estimates $\hat{x}_k(n) \triangleq [\hat{x}_k^{(1)}(n), \dots, \hat{x}_k^{(N)}(n)]^T$ according to (3.5). Substitution for $\hat{x}_k$ with $x_k + \Delta x_k$ (where $x_k = [x_k^{(1)}(n), \dots, x_k^{(N)}(n)]^T$ is the vector of the true longitudinal positions at the time-step k), and noting that $x_k(n+1) = x_k(n)$, one can note that (3.5) reduces to,

$$\Delta x_k^{(i)}(n+1) = \Delta x_k^{(i)}(n) + \Delta t_n \sum_{j \in \mathcal{N}_i} (\Delta x_k^{(j)}(n) - \Delta x_k^{(i)}(n)), \quad (3.6)$$

where Δt_n shall be such that the poles of the discrete system in Equation (3.6) lie inside the unit circle, and since Equation (3.6) can be written as,

$$\Delta x_k(n+1) = \Delta x_k(n) - \Delta t_n L \Delta x_k(n) = V(I - \Delta t_n \Lambda) V^{-1} \Delta x_k(n),$$

where $L = V\Lambda V^{-1}$, and where V and V^{-1} are the right and left eigenvectors respectively, and Λ is the diagonal matrix of the eigenvalues of L , then Δt_n should be such that $1 > \Delta t_n \lambda_2$ and $1 > \Delta t_n \lambda_N$, and the sufficient condition for the system to be stable is that $\Delta t_n < 1/N$. Furthermore, If one partitions the Laplacian matrix L as,

$$L = \begin{bmatrix} \ell_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix}$$

the continuous-time representation of (3.6) in a compact form could be written as,

$$\Delta \dot{x}_k = - \begin{bmatrix} 1 & 0 \\ L_{21} & L_{22} \end{bmatrix} \Delta x_k \quad (3.7)$$

where $\Delta x_k = [\Delta x_k^{(1)}, \dots, \Delta x_k^{(N)}]^T$ and $\Delta x_k^{(1)}(0) = 0$. Through linear transformation of (3.7) using T , where,

$$T = \begin{bmatrix} 1 & \mathbf{0}_{(1 \times N-1)} \\ -\mathbf{1}_{(N-1 \times 1)} & I_{(N-1 \times N-1)} \end{bmatrix},$$

and considering that $\Delta x_k^{(1)} = 0$, results in $(T\Delta \dot{x}_k) = -TLT^{-1}(T\Delta x_k)$, which finally yield,

$$\begin{aligned} \Delta \dot{x}_k^{(1)} &= 0, \\ \Delta \dot{x}_k^{(2:N)} &= -L_{22}\Delta x_k^{(2:N)}. \end{aligned} \quad (3.8)$$

However, it can be noted that $L_{22} > 0$, since for any given vector $v \neq 0$ we have,

$$\begin{bmatrix} 0 & v^T \end{bmatrix} L \begin{bmatrix} 0 \\ v \end{bmatrix} = \begin{bmatrix} 0 & v^T \end{bmatrix} \begin{bmatrix} \ell_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix} \begin{bmatrix} 0 \\ v \end{bmatrix} > 0.$$

This is obvious since only vector $\mathbf{1}$ can yield $\mathbf{1}^T L \mathbf{1} = 0$, and any other vector including $[0, v]^T$ would result a positive value. Hence, $\Delta \dot{x}_k^{(2:N)} = -L_{22} \Delta x_k^{(2:N)}$ results in $\lim_{n \rightarrow \infty} \Delta x_k^{(2:N)} = 0$, which is a solution to the problem statement, as long as we assume that the range-finders are ideal sensors. However, this is not a valid assumption in a real-world. That is, in real-world, sensor readings are obtained as $\omega_k^{(i,j)} + \Delta \omega_k^{(i,j)}$, where $\Delta \omega_k^{(i,j)}$ is the non-deterministic error of the LiDAR (or RADAR) sensor, with a given probability distribution [132]. Inclusion of $\Delta \omega_k^{(i,j)}$ in (3.5), extends (3.8) to,

$$\Delta \dot{x}_k^{(2:N)} = -L_{22}\Delta x_k^{(2:N)} + \Delta \omega_k^{(2:N)}, \quad (3.9)$$

where $\Delta \omega_k^{(i)} = \sum_{j \in \mathcal{N}_i} \Delta \omega_k^{(i,j)}$. Consensus in (3.9) results in a network error, since the solution of (3.9) at steady state yields $\Delta x_k^{(2:N)} \rightarrow L_{22}^{-1} \Delta \omega_k^{(2:N)}$, and the total network error would become,

$$\begin{aligned} \sum_{i=1}^N \mathbb{E}[(\hat{x}_k^{(i)} - x_k^{(i)})^2] &= \sum_{i=1}^N \mathbb{E}[(\Delta x_k^{(i)})^2] \\ &\rightarrow \mathbb{E}[(\Delta \omega_k^{(2:N)})^T L_{22}^{-2} (\Delta \omega_k^{(2:N)})]. \end{aligned} \quad (3.10)$$

Now since,

$$(\Delta\omega_k^{(2:N)})^T L_{22}^{-2} (\Delta\omega_k^{(2:N)}) \leq (\Delta\omega_k^{(2:N)})^T \lambda_{min}^{-2} (\Delta\omega_k^{(2:N)}),$$

(where λ_{min} is the smallest eigenvalue of L_{22}) we have,

$$\sum_{i=1}^N \mathbb{E}[(\hat{x}_k^{(i)} - x_k^{(i)})^2] \leq \lambda_{min}^{-2} \sum_{i \in \mathcal{N}} \sum_{j \in \mathcal{N}_i} \mathbb{E}[(\Delta\omega_k^{(i,j)})^2], \quad (3.11)$$

due to the fact that one can consider $\mathbb{E}[(\Delta\omega_k^{(i_1)})^T (\Delta\omega_k^{(i_2)})] = 0$, $\forall i_1 \neq i_2$. The ‘‘Network Error Gain’’ of the graph (denoted by κ) can be defined as the ratio of the total network error to the total sensor error, and can be a metric to evaluate the performance of the network topology, with respect to the minimal distribution of sensor errors. In the above sense one can determine an upper bound for the network error gain as,

$$\kappa(\mathcal{G}) := \frac{\sum_{i=1}^N \mathbb{E}[(\hat{x}_k^{(i)} - x_k^{(i)})^2]}{\sum_{i \in \mathcal{N}} \sum_{j \in \mathcal{N}_i} \mathbb{E}[(\Delta\omega_k^{(i,j)})^2]} \leq \lambda_{min}^{-2}. \quad (3.12)$$

Remark 1: Equation (3.12) shows that a better localization can be achieved in a network with higher connectivity. In particular, for a fully connected network we have $\kappa(\mathcal{G}) \leq 1/N^2$. This implies that one can expect ideal localization for a sufficiently large and fully connected network (assuming that $\mathbb{E}[\sum_{i \in \mathcal{N}} \sum_{j \in \mathcal{N}_i} \Delta\omega_k^{(i,j)}] = 0$).

Remark 2: The authors in [133], have shown that for any vector $f \in \mathbb{R}^N$ on the vertex set $\mathcal{N}$, we have,

$$\lambda_{min} \leq \frac{\sum_{(i,j) \in \mathcal{E}} (f(v_i) - f(v_j))^2}{\sum_{i \in \mathcal{N}} f^2(v_i)}. \quad (3.13)$$

Now let us define $f(v_i)$ as the distance of v_i with respect to a leader (i.e., shortest number of communication links from agent i to the leader). Then the numerator in (3.13) represents the total number of ‘‘effective’’ communication links (defined as one that results in $f(v_i) - f(v_j) \neq 0$) in $\mathcal{G}$, and the denominator represents the sum of square distances of the agents with respect to the leader. Therefore, it follows that in any given multi-agent system a more accurate localization can be achieved, by reducing the diameter of the network (i.e., distance of the farthest agent to the leader), and increasing the number of effective communication channels between the agents.

3.2.3 Simulations and Case Studies

Our case study is comprised of a multi-agent system of UAVs with $N = 10$ agents, as demonstrated in Figure 3.2.

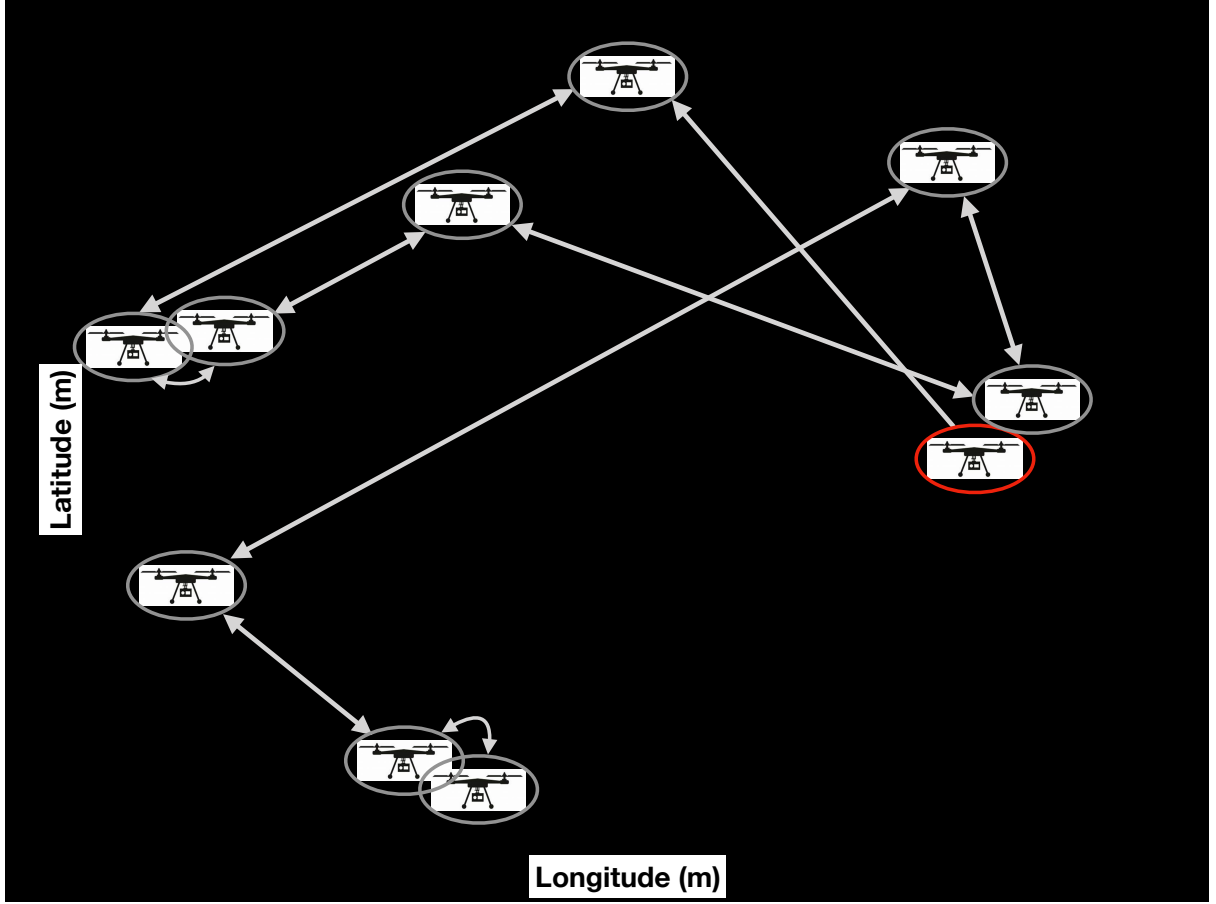


Figure 3.2: The x-y location of a multi-agent system of UAVs with 10 agents, with their true positions with respect to an arbitrary origin. The axes are scaled in meters, and the elevation has been omitted for simplicity and better clarity of the figure.

We have assumed that Agent 1 (Leader) has a deterministic position (indicated by the red ellipse in Figure 3.2), while agents 2 to 10 are not covered by the GNSS service, hence a partially denied GNSS environment. Under this circumstance, we have performed a Monte-Carlo simulation for the case where the position of the UAVs are estimated according to the motion models of the UAVs with typical actuator and sensor uncertainties, and environmental disturbances. Each black circle in Figure 3.3, and Figure 3.4, indicates a dead reckoning estimated position of a UAV on a stand-alone basis (in other words, the information pertaining distances between the UAVs have been neglected). Therefore, the black area in the following figures can be a representation of the probability distribution of UAV positions without cooperative sensing. In parallel, we have performed our proposed cooperative sensing method as in (3.5) to improve the localization accuracy, and Monte-Carlo results (based on cooperative sensing) in “red”, to illustrate the performance of cooperative sensing.

The “red” samples in Figure 3.3 represent Monte-Carlo position estimations of the

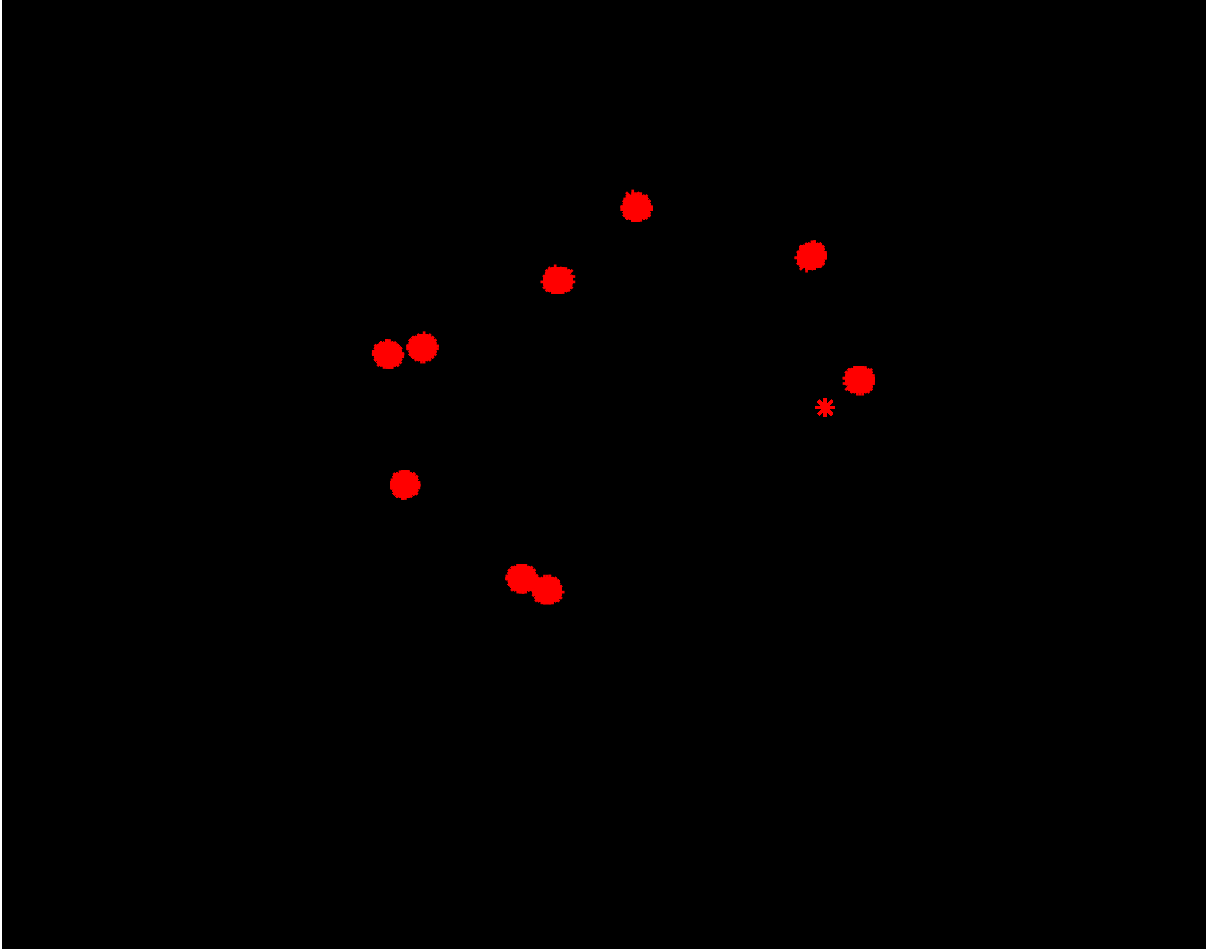


Figure 3.3: Monte-Carlo simulations of cooperative sensing method (in red) in comparison with the dead-reckoning positioning estimation (in black) for a fully connected system of UAVs, as depicted in Figure 3.2. Concentration of the red samples in comparison to the black area represents the improved accuracy in localization. The position of the leader is represented by the same marker in every observation due to its deterministic nature, hence 100% accuracy. However, the variance of all other agents' positions is not zero (due to the error in range-finders) but equal (due to the fully connected topology).

multi-agent system of UAVs (depicted in Figure 3.2) for 1000 samples based on cooperative sensing in a fully connected topology, as opposed to the topology that illustrated in Figure 3.2, which is a radial configuration (where agents communicate in a chain-wise fashion to span a larger geographic space). The same experiment has been repeated in Fig 3.4 with a fully radial communication topology as exactly illustrated in Figure 3.2. The actual position of the leader and all other agents are the same in all the three figures, except that the localization in Figure 3.4 has a larger network error due to the network topology resulting in a larger $\kappa(\mathcal{G})$.

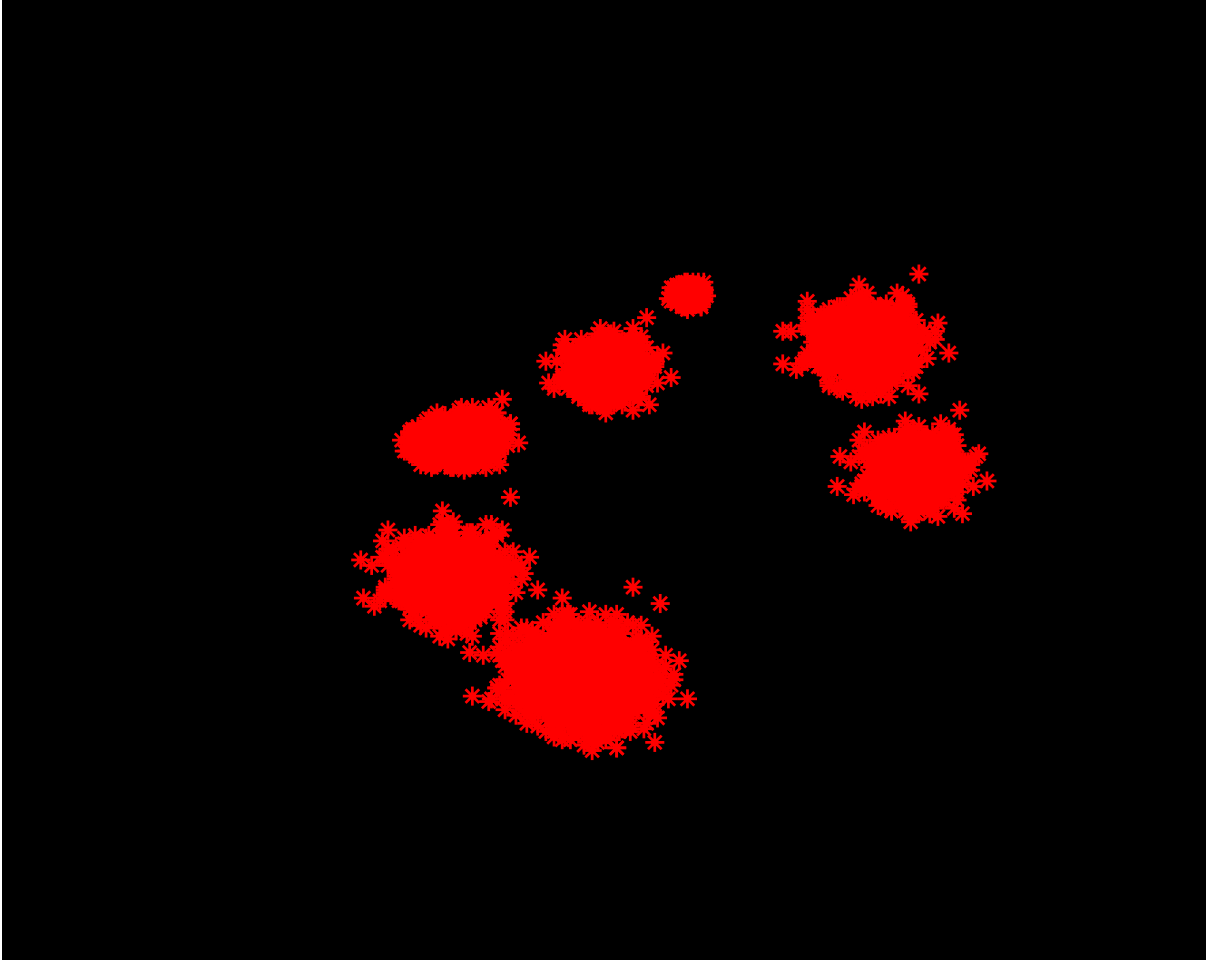


Figure 3.4: Results of Monte-Carlo simulations for the network topology of Figure 3.2. Localization error is increased as the UAVs are distanced (communication-wise, not geographically) from the leader. This is opposed to the case in Figure 3.3, where the network error was equally distributed among the agents.

3.2.4 Conclusion

In this section we have investigated a novel localization method for a multi-agent system of UAVs, referred to as the “cooperative sensing”, where only part of the network has access to GNSS, hence, “partially denied GNSS environment”. It is shown that cooperative sensing can eliminate sensor uncertainties, and environmental disturbances (except range-finder errors), which significantly improves the overall navigation error in multi-agent systems. This work has been extended for environments with fully GNSS-denied services in the next section. The problem statement and the methodology would be similar to what has been discussed in this section, except that we will explain the methodology in more depth and in a continuous time-domain.

3.3 Cooperative Localization of Multi-Agent Unmanned Aerial Vehicle (UAV) Networks in Intelligent Transportation Systems

UAVs are defined as Dynamic Remotely Operated Navigation Equipment (DRONES) that are autonomously controlled without onboard pilots [157]. The authors in [158] categorize navigation in four phases, namely, “perception”, “localization”, “cognition” and “path planning”, where perception is an information collection system utilizing the sensing apparatus onboard the UAV to capture surrounding environment of the UAV, and localization is the process that is used by the UAV to locate its position in the air-space with respect to a given coordinate system, and cognition is a term borrowed from neuroscience that refers to a computational process onboard the vehicle to build a mental representation of the air-space and use it to guide movement. UAVs can navigate through their flight path based on predefined set of waypoints if there is continuous access to the GNSS service [92]. However, as explained earlier there are challenging scenarios in which UAVs are required to deploy self-awareness in GNSS-denied environments, and find an optimal path to their destination through environmental sensing. The authors in [102] define self-awareness as a meta-capability which includes perception, localization, path planning and motion control, by taking advantage of the on-board sensing devices. Furthermore, the relative ease by which GNSS-based navigation can be jammed (through denial of reception by a competing signal), or spoofed (through deliberate introduction of a false signal) makes GNSS based localization vulnerable to cyberattacks [99]- [101]. The authors in [102] have concluded that the vastly growing and nowadays complex UAV applications are pushing control requirements beyond human-in-the-loop capabilities and motivates research areas into fully autonomous navigation methodologies which has been the main motivation of the work developed in this section.

This section is an extension to the previous section that outlines a cooperative localization scheme in partially-denied GNSS environments where at least an agent in the network exists with access to GNSS, or in a fully GNSS denied environment where at least an agent can have C-V2X messaging to/from a stationary infrastructure with known position, referred to as an anchor. There are other recent articles in the literature that discuss localization in GNSS denied environments, where vehicles take advantage of an environment that is embedded with geographic position marks. For example, the authors in [165] take advantage of stray radio signals emitted from a land-based infrastructure with known position, and [166, 169] take advantage of road semantics such as lane lines

and poles, or RSU with given positions. Alternatively, as explained previously other research work tend to facilitate localization in GNSS denied environment, through fusion of onboard sensing apparatus [114]- [121].

3.3.1 Related Works

Cooperative Navigation is a relatively new subject in the literature encompassing autonomous navigation. Reference [159] proposed cooperative localization in a swarm of mobile sensors using Covariance Intersection (CI) algorithm. The authors in [160] have suggested multi-UAVs in a cooperative fashion to circumvent inadequacies of the single-UAV three-dimensional occupancy grid mapping. [161] defines Cooperative Intelligent Transport Systems (C-ITS) and elaborates the fifth-generation (5G) wireless technology to support cooperative mobility. [162] is a recent survey on 5G technology for UAVs. [163] is another recent survey on sensor selection and placement for assisting cooperative mobility. Reference [164] is an excellent recent research work that compares cooperative localization methodologies in modern smart transportation. Cooperative localization in GPS-denied environments is the main focus of this work and tries to present the advantages of cooperative navigation from a different angle, for the purpose of autonomous localization.

The authors in [110] have identified that mapping in dynamic environments can lead to serious errors in the resulting maps such as spurious objects or misalignments due to localization errors. Nevertheless, there are several publications available in the literature where the authors have tested a prototype SLAM product in a relevant environment. For instance, the authors in [111] have introduced a vision-IMU perception algorithm where a visual-aided (Inertial Navigation System) INS is tested in a simulated known environment (software in the loop). [112] deploys laser rangefinders, IMU and vision-based sensing for full GNSS-denied navigation, that is verified on a prototype in an unknown cluttered relevant environment. The authors in [113] have utilized vision, IMU, and sonar sensing for full GNSS-denied navigation and tested the prototype in a relevant environment. In addition to the above, several other research works are available in the literature that have addressed sensor-fusion UAV navigation in GNSS-denied environments [114]- [121]. A more recent class of research work are trying to take advantage of the stray radio signals to elicit the 3-D space location of a given point [165].

The conclusion derived from the above literature review is that localization solutions infusing multiple sensing, perception, and cognition techniques yield better performance in comparison with IMU sensors alone. For instance, the authors in [166] have recently

integrated onboard GNSS and INS systems, with the precise localization capabilities of road semantics, such as lane lines and poles, to achieve high accurate positioning. With the advent of the UAV-assisted Cellular Vehicle-to-Everything (C-V2X) communication technology, UAVs can periodically exchange Cooperative Awareness Messages (that contain UAV specific information such as vehicle speed, position, and predicted path in accordance to the European Telecommunications Standards Institute) and Basic Safety Messages (containing vehicle safety-related information, according to SAE J2735 Intelligent Transportation Systems (ITS) standards) with surrounding network nodes such as other UAVs, ground based vehicles, and infrastructures. [167] outlines a state-of-art peer-to-peer backbone for aerial data sharing. [168] utilizes UAVs as data collectors for exchanging data between IoT devices. The authors in [169] have recently formulated a Road Side Unit (RSU) based cooperative localization scheme for lane-level positioning accuracy of ground-based autonomous vehicles in GNSS denied environments, using C-V2X technology. The present paper proposes a UAV-assisted C-V2X network of multi-agent UAVs that periodically exchange their perceived positions in space with their neighbouring UAVs, to correct their estimated positions based on LiDAR-measured air-distances, and without necessity of messaging with static infrastructures such as RSU.

3.3.2 Contributions of the Section

The main contribution of this section is formulation of a localization filtering algorithm that compensates the positioning error of individual UAVs in large connected networks, by integrating the available sensing resources in the network of the UAVs, and without reliance on land-based position marks or stray radio signals (which is the state-of-the-art in GNSS denied localization, according to the best knowledge of the author of this thesis). Mitigation of the odometry positioning error is carried out through cooperation with other UAVs in the network, and consensus among the UAVs over their true positions. This would be especially advantageous in scenarios where flocks of UAVs are flying in unknown isolated airspace, or where access to GNSS signals are denied or spoofing cyberattacks are present. In an urban airspace where stationary anchors are present, the proposed algorithm improves the positioning error, through combination of the UAV's sensing resources and distribution of the total network error equally among the UAVs, in accordance to the law of large numbers. The Cooperative localization technique introduced in this paper is a multi-agent filter that surpasses the accuracy of the existing statistical optimization methods.

3.3.3 Problem Statement

Let the undirected graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{A})$ represent a connected wireless network, where $\mathcal{N}$ is the set of nodes representing N number of vehicles (referred to as agents), $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$ representing the set of edges, and $\mathcal{A} = [a_{ij}]_{N \times N}$, $a_{ij} \in \{0, 1\}$ the adjacency matrix, where $i \in \{1, \dots, N\}$ denotes the reference number of the agent. The elements of $\mathcal{A}$ are defined such that $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$ if $(i, j) \notin \mathcal{E}$. Additionally, let $\mathcal{N}_i$ denote the set of neighbours of agent i (i.e., agents whose elements in the Adjacency is $a_{ij} = 1$). Finally, the Laplacian matrix $L \triangleq [\ell_{ij}] \in \mathbb{R}^{n \times n}$ associated to $\mathcal{G}$ is defined where,

$$\ell_{ii} = \sum_{j=1}^N a_{ij} = \sum_{i=1}^N a_{ji}, \text{ and } \ell_{ij} = -a_{ij}, \forall i \neq j. \quad (3.14)$$

Additionally, let $\mathbf{x}^{(i)}(t) = [x^{(i)}(t), y^{(i)}(t), z^{(i)}(t)]^T \in \mathbb{R}^3$ denote the true three-dimensional position of vehicle i at time t , with reference to a given coordinate system. It is further assumed that the motion model of UAV i is given by,

$$\begin{aligned} \dot{\mathbf{x}}^{(i)}(t) &= \mathbf{v}^{(i)}(t) \\ \dot{\mathbf{v}}^{(i)}(t) &= \frac{1}{m} \mathbf{u}^{(i)}(t) - \frac{1}{m} G + \frac{1}{m} \mathbf{w}^{(i)}(t) \\ \vartheta^{(i)}(t) &= M(\eta^{(i)}) \ddot{\eta}^{(i)}(t) + C(\eta^{(i)}, \dot{\eta}^{(i)}) \dot{\eta}^{(i)}(t) \end{aligned} \quad (3.15)$$

where m is the UAV mass, $\mathbf{v}^{(i)}$ is the three dimensional airspeed, G is the force of gravity, $\eta^{(i)} = [\theta, \phi, \psi]^T$ is the attitude vector of the UAV, and $\mathbf{w}^{(i)}$ is an unknown disturbance force with zero mean, where $\mathbb{E}[\mathbf{w}^{(i)}(t)] = 0$, $\forall t \in \mathbb{R}^+$, and

$$\mathbf{u}^{(i)}(t) = f(t) \begin{bmatrix} \cos \psi \sin \theta \cos \phi + \sin \psi \sin \phi \\ \sin \psi \sin \theta \cos \phi - \cos \psi \sin \phi \\ \cos \phi \cos \theta \end{bmatrix}$$

is the thrust vector, all in the inertial reference frame, and $\vartheta^{(i)} = [\vartheta_\phi, \vartheta_\theta, \vartheta_\psi]^T$ is the propeller torque vector such that,

$$\begin{bmatrix} f \\ \vartheta_\phi \\ \vartheta_\theta \\ \vartheta_\psi \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -d_\phi & -d_\phi & d_\phi & d_\phi \\ d_\theta & -d_\theta & d_\theta & -d_\theta \\ c_\vartheta & -c_\vartheta & -c_\vartheta & c_\vartheta \end{bmatrix} \begin{bmatrix} f_{1_k} \\ f_{2_k} \\ f_{3_k} \\ f_{4_k} \end{bmatrix} \quad (3.16)$$

where d_ϕ, d_θ , and c_ϑ are known constants which denote the half of roll motor-to-motor distance, half of pitch motor-to-motor distance, and the relationship between the thrust force f and its corresponding torque, respectively, and where $M(\eta^{(i)})$, $C(\eta^{(i)}, \dot{\eta}^{(i)})$ represent the diagonal moment of inertia tensor, and the Coriolis matrix, respectively, and

where G is the gravity force in the inertial reference frame.

Equation (4.4) can be used to obtain an odometry representation of the UAV 3-D airspeed that will be associated with errors resulting from the onboard sensors and actuator imperfections. Therefore, one can assume that given Equation (4.4) and onboard IMU sensors $\bar{\mathbf{v}}^{(i)}(t) = \mathbf{v}^{(i)}(t) + \Delta\mathbf{v}^{(i)}(t)$ is available, where $\Delta\mathbf{v}^{(i)}$ is assumed to be an unknown zero sample mean error, i.e., $\mathbb{E}_i[\Delta\mathbf{v}^{(i)}(t)] = \frac{1}{N} \sum_{i=1}^N \Delta\mathbf{v}^{(i)}(t) = 0$. Then the approximate position of the UAV can be derived through an odometry model that is given by,

$$\bar{\mathbf{x}}^{(i)}(t) = \mathbf{x}^{(i)}(t_0) + \int_{\tau=t_0}^t \bar{\mathbf{v}}^{(i)}(\tau) d\tau \quad (3.17)$$

where $\bar{\mathbf{x}}^{(i)}(t)$ denotes the 3-D odometry position of the UAV, and $\mathbf{x}^{(i)}(t_0)$ denotes the true position of the UAV at some reference point t_0 where $\mathbf{x}^{(i)}(t_0)$ is available. Therefore, integration of $\Delta\mathbf{v}^{(i)}(t)$ over time (in Equation (3.17)) can be regarded as a dominant factor for localization error in odometry (also referred to as dead reckoning). The author further denotes $\mathbf{x}(t) = [\mathbf{x}^{(1)}(t), \mathbf{x}^{(2)}(t), \dots, \mathbf{x}^{(N)}(t)]^T$ as the true position of the network of UAVs, and $\bar{\mathbf{x}}(t) = [\bar{\mathbf{x}}^{(1)}(t), \bar{\mathbf{x}}^{(2)}(t), \dots, \bar{\mathbf{x}}^{(N)}(t)]^T$ as the odometry position estimation of the network.

Given the above, let $t = kT_s \in \mathbb{R}^+$ and assume that kT_s , $k \in \mathbb{N}^+$ represents a set of points at which the true position $\mathbf{x}^{(i)}(kT_s)$ is required to be estimated from $\bar{\mathbf{x}}^{(i)}(kT_s)$, where $T_s \in \mathbb{R}^+$ is an arbitrarily small sampling period, and $k \in \mathbb{N}^+$. Then the objective of this section is to find $\hat{\mathbf{x}}(kT_s + \Delta t) \in \mathbb{R}^3$, such that $\|\hat{\mathbf{x}}(kT_s + \Delta t) - \mathbf{x}(kT_s)\|^2$ is minimum, where $\Delta t \in [0, T_s]$ represents a small transient time. In order to accomplish this objective, the author considers an LTI filter with an impulse response $h(t)$, and has to find an excitation $\hat{\mathbf{u}}(t)$ for the filter, such that,

$$\hat{\mathbf{x}}(kT_s + \Delta t) \triangleq \bar{\mathbf{x}}(kT_s) + \hat{\mathbf{u}}(kT_s + \Delta t) * h(kT_s + \Delta t), \quad (3.18)$$

so that $\hat{\mathbf{x}}(kT_s + \Delta t) \rightarrow \mathbf{x}(kT_s)$, as $\Delta t \rightarrow T_s$ (for all k), where $\hat{\mathbf{u}}(kT_s + \Delta t) * h(kT_s + \Delta t)$ is the error compensation term, and is intended to compensate the error in the odometry model $\bar{\mathbf{x}}(kT_s)$.

Remark 8. It would be intuitive to realize the similarity of Equation (3.18) with Kalman filter, where,

$$\hat{\mathbf{x}}(kT_s) \triangleq \bar{\mathbf{x}}(kT_s) + K(\mathbf{z}(kT_s) - \bar{\mathbf{x}}(kT_s))$$

and where $\mathbf{z}(kT_s)$ is a position observation (if existing), and K is the Kalman filter gain. In Equation (3.18), $\hat{\mathbf{u}}(kT_s + \Delta t) * h(kT_s + \Delta t)$ is the term that replaces $K(\mathbf{z}(kT_s) - \bar{\mathbf{x}}(kT_s))$, since $\mathbf{z}(kT_s)$ is not available in our problem.

However, $\bar{\mathbf{x}}(kT_s)$ and $\mathbf{x}(kT_s)$ are stochastic processes, since $\mathbf{x}(kT_s)$ is affected by random disturbances and unknown actuator errors. Therefore, in a more realistic framework the objective would be,

$$\min_{h(t)} \lim_{\Delta t \rightarrow T_s} \mathbb{E}[\|\hat{\mathbf{x}}(kT_s + \Delta t) - \mathbf{x}(kT_s)\|^2], \forall i \in \mathcal{N}. \quad (3.19)$$

implying minimum steady state error in a mean-sense. Objective (3.19) could be also written along all three axes as,

$$\hat{x}(kT_s + \Delta t) \triangleq \hat{u}_x(kT_s + \Delta t) * h(kT_s + \Delta t) + \bar{x}(kT_s),$$

where $\hat{u}_x$ is the filter excitation $\hat{\mathbf{u}}$ along the x -axis (to be determined), and $*$ denotes the convolution operator, and where the same applies to y -axis, and z -axis in a similar fashion. However, if $\Delta \mathbf{x}^{(i)}(kT_s + \Delta t)$ denotes the filter error, one can write,

$$\hat{\mathbf{x}}^{(i)}(kT_s + \Delta t) = \mathbf{x}^{(i)}(kT_s) + \Delta \mathbf{x}^{(i)}(kT_s + \Delta t), \quad (3.20)$$

and the objective in (3.19) could be equivalently written as,

$$\min_{h(t)} \lim_{\Delta t \rightarrow T_s} \mathbb{E}[\|\Delta \mathbf{x}^{(i)}(kT_s + \Delta t)\|^2], \forall i \in \mathcal{N}, \forall k \in \mathbb{N}^+, \quad (3.21)$$

where $\|\Delta \mathbf{x}^{(i)}(kT_s + \Delta t)\|^2 = (\Delta x^{(i)}(kT_s + \Delta t))^2 + (\Delta y^{(i)}(kT_s + \Delta t))^2 + (\Delta z^{(i)}(kT_s + \Delta t))^2$. Obviously, the objective in (3.21) is satisfied if the variance $\text{VAR}(\Delta x^{(i)}(kT_s + \Delta t))$ can be minimized for all i and k by a correct choice for $h(t)$, since in this case the same would apply for $\Delta y^{(i)}(kT_s)$, and $\Delta z^{(i)}(kT_s)$. Therefore, it would be sufficient to concentrate on the localization policy for the x -axis only, noting that the same would apply for the other two axes in a similar fashion.

3.3.4 Assumptions and Definitions

We assume that UAVs are equipped with onboard rangefinders to determine the relative range of surrounding agents and static obstacles. However, rangefinders (such as LiDARs) are devices with stochastic uncertainties, as explained in [132, 170]. Therefore, given the relative range $\omega^{(i,j)}(kT_s) = x^{(i)}(kT_s) - x^{(j)}(kT_s)$, $j \in \mathcal{N}_i$, the rangefinder reads $\omega^{(i,j)}(kT_s) + \Delta \omega^{(i,j)}(kT_s)$, where $\Delta \omega^{(i,j)}(kT_s)$ is a random error that i reads when finding its range to j , along the x -axis.

Assumption 5. Let $\Delta t \in [0, T_s]$ be sufficiently small so that $\omega^{(i,j)}(kT_s + \Delta t) \approx \omega^{(i,j)}(kT_s)$. This implies that although the vehicles are in continuous motion, the displacement can be considered as negligible over Δt .

Assumption 6. It is assumed that $\Delta x^{(i)}(kT_s)$'s are zero sample mean identically independent distributed (i.i.d) random variables for all i and k , that is,

$$\begin{aligned} \mathbb{E}[\Delta x^{(i)}(kT_s) \Delta x^{(j)}(kT_s)] &= \\ \mathbb{E}[\Delta x^{(i)}(kT_s)] \mathbb{E}[\Delta x^{(j)}(kT_s)] &= 0, \forall i, j \in \mathcal{N}, \end{aligned}$$

and,

$$\lim_{N=|\mathcal{N}| \rightarrow \infty} \sum_{i \in \mathcal{N}} \Delta x^{(i)}(kT_s) = 0.$$

This assumption implies that while individual sensors may have drift errors, the sum of the samples cancel out individual drifts as well as the white noise errors associated with each sensor.

Assumption 7. It is further assumed that $\mathbb{E}[\Delta \omega^{(i,j)}(kT_s)] = 0, \forall i \in \mathcal{N}, j \in \mathcal{N}_i$, and,

$$\begin{aligned} \mathbb{E}[\Delta \omega^{(i,j_1)}(kT_s) \Delta \omega^{(i,j_2)}(kT_s)] &= \\ \mathbb{E}[\Delta \omega^{(i,j_1)}(kT_s)] \mathbb{E}[\Delta \omega^{(i,j_2)}(kT_s)] &= 0, \end{aligned}$$

for all $i \in \mathcal{N}, j_1, j_2 \in \mathcal{N}_i$, implying that rangefinder uncertainties, are mutually independent zero sample mean random variables too.

Definition 6. Given that $\Delta x(kT_s + \Delta t) = [\Delta x^{(1)}(kT_s + \Delta t), \dots, \Delta x^{(N)}(kT_s + \Delta t)]^T$, the network error of the cooperative localization method along the x -axis, at time-step k , is defined as,

$$\begin{aligned} &\lim_{\Delta t \rightarrow T_s} \mathbb{E}[|\Delta x(kT_s + \Delta t)|^2] \\ &= \lim_{\Delta t \rightarrow T_s} \mathbb{E}[(\Delta x(kT_s + \Delta t))^T \Delta x(kT_s + \Delta t)] \\ &\triangleq \sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}), \end{aligned}$$

where $\Delta x^{(i)}(kT_s + \Delta t) = \hat{x}^{(i)}(kT_s + \Delta t) - x^{(i)}(kT_s + \Delta t)$, and the network error of the odometry localization method along the x -axis, at time-step k , as,

$$\mathbb{E}[|\bar{x}(kT_s) - x(kT_s)|^2] \triangleq \sigma_{\Delta x(kT_s)}^2(\text{Odometry}).$$

Additionally, the network sensor error is further defined as,

$$\mathbb{E}[|\Delta \omega(kT_s)|^2] = \sum_{i \in \mathcal{N}} \sum_{j \in \mathcal{N}_i} \mathbb{E}[(\Delta \omega^{(i,j)}(kT_s))^2] \triangleq \sigma_{\Delta \omega(kT_s)}^2,$$

and the Cooperative Localization Error Gain (CLEG) along the x -axis will be defined as,

$$CLEG = \frac{\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})}{\sigma_{\Delta \omega(kT_s)}^2}.$$

The cooperative localization error gain is a metrics to evaluate the total positioning error in a network. It will be shown later in Section [3.3.6](#) that the network error in a cooperative localization scheme depends on the network connectivity, and the topological diameter, as well as network size.

3.3.5 Cooperative Localization in Multi-Agent Networks

For the time being, let the sensor error be ignored and assume ideal ranging devices for the vehicles, where $\omega^{(i,j)}(kT_s) = x^{(i)}(kT_s) - x^{(j)}(kT_s)$, $j \in \mathcal{N}_i$, and where $\omega^{(i,j)}(kT_s)$ s are measurable for all i , and each time kT_s . In Section 3.3.6, sensor errors are taken into account and the section analyzes CLEG for a realistic case, and then compares the network error analytically in a network of UAVs, with and without cooperative localization. However, imagine the LTI filter discussed in Equation (3.18), to be in accordance to the block diagram in Figure 3.5, and Theorem 7 below.

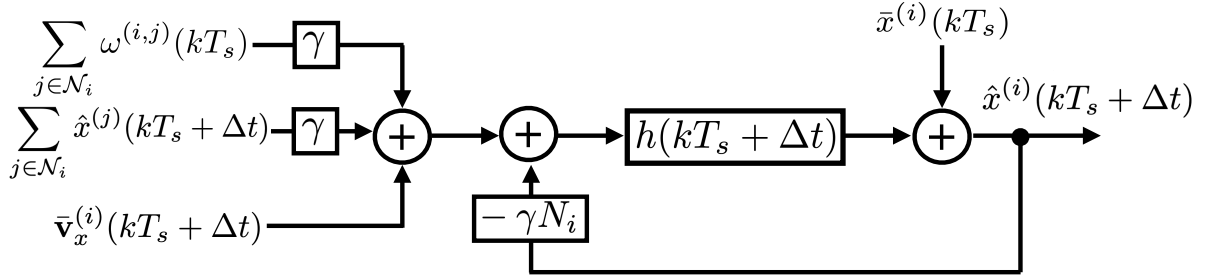


Figure 3.5: The LTI filter and the associated block diagram as a function of $\bar{x}^{(i)}(kT_s)$, and the onboard sensors, as well as the filter output of the neighbour UAVs. The input to the filter is the Odometry localization sample $\bar{x}^{(i)}(kT_s)$, and the onboard sensor information taken from the rangefinders, and the air-speed along the x -axis. The filter feedback gain γN_i is a parameter that will be selected later in this paper, where N_i is the number of neighbours to i , and γ is a positive scalar.

Theorem 7. *In a large connected and balanced network with graph $\mathcal{G}$, where $N \rightarrow \infty$, the LTI filter with the impulse response $h(kT_s + \Delta t) = \varrho(kT_s) - \varrho(kT_s + \Delta t)$ provides accurate positioning in a steady state (i.e., $\lim_{N \rightarrow \infty} \sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) = 0$), if $\hat{x}^{(i)}(kT_s) = \bar{x}^{(i)}(kT_s)$, $\forall k \in \mathbb{N}^+$, where $\varrho(\cdot)$ is the unit step function, and where the inputs to the filter are depicted in Figure 3.5.*

Proof. Let $\hat{\mathbf{u}}(kT_s + \Delta t)$ in Equation (3.18) along the x -axis be,

$$\begin{aligned} \hat{u}_x^{(i)}(kT_s + \Delta t) &= \gamma \sum_{j \in \mathcal{N}_i} (\hat{x}^{(j)}(kT_s + \Delta t) - \hat{x}^{(i)}(kT_s + \Delta t) \\ &\quad + \omega^{(i,j)}(kT_s)) + \bar{\mathbf{v}}_x^{(i)}(kT_s + \Delta t) \end{aligned}$$

where $x^{(j)}(kT_s + \Delta t) - x^{(i)}(kT_s + \Delta t) + \omega^{(i,j)}(kT_s) = 0$ (with reference to the Assumptions). One would simply deduce that,

$$\sum_{j \in \mathcal{N}_i} (\hat{x}^{(j)}(kT_s + \Delta t) - \hat{x}^{(i)}(kT_s + \Delta t) + \omega^{(i,j)}(kT_s))$$

$$= \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(kT_s + \Delta t) - \Delta x^{(i)}(kT_s + \Delta t)).$$

Furthermore, with due attention to the definition of the impulse response $h(t)$, it follows that,

$$\begin{aligned} \hat{u}_x^{(i)}(kT_s + \Delta t) * h(kT_s + \Delta t) &= \\ \int_{\tau=-\infty}^{\infty} \hat{u}_x^{(i)}(\tau - kT_s - \Delta t) h(\tau) d\tau &= \int_{kT_s}^{kT_s + \Delta t} \hat{u}_x^{(i)}(\tau) d\tau. \end{aligned}$$

Following simple manipulations, the equation of the filter output can be written as,

$$\begin{aligned} \hat{x}^{(i)}(kT_s + \Delta t) &= \bar{x}^{(i)}(kT_s) + \int_{kT_s}^{kT_s + \Delta t} \bar{\mathbf{v}}_x^{(i)}(\tau) d\tau \\ &+ \int_{kT_s}^{kT_s + \Delta t} \gamma \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(\tau) - \Delta x^{(i)}(\tau)) d\tau. \end{aligned}$$

However, since the theorem assumes that $\hat{x}^{(i)}(kT_s) = \bar{x}^{(i)}(kT_s)$, one can use Equation (3.20) to write,

$$\bar{x}^{(i)}(kT_s) = x^{(i)}(kT_s) + \Delta x^{(i)}(kT_s), \quad (3.22)$$

and by derivation and substitution for $\hat{x}^{(i)}$, $\bar{x}^{(i)}$, it follows that,

$$\begin{aligned} \dot{x}^{(i)}(kT_s + \Delta t) + \Delta \dot{x}^{(i)}(kT_s + \Delta t) &= \dot{x}^{(i)}(kT_s) + \Delta \dot{x}^{(i)}(kT_s) \\ &+ \bar{\mathbf{v}}_x^{(i)}(kT_s + \Delta t) - \bar{\mathbf{v}}_x^{(i)}(kT_s) \\ &+ \gamma \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(kT_s + \Delta t) - \Delta x^{(i)}(kT_s + \Delta t)) \\ &- \gamma \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(kT_s) - \Delta x^{(i)}(kT_s)), \end{aligned}$$

and noting that $\dot{x}^{(i)}(kT_s + \Delta t) - \bar{\mathbf{v}}_x^{(i)}(kT_s + \Delta t) = \dot{x}^{(i)}(kT_s) - \bar{\mathbf{v}}_x^{(i)}(kT_s)$ for a small Δt , one can write,

$$\Delta \dot{x}^{(i)}(kT_s) = \gamma \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(kT_s) - \Delta x^{(i)}(kT_s)),$$

and,

$$\Delta \dot{x}^{(i)}(kT_s + \Delta t) = \gamma \sum_{j \in \mathcal{N}_i} (\Delta x^{(j)}(kT_s + \Delta t) - \Delta x^{(i)}(kT_s + \Delta t))$$

which in a vector form can be written as,

$$\Delta \dot{x}(kT_s + \Delta t) = -\gamma L \Delta x(kT_s + \Delta t). \quad (3.23)$$

One can observe that Equation (3.23) is a consensus control protocol for the error vector $\Delta x(kT_s + \Delta t)$, with the solution,

$$\Delta x(kT_s + \Delta t) = e^{-\gamma L \Delta t} \Delta x(kT_s). \quad (3.24)$$

Therefore, given a balanced graph $\mathcal{G}$, the steady state output of the filter is reduced to,

$$\lim_{\gamma\Delta t \rightarrow \infty} \Delta x(kT_s + \Delta t) = \frac{1}{N} \sum_{i=1}^N \Delta x^{(i)}(kT_s) \mathbf{1}_N,$$

where γ is assumed to be a very large positive scalar, and $\Delta t \rightarrow T_s$, where,

$$\Delta x^{(i)}(kT_s) = \hat{x}^{(i)}(kT_s) - x^{(i)}(kT_s) = \bar{x}^{(i)}(kT_s) - x^{(i)}(kT_s),$$

and where $\mathbf{1}_N$ is a column vector of ones with N rows. In other words,

$$\lim_{\gamma\Delta t \rightarrow \infty} \Delta x^{(i)}((k+1)T_s) = \frac{1}{N} \sum_{i=1}^N \Delta x^{(i)}(kT_s), \quad \forall i \in \mathcal{N},$$

and clearly, $\lim_{N \rightarrow \infty} \lim_{\gamma\Delta t \rightarrow \infty} \Delta x^{(i)}(kT_s) = 0, \quad \forall k > 0$. However, above also implies that $\Delta x^{(i)}((k+1)T_s)$ is the random mean of $\Delta x^{(i)}(kT_s)$ over all i , for all k . Therefore, according to Assumption [6](#),

$$\lim_{\gamma\Delta t \rightarrow \infty} \mathbb{E}[\Delta x^{(i)}((k+1)T_s)] = 0,$$

and,

$$\lim_{\gamma\Delta t \rightarrow \infty} \text{VAR}[\Delta x^{(i)}((k+1)T_s)] = \frac{1}{N} \text{VAR}[\Delta x^{(i)}(kT_s)],$$

implying that for a sufficiently large γ , $\Delta x^{(i)}((k+1)T_s) \rightarrow 0, \quad \forall i \in \mathcal{N}$ (as $\Delta t \rightarrow T_s$), which completes the proof of the theorem. $\blacksquare$

Remark 9. Theorem [7](#) implies that the filter in Figure [3.5](#) takes samples $\bar{x}^{(i)}(kT_s)$ as initial values for $\hat{x}^{(i)}(kT_s)$ (at the beginning of each time interval $[kT_s, kT_s + \Delta t]$, $k \in \mathbb{N}^+$), and as $\Delta t \rightarrow T_s$, $\hat{x}^{(i)}(kT_s + \Delta t)$ gets closer and closer to the true position $x^{(i)}(kT_s)$. Recall that $\gamma\Delta \rightarrow \infty$ is practically equivalent to $\Delta t \rightarrow T_s$, since a sufficiently large $\gamma \in \mathbb{R}^+$ has been selected. An optimal value for $\gamma\Delta t$ will be derived later in order to achieve a minimal network error when range-finder sensor error is present.

Theorem [7](#) implies that cooperative localization provides a smaller error in a mean square sense, when estimating the position of a group of vehicles in a connected network by N times, if the vehicles exchange their filtered positions $\hat{x}^{(i)}(kT_s + \Delta t)$, $\Delta t \in [0, T_s]$ (in accordance with Figure [3.5](#)), as part of the cooperative awareness messages, rather than the usual $\bar{x}^{(i)}(kT_s)$ suggested by SAE J2735 Intelligent Transportation Systems standards. When the number of agents N is very large one will have $\lim_{\gamma\Delta t \rightarrow \infty} \mathbb{E}[(\Delta x^{(i)}(kT_s + \Delta t))^2] \rightarrow 0, \quad \forall i \in \mathcal{N}$, implying that $\Delta x^{(i)}(kT_s + \Delta t) \rightarrow 0$, as $\Delta t \rightarrow \infty$, which means precise localization. Cooperative localization scheme of a network with three vehicles has been illustrated in Figure [3.6](#). We have seen in Section [3.1.2](#) that the regression filtering technique is also available for reducing localization error, and one can optimize

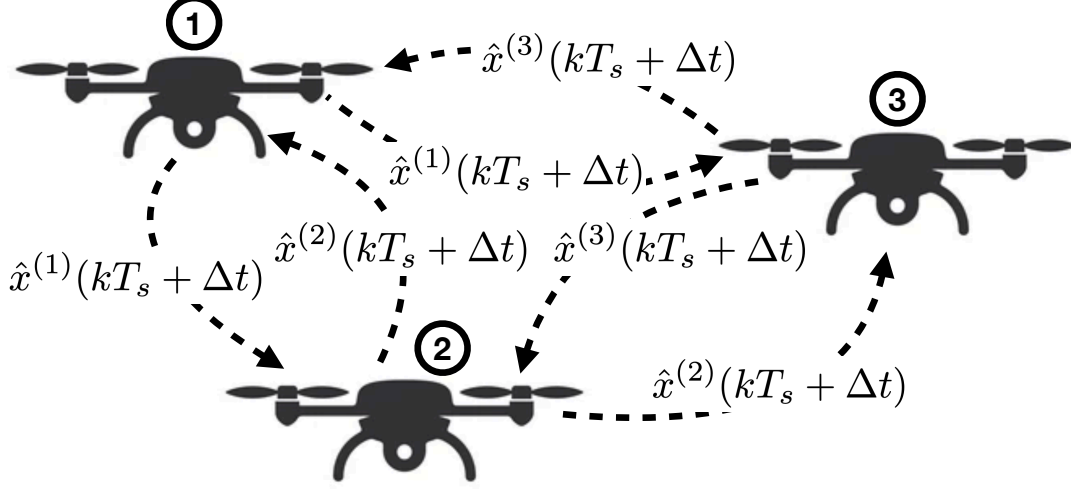


Figure 3.6: A distributed cooperative localization scheme for a MAS with 3 agents. Each agent i recursively transmits its self-estimated position $\hat{x}^{(i)}(kT_s + \Delta t)$ continuously to its neighbours, until a relative consensus is achieved in the network (and that is when $\hat{x}^{(i)}(kT_s + \Delta t)$ reaches a steady state).

positioning error by means of a minimum-mean-square-error (MMSE) filter to obtain $\min_{H_k} \mathbb{E}[||x(kT_s) - H_k \bar{x}(kT_s)||^2]$, directly from $\bar{x}^{(i)}(kT_s)$'s. In that case a centralized control unit would be required to process the odometry estimated positions of all vehicles, and find H_k that provides a more accurate position, namely $z(kT_s) = H_k \bar{x}(kT_s)$, and transmit $z^{(i)}(kT_s)$ back to each agent as an improved positioning estimation to use for navigation purposes, instead of $\bar{x}^{(i)}(kT_s)$. This is illustrated in Figure 3.7. It is later shown that proposed distributed cooperative localization in Figure 3.6 is beneficial to the centralized MMSE cooperative localization (regression filtering technique) in Figure 3.7, by a factor of $N/2$.

3.3.6 Theoretical Results

Theorem 7 introduces the main philosophy behind cooperative localization. In a limited time duration Δt there would be an error associated with the transient response of the LTI filter and insufficient time for consensus that will be discussed in Theorem 8 below.

Theorem 8. *In any connected and balanced graph $(\mathcal{G})$, where $N \rightarrow \infty$, and where $\Delta\omega^{(i,j)}(kT_s) \approx 0$, and given a set of initial odometry estimates, $\bar{x}(kT_s) = [\bar{x}^{(1)}(kT_s), \dots, \bar{x}^{(N)}(kT_s)]^T$, cooperative localization guarantees an arbitrarily small mean-sense positioning error $\epsilon = e^{-\gamma\lambda_2\Delta t} \sigma_{\Delta x(kT_s)}(\text{Odometry})$, where,*

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) < \epsilon^2,$$

and where λ_2 is the second smallest eigenvalue of L .

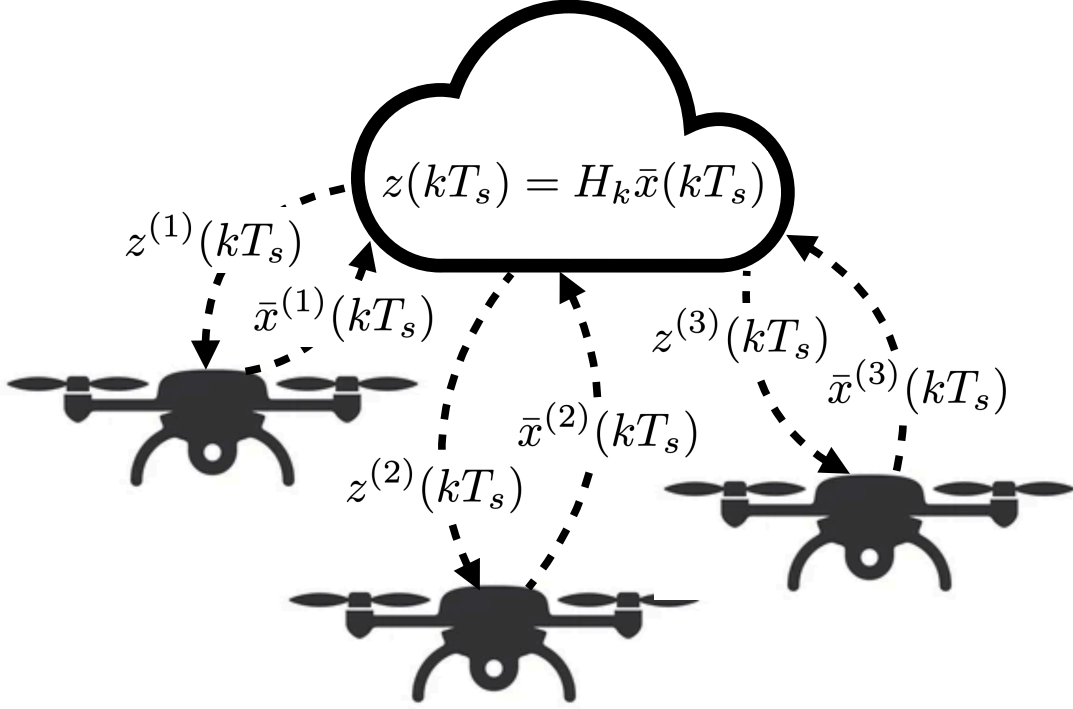


Figure 3.7: A centralized Minimum-Mean-Square-Error (MMSE) based localization (referred to as regression filtering in Section 3.1.2) of a MAS with 3 agents. Every agent transmits its self-estimated position $\bar{x}(kT_s)$ at each time-step kT_s , and a centralized computation center derives H_k and transmits the corrected positions $z(kT_s) = H_k \bar{x}(kT_s)$ back to the agents.

Proof. The proof begins with Equation (3.23). One can write,

$$\Delta x(kT_s + \Delta t) = \quad (3.25)$$

$$\frac{1}{N} \sum_{i=1}^N \Delta x^{(i)}(kT_s) \mathbf{1}_N + \sum_{j=2}^N v_j e^{-\gamma \lambda_j \Delta t} v_j^T \Delta x(kT_s),$$

where, λ_j and v_j are the j^{th} eigenvalue and its corresponding eigenvector in L , respectively, and $\mathbf{1}_N = [1, \dots, 1]_{1 \times N}^T$. For a sufficiently large N one will have, $\frac{1}{N} \sum_{i=1}^N \Delta x^{(i)}(kT_s) \mathbf{1}_N \approx \mathbb{E}[\Delta x^{(i)}(kT_s)] \mathbf{1}_N = \mathbf{0}_N$, and Equation (3.25) reduces to,

$$\Delta x(kT_s + \Delta t) = \sum_{i=2}^N v_i e^{-\gamma \lambda_i \Delta t} v_i^T \Delta x(kT_s), \quad (3.26)$$

and,

$$\begin{aligned} \Delta x(kT_s + \Delta t)^T \Delta x(kT_s + \Delta t) = \\ \Delta x(kT_s)^T \left(\sum_{i=2}^N \sum_{j=2}^N v_j e^{-\gamma \lambda_j \Delta t} v_j^T v_i e^{-\gamma \lambda_i \Delta t} v_i^T \right) \Delta x(kT_s) \end{aligned}$$

where, $v_j^T v_i = 0, \forall i \neq j$, and $v_i^T v_i = 1, \forall i$. Therefore, one can write,

$$\Delta x(kT_s + \Delta t)^T \Delta x(kT_s + \Delta t) =$$

$$\Delta x(kT_s)^T \left(\sum_{i=2}^N v_i e^{-2\gamma\lambda_i\Delta t} v_i^T \right) \Delta x(kT_s).$$

However, $\sum_{i=2}^N e^{-2\gamma\lambda_i\Delta t} \leq \sum_{i=2}^N e^{-2\gamma\lambda_2\Delta t}$. Therefore,

$$\begin{aligned} \Delta x(kT_s + \Delta t)^T \Delta x(kT_s + \Delta t) &\leq \\ \Delta x(kT_s)^T e^{-2\gamma\lambda_2\Delta t} \Delta x(kT_s). \end{aligned}$$

Also, considering that $\mathbb{E}[\Delta x(kT_s)^T \Delta x(kT_s)] = \sigma_{\Delta x(kT_s)}^2(\text{Odometry})$, it follows that,

$$\begin{aligned} \mathbb{E}[\Delta x(kT_s + \Delta t)^T \Delta x(kT_s + \Delta t)] &< \\ e^{-2\gamma\Delta t\lambda_2} \sigma_{\Delta x(kT_s)}^2(\text{Odometry}), \end{aligned}$$

or,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) < e^{-2\gamma\lambda_2\Delta t} \sigma_{\Delta x(kT_s)}^2(\text{Odometry}) \quad (3.27)$$

and finally assuming,

$$\epsilon = e^{-\gamma\lambda_2\Delta t} \sigma_{\Delta x(kT_s)}(\text{Odometry}), \quad (3.28)$$

it follows that $\mathbb{E}[(\hat{x}^{(i)}(t+\Delta t) - x^{(i)}(kT_s))^2] \leq \epsilon^2$, which completes the proof of the theorem. ■

For cases where there are limited agents, integrating Theorem 7 and 8, it follows that,

$$\begin{aligned} \sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) &< \\ \left(\frac{1}{N} + e^{-2\gamma\lambda_2\Delta t} \right) \sigma_{\Delta x(kT_s)}^2(\text{Odometry}), \end{aligned} \quad (3.29)$$

and one has to select $\gamma\Delta t$ such that $e^{-2\gamma\lambda_2\Delta t}$ is negligible for all possible network topologies. However, the significance of Theorem 8 can be realized by considering the example of a UAV's vertical landing in a network where GNSS service is denied. Then, Equation (3.29) can be used to evaluate the minimum admissible consensus interval Δt , to be able to land without violating the perimeters of the landing spot. Additionally, one can use Theorem 7 and 8 to evaluate the effect of spoofing cyberattacks on a given UAV such as m in a connected network of UAVs performing cooperative localization. Lemma 3 explains how cooperative localization can mitigate spoofing cyberattacks on a fleet of vehicles.

Lemma 3. *Let $\Delta\tilde{x}^{(m)}(kT_s)$ denote the positioning displacement induced on agent $m \in \mathcal{N}$, as a result of a spoofing cyberattack on m , where the agents are connected in a balanced graph $\mathcal{G}$, and where the agents perform cooperative localization. In this case, if the spoofed position of agent m is characterized as $x^{(m)}(kT_s) + \Delta\tilde{x}^{(m)}(kT_s)$, then cooperative localization induces a smaller error $\frac{1}{N}\Delta\tilde{x}^{(m)}(kT_s)$ to all the agents in $\mathcal{N}$, including m .*

The proof of the lemma is omitted. However, this phenomenon entails significant benefit in applications where spoofing cyberattack resiliency is concerned. For instance, one may imagine a fleet of naval vessels, where a large number of miniature drones will be deployed to navigate along with the vessel over a certain altitude, and form a *cyberattack shield* in order to distribute and absorb the cyberattack as implied in Lemma 3.

Remark 10. *Additionally, cooperative localization with at least one anchored UAV (such as UAV-0 with a deterministic position, where $\Delta\tilde{x}^{(0)}(kT_s) = 0, \forall k$) requires all other UAVs to achieve deterministic positions as a result of consensus, According to Remark 0, due to the fact that in an anchored UAV $\Delta\dot{\tilde{x}}^{(0)}(kT_s) = 0$. This implies that spoofing cyberattacks are contained in any “Anchored” cooperative localization scheme.*

In the next section the effect of rangefinder errors will be taken into account, and new bounds for the network error $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})$ will be introduced. Before this, Lemma 4 introduces as an alternative scenario that would yield accurate localization through cooperative localization in an ideal scenario (again neglecting sensor errors) with the aid of a anchor node. An “anchor node” is a stationary or mobile agent with known true position. A practical application can be in Advanced Air Mobility (AAM) applications where large numbers of UAV share urban airspace, while GPS signals are obscured for certain portion of the traffic, and available to part of the traffic. It will be shown that under this condition every vehicle in the AAM could achieve accurate localization, as long as the network is connected and a cooperative localization control protocol is applied in the network.

Lemma 4. *Let $\mathcal{G}$ denote a connected and balanced graph of a multi-agent system, and let $\Delta x^{(m)}(kT_s) = 0, \forall k \in \mathbb{N}$, for an arbitrary agent m (assuming $\Delta\omega^{(i,j)}(kT_s) \approx 0, \forall i, j \in \mathcal{N}$). In this case,*

$$\lim_{\Delta t \rightarrow T_s} \hat{x}^{(i)}(kT_s + \Delta t) \rightarrow x^{(i)}(kT_s), \forall i \in \mathcal{N},$$

if all the agents except agent m take part in a cooperative localization process (i.e., that is if $\hat{x}^{(m)}(kT_s + \Delta t) = \hat{x}^{(m)}(kT_s), \forall \Delta t$).

The proof has been provided in what followed Equation (3.8), and will not be repeated again here. Agent(s) m with deterministic positions with $\Delta x^{(m)}(kT_s) = 0$ are referred to as anchor nodes, as explained before. Any cooperative localization setting with one or more anchor nodes emulates a network with infinite number of agents.

The idea introduced in this subsection has neglected sensor errors in order to realize conceptual merits of cooperative localization. The next subsection will examine a more practical aspect of cooperative localization by including the sensor error in the derivations, and will improvise new conditions to attain optimal error gain and to minimize the

network localization error.

One can simply modify Equation (3.23) to account for $\Delta\omega^{(i,j)}(kT_s)$. In this case,

$$\Delta\dot{x}(kT_s + \Delta t) = -\gamma L \Delta x^{(i)}(kT_s + \Delta t) + \gamma \Delta\omega(kT_s), \quad \forall k \in \mathbb{N}. \quad (3.30)$$

It may be noted that Equation (3.30) is unstable due to rank deficiency of L . Therefore, $\gamma \Delta t$ has to be chosen such that Equation (3.30) results in a minimal $\sigma_{\Delta x(kT_s)}^2$ (Coop-Localization). If Δt is a sufficiently small time interval, so that one can assume negligible mobility for the vehicles during Δt , then $\omega(kT_s + \Delta t)$ can be assumed constant through $[kT_s, kT_s + \Delta t]$, $\forall k$. Therefore, it would be sufficient to once read $\omega(kT_s)$ in each time-step kT_s , and assume a constant $\Delta\omega(kT_s + \Delta t)$. However, the problem would still remain, being optimization of $\gamma\Delta t$, so that the CLEG is minimized.

Theorem 9. *Let $\mathcal{G}$ denote a connected multi-agent system with N agents. The network error gain is minimal if $\gamma\lambda_2\Delta t = N$.*

Note that in this case Equation (3.28) would simply reduce to $\epsilon = e^{-N}\sigma_{\Delta x(kT_s)}$ (Odometry).

Proof. The solution of Equation (3.30) is,

$$\begin{aligned} \Delta x(kT_s + \Delta t) &= e^{-\gamma L \Delta t} \Delta x(kT_s) + \int_{\tau=kT_s}^{kT_s + \Delta t} e^{-\gamma L(kT_s + \Delta t - \tau)} \Delta\omega(kT_s) d\tau \\ &= e^{-\gamma L \Delta t} \Delta x(kT_s) + \int_{\tau=0}^{\Delta t} e^{-\gamma L \tau} \Delta\omega(kT_s) d\tau. \end{aligned} \quad (3.31)$$

Let $v_1 = \frac{1}{\sqrt{N}}\mathbf{1}$, $v_2, \dots, v_N$, denote the right set of eigenvectors of L , corresponding to the eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_N$, respectively. Then,

$$e^{-\gamma L \Delta t} = \frac{1}{N} \mathbf{1} e^{-\gamma \lambda_1 \Delta t} \mathbf{1}^T + v_2 e^{-\gamma \lambda_2 \Delta t} v_2^T + \dots + v_N e^{-\gamma \lambda_N \Delta t} v_N^T, \quad (3.32)$$

where $\lambda_1 = 0$. Integration from 0 to Δt , results,

$$\int_{\tau=0}^{\Delta t} e^{-\gamma L \tau} d\tau = \frac{\Delta t}{N} \mathbf{1} \mathbf{1}^T + \sum_{i=2}^N v_i \frac{1 - e^{-\gamma \lambda_i \Delta t}}{\lambda_i} v_i^T,$$

and Equation (3.31) reduces to,

$$\begin{aligned} \Delta x(kT_s + \Delta t) &= \frac{1}{N} \mathbf{1} \mathbf{1}^T \Delta x(kT_s) + \frac{\gamma \Delta t}{N} \mathbf{1} \mathbf{1}^T \Delta\omega(kT_s) \\ &+ \sum_{i=2}^N v_i e^{-\gamma \lambda_i \Delta t} v_i^T \Delta x(kT_s) + \sum_{i=2}^N v_i \frac{1 - e^{-\gamma \lambda_i \Delta t}}{\lambda_i} v_i^T \Delta\omega(kT_s). \end{aligned} \quad (3.33)$$

For a sufficiently large $\gamma\lambda_2\Delta t$, where one can consider $e^{-\gamma\lambda_i\Delta t} \leq e^{-\gamma\lambda_2\Delta t} \approx 0$, Equation (3.33) further reduces to,

$$\Delta x(kT_s + \Delta t) \approx \frac{1}{N} \mathbf{1}^T \Delta x(kT_s) + \frac{\gamma \Delta t}{N} \mathbf{1}^T \Delta \omega(kT_s) + \sum_{i=2}^N v_i \frac{1}{\lambda_i} v_i^T \Delta \omega(kT_s). \quad (3.34)$$

The term $\frac{\gamma \Delta t}{N} \mathbf{1}^T + \sum_{i=2}^N v_i \frac{1}{\lambda_i} v_i^T$ can be further simplified, considering that,

$$\frac{\gamma \Delta t}{N} \mathbf{1}^T = [\mathbf{1} \ v_2 \ \dots \ v_N] \begin{bmatrix} \frac{\gamma \Delta t}{N} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} \mathbf{1}^T \\ v_2^T \\ \vdots \\ v_N^T \end{bmatrix}$$

and,

$$\sum_{i=2}^N v_i \frac{1}{\lambda_i} v_i^T = [\mathbf{1} \ v_2 \ \dots \ v_N] \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & \frac{1}{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{\lambda_N} \end{bmatrix} \begin{bmatrix} \mathbf{1}^T \\ v_2^T \\ \vdots \\ v_N^T \end{bmatrix}.$$

However, $L = V \Lambda V^{-1}$ can be written as,

$$L = [\mathbf{1} \ v_2 \ \dots \ v_N] \begin{bmatrix} \lambda_1 = 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_N \end{bmatrix} \begin{bmatrix} \mathbf{1}^T \\ v_2^T \\ \vdots \\ v_N^T \end{bmatrix},$$

where V is the matrix of right eigenvectors of L such that $V^{-1} = V^T$ (in a balanced network), and Λ is the diagonal matrix of the eigenvalues of L associated with V . In a similar way one can denote,

$$\frac{\gamma \Delta t}{N} \mathbf{1}^T + \sum_{i=2}^N v_i \frac{1}{\lambda_i} v_i^T \triangleq L_\gamma^{-1}$$

where L_γ is a full-rank version of L , that is,

$$L_\gamma = [\mathbf{1} \ v_2 \ \dots \ v_N] \begin{bmatrix} \frac{N}{\gamma \Delta t} & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_N \end{bmatrix} \begin{bmatrix} \mathbf{1}^T \\ v_2^T \\ \vdots \\ v_N^T \end{bmatrix}.$$

In conclusion, Equation (3.34) can be written as,

$$\Delta x(kT_s)(\Delta t) \approx \frac{1}{N} \mathbf{1}^T \Delta x(kT_s) + L_\gamma^{-1} \Delta \omega(kT_s), \quad (3.35)$$

where L_γ depends on $\gamma \Delta t$ and the eigenstructure of L . Equation (3.35) reveals that the total network error in a cooperative localization scenario, is composed of two terms, namely, (1) the mean network error,

$$\frac{1}{N} \mathbf{1} \mathbf{1}^T \Delta x(kT_s) = \frac{\sum_{i=1}^N \Delta x^{(i)}(kT_s)}{N} \mathbf{1}, \quad (3.36)$$

and, (2) the network sensor error,

$$L_\gamma^{-1} \Delta \omega(kT_s) = L_\gamma^{-1} \sum_{j \in \mathcal{N}_i} \Delta \omega^{(i,j)}(kT_s). \quad (3.37)$$

Considering that $\mathbb{E}[\Delta x^T(kT_s) \Delta \omega(kT_s)] = 0$, and $\mathbb{E}[\Delta x^{(i)}(kT_s) \Delta x^{(j)}(kT_s)] = 0$, one can obtain the total network error $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})$, as,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) = \frac{\sigma_{\Delta x(kT_s)}^2(\text{Odometry})}{N} + \mathbb{E} [\Delta \omega^T(kT_s) L_\gamma^{-2} \Delta \omega(kT_s)],$$

since $(L_\gamma^{-1})^T L_\gamma^{-1} = L_\gamma^{-2}$. Consequently, an upper bound for the total network error can be obtained as,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) \leq \frac{\sigma_{\Delta x(kT_s)}^2(\text{Odometry})}{N} + \frac{\sigma_{\Delta \omega(kT_s)}^2}{\lambda_{\min}^2(L_\gamma)}. \quad (3.38)$$

For a sufficiently large network, the first term on the right hand side of Inequality (3.38) diminishes, and one can deduce an upper bound for the network error gain as,

$$\frac{\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})}{\sigma_{\Delta \omega(kT_s)}^2} \leq \frac{1}{\lambda_{\min}^2(L_\gamma)}, \quad (3.39)$$

when $N \rightarrow \infty$, which provides a performance metric for a cooperative localization application. Optimal performance can be expected by maximizing $\lambda_{\min}(L_\gamma)$, and for a given N and λ_2 , this can be guaranteed if $\frac{N}{\gamma \Delta t} \geq \lambda_2$, or $N \geq \gamma \lambda_2 \Delta t$. In the meantime, one may note from Theorem (8) and Equation (3.28), that,

$$\epsilon = e^{-\gamma \lambda_2 \Delta t} \sigma_{\Delta x(kT_s)}(\text{Odometry}),$$

implying that $\gamma \lambda_2 \Delta t$ has to be maximized to reduce ϵ . This constraint together with $N \geq \gamma \lambda_2 \Delta t$ provides an optimal performance criteria, to be,

$$\gamma \lambda_2 \Delta t = N \quad (3.40)$$

which completes the proof of the theorem. ■

Given a multi-agent network with N agents, one can expect the largest λ_2 for a fully connected network. In this case $\lambda_2 = N$, and,

$$\frac{\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})}{\sigma_{\Delta \omega(kT_s)}^2} \leq \frac{1}{N^2},$$

also implying that the accuracy of positioning estimation in a cooperative localization framework improves with connectivity in the network. Furthermore, for a sufficiently

large and well connected network it would be possible to estimate localization precisely, regardless of the network sensor error. Additionally, it can be observed that in a fully connected network, the optimal condition requires $\gamma\Delta t = 1$.

The derivations have so far provided the total network error in its general term in a cooperative localization framework according to Equation (3.38). It is interesting to evaluate the performance of cooperative localization in comparison to the existing statistical methods that can optimally estimate unknown system states in mean square sense. For example, Kalman filter is one of those methods that can optimally estimate $x(kT_s)$ provided that there is a measurement vector such as $z(kT_s)$ which unfortunately does not exist in a GNSS denied environment. However, since the problem concerns a MAS of mobile vehicles, one might consider to optimally estimate $x(kT_s)$ through a linear transformation of $\bar{x}(kT_s)$, by an unknown matrix H_k , with the constraint,

$$\min_{H_k} \mathbb{E}[||x(kT_s) - H_k \cdot \bar{x}(kT_s)||^2].$$

Theorem 10 below shows that the proposed cooperative localization method provides $N/2$ times better performance in comparison to a minimum-mean-square-sense localization technique such as $H_k \cdot \bar{x}(kT_s)$. In order to be able to make a fair comparison between the two cases, it is assumed that the network sensor error is negligible.

Theorem 10. *Let $\mathcal{G}$ denote a connected balanced graph of a MAS with N agents, where $\mathbb{E}[||\Delta\omega(kT_s)||^2] = 0$. The optimal linear transformation H_k that minimizes $\mathbb{E}[||x(kT_s) - H_k \cdot \bar{x}(kT_s)||^2]$ is $N/2$ times less accurate in comparison with cooperative localization, i.e.,*

$$\min_{H_k} \mathbb{E}[||x(kT_s) - H_k \bar{x}(kT_s)||^2] \geq \frac{N}{2} \sigma_{\Delta x(kT_s)}^2 (\text{Coop-Localization}).$$

Proof. $x(kT_s) = [x^{(1)}(kT_s), \dots, x^{(N)}(kT_s)]^T$ denotes the true positions of given odometry calculations $\bar{x}(kT_s) = [\bar{x}^{(1)}(kT_s), \dots, \bar{x}^{(N)}(kT_s)]^T$. Let there be a vector function $z(kT_s) = [z^{(1)}(kT_s), \dots, z^{(N)}(kT_s)]^T$, where $z^{(i)}(kT_s) = \sum_{j=1}^N h_{ij} \bar{x}^{(j)}(kT_s)$. The first objective is to find h_{ij} 's such that $\mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))^2]$ is the minimum for all i . In a compact form let $H_k = [h_{ij}]$, and $z(kT_s) = H_k \bar{x}(kT_s)$, that is,

$$[z^{(1)}(kT_s), \dots, z^{(N)}(kT_s)]^T = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1N} \\ h_{21} & h_{22} & \dots & h_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N1} & h_{N2} & \dots & h_{NN} \end{bmatrix} \begin{bmatrix} \bar{x}^{(1)}(kT_s) \\ \bar{x}^{(2)}(kT_s) \\ \vdots \\ \bar{x}^{(N)}(kT_s) \end{bmatrix}.$$

The objective is to find h_{ij} 's such that $\mathbb{E}[(x(kT_s) - z(kT_s))^T(x(kT_s) - z(kT_s))]$ is minimum. This implies that,

$$\frac{\partial \mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))^2]}{\partial [h_{i1}, h_{i2}, \dots, h_{iN}]} = 0, \forall i$$

where,

$$z^{(i)}(kT_s) = [h_{i1}, \dots, h_{iN}]^T [\bar{x}^{(1)}(kT_s), \dots, \bar{x}^{(N)}(kT_s)].$$

Through expansion, it follows that,

$$\mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s)) \frac{\partial z^{(i)}(kT_s)}{\partial [h_{i1}, h_{i2}, \dots, h_{iN}]}] = 0, \forall i,$$

where,

$$\frac{\partial z^{(i)}(kT_s)}{\partial [h_{i1}, \dots, h_{iN}]} = [\bar{x}^{(1)}(kT_s), \dots, \bar{x}^{(N)}(kT_s)].$$

In other words, minimizing $\mathbb{E}[||x(kT_s) - z(kT_s)||^2]$ is equivalent to having,

$$\begin{bmatrix} \mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))\bar{x}^{(1)}(kT_s)] \\ \mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))\bar{x}^{(2)}(kT_s)] \\ \vdots \\ \mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))\bar{x}^{(N)}(kT_s)] \end{bmatrix} = \mathbf{0}_{N \times 1}, \forall i,$$

that is,

$$\mathbb{E}[(x^{(i)}(kT_s) - z^{(i)}(kT_s))\bar{x}^{(j)}(kT_s)] = 0, \forall i, j. \quad (3.41)$$

Substituting for $z^{(i)}(kT_s)$ in Equation (3.41) yields,

$$\mathbb{E}[x(kT_s)\bar{x}^T(kT_s)] = \mathbb{E}[(H_k \bar{x}(kT_s))\bar{x}^T(kT_s)]$$

or,

$$\mathbb{E}[x(kT_s)\bar{x}^T(kT_s)] = H_k \mathbb{E}[\bar{x}(kT_s)\bar{x}^T(kT_s)]$$

and finally resulting that,

$$H_k = \mathbb{E}[x(kT_s)\bar{x}^T(kT_s)] \left(\mathbb{E}[\bar{x}(kT_s)\bar{x}^T(kT_s)] \right)^{-1} \quad (3.42)$$

The term $(\mathbb{E}[\bar{x}(kT_s)\bar{x}^T(kT_s)])^{-1}$ in Equation (3.42) is possible to derive through Monte-Carlo methods. This is due to the fact that one can take samples from the known distribution $p(\bar{x}(kT_s))$ for all k 's. However, since the distribution $p(x(kT_s))$ is not accessible, the term $\mathbb{E}[x(kT_s)\bar{x}^T(kT_s)]$ is not derivable.

Nevertheless, let $p(x(kT_s))$ be assumed to be accessible, and proceed to determine the error function $\mathbb{E}[(x(kT_s) - z(kT_s))^T(x(kT_s) - z(kT_s))]$, and compare it with the network error derived through cooperative localization. Equation (3.41) reveals that the optimal

condition to minimize the network error $\mathbb{E}[(x(kT_s) - z(kT_s))^T(x(kT_s) - z(kT_s))]$ is satisfied when $\mathbb{E}[(x(kT_s) - z(kT_s))\bar{x}^T(kT_s)] = 0$. Therefore, under optimal conditions,

$$\begin{aligned} & \mathbb{E}[(x(kT_s) - z(kT_s))(x(kT_s) - z(kT_s))^T] \\ &= \mathbb{E}[(x(kT_s) - z(kT_s))x^T(kT_s)] \\ &= \mathbb{E}[(x(kT_s) - H_k\bar{x}(kT_s))x^T(kT_s)] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] - H_k\mathbb{E}[\bar{x}(kT_s)x^T(kT_s)], \end{aligned}$$

and substitution for H_k from Equation (3.42) results that,

$$\begin{aligned} & \mathbb{E}[(x(kT_s) - z(kT_s))(x(kT_s) - z(kT_s))^T] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] - \mathbb{E}[x(kT_s)x_{k|k-1}^T] (\mathbb{E}[\bar{x}(kT_s)x_{k|k-1}^T])^{-1} \mathbb{E}[\bar{x}(kT_s)x^T(kT_s)]. \end{aligned} \quad (3.43)$$

Since, for $\Delta t = 0$, cooperative localization simply reduces to odometry, one may note that $\bar{x}(kT_s) = x(kT_s) + \Delta x(kT_s)$, and Equation (3.43) can be further simplified, as,

$$\begin{aligned} \mathbb{E}[x(kT_s)x_{k|k-1}^T] &= \mathbb{E}[x(kT_s)(x^T(kT_s) + \Delta x^T(kT_s))] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[x(kT_s)\Delta x^T(kT_s)], \end{aligned}$$

where $\mathbb{E}[x(kT_s)\Delta x^T(kT_s)] = \mathbb{E}[x(kT_s)]\mathbb{E}[\Delta x(kT_s)] = 0$. Substituting $\mathbb{E}[x(kT_s)\bar{x}^T(kT_s)]$, and $\mathbb{E}[x^T(kT_s)\bar{x}(kT_s)]$, for $\mathbb{E}[x(kT_s)\bar{x}^T(kT_s)]$, and $\mathbb{E}[x^T(kT_s)\bar{x}(kT_s)]$, respectively, in Equation (3.43) follows that,

$$\begin{aligned} & \mathbb{E}[(x(kT_s) - z(kT_s))(x(kT_s) - z(kT_s))^T] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] - \mathbb{E}[x(kT_s)x^T(kT_s)] (\mathbb{E}[\bar{x}(kT_s)x_{k|k-1}^T])^{-1} \mathbb{E}[x(kT_s)x^T(kT_s)]. \end{aligned} \quad (3.44)$$

Additionally,

$$\begin{aligned} \mathbb{E}[\bar{x}(kT_s)x_{k|k-1}^T] &= \mathbb{E}[(x(kT_s) + \Delta x(kT_s))(x^T(kT_s) + \Delta x^T(kT_s))] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)] \end{aligned}$$

and Equation (3.43) can be written as,

$$\begin{aligned} & \mathbb{E}[(x(kT_s) - z(kT_s))(x(kT_s) - z(kT_s))^T] \\ &= \mathbb{E}[x(kT_s)x^T(kT_s)] - \mathbb{E}[x(kT_s)x^T(kT_s)] \\ & \quad (\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1} \\ & \quad \mathbb{E}[x(kT_s)x^T(kT_s)] \end{aligned}$$

$$\begin{aligned}
&= \mathbb{E}[x(kT_s) \cdot x^T(kT_s)] \\
&(\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1} \\
&(\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)]) \\
&\quad - \mathbb{E}[x(kT_s)x^T(kT_s)] \\
&(\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1} \\
&\quad \mathbb{E}[x(kT_s)x^T(kT_s)] \\
&= \mathbb{E}[x(kT_s)x^T(kT_s)] \\
&(\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1} \\
&(\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)]) \\
&\quad - \mathbb{E}[x(kT_s)x^T(kT_s)]
\end{aligned}$$

and finally,

$$\begin{aligned}
&\mathbb{E}[(x(kT_s) - z(kT_s))(x(kT_s) - z(kT_s))^T] = \\
&\mathbb{E}[x(kT_s)x^T(kT_s)](\mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1}\mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)].
\end{aligned} \tag{3.45}$$

Equation (3.45) provides a comparison between a cooperative localization error, and a statistical minimum mean square error (MMSE) based optimization, where it is previously learned that given negligible sensor errors,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) \leq \frac{\sigma_{\Delta x(kT_s)}^2(\text{Odometry})}{N}.$$

On the other hand, according to Equation (3.45) the localization estimation error in an optimal mean-square-sense is

$$\begin{aligned}
&\min_{H_k} \mathbb{E}[||x(kT_s) - H_k \bar{x}(kT_s)||^2] \triangleq \sigma_{\Delta x(kT_s)}^2(\text{MMSE}) \\
&= \mathbf{Trace}(\mathbb{E}[x(kT_s)x^T(kT_s)](\mathbb{E}[x(kT_s)x^T(kT_s)] \\
&\quad + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)])^{-1})\sigma_{\Delta x(kT_s)}^2(\text{Odometry}),
\end{aligned} \tag{3.46}$$

which is in any case superior to the odometry error $\sigma_{\Delta x(kT_s)}^2(\text{Odometry})$, since $\mathbb{E}[x(kT_s)x^T(kT_s)] < \mathbb{E}[x(kT_s)x^T(kT_s)] + \mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)]$. However, to obtain a quantitative comparison between $\sigma_{\Delta x(kT_s)}^2(\text{MMSE})$ and $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})$, one may reasonably expect that,

$$\mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)] < \mathbb{E}[x(kT_s)x^T(kT_s)],$$

therefore,

$$\mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)] + \mathbb{E}[x(kT_s)x^T(kT_s)] < 2 \mathbb{E}[x(kT_s)x^T(kT_s)]$$

or,

$$\mathbb{E}[x(kT_s)x^T(kT_s)](\mathbb{E}[\Delta x(kT_s)\Delta x^T(kT_s)] + \mathbb{E}[x(kT_s)x^T(kT_s)])^{-1} > \frac{1}{2}I$$

and substitution in Equation (3.46) yields that,

$$\sigma_{\Delta x(kT_s)}^2(\text{Odometry}) > \sigma_{\Delta x(kT_s)}^2(\text{MMSE}) > \frac{1}{2}\sigma_{\Delta x(kT_s)}^2(\text{Odometry}) \quad (3.47)$$

and in comparison to $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})$, one may deduce that,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) < \frac{2}{N}\sigma_{\Delta x(kT_s)}^2(\text{MMSE}) \quad (3.48)$$

which completes the proof of the theorem. ■

3.3.7 Simulations

This section will bring several examples of GNSS-independent localization in multi-agent systems, with and without cooperative localization. The motion model of a miniature quadcopter is used in this simulation to derive an initial odometry localization $\bar{x}(kT_s)$ at a given time-step kT_s , that is plotted in “black”, where UAVs are flying independently from other UAVs in a flock and on a separate path from others in a 2-D plane, and where atmospheric disturbances are present. However, although the UAVs in the flock are dynamically independent, they are continuously exchanging filtered positions $\hat{x}(kT_s + \Delta t)$ with each other on a continuous-time basis, as in Figure 3.6. Therefore, the UAVs inject $\bar{x}(kT_s)$ to their filter, and take the output of the filter $\hat{x}(kT_s + \Delta t)$ to communicate with each other, until a relative consensus is achieved in the network, where $\Delta t \leq T_s$, and $\gamma = N/(\lambda_2 \Delta t) \geq N/(\lambda_2 T_s)$. Then $\hat{x}(t + \Delta t)$ is used by the flock as their accurate positions $x(T_s)$, and is plotted in “red” colour. Obviously, Δt is a relatively small transient settling time with respect to T_s , such that one can assume that there is negligible mobility within Δt . The above scenario is repeated numerous times for random IMU sensor and LiDAR errors to show how the samples will be dispersed. The more disperse the samples, the less accurate the estimation model. In general, “black” samples representing odometry models are proven to be more dispersed (i.e., greater $\mathbb{E}[||\bar{x}(kT_s) - x(kT_s)||^2]$), in comparison to the “red” samples (representing cooperative localization), showing less error variance (i.e., lower $\mathbb{E}[||\hat{x}(t + \Delta t) - x(kT_s)||^2]$).

The horizontal axis represents the longitudinal position of the vehicle with respect to an arbitrary origin, and the scales are also set arbitrarily since comparison between

the cases with and without cooperative localization has been the focus of the simulations. The vertical axis is also representing an imaginary latitude with respect to the origin with arbitrary scale. The first scenario as depicted in Figure 3.8 represents the distribution of $\bar{x}(kT_s)$ (odometry localization), and $\hat{x}(t + \Delta t)$ (cooperative localization), for a network, where $N = 4$. It is evident that cooperative localization is advantageous over odome-

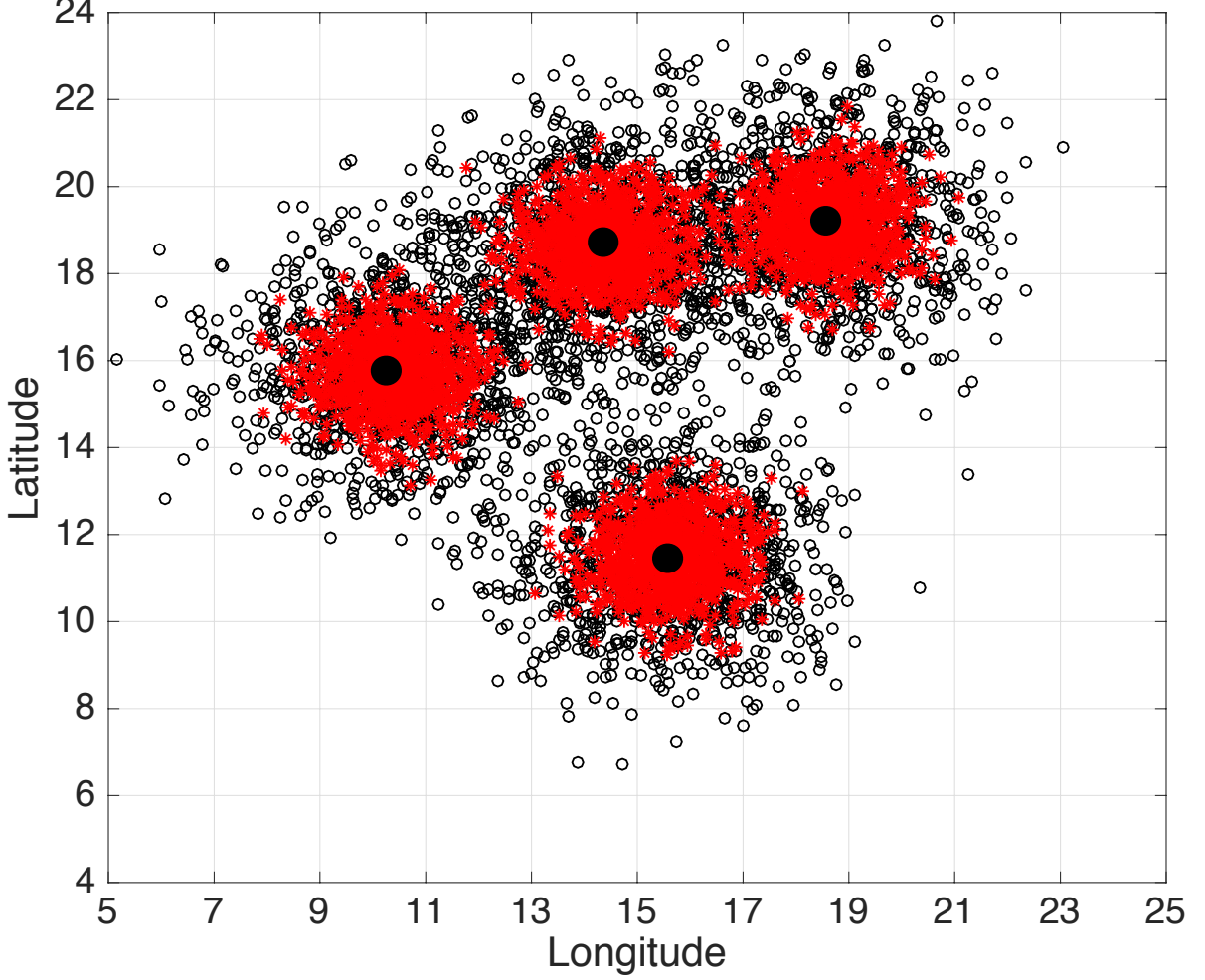


Figure 3.8: Comparison of localization error in estimation of individual agents' $\bar{x}^{(i)}(kT_s)$ (in black) where conventional estimation techniques using motion models and IMU sensors are used, and cooperative localization (in red), for $N = 4$. The horizontal and vertical axis display longitudinal and lateral positions with respect to an arbitrary origin, with arbitrary scale. Ground truth position is indicated as the center of the mass of the (red) particles.

try estimation, as the “red” samples are less dispersed in comparison with the “black”. Ideally, for a 100% accurate localization one may expect the “red” particles to converge to the center of their mass, that represents the ground truth position in each case. The sensor error in this scenario has been selected moderately to illustrate the advantage of cooperative localization under realistic scenarios for small networks.

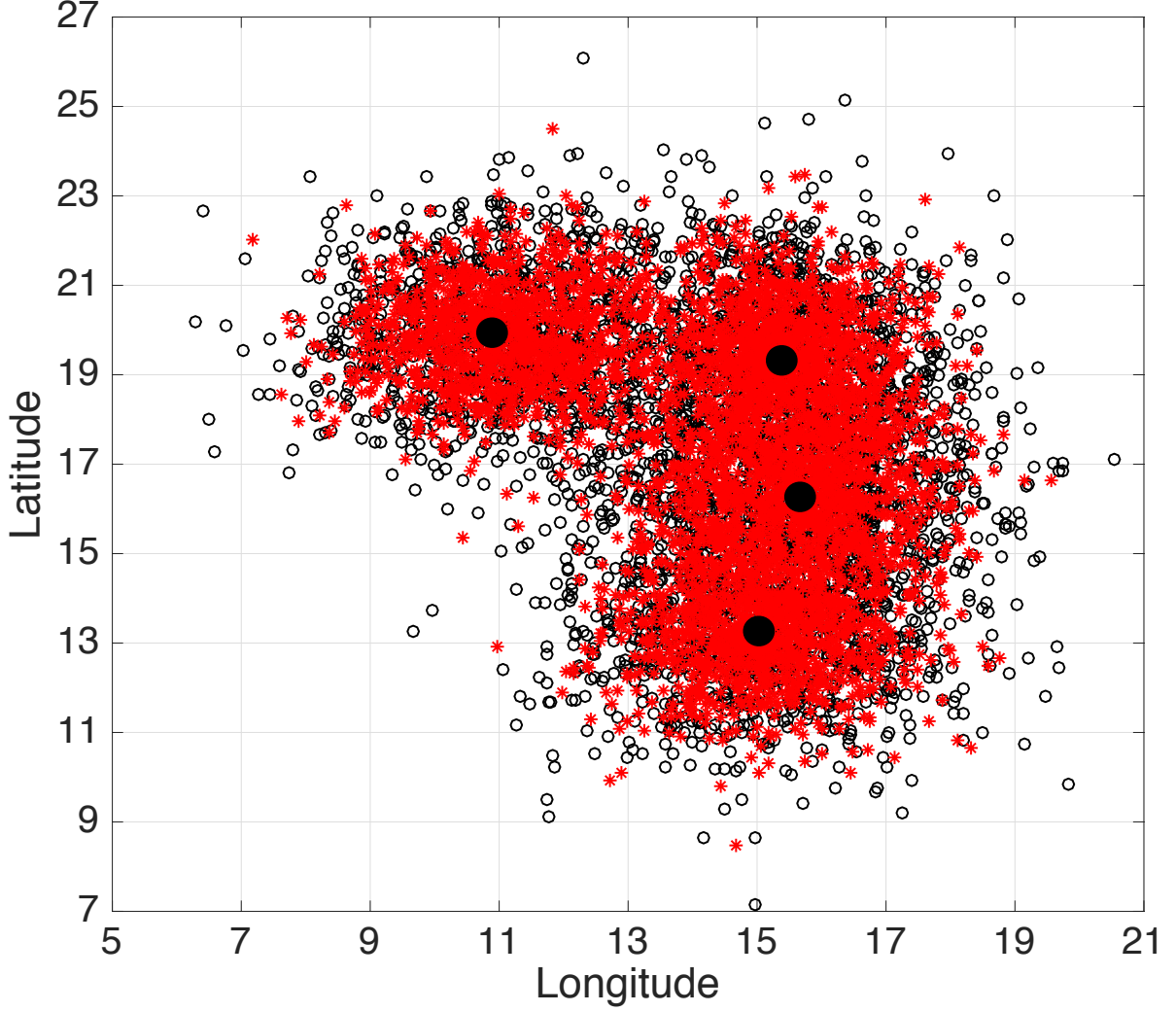


Figure 3.9: Localization error in a multi-agent system with $N = 4$, where low-grade sensors with higher errors are employed. It can be seen that there is little to no advantage in deploying cooperative localization in comparison with conventional (individually based) estimations. Ground truth position is indicated in the center of the mass of the (red) particles.

Figure 3.9 is a modified version of localization error in a multi-agent system of $N = 4$ with higher sensor errors in comparison with Figure 3.8. It can be seen that there is little to no advantage in deploying cooperative localization in comparison with conventional (individually based) estimations, where low grade sensors are adopted. It is therefore expected that cooperative localization may not seem an advantage in small networks since in addition to the divided drift error (i.e., $\sigma_{\Delta x(kT_s)}^2/N$), the sensor error component (that is $\sigma_{\Delta \omega(kT_s)}^2/\lambda_{min}^2(L_\gamma)$ as specified in Equation (3.38) is also playing role. Especially, this can become a remarkable error for the cases where the connectivity of the network is low (i.e., small $\lambda_{min}(L_\gamma)$). Figure 3.10 demonstrates a scenario where a network of $N = 9$ agents are deployed. In every scenario, the simulation is set to assume a random position in the map. Denoting $\sigma_{\Delta x(kT_s)}^2(\text{Odometry})$ as the original estimation

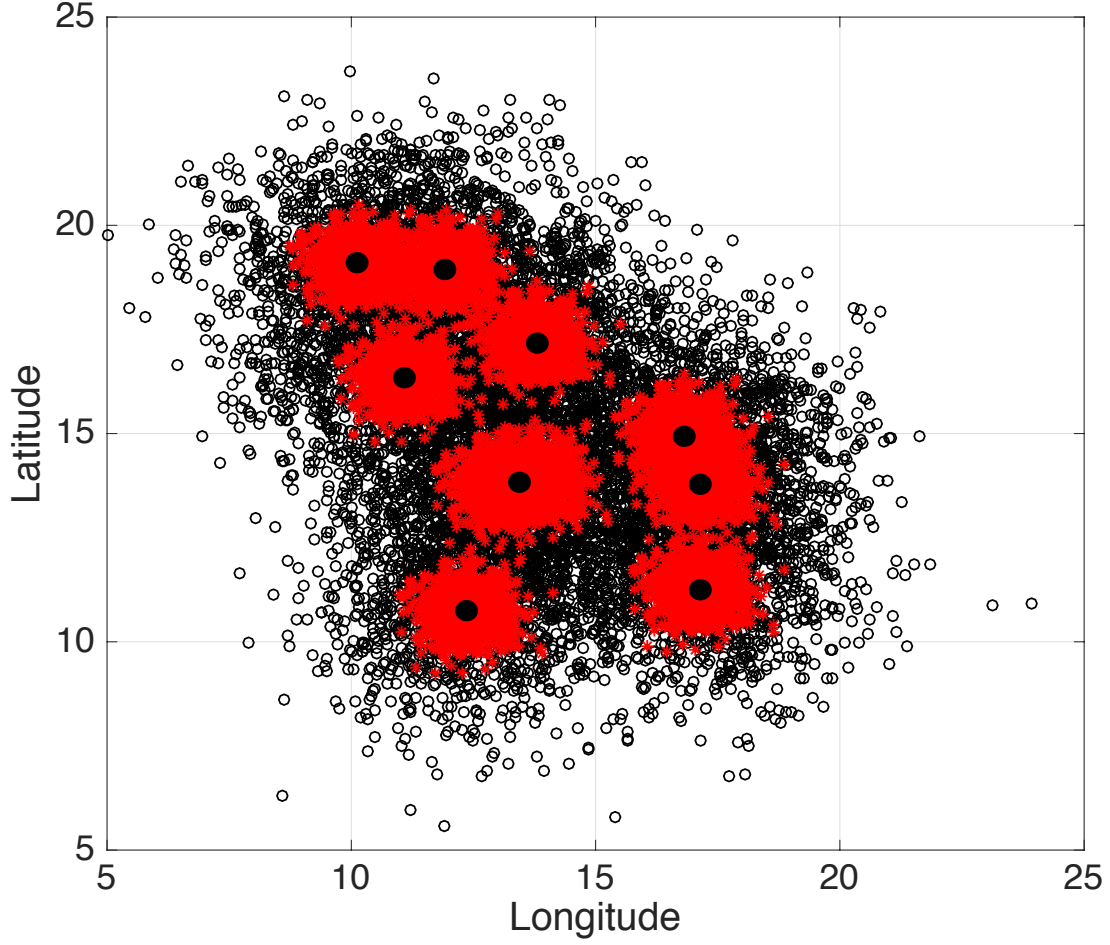


Figure 3.10: A similar case study deploying $N = 9$ agents. In comparison with Figure 3.8 it can be evident that the performance of cooperative localization takes clear advantage over odometry due to less dispersed red samples. Ground truth positions are indicated as the center of the mass of the (red) particles.

error of the network, the total network error achieved through cooperative localization can be derived by Equation (3.38) as,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) \leq \frac{\sigma_{\Delta x(kT_s)}^2(\text{Odometry})}{N} + \frac{\sigma_{\Delta \omega(kT_s)}^2}{\lambda_{\min}^2(L_\gamma)}.$$

where $\sigma_{\Delta x(kT_s)}^2(\text{Odometry})$ is represented by the “black” area in Figure 3.10, and $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})$ is represented by the “red” area. Figure 3.11 illustrates a similar case study with $N = 7$ with the exception that low-grade sensors are used in Figure 3.11 for localization. The advantage of cooperative localization in each scenario could be visualized by comparing the span of the “red” area to the span of the “black” area. Figure 3.12 is the case for $N = 20$ indicating that cooperative localization performs better as N grows. Figure 3.13 illustrates cooperative localization for a fully connected network with $N = 100$ agents, that demonstrates almost perfect localization. Comparison of the size of the “red to

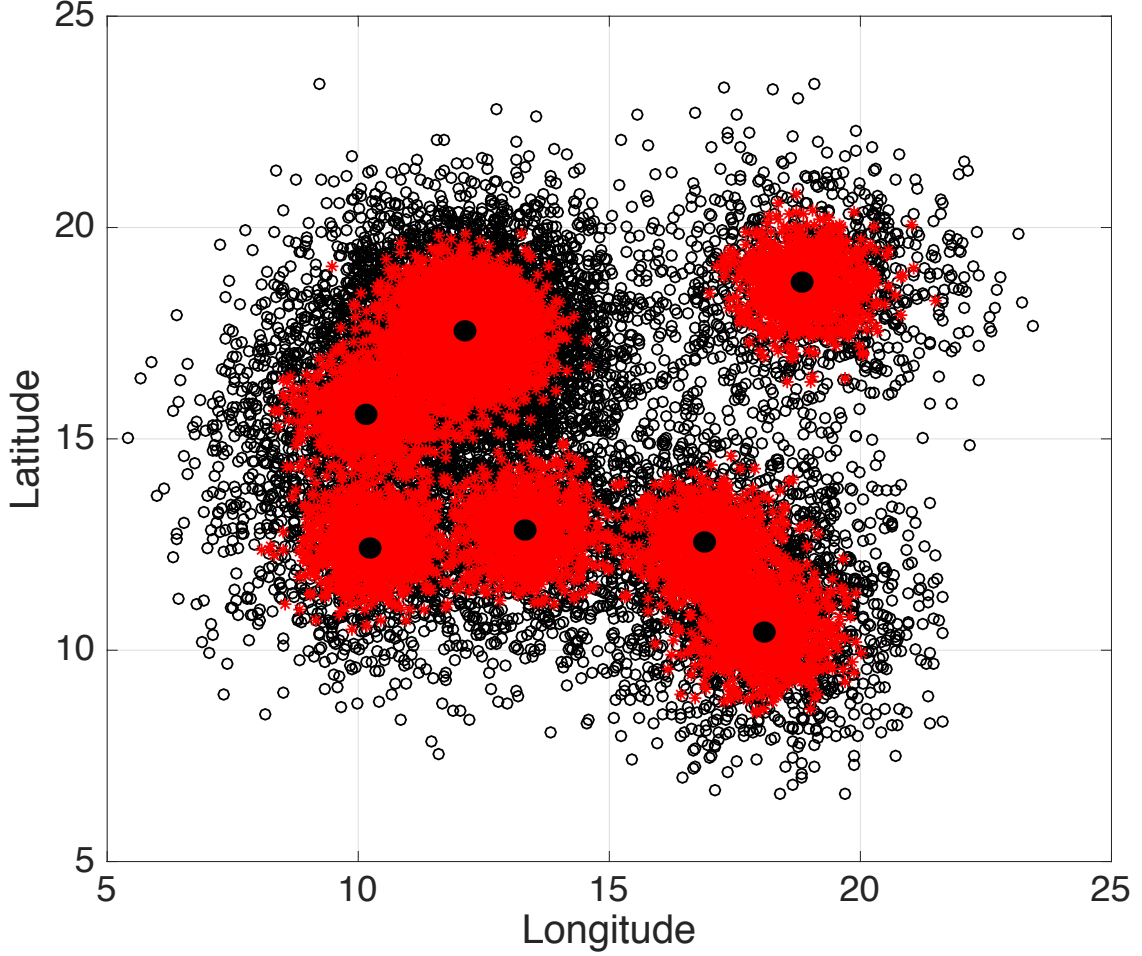


Figure 3.11: Localization with $N = 7$ and low-grade sensors. Ground truth positions are indicated as the center of the mass of the red particles.

black” areas indicate 6.6%, implying more than 15 times improvement. Figure 3.14 illustrates a similar case study as depicted in Figure 3.13 (where $N = 100$), with lower network connectivity (i.e., smaller λ_2). Since $\lambda_{\min}(L_\gamma) = \lambda_2$, Equation (3.38) can be written as,

$$\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization}) \leq \frac{\sigma_{\Delta x(kT_s)}^2(\text{Odometry})}{N} + \frac{\sigma_{\Delta \omega(kT_s)}^2}{\lambda_2^2}$$

where it can be evident that low network connectivity results in a large $\frac{\sigma_{\Delta \omega(kT_s)}^2}{\lambda_2^2}$. Multi-agent system theories have provided lower and higher bounds for λ_2 , as,

$$\frac{4}{N \text{diam}(\mathcal{G})} \leq \lambda_2 \leq \frac{N}{N-1} \ell_{\min} \quad (3.49)$$

where $\text{diam}(\mathcal{G})$ is the diameter of the graph, defined to be the largest number of vertices that must be traversed in order to travel between one vertex to another, and $\ell_{\min}$ is the minimum degree of vertices. Connectivity and the effect of the network diameter can

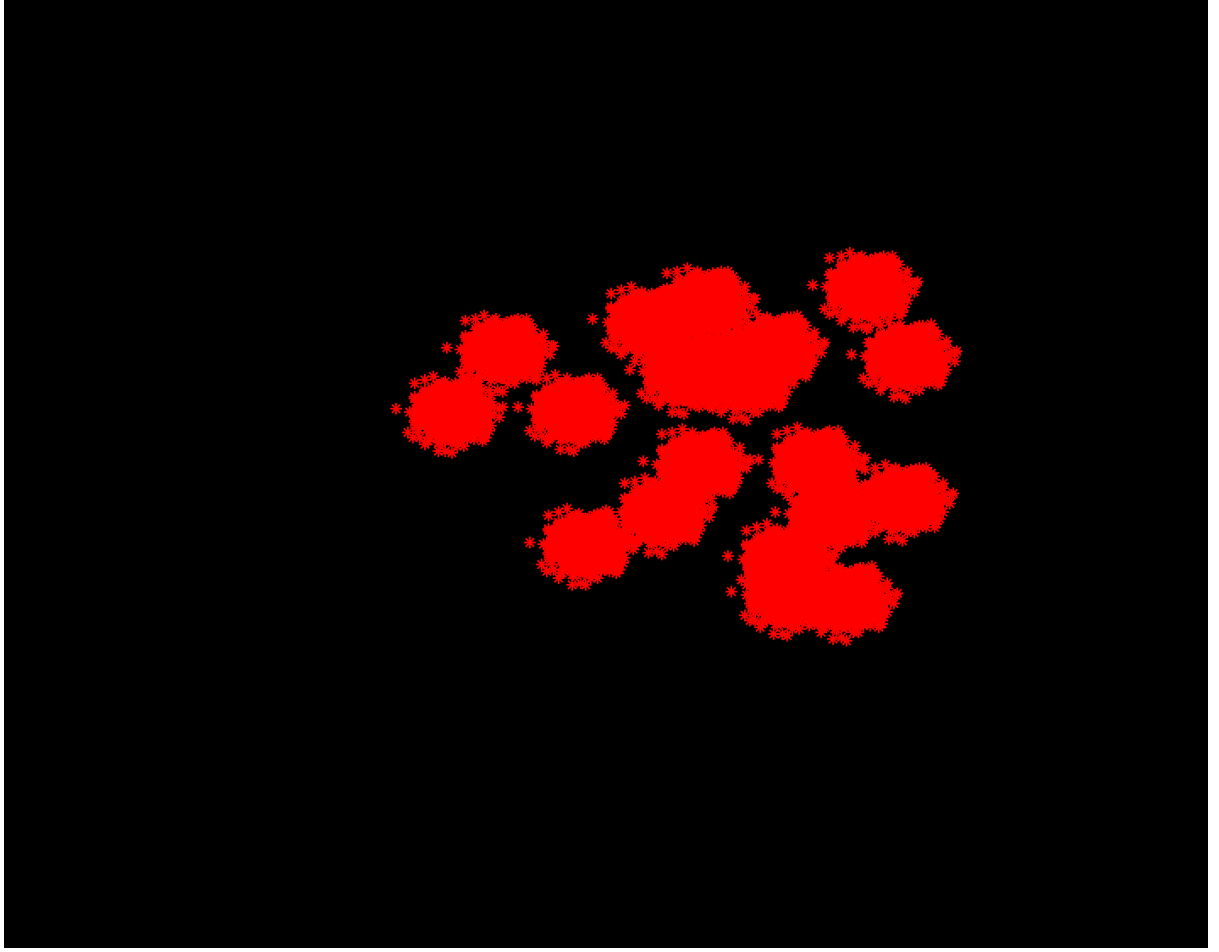


Figure 3.12: Case study where $N = 20$, with high-grade sensors. The red to black area is further reduced to 35% indicating better cooperative localization performance as N grows.

be explained in Figure 3.15 and Figure 3.16 below. Figure 3.15 represents cooperative localization in a setting with one anchor node whose ground truth position is known, such as in a landmark equipped with a radio transmitting device, that is periodically transmitting its position to all neighbouring agents. The anchor node is shown in the figure with an asterisk and a zero variance (since the position of the anchor node is a deterministic parameter). The network is fully connected and every other node in the network is able to determine its own position through direct cooperation with the anchor. As a result, cooperative localization is most accurate when the network is infinitely large. Figure 3.16 is the same case study discussed in Figure 3.15, except that this time a network with a large diameter and low connectivity is simulated, where the agents are serially connected to the anchor node as in a chain. The ground truth position of the anchor node and every other node is the same as in Figure 3.15. The node that is immediately connected to the anchor has the highest accuracy that is characterized by a relatively low variance (or spread) in comparison with the others. The agents that are farther away from the anchor have lower positioning accuracy, and as the radio distance

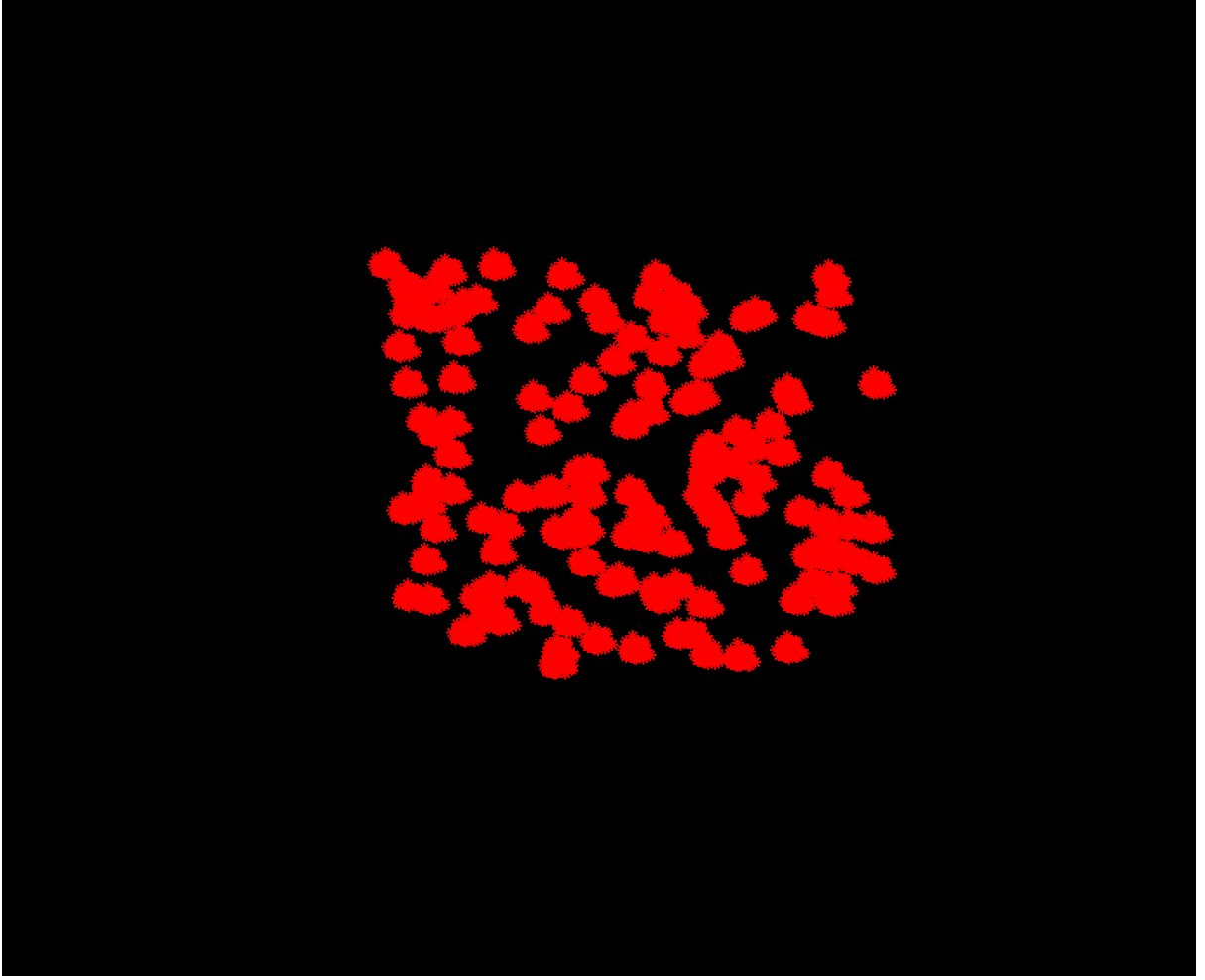


Figure 3.13: Almost perfect localization is possible through cooperative localization with $N = 100$ or more agents. The performance represented by the size of the red to black areas indicate that localization can be improved by more than 15 times. The red samples are gradually converging to a single point, which shows moving toward a perfect localization as the number of agents become larger and larger.

from the anchor is increased in the chain the variance of the estimated position increases, showing added error that is due to indirect cooperation with the anchor. The last case study corresponds to cases where $\gamma\Delta t$ is not optimized. The effect of an inappropriate selection of $\gamma\Delta t$ has been shown in Figure 3.17, that is a replication of the case in Figure 3.13, except where the value for γ has been selected slightly larger than optimal (i.e., $\gamma\lambda_2\Delta t = N$), and where Δt is decided in accordance with the vehicle air-speed, ensuring that the vehicle displacements are negligible in Δt . The error has become excessive and beyond acceptance, implying that one has to optimize $\gamma\Delta t$ in order to tune the process for a minimal network error.

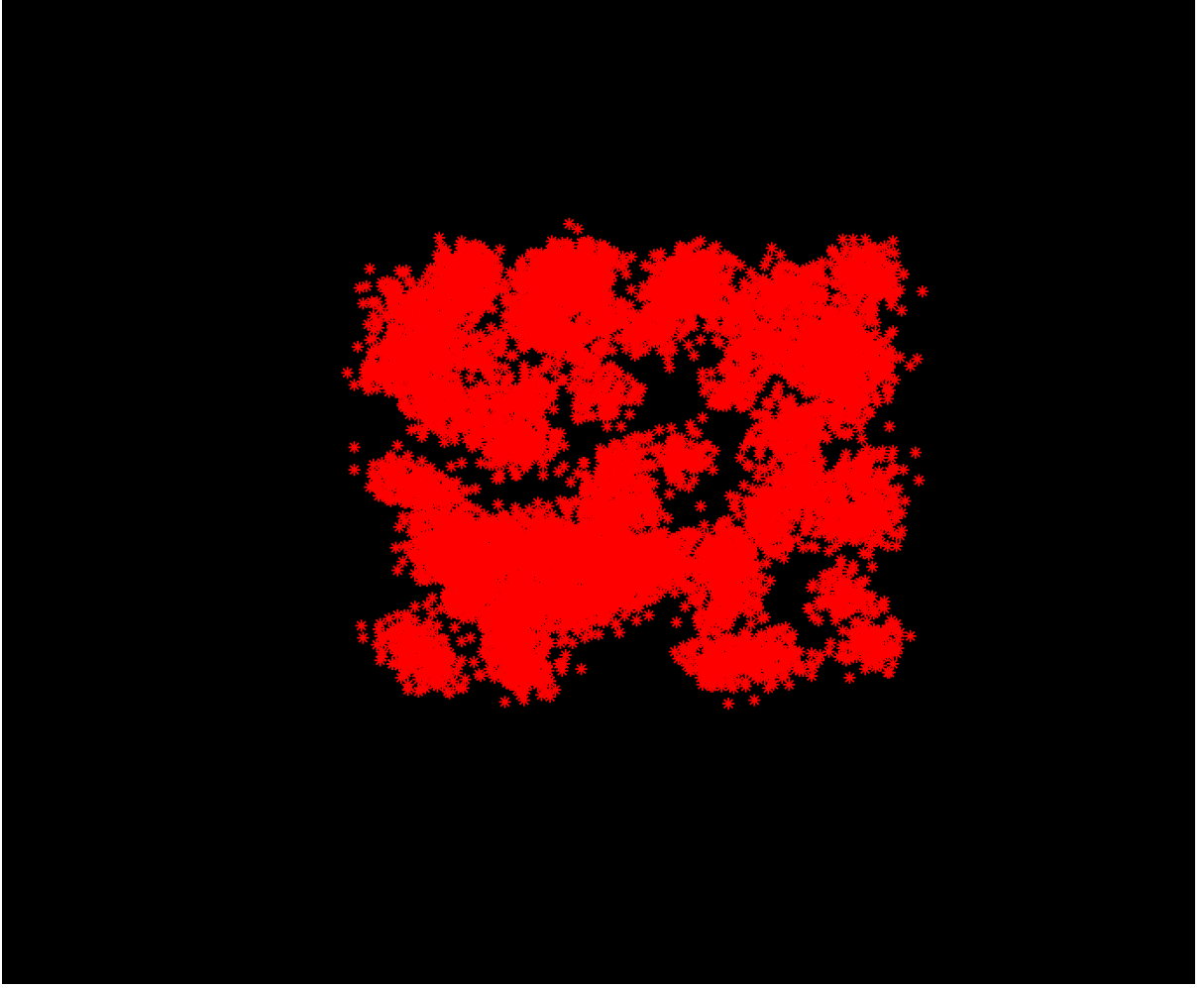


Figure 3.14: Similar case study depicted in Figure 3.13 is illustrated for $N = 100$, where the connectivity of the network reduced.

3.3.8 Discussions and Clarifications

The purpose of this section is to relate the simulations and case studies in Section 3.3.7 with the theoretical results derived in the previous sections. The following discussions are a handful of controversial aspects:

Ground Truth Positions

Assumption 6 requires a zero-mean estimation error for every agent in the network. This implies that if the motion models of the vehicles in Equations (4.4) and (4.5) were accurate representations of the actual motion, and if a motion experiment could be infinitely repeated from an origin to a destination, then the UAVs mean-sense-motion could be precisely derived from the motion equations and the IMUs, since the measurement error of healthy instrumentation are assumed to be non-biased. This implies that the ground truth position for the case studies in Section 3.3.7 is the center of the mass of the “red”

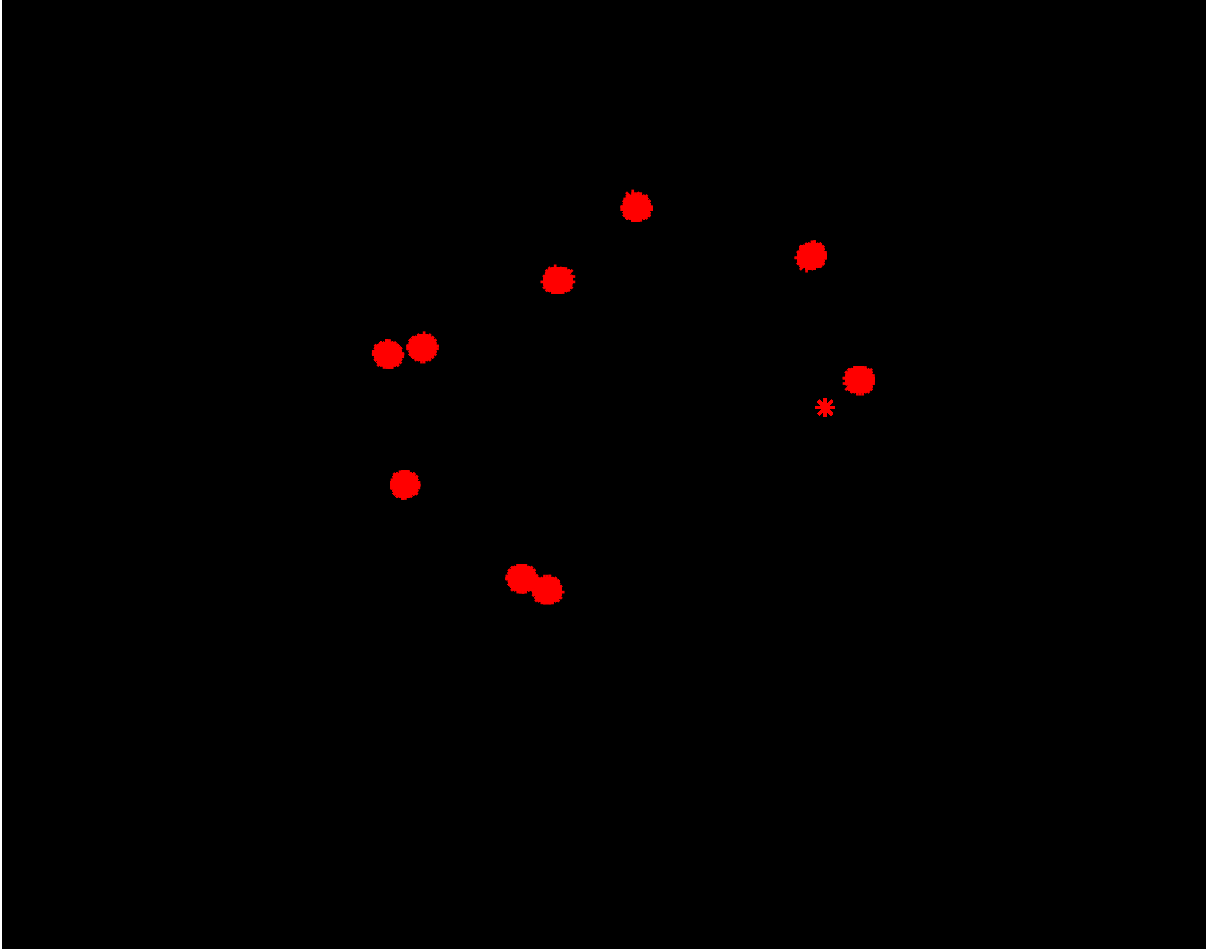


Figure 3.15: Emulation of a fully connected network with infinite number of agents, through an anchor node. The anchor node is an agent with a ground truth position (as shown with an asterisk). It can be observed that the asterisk has zero-variance implying that the position is deterministic as opposed to a random variable. Other agents in the network attain a very accurate position through direct cooperation with the anchor.

particles, since each particle is a representation of a motion experiment. Specifically, Figure 3.15 is an emulation of a network with infinite agents and ideal range-finders. Since it is practically impossible to simulate infinite agents, the case study is an emulation through the aid of an anchor node, as in Lemma 4. The anchor node is represented by an asterisk in the figure having a zero variance, i.e., deterministic position. All other nodes in the graph are directly or indirectly cooperating with the anchor node.

Remark 11. *Each anchor node is equivalent to a fully connected network with infinite agents.*

The proof is straightforward, and omitted due to space constraints. However, the small variance in the estimation of the position of the non-anchor agents is due to intrinsic numerical error in the LTI filter, as well as limited consensus times Δt in Theorem 8.

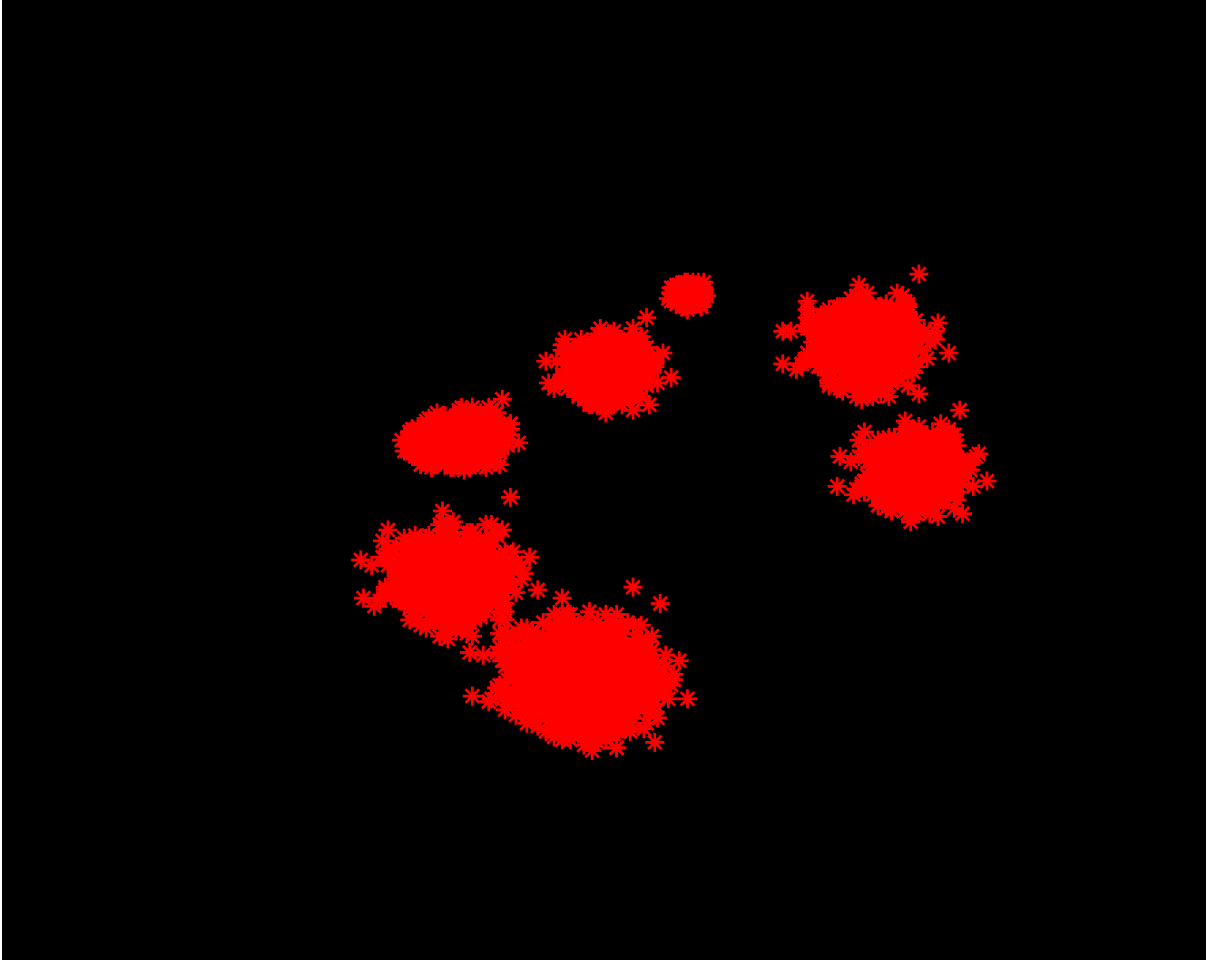


Figure 3.16: The case study is the same as in Figure 3.15 with the difference that the topology of this case study associates the lowest connectivity characterized by a chain-wise connection, hence a large diameter. The agent that is immediate to the anchor has the best accuracy in the network, and as agents get farther distanced in the network from the anchor, their tendency in cooperation with the anchor becomes more and more indirect, and as a result attain more and more error.

rendering a negligible error. Let us remember that in this case the error of the range-finders have been neglected.

Performance Metrics

The quantitative performance of cooperative localization can be assessed by evaluating the variance ratio $\sigma_{\Delta x(kT_s)}^2(\text{Coop-Localization})/\sigma_{\Delta x(kT_s)}^2(\text{Odometry})$. This ratio can be numerically evaluated by particle filters, and alternatively, a rough evaluation can also be attained by inspection of the density of the “red” to “black” areas in each case study. For example, Figures 3.12 and 3.10 are similar experiments in terms of network topology, with the exception that the number of agents have increased from $N = 9$ to $N = 20$

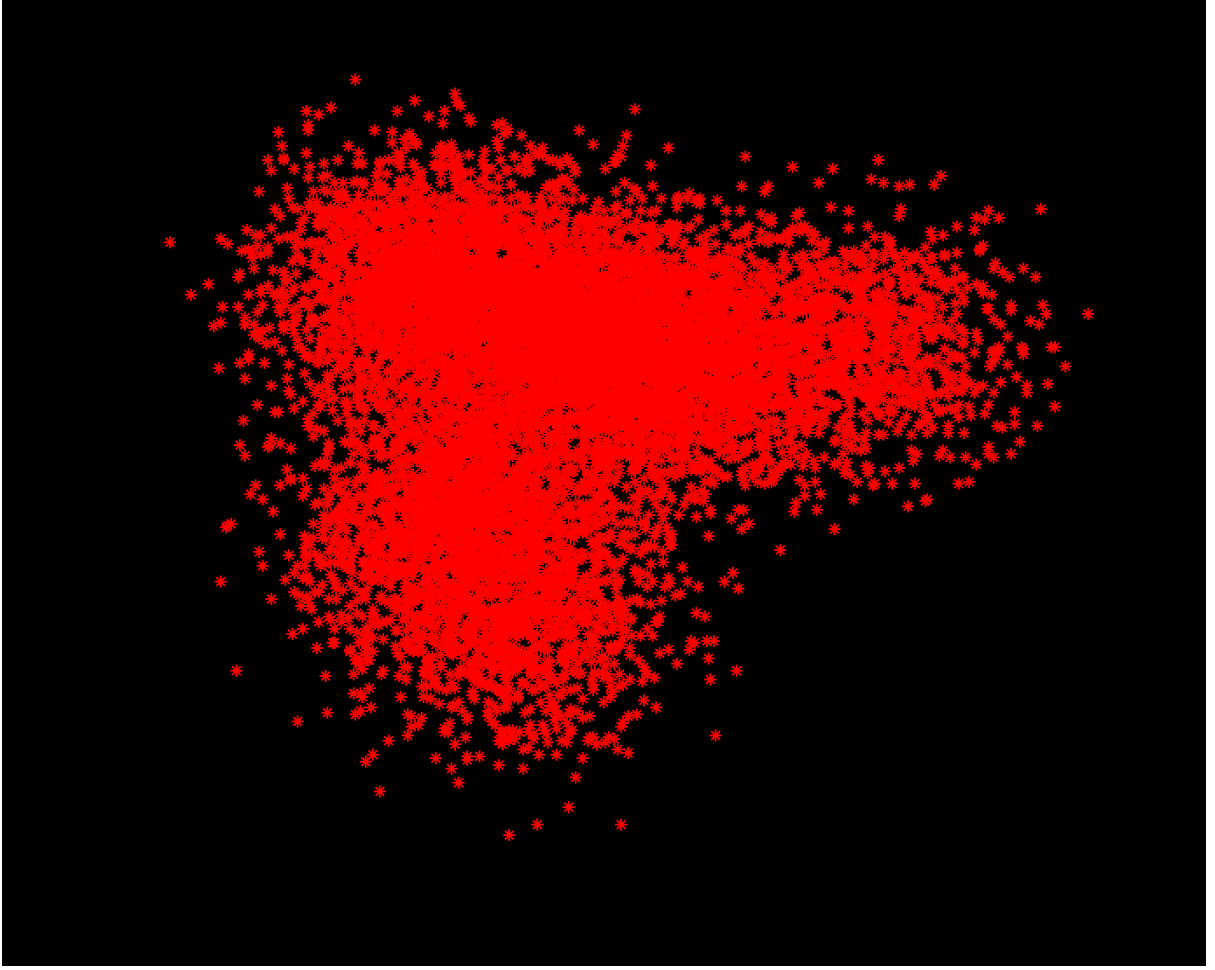


Figure 3.17: Alternative resources of information in a fleet of vessels. Distance between the vessels detected by the radars are redundant to the locations observed by PNTs.

in the two case studies. As a result, the spread of the “red” areas in comparison to the “black” has reduced from 50% to 35%, and even to 6.6% for $N = 100$ in Figure 3.13, which is a quantitative metrics to evaluate localization performance as the network size is increased. Performance comparison between the figures is summarized in Table 3.1.

Network Connectivity

Equation (3.38) explains the importance of graph connectivity (i.e., λ_2) for reducing the network error in a cooperative localization scheme. In an optimal sense, where $\gamma\lambda_2\Delta t = N$, and $\lambda_{\min}(L_\gamma) = \lambda_2$, the network error can be mitigated by, (1) increasing the size of the network N , or equivalently utilization of one or more anchor nodes (as in Remark 11), and (2) by reducing the range-finders error. Commercial range-finders have unavoidable intrinsic detection error, therefore, the only practical way to optimize the overall performance of a cooperative localization network is to increase the network

Table 3.1: Cooperative Localization Performance Comparison

Figure No.	Network Size	Coop. Localization Error Reduction	Sensor Type
Fig. 4	N=4	87%	Baseline
Fig. 5	N=4	95%	Low-Grade
Fig. 6	N=9	50%	Baseline
Fig. 8	N=20	35%	Baseline
Fig. 9	N=100	6.6%	Baseline

connectivity λ_2 , and that is by reducing the graph diameter, as in Equation (3.49). Figure 3.15 and Subsection 3.3.8 has shown the effect of a very large network in reducing the error of the network, in a simulation where the range-finders were ideal instruments. In case of ideal rangefinders, $\sigma_{\Delta\omega(kT_s)}^2 = 0$, and the network connectivity λ_2 does not play role in Equation (3.38). However, situation changes in a practical scenario where $\sigma_{\Delta\omega(kT_s)}^2 \neq 0$. Figure 3.16 is a simulation case identical to Figure 3.15 except that range-finders' error were taken into account, and where the topology of the network was changed to a radial network, where the anchor agent was on one side of a line, and the others were sequentially linked to one another and finally to the anchor (as in a chain), hence a very large diameter. It is evident in Figure 3.16 that the agent immediately connected to the anchor has the smallest estimation variance, and the variance in the positioning estimation grows, as the agents get farther away from the anchor in the chain. It is worth noting from the figure that network neighbours are not necessarily physical neighbours. Obviously, if the topology of the graph changes to a fully connected network then the size of each red spot will be equal to the smallest red spot, and in case ideal range-finders are used, then Figure 3.16 transforms to Figure 3.15.

Initial Localization Error

Equation (3.24) shows that for a sufficiently large γ , the cooperative localization error,

$$\lim_{\Delta t \rightarrow T_s} \Delta x^{(i)}(kT_s + \Delta t) = \frac{1}{N} \sum_{i=1}^N \Delta x^{(i)}(kT_s), \quad \forall i \in \mathcal{N}, \quad (3.50)$$

and is independent to the initial error $\Delta x^{(i)}(kT_s)$, as long as N is sufficiently large. The initial network error of a large network can be visualized by the “black” area in Figure 3.15, which reduces to the small “red” spots in a short time $\Delta t \rightarrow T_s$ (assuming ideal range-finders), hence, the initial amplitude of the error will have no effect on the final

cooperative localization error, in large networks. In case of smaller networks the localization error will be the mean of the network's error, and will not be very advantageous in comparison to ordinary odometry localization. Hence, cooperative localization would be particularly favourable in large networks, such as in future Urban Air Mobility (UAM).

Time-Step Correction

Equation (3.50) implies that the cooperative localization error $\Delta x^{(i)}(kT_s)$ at each time-step k is a sample mean of the cooperative localization error at the preceding time-step $k - 1$. Therefore, according to the Laws of Large Numbers $\mathbb{E}[\Delta x^{(i)}(kT_s)] = \mathbb{E}[\Delta x^{(i)}((k - 1)T_s)]$, and the variance $\text{VAR}(\Delta x^{(i)}(kT_s)) = \frac{1}{N} \text{VAR}(\Delta x^{(i)}((k - 1)T_s))$ assuming that $\Delta x^{(i)}((k - 1)T_s)$'s are i.i.d. random variables for all k , and $i \in \mathcal{N}$. Additionally, the Central Limit Theorem in statistics implies that the probability distribution of the random variable $\Delta x^{(i)}(kT_s)$ approaches to a Gaussian distribution as $N \rightarrow \infty$ (regardless of the pdf of the initial odometry error $\Delta \bar{x}^{(i)}(T_s)$ derived from the initial true position $x^{(i)}(0)$). In other words, cooperative localization error becomes smaller and smaller at every time-step as opposed to the localization error derived from odometry and IMU sensors that gets larger and larger at each successive time-step.

Collision Avoidance

The conventional localization method through odometry in Figure 3.13 clearly indicates a very high possibility of collision between the UAVs sharing the airspace, based on the present clearances between the vehicles. This is due to the fact that the probability space of the presence of the vehicles illustrated by the “black” markers have significant overlap, implying that a much larger clearance have to be practiced between the UAVs in order to avoid collision. This indicates that a much larger airspace is required to securely accommodate the given traffic, which also indicates inefficient use of the airspace. In contrast to the odometry localization, cooperative localization in Figure 3.13 provides a far less probability of collision among the airspace users as the probability space of the UAV positions has significantly diminished comparing odometry localizations. This implies a far more efficient use of the airspace. Practically, the minimum required spacing between vehicles should exceed twice the localization error in order to ensure collision avoidance. This implies that the minimum airspace for a 99% secure navigation should exceed $N\pi(2.54^2 \text{VAR}(\Delta \mathbf{x}^{(i)}(kT_s)))$ for all k (where 2.54 is the z-score for a probability of 99%), assuming a sufficiently large N (for the pdf of $\Delta \mathbf{x}^{(i)}(kT_s)$ to be a Gaussian distribution).

Rural vs. Urban Air Mobility

The conceptual foundation of cooperative localization is established upon three main pivots, namely,

1. Network size N (that is responsible for attenuating the odometry error): An urban air mobility system is generally associated with large number of connected aerovehicles randomly flying in a often dense airspace, where strict traffic control rules prevail. A dense airspace may also imply lower clearance requirements, and finally more stringent localization standards, to ensure precise flight paths for collision avoidance. This provides ideal grounds for cooperative localization, since range-finder detection ranges are often low range and more suitable for urban areas, in comparison to a rural airspace where distances between UAVs are relatively larger.
2. Network connectivity λ_2 (that is responsible for attenuating the range-finders error): In urban airspaces, stationary landmarks and poles can serve as anchor nodes, if equipped with radio transmitters to disseminate their ground truth position to a surrounding neighbourhood. Each anchor node technically functions similar to an infinitely large and fully connected network. The ultimate effect is equivalent to a smaller topological diameter, regardless of the physical span of the airspace. A smaller network diameter then attenuates range-finders error resulting in an improved localization, as discussed in Subsection [3.3.8](#). In conclusion, an urban airspace is not only advantageous for reducing the odometry error in the network (due to large N), but also advantageous for attenuation of the range-finder error, resulting an overall favourable localization, in comparison with rural environments (refer to Equation [\(3.38\)](#)).
3. LTI filter gain γ (that is responsible for attenuating the transient error in the LTI filter): Theorem [9](#) optimally requires $\gamma\lambda_2\Delta t = N$, implying that $\gamma\Delta t$ has to be decided according to the network size N and the connectivity λ_2 . This further implies that the consensus error component $\epsilon = e^{-\gamma\lambda_2\Delta t}\sigma_{\Delta x(kT_s)}(\text{Odometry})$ that is due to insufficient consensus time (in Theorem [8](#)) can be improved in large and well connected networks, where γ can be large. Therefore, urban environments are again more favourable candidates for cooperative localization, especially when high speed mobility is a concern.

In conclusion, one can deduce that cooperative localization is very efficient for urban air mobility, and less efficient in rural applications.

Centralized vs. Distributed Localization

A centralized localization system requires airspace users to communicate with a central computing station that collects information from the network, and transmits more accurate positioning estimations to the aero-vehicles, as depicted in Figure 3.7. This arrangement makes the overall system vulnerable to spoofing cyberattacks since intrusion of a single GPS link could paralyze positioning estimations of the victim and consequently threaten the security of the traffic system. Cooperative localization proposed in this article is a fully distributed localization system, and consequently a spoofing cyberattack on any communication link is equally distributed among the network population according to Lemma 3, mitigating the overall impact. Furthermore, existence of at least one anchor node in the network could eliminate the spoofing threat, entirely.

Cooperative Localization in Dense UAV Networks

The disadvantage of the proposed cooperative localization method is in the time-delay of the LTI filter discussed in Theorem 7. According to the theorem $\lim_{\Delta t \rightarrow T_s} \Delta x^{(i)}(kT_s + \Delta t) = 0, \forall i \in \mathcal{N}$, when $N \rightarrow \infty$, implying that $\lim_{\Delta t \rightarrow T_s} \hat{x}^{(i)}(kT_s + \Delta t) = x^{(i)}(kT_s)$. In other words, a given vehicle may attain a true position $x^{(i)}(kT_s)$ only after lapse of a certain time-delay $\Delta t \rightarrow T_s$. This is an inevitable characteristic of dynamic LTI filters, that require a transient period to settle. In conclusion, in fast mobility applications cooperative localization is concomitant with a mobility error $\bar{\mathbf{v}}^{(i)}\Delta t$ that requires to be taken into account as a safe clearance with neighbouring mobile agents and obstacles. In dense environments flight clearances are scarce. As a result, cooperative localization in dense airspaces could be problematic, especially in high speed air mobility.

Future ITS Standards and Practical Implementation

Cooperative localization can be a secure and accurate localization candidate for the future urban air mobility, as it inflicts no any extra burden to the information system infrastructure. Articles [172, 173] outline information exchange systems in UAM and modern Urban Air Traffic Control (UTC). Aero-vehicles in UAM transmit real-time momentary positions as part of their situational awareness messages to the traffic control system, and surrounding aero-vehicles. These awareness messages are all that is required for cooperative localization to be practically implemented inside vehicle controllers through a simplified algorithm, in case a few additional assumptions can be made. Given that C-V2X and V2V are digital communication protocols, the simplified cooperative localization algorithm will be explained in a discrete-time system framework. The emerging 5G and

6G technologies enable fast and secure exchange of information messages in a V2V wireless tele-communication infrastructure in modern ITS, where the transportation speed of information messages can transcend far beyond the physical mobility of the network, and even multiple time-steps $k_m T_s$, such that if $x_k^{(i)} \triangleq x^{(i)}(k T_s)$ denotes the true position of a UAV, then $x_k^{(i)} \approx x_{k+1}^{(i)} \approx \dots \approx x_{k+k_m}^{(i)}$, $\forall i, k$. Under this condition, it is possible to implement a simplified version of the cooperative localization LTI filter in Theorem 7, as below. Let $\hat{x}_k^{(i)} = \bar{x}_k^{(i)}$ denote the initial positioning estimate of a given aero-vehicle i derived from an odometry model, at a particular time-step k , and $\omega_k^{(i,j)}$ denote the range of i to j measured by a range-finder on vehicle i . Also, let all aero-vehicles in the network perform a series of simple computational iterations,

$$\begin{aligned}\hat{x}_{k+1}^{(i)} &= \hat{x}_k^{(i)} + \gamma T_s \sum_{\forall j \in \mathcal{N}_i} (\hat{x}_k^{(j)} - \hat{x}_k^{(i)} + \omega_k^{(i,j)}), \\ \hat{x}_{k+2}^{(i)} &= \hat{x}_{k+1}^{(i)} + \gamma T_s \sum_{\forall j \in \mathcal{N}_i} (\hat{x}_{k+1}^{(j)} - \hat{x}_{k+1}^{(i)} + \omega_k^{(i,j)}),\end{aligned}$$

and so forth, until $\hat{x}_{k+k_m}^{(i)}$ settles to a steady state. One can simply show that a steady state $\hat{x}_{k+k_m}^{(i)}$ exists, where $\hat{x}_{k+k_m}^{(i)} \approx x_k^{(i)} \approx x_{k+k_m}^{(i)}$, hence, real-time localization. Moreover, ITS standards are nowadays requiring more stringent criteria for bandwidth, security, and latency, enabling cooperative localization to be implemented in relatively high-speed applications and dense airspaces, with a negligible computational burden on the aero-vehicle controllers. Additionally, interoperability standards in modern ITS enable large connected networks with sufficient connectivity, and low topological diameters, which are all among very favourable characteristics for cooperative localization.

3.3.9 Conclusion of the Chapter and Future Works

The present work involves GNSS-Independent localization through a multi-agent system of cooperating agents, where the agents tend to correct their perceived positions with reference to perceptions of their neighbouring agents through consensus, and relative ranges to their neighbours, sensed by their onboard rangefinders (i.e., LiDARs, vision-cameras, etc.). It has been shown that perfect localization is possible if the network is sufficiently large and well connected. Cooperative localization is also advantageous for resiliency against false data injection cyberattacks on certain sensors, through a formation referred to as “cyberattack shield”, where miniature suicidal drones can be deployed to protect a fleet of ground or marine vehicles against cyberattacks, by absorption of the attack intrusion vector. However, consensus in the information exchange system does not converge when sensor error is present, and causes instability in the localization process. In real world scenarios where sensor errors are inevitable a “relative consensus” is considered

where exchange of information among the agents takes place in the certain time interval. Optimization of the duration and consensus speed of the MAS yields important results to minimize the network positioning error in the localization process, and has been a focus of the present work. In order to evaluate the performance of cooperative localization, a minimum-mean-square-error (MMSE) based optimization has been developed for the MAS, and it is shown that cooperative localization reduces network error (at least) by a factor of $N/2$, where N is the number of agents.

Case studies and simulations have verified the theoretical results achieved in this work, and has shown that cooperative localization can have remarkable advantages in improving positioning error when the network is large and well connected. It has been found that the topology of the multi-agent network has direct impact on the performance of cooperative localization, and consequently on accurate localization. Rangefinder errors are also proven to have remarkable impact on the performance of the process. Therefore, it is advisable that further works be directed on alternative consensus protocols, in an attempt to facilitate cooperative localization in radial networks, or in networks where connectivity is insufficient. It is also beneficial to investigate methodologies that may alleviate rangefinder errors.

Chapter 4

Anti-Spoofing Aided Technology for Urban Air Mobility: Ground Command Authentication

Smart Mobility is one of the pivots of smart cities, and it refers to the advanced use of technologies to address urban transportation challenges, including traffic congestion and its environmental impacts through adaptation of smart traffic lights and urban infrastructure, unmanned vehicular technology, shared mobility, adoption of electric vehicles for conservation of carbon emissions, unmanned vehicles, etc. [174]. Recently, the academia and the industry have made substantial investments to augment urban transportation with a new paradigm referred to as Urban Air Mobility (UAM), in which people and goods are transported in congested and diverse urban airspaces through manned and Autonomous Aerial Vehicles (UAVs) [175]. In-progress developments made by Uber Elevate, Amazon Prime Air, and NASA's Unmanned Traffic Management (UTM) are examples of industrial attempts aiming at development of UAM. In the following paragraphs it will be explained that authentication algorithms that are intertwined with the structural airspace and the traffic management system plays a significance role to avoid adversarial spoofing and catastrophic pervasive havoc in the UAM network. Therefore, let us briefly introduce the structural airspace and the underlying concepts of UTM to realize the potential threats that are involved with UAM.

Reference [172] outlines the principles of UTM and defines the scope of services and responsibilities of the stakeholders that are active in UTM. The document defines the UAS Service Supplier (USS) as a bridge between the Federal Aviation Administration (FAA) of the United States and UAS Operators, that are responsible to operate the aerial vehicles in accordance with UTM operational requirements that enable safe and efficient

use of airspace. Then, the USS provides broadcast information to the operators about instantaneous flight constraints (including dynamic geo-fencing constraints, and reserved paths for emergency public services, public safety notifications, etc.). The USS Network is an information network that enables the USSs to interconnect and exchange information such as airspace constraints across the network to serve situational awareness for UTM participants. Additionally, the Vehicle-to-Vehicle (V2V) network allows aircrafts and small UAVs to share real-time information to their neighbouring vehicles (including identification, and momentary positions), and radio communication between the UAS operators and the USS about flight intents (including planned flight paths and expected trajectories). However, it is important to note that the primary means of communication and coordination between the stakeholders is through a distributed information network (unlike the traditional pilots-to-traffic-control voice messages). Therefore, the FAA makes real-time air space constraints available to the UAS operators (through the USS), who are individually responsible to operate the UAS in a safe and efficient fashion and within the constraints set by the FAA, and through coordination with other operators, without receiving any additional air traffic service.

In order to comply with the above UTM framework, the authors in [173] define the traffic network as a set of nodes that may include the UAS and operators, and a set of communication links that interconnects the nodes together. They also define a flight plan as a time-position 4D trajectory that is dictated by the UAV operators to the low-level control system of the UAVs as the intended flight path. They further state that an operator will need to specify the origin, destination, and the sequence of discrete positions that the UAS will travel during a task. This will ensure coordination and conflict avoidance between the vehicles sharing the same airspace at any time. The International Civil Aviation Organization (ICAO) has set principles for Conflict Detection and Resolution (CDR) methods to ensure separation between UAVs in an integrated airspace as a primary guideline in UTM [177], where CDR broadly refers to the process of coordination among several UAS operators to ensure separation and collision avoidance between UAVs in an integrated airspace. The authors in [179] have proposed three layers of CDR redundancy in different phases of UAV flights, namely, pre-flight CDR, in-flight CDR, and collision avoidance. On the other hand, according to [180] “Multi-Agent Pathfinding (MAPF) problem is the fundamental problem of planning paths for multiple UAVs, where the key constraint is that the UAVs will be able to follow these paths concurrently without colliding with each other”. The authors in [181] have shown that the pre-flight CDR problem can be formulated as a MAPF problem, while the authors in [178] have quoted that the standard MAPF formulation does not capture real-world considerations

such as those of UTM since “firstly, most existing works in MAPF assume a centralized setting, where each agent (i.e., an UAV) executes a unique path determined by a central computing entity, and secondly, they assume that a global cost is minimized over all agents, whereby all agents are cooperative such that no agent is prioritized over another, and any agent may be instructed to take a longer path to avoid conflicts”.

As stated earlier, it would be desirable to consider multiple UAS operators and prioritize the UAVs based on the services that they render. For example, it is desirable to give priority to medical evacuations and rescue services and public safety over air taxi in MAPF, and this requires certain considerations in the formulation of the MAPF and CDR problems. The authors in [176] stress that these services cannot be delivered in a centralized fashion, quoting that efficient transport of people and goods to their destinations requires an entirely new concept for air traffic control based on the principles contained in the Airborne Trajectory Management (ABTM) concept [182,183]. ABTM provides flight safety by de-centralizing the function of managing trajectories of airborne vehicles, locating it in the vehicles themselves rather than in one or more ground-based pilot, and they believe that this level of autonomy is anticipated to make UAM economically viable and invulnerable to catastrophic losses of service, to which centralized control systems are prone. This implies that although ground nodes may transmit a set of waypoints to the UAVs, but low level control actions and flight safety services have to be implemented within the UAVs and not via transmission. In conclusion, [176] summarizes ABTM traffic management principles for achieving UAM and maintaining safety in the presence of the traffic density through certain principles as follows,

- Planing each flight independently on the most efficient route, avoiding obstacles and protected airspace (i.e., MAPF),
- Dynamically geo-fencing airport runways and other protected operations,
- Ensuring separation and collision avoidance (i.e., CDR) through cooperation among adjacent vehicles,
- Ensure spot availability before landing or initiating launch operations.

Administration of the above UAM principles can be facilitated by consideration of the airspace as a connected graph. The authors in [184] have defined the airspace as “airways” and “nodes”, where airways are considered as the edges of a graph that interconnect the nodes, representing a corridor for an aircraft to traverse from one node to the next, and the nodes are discretized grids in the airspace in which only one aircraft can be present at any time. With this convention, path planing can be reduced to the

problem of finding the shortest path in a graph, and dynamic geo-fencing can be managed by means of adding and removing edges in the graph, hence, dynamically availing or removing access to certain grids in the airspace. Consequently, UTM and UAM can be implemented through continuous exchange of wireless messages between the aircrafts and ground controllers as well as aircrafts to aircrafts. It is now realizable that authentication of the telecommunicated messages plays a vital role in the security of the air transportation system, given the open wireless network, and this has given birth to a new line of research works dedicated to the subject of authentication and counter-spoofing methodologies in modern UAV technologies.

The authors in [185,186] state that authentication of the control signals received by UAVs is of vital significance at the UAV, since malicious adversaries are able to forge control commands and illegitimately takeover the traveling path of the UAV, due to the openness of the wireless environment. Therefore, their work as well as many subsequent works aim at constructing a test framework to authenticate transmitters and recognize if a guidance command is legit or illegitimate. Traditional upper-layer authentication methods (e.g., [187,188]) rely on security measures that are implemented at the higher layers of the communication protocols such as the application layer, the transport layer, or the session layer, whereas the lower-layer authentication typically involves the data link, or the network layer, and the Physical Layer Authentication (PLA). For example, a PLA technique is briefly presented below. The authors in [189] define the communication rate (in terms of bits per second per hertz) of an agent over a given link as the ratio of the agent's total transmitting power over a communication channel (that is the transmission power multiplied by the gain of the particular channel, plus a gaussian parasitic power) to the power of the parasitic signal, in a logarithmic scale.

Furthermore, the secrecy rate of a ground node over an eavesdropper is defined as the difference between the communication rate of the ground node to the UAV, and the communication rate of the ground node to the eavesdropper. In a similar fashion, one may assume that the destructive utility of an adversary could be evaluated by the communication rate of the adversary over the link between the adversary and its victim. Clearly, a cyber-physically secure trajectory is one that maximizes the communication rate of the ground node and simultaneously minimizes the communication rate of the adversaries. Therefore, optimization of the waypoints transmitted from the ground station to the remotely operated UAVs seem to be a possible solution for securing the UAVs against spoofing attacks.

The authors in [190] have recently performed an excellent literature review with respect to upper and lower layer UAV to ground authentication, and particularly the latest physical layer authentication methods. The authors in [191] aim to protect a ground node receiver against eavesdropper's spoofing attacks on a given UAV transmitted information, and suggest to plan an optimal trajectory with energy constraints for the UAV that tends to minimize its distance to the ground node while maximizing its distances to the eavesdroppers. This effectively decreases the Signal to Noise Ratio (SNR) of the information received by the eavesdroppers and mitigates the likelihood of information decoding by the eavesdroppers. The authors in [192] have introduced a probabilistic approach to enable UAV receivers authenticate legitimate ground based transmitters from eavesdropper spoofing attacks, by measuring the difference of signal to noise ratios (delta SNR) of adjacent transmissions received from incoming communication channels, and the problem is to optimize a threshold for the delta SNR that minimizes the probability of a deception (that is an eavesdropper be mistakenly taken for the authentic ground node), while conserving the probability of a false alarm (i.e., an eavesdropper be mistakenly taken for the ground node).

Reference [193] aims at protecting a UAV against adversaries targeting ground control stations via malware. The article assumes that the malware is capable of injecting a harmonic attack with a cyclic trajectory or in the form of a decaying signal, that is added to the desired trajectory commanded by the ground node. The article then develops an attack observer that monitors the desired trajectory error and aims at compensating the error, through transmission of a corrective command from the ground node. The authors in [194] also aim at formulating a physical layer authentication algorithm to differentiate a legitimate transmitter from several unknown spoofers without having access to a complete prior knowledge, using a Bayesian variational algorithm. Following former research works, the authors in [195] define Secrecy Vulnerable Regions (SVR) as a region where the the secrecy rate of the ground node being above a certain threshold is unlikely (in terms of a certain probability), and the Hijacking Vulnerable Region (HVR) as a region where a given adversary can effectively spoof a UAV victim and take over the control of the UAV from the ground node. The authors conclude that HVR could be determined by the intersection of the SVR and a blocking region in which the SNR from the ground node is insufficient for a recipient UAV to correctly decode the authentic command. The article then formulates an optimization problem over the power consumption of a set of slave UAVs in a network that tend to counterattack an adversary by minimizing the HVR through interfering signals to the adversary.

Reference [196] outlines a zero-sum game theoretic model for a UAV to detect a spoofer, where the UAV tries to adjust a detection threshold that compares the Received Signal Strength (RSS) of two consecutive transmissions, in which the first transmission is assumed to be authentic, and the second would be classified as authentic if its RSS lies within the threshold from the RSS of the authentic signal. The spoofer on the other hand is trying to adjust its attack probability, where the article assumes that the utility of the UAV and the attacker are always equal, hence a zero-sum game. The paper then proves that a Nash equilibrium exists where neither the UAV nor the spoofer can increase their respective utilities by changing their strategies, and the equilibrium takes place when the payoff of the UAV for accepting a legitimate command plus the UAV's cost of accepting a spoofing signal is greater than or equal to the cost of the spoofer in launching the attack.

The objective of the authors in [197] is to address the desired trajectory spoofing problem where a spoofer intends to takeover the trajectory control of a UAV that is transmitted from a ground controller, by adding an attack signal to the authentic command. However, the protective measure administered by the ground controller is to compensate for the added attack signal, even before the spoofer manipulation, so that it nullifies the attack. However, the authors assume that the attack signal model is known by the ground controller. The authors in [198] have used encryption and decryption methods on the physical properties of the transmitted signals for authentication of the transmitter. Finally, reference [199] has very recently proposed a John Boyd's Observation-Oriented-Decision-Action (OODA) loop together with a cooperative jamming leverage of a group of UAVs to ensure secure remote control actions.

In conclusion, the brief literature survey explained above suggests that physical layer authentication techniques while being robust to a variety of spoofing attacks demonstrate poor performance with respect to other types of threats such as replay attacks, since smart adversaries have the capability to record authentic signals and impersonate a legit transmitter. Other characteristics of the signal physical layer such as signal strength or carrier frequency are sensitive to environmental conditions such as multi-path propagation, line-of-sight dependency, and high mobility of the UAVs. Moreover, in dense airspaces with abundant vehicles as in the Urban Air Mobility (UAM) uniqueness of the physical properties of signals may pose challenge and exert excessive computational burden on the ground nodes as well as the UAVs. On the other hand, upper-layer authentication methods also pose certain disadvantages such as encryption-decryption overheads, vulnerability against insider threats, scalability, and network dependencies. Especially, with the advent of modern traffic control methodologies, multi-agent systems

are becoming more and more popular for propagation of emergency messages, dynamic geo-fencing rules, etc. throughout the network, thanks to their reliability and robustness against peer-to-peer communication failures. In these networks certain PLA techniques, and upper/lower-layer authentication methodologies may gradually fade away or abolish, and complementary intelligent authentication techniques may become required for secure and remote control of UAVs.

4.1 Contributions

As it is apparent from the literature review, the existing remote authentication solutions in the literature rely on features and characteristics of the physical layers of transmitted signals, or encryption and decryption protocols at the presentation layers. The existing methodologies while useful in peer-to-peer applications, do not seem applicable for UAM and short-range transmission scenarios, where information is severally relayed between remote controllers and aerial vehicles. This is due to the fact that features and characteristics of physical layers of transmitted signals are not predictable, as relaying stations vary in space and in time. Therefore, it seems necessary to develop more advanced and intelligent authentication techniques that are independent from transmitted signals, and rather rely on the content of the information, as opposed to physical features. This article introduces a novel approach to the problem of remote controller authentication, that aims at corroborating remote commands by means of consistency checks on static and dynamic features of commands. In particular, waypoint commands that do not constitute a coherent path with prior waypoints are less likely considered as trustworthy waypoints, or commands that do not control the motion of the vehicle in a dynamically efficient manner (from an energy conservation point of view) with respect to optimal acceleration/deceleration patterns, are unlikely trustworthy commands. Same applies to commands that do not adhere to the latest traffic rules and geo-fencing constraints. Since adherence to these constraints requires knowledge of prior commands and unique dynamic characteristics of vehicles, it would be unlikely for adversarial intruders to impersonate legitimate ground controllers. The authors of this paper believe that the present approach is unprecedented and could contribute to state of the art vehicular technologies.

4.2 Problem Statement

This chapter concerns one of the pivots of “secure navigation” as illustrated in Figure 1.6, that encompasses authentication of pairs of position-speed commands transmitted by the GCC (i.e., the “Cloud” in Figure 1.6) to UAVs, that consist the desirable trajectory

$\mathcal{X}_{0:n} \triangleq \{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_n\}$, $\mathcal{V}_{0:n} \triangleq \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ of the UAV from an origin $\mathbf{x}_0$ in the 3-D space to its destination $\mathbf{x}_n$, where $\mathbf{x}_k = [x_k, y_k, z_k]^T \in \mathcal{S} \subset \mathbb{R}^3$ represents the present position of the UAV in the airspace $\mathcal{S}$ at the present time-step k , with reference to a given inertial reference frame, and where $\mathbf{v}_k \in \mathbb{R}^3$ represents the linear 3-D velocity of the UAV with respect to the same reference frame. We let $\mathbf{x}_i, \mathbf{v}_i$, $k < i < n$ and $\mathbf{x}_j, \mathbf{v}_j$, $k < i < j < n$ denote future ground commands instructing the autopilot of the UAV to arrive at $\mathbf{x}_i$ and $\mathbf{x}_j$ at time-steps i and j , respectively, and at linear airspeeds $\mathbf{v}_i, \mathbf{v}_j$, hence, a designated trajectory $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ over the next two time-steps from k . The problem is to validate the flight path $\mathcal{X}_{i,j,\dots,n}$ and the designated air speeds $\mathcal{V}_{i,j,\dots,n}$ given a set of prior authentic conditions $\mathcal{C}_k = \{\mathcal{X}_{0:k}, \mathcal{V}_{0:k}, \mathcal{M}_k, \mathcal{D}\}$, where $\mathcal{X}_{0:k}, \mathcal{V}_{0:k}$ denote the set of prior waypoints and speeds, and where $\mathcal{M}_k$ represents the airspace map, and $\mathcal{D}$ denotes the dynamic constraints for the vehicle as defined in the next section. In this context “legitimacy” of a pair of commands $\mathbf{x}_i, \mathbf{v}_i$, with respect to $\mathcal{C}_k$, is defined as the likelihood of the commands being compliant to $\mathcal{C}_k$, and is denoted by the probability distribution function (pdf) $p(a_i|\mathbf{x}_i, \mathbf{v}_i, a_{0:k}, \mathcal{C}_k)$, where a_i is a binary event denoting that commands issued at time-step i are trustworthy, also implying that the ground command and control center transmitting i^{th} command is authentic.

Problem 3. *Therefore, our objective in this chapter is to evaluate $p(a_{i:n}|\mathbf{x}_{i:n}, \mathbf{v}_{i:n}, a_{0:k}, \mathcal{C}_k)$, where,*

$$p(a_{i:n}|\mathbf{x}_{i:n}, \mathbf{v}_{i:n}, a_{0:k}, \mathcal{C}_k) = \prod_{\ell=i}^n p(a_\ell|\mathbf{x}_\ell, \mathbf{v}_\ell, a_{0:k}, \mathcal{C}_k), \quad (4.1)$$

where the command at time-step ℓ is defined to be trustworthy, if,

$$p(a_\ell|\cdot) \geq \gamma_{\mathcal{C}}, \quad (4.2)$$

where $0 < \gamma_{\mathcal{C}} < 1$ is a predefined threshold.

Equation (4.1) is the “authentication function” that is computed by the processors on-board the UAV, and facilitates the UAV to derive the waypoints “trustworthiness function”,

$$p(\mathbf{x}_{i:n}|a_{i:n}, \mathbf{v}_{i:n}, a_{0:k}, \mathcal{C}_k) \propto p(a_{i:n}|\mathbf{x}_{i:n}, \mathbf{v}_{i:n}, a_{0:k}, \mathcal{C}_k) p(\mathbf{x}_{i:n}|\mathcal{M}_k) \quad (4.3)$$

where $p(\mathbf{x}_{i:n}|\mathcal{M}_k) \in \{0, 1\}$ is the “geo-fencing rule”, where $p(\mathbf{x}_{i:n}|\mathcal{M}_k) = 1$ determines that $\mathbf{x}_{i:n}$ could be safely obliged by the autopilot, with due consideration to the latest available air-corridors in the map $\mathcal{M}_k$, hence, ensuring collision avoidance, and a prioritized access to the airspace. On the other hand, $p(\mathbf{x}_{i:n}|\mathcal{M}_k) = 0$ implies that $\mathbf{x}_{i:n}$ according to the map are violating the geo-fencing rules and have to be avoided by

the autopilot as future waypoints. In conclusion, $p(\mathbf{x}_{i:n}|a_{i:n}, \mathbf{v}_{i:n}, a_{0:k}, \mathcal{C}_k)$ serves as an overview of all trustworthy airspace locations, perceived by the UAV that can aid secure and resilient navigation with respect to spoofing cyberattacks.

4.3 Definitions and Assumptions

Let us consider the airspace $\mathcal{S}$ as a directed graph $\mathcal{G} = (\mathcal{N}_m, \mathcal{E}_m)$, where $\mathcal{N}_m = \{\ell_1, \dots, \ell_n\}$ denotes an indexed set of discrete and equally sized grids in the airspace, so that there would be a one-to-one correspondence between any arbitrary position $\mathbf{x}_i \in \mathcal{S}$ and $\ell_i \in \mathcal{N}_m$, vice versa (i.e., $\mathbf{x}_i \leftrightarrow \ell_i$). The set of edges $\mathcal{E}_m$ represent all available airway corridors that connect the grids to their adjacent ones, so that given $\mathbf{x}_i \leftrightarrow \ell_i$ and $\mathbf{x}_j \leftrightarrow \ell_j$, $(\ell_i, \ell_j) \in \mathcal{E}_m$ implies that there exists an available airway corridor from $\mathbf{x}_i \rightarrow \mathbf{x}_j$, and $(\ell_i, \ell_j) \notin \mathcal{E}_m$ implies that the UAV cannot traverse from $\mathbf{x}_i \rightarrow \mathbf{x}_j$. This convention allows the UTM system to restrict airspace users from entering a protected area by removing certain edges from the edge set. It is noted that $\mathcal{G}$ is a dynamic structure that is instantaneously updated by UAM authorities, to reflect the latest geo-fencing rules and the traffic status.

Definition 7. *Map is a function $g(\cdot)$ that maps every point $\mathbf{x}_i \in \mathcal{S}$ to its corresponding node $\ell_i \in \mathcal{N}_m$, and determines all its available adjacent spaces $\mathbf{x}_j \in \mathcal{S}$. Therefore,*

$$g(\mathbf{x}_i) = \mathbf{x}_{j_1}, \mathbf{x}_{j_2}, \dots, \forall \mathbf{x}_{j_i}$$

where $(\ell_i, \ell_{j_i}) \in \mathcal{E}_m$, and $\mathcal{M}_k$ is the temporal adjacency matrix of all the points in the airspace with respect to the latest version of $\mathcal{G}$.

The linearized continuous-time motion equations of the Quadcopter in an inertial reference frame is given by,

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{v} \\ m\dot{\mathbf{v}} &= -m\kappa_v\mathbf{v} + F - G + \nu_f \\ \vartheta &= M(\eta)\ddot{\eta} + C(\eta, \dot{\eta})\dot{\eta} \end{aligned} \tag{4.4}$$

where $\mathbf{x} = [\mathbf{x}_x, \mathbf{x}_y, \mathbf{x}_z]^T$, $\mathbf{v} = [\mathbf{v}_x, \mathbf{v}_y, \mathbf{v}_z]^T \in \mathbb{R}^3$ denote the position and the linear speed of the vehicle, respectively, $m\kappa_v\mathbf{v}$ ($m, \kappa_v \in \mathbb{R}^+$) represents the drag force, $F \in \mathbb{R}^3$ denotes the propeller force, $\eta = [\phi, \theta, \psi]^T$ represents the attitude Euler angles consisting of the roll angle ϕ , pitch angle θ , and the yaw angle ψ in the inertial reference frame, and where $G = [0, 0, mg]^T$ denotes the force of gravity, and ν_f is an unknown disturbance force, and where $M(\eta), C(\eta, \dot{\eta})$ represent the diagonal moment of inertia tensor, and the Coriolis matrix, respectively, and finally where $\vartheta = [\vartheta_\phi, \vartheta_\theta, \vartheta_\psi]^T$ is the propeller torque vector. Additionally, the propellers' total force f in the inertial reference frame is given by,

$$F = f \begin{bmatrix} \cos \psi \sin \theta \cos \phi + \sin \psi \sin \phi \\ \sin \psi \sin \theta \cos \phi - \cos \psi \sin \phi \\ \cos \phi \cos \theta \end{bmatrix}$$

where,

$$\begin{bmatrix} f \\ \vartheta_\phi \\ \vartheta_\theta \\ \vartheta_\psi \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -d_\phi & -d_\phi & d_\phi & d_\phi \\ d_\theta & -d_\theta & d_\theta & -d_\theta \\ c_{\vartheta_f} & -c_{\vartheta_f} & -c_{\vartheta_f} & c_{\vartheta_f} \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix} \quad (4.5)$$

and where d_ϕ , d_θ , and c_{ϑ_f} are known constants which denote the half roll motor-to-motor distance, half pitch motor-to-motor distance, and the relationship between the thrust force and its corresponding torque, respectively, and where $f_1, \dots, f_4$ are the forces produced by the rotors.

Assuming that $\nu_f \approx 0$, we let $\vartheta = K_{e_\eta} \Delta \eta + K_{e_\omega} \Delta \dot{\eta}$ (inspired from [122, 123]), where $\Delta \eta \triangleq \eta - \eta_d$ for an arbitrary desired reference attitude η_d , and $F = G + m\kappa_v \mathbf{v} + m\lambda_v \Delta \mathbf{v} - m\lambda_x \Delta \mathbf{x}$, where $\Delta \mathbf{x} = \mathbf{x} - \mathbf{x}_d$, and $\Delta \mathbf{v} = \mathbf{v} - \mathbf{v}_d$, where $[\mathbf{x}_d^T, \mathbf{v}_d^T]^T$ is the desirable reference state. From the above equations of motion and the designated control law for ϑ, F it follows that,

$$\begin{bmatrix} \Delta \dot{\eta} \\ \Delta \ddot{\eta} \end{bmatrix} = \begin{bmatrix} 0 & I \\ M^{-1}(\eta)K_{e_\eta} & M^{-1}(\eta)(K_{e_\omega} - C(\eta, \dot{\eta})) \end{bmatrix} \begin{bmatrix} \Delta \eta \\ \Delta \dot{\eta} \end{bmatrix}.$$

The sufficient condition for $\eta \rightarrow \eta_d$ would be to have,

$$\begin{bmatrix} 0 & I \\ M^{-1}(\eta)K_{e_\eta} & M^{-1}(\eta)(K_{e_\omega} - C(\eta, \dot{\eta})) \end{bmatrix} < 0,$$

and since $M^{-1}(\eta) > 0$, by choosing $K_{e_\omega} = K'_{e_\omega} + C(\eta, \dot{\eta})$, it would be sufficient to choose $K_{e_\eta}, K'_{e_\omega}$ such that,

$$\begin{bmatrix} 0 & I \\ K_{e_\eta} & K'_{e_\omega} \end{bmatrix} < 0.$$

In order to satisfy the above condition we note that the eigenvalues of this matrix would be the roots of the characteristic equation,

$$\Lambda^2 + \Lambda M^{-1}(\eta)K'_{e_\omega} + M^{-1}(\eta)K_{e_\eta} = 0,$$

and if $K'_{e_\omega} = M(\eta)(\Lambda_1 + \Lambda_2)$, and $K_{e_\eta} = M(\eta)(\Lambda_1 \cdot \Lambda_2)$, the characteristic equation would then reduce to,

$$(\Lambda + \Lambda_1)(\Lambda + \Lambda_2) = 0,$$

where Λ_1, Λ_2 are positive diagonal matrices with arbitrary elements representing desirable eigenvalues (time-constants).

In conclusion, one may choose Λ_1, Λ_2 with appropriate time constants for desirable settling time of the attitude and the rotational speed. Then, we let,

$$\begin{aligned} K_{e_\eta} &= M(\eta)(\Lambda_1 \cdot \Lambda_2), \\ K_{e_\omega} &= C(\eta, \dot{\eta}) - M(\eta)(\Lambda_1 + \Lambda_2), \end{aligned} \tag{4.6}$$

and use the control law $\vartheta = K_{e_\eta}\Delta\eta + K_{e_\omega}\Delta\dot{\eta}$, to drive the torque and finally attain desirable attitude and rotational speed. Furthermore, the longitudinal equations of motion would transform to,

$$\begin{aligned} \Delta\dot{\mathbf{x}} &= \Delta\mathbf{v} \\ \Delta\dot{\mathbf{v}} &= -\lambda_x\Delta\mathbf{x} + \lambda_v\Delta\mathbf{v} \end{aligned} \tag{4.7}$$

and if $\lambda_x > 0$, and $\lambda_v < 0$, by application of the linear control law $F = G + m\kappa_v\mathbf{v} + m\lambda_v\Delta\mathbf{v} - m\lambda_x\Delta\mathbf{x}$, one could compute f , where it finally follows that $\mathbf{x} \rightarrow \mathbf{x}_d$, and $\mathbf{v} \rightarrow \mathbf{v}_d$.

Definition 8. Let $\phi_d = 0$, and ψ_d be such that the UAV heads toward $\mathbf{x}_d$ at all times, and $F_z = f \cos \theta_d = mg$, i.e., a constant altitude flight. Additionally, let $|\Delta\mathbf{x}| = \Delta x$, and $|\Delta\mathbf{v}| = \Delta v$. We denote $\mathcal{D}$ as the control law for ϑ, F (and consequently the quad-rotor forces $f_1, \dots, f_4$) so that $\eta \rightarrow \eta_d$, and $\Delta x \rightarrow 0$, $\Delta v \rightarrow 0$, in an optimal fashion with respect to an energy conservation point of view.

Assumption 8. It is assumed that $\mathcal{D}, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}$ is available to the GCC, and is not available to malicious intruders and adversaries. On the other hand, $\mathcal{M}_k$ and $\mathbf{x}, \mathbf{v}$, are assumed to be known to the GCC as well as adversaries, since they are transmitted information at the present time, by the UTM, and the UAV (as self-awareness tele-metered data), respectively.

Remark 12. Assumption [8](#) would be valid if it could be assumed that $\mathcal{X}_{0:k}, \mathcal{V}_{0:k}$ are prior information and available to adversaries only if they can monitor all prior commands transmitted from the GCC. Furthermore, availability of $\mathcal{D}$ implies availability of η_d which is never transmitted by the GCC and is a mere convention that is set inside the autopilot. In other words, the GCC may adopt a different η_d , hence, a different $\mathcal{D}$.

As $\phi_d = 0$, and ψ_d is the angle connecting $\mathbf{x}$ to $\mathbf{x}_d$, the vehicle is subject to a longitudinal motion from $\mathbf{x} \rightarrow \mathbf{x}_d$ with no lateral displacement. Therefore, the thrust vector $F = [F_x, F_y, F_z]^T = [f \cos \psi \sin \theta, f \sin \psi \sin \theta, f \cos \theta]^T$, where $f \cos \theta_d = mg$, and $f \sin \theta$ would be the driving force responsible for the longitudinal motion. As a result, one could write,

$$f \sin \theta_d = m\kappa_v |\mathbf{v}| + m\lambda_v |\Delta \mathbf{v}| - m\lambda_x |\Delta \mathbf{x}|, \quad (4.8)$$

from which it follows that $\tan \theta_d = \frac{\kappa_v}{g} |\mathbf{v}| + \frac{\lambda_v}{g} |\Delta \mathbf{v}| - \frac{\lambda_x}{g} |\Delta \mathbf{x}|$, providing the instantaneous value for θ_d and f . In conclusion, knowing $\eta_d = [\phi_d, \theta_d, \psi_d]^T$ and f , the autopilot evaluates $\vartheta = [\vartheta_\phi, \vartheta_\theta, \vartheta_\psi]^T = K_{e_\eta} \Delta \eta + K_{e_\omega} \Delta \dot{\eta}$ using onboard sensors, and finally derives $f_1, \dots, f_4$ from Equation (4.5), providing the complete control algorithm to drive the quadcopter from any present position and linear velocity $\mathbf{x}, \mathbf{v}$ to a desirable $\mathbf{x}_d, \mathbf{v}_d$ at a constant altitude, as explained earlier.

Definition 9. *Analysis of the energy for hovering and rotational maneuvers are beyond the scope of this paper, since the objective of the GCC is to calculate future commands $\mathbf{x}_i, \mathbf{v}_i$ given the present $\mathbf{x}_k, \mathbf{v}_k$ so that the energy for the motion $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i$ is optimal, i.e., $\{\mathbf{x}_i, \mathbf{v}_i | \min_{\mathbf{x}_k} \int_{\mathbf{x}_k}^{\mathbf{x}_i} f \sin \theta d\mathbf{x}\}$, and is defined as dynamic optimality.*

As discussed in the literature review, ABTM traffic management principles require all flight paths to be planned independently, in order to follow the most efficient route from the origin to the destination, implying that if $\mathcal{X}_{0:k} = \{\mathbf{x}_0, \dots, \mathbf{x}_k\}$ is a subset of the complete flight path $\mathcal{X}_{0:n}$, then the waypoints have to constitute a minimal cost function such as,

$$h(\mathbf{x}_0, \mathbf{x}_n) \triangleq \min_{\mathbf{x}_i} \sum_{i=0}^{n-1} \|\mathbf{x}_{i+1} - \mathbf{x}_i\|, (\ell_i, \ell_{i+1}) \in \mathcal{E}_m(k), \forall i, \quad (4.9)$$

given the constraints in the map, and the geo-fencing rules. Let $\mathcal{X}_{0:n}^* \triangleq \{\mathbf{x}_i | \sum_{i=0}^{n-1} \|\mathbf{x}_{i+1} - \mathbf{x}_i\| = h(\mathbf{x}_0, \mathbf{x}_n)\}$ denote the set of waypoints that constitute the most efficient path from $\mathbf{x}_0$ to $\mathbf{x}_n$.

Assumption 9. *We assume that $\mathcal{X}_{0:k} = \mathcal{X}_{0:k}^*$ and let $p(a_i | \mathbf{x}_i \in \mathcal{X}_{0:n}^*, \mathcal{M}_k) = \gamma_s$ imply that any waypoint $\mathbf{x}_i$ that lies on some efficient route $\mathcal{X}_{0:n}^*$ has a probability γ_s of being trustworthy, and a chance of $1 - \gamma_s$ being an adversarial intrusion.*

4.4 Research Results

Let us initially recall that for a set of probabilistic events A, B, C , Bayes' rule indicates that,

$$p(B|A) = \frac{p(A|B)p(B)}{p(A)},$$

where the denominator, $p(A) = \int_B p(A|B)p(B)dB$ is a normalization factor, to ensure that the sum of $p(A|B)p(B)$ for all possible values in B , results in one. Therefore, one can write $p(B|A) \propto p(A|B)p(B)$. Additionally, for all probabilistic events C , one can write,

$$\begin{aligned}
p(B|A, C) &= \frac{p(A|B, C)p(B, C)}{p(A, C)} \\
&= \frac{p(A|B, C)p(B|C)p(C)}{p(A|C)p(C)} = \frac{p(A|B, C)p(B|C)}{p(A|C)},
\end{aligned}$$

implying that conditions (such as C) can be added to the sides of the Bayes' rule. Finally, for any independent set of events $C_1, C_2, \dots, C_n$, one can write,

$$\begin{aligned}
p(A|C_1, C_2, \dots, C_n) &\propto \\
p(C_1|A, C_2, \dots, C_n) &p(A|C_2, \dots, C_n),
\end{aligned}$$

where $p(C_1|A, C_2, \dots, C_n) = p(C_1|A)$ (since it was assumed that C_1 is independent from $C_2, \dots, C_n$), and $p(C_1|A) \propto p(A|C_1) p(C_1)$.

In a similar fashion, $p(A|C_2, \dots, C_n) \propto p(A|C_2) p(C_2) p(A|C_3, \dots, C_n)$, and so forth. Therefore,

$$p(A|C_1, C_2, \dots, C_n) \propto \prod_{i=1}^n p(A|C_i) p(C_i) \propto \prod_{i=1}^n p(A|C_i). \quad (4.10)$$

Equation (4.10) can be readily applied to the problem statement and results as,

$$p(a_i|\mathbf{x}_i, \mathbf{v}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}, \mathcal{M}_k, \mathcal{D}) \propto \quad (4.11)$$

$$p(a_i|\mathbf{x}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{M}_k) p(a_i|\mathbf{x}_i, \mathbf{v}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}, \mathcal{D}),$$

where $p(a_i|\mathbf{x}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{M}_k)$ is the static authenticity function, and $p(a_i|\mathbf{x}_i, \mathbf{v}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}, \mathcal{D})$ is the dynamic authenticity function, and $a_{0:k}$ assumes that all prior commands are trustworthy. The remainder of this section concentrates on developing models for static and dynamic authenticity functions.

4.4.1 Static Authentication

Let us begin by introducing a theorem and a lemma that helps identify primary conditions that yield static authenticity of an arbitrary point $\mathbf{x}_i \in \mathcal{S}$, given $\mathcal{X}_{0:k}, \mathcal{M}_k$.

Theorem 11. *Let $\mathcal{X}_{0:n}^* \subset \mathcal{S}$ denote the set of waypoints on a most efficient path from $\mathbf{x}_0$ to $\mathbf{x}_n$ passing through $\mathcal{X}_{0:k}$ (that is, $\mathcal{X}_{0:k} = \{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_n\} \subset \mathcal{X}_{0:n}^*$). For any arbitrary point $\mathbf{x}_i \in \mathcal{X}_{0:n}^*$, $0 < k < i < n$, one would have $h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) = h(\mathbf{x}_0, \mathbf{x}_i)$.*

Proof. It has to be shown that,

$$\mathbf{x}_i \in \mathcal{X}_{0:n}^* \implies h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) = h(\mathbf{x}_0, \mathbf{x}_i).$$

Clearly, the condition $\mathbf{x}_i \in \mathcal{X}_{0:n}^*$ is equivalent to writing $\mathcal{X}_{0:n}^* = \mathcal{X}_{0:i}^* \cup \mathcal{X}_{i:n}^*$, which implies that,

$$h(\mathbf{x}_0, \mathbf{x}_i) + h(\mathbf{x}_i, \mathbf{x}_n) = h(\mathbf{x}_0, \mathbf{x}_n). \quad (4.12)$$

Additionally, $\mathcal{X}_{0:k} \subset \mathcal{X}_{0:n}^*$ further implies that,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_n) = h(\mathbf{x}_0, \mathbf{x}_n). \quad (4.13)$$

However, since $\mathbf{x}_i \in \mathcal{X}_{k:n}^*$, then $\mathcal{X}_{k:n}^* = \mathcal{X}_{k:\ell}^* \cup \mathcal{X}_{\ell:n}^*$, or,

$$h(\mathbf{x}_k, \mathbf{x}_i) + h(\mathbf{x}_i, \mathbf{x}_n) = h(\mathbf{x}_k, \mathbf{x}_n), \quad (4.14)$$

and substituting $h(\mathbf{x}_k, \mathbf{x}_n)$ from Equation (4.14) in Equation (4.13) results,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) + h(\mathbf{x}_i, \mathbf{x}_n) = h(\mathbf{x}_0, \mathbf{x}_n), \quad (4.15)$$

Deducing the sides of Equation (4.12) from Equation (4.15) reveals that,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) = h(\mathbf{x}_0, \mathbf{x}_i),$$

which completes the proof of the theorem. ■

Lemma 5. *If $\mathbf{x}_i \in \mathcal{X}_{0:n}^* \subset \mathcal{S}$, and $\mathcal{X}_{0:k} \subset \mathcal{X}_{0:i}^*$, then $\mathcal{X}_{0:n}^* = \mathcal{X}_{0:k} \cup \mathcal{X}_{k:i}^* \cup \mathcal{X}_{i:n}^*$.*

Proof. The lemma is trivial, since according to Theorem 11, $\mathcal{X}_{0:k} \subset \mathcal{X}_{0:i}^*$ implies that,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) = h(\mathbf{x}_0, \mathbf{x}_i),$$

and if there exists an $\mathbf{x}_i \in \mathcal{X}_{0:n}^* \subset \mathcal{S}$, then it follows that,

$$h(\mathbf{x}_0, \mathbf{x}_i) + h(\mathbf{x}_i, \mathbf{x}_n) = h(\mathbf{x}_0, \mathbf{x}_n).$$

Substituting $h(\mathbf{x}_0, \mathbf{x}_i)$ from the first equation into the above equation results in,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) + h(\mathbf{x}_i, \mathbf{x}_n) = h(\mathbf{x}_0, \mathbf{x}_n),$$

which implies that,

$$\mathcal{X}_{0:n}^* = \mathcal{X}_{0:k} \cup \mathcal{X}_{k:i}^* \cup \mathcal{X}_{i:n}^*,$$

and this completes the proof of the lemma. ■

The important conclusion that can be derived from Theorem 11, and Lemma 5, is that for any arbitrary point $\mathbf{x}_i \in \mathcal{S}$, equation $h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) = h(\mathbf{x}_0, \mathbf{x}_i)$ would be a sufficient condition to ensure that $\mathbf{x}_i \in \mathcal{X}_{0:n}^*$ at least for some destination $\mathbf{x}_n$, if there exists an efficient path in $\mathcal{M}_k$ from $\mathbf{x}_i \rightarrow \mathbf{x}_n$. Therefore, one may conclude that,

$$h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) \neq h(\mathbf{x}_0, \mathbf{x}_i) \Rightarrow P(a_i | \mathbf{x}_i, \mathcal{X}_{0:k}) < \gamma_s,$$

and this suggests that $h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) - h(\mathbf{x}_0, \mathbf{x}_i)$ could be a metric to evaluate the consistency between $\mathbf{x}_i$ and the prior $\mathcal{X}_{0:k}$, since a large $h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) - h(\mathbf{x}_0, \mathbf{x}_i)$ implies a considerable drift for $\mathbf{x}_i$ from the optimal path $\mathcal{X}_{0:k} \cup \mathcal{X}_{k:i}^*$, hence, a lower likelihood for trustworthiness of $\mathbf{x}_i$. Consequently, it would seem reasonable to assume that,

$$p(a_i|\mathbf{x}_i, a_{0:k}, \mathcal{X}_{0:k}, \mathcal{M}_k) = \gamma_s e^{-\gamma_s (h(\mathbf{x}_0, \mathbf{x}_k) + h(\mathbf{x}_k, \mathbf{x}_i) - h(\mathbf{x}_0, \mathbf{x}_i))}. \quad (4.16)$$

Equation (4.16) provides a pdf model for the trustworthiness of $\mathbf{x}_i$, where γ_s is a weight factor that determines the weight for the static authentication relative to the dynamic authentication.

4.4.2 Dynamic Authentication

The purpose of this subsection is developing a theoretical basis for evaluation of $p(a_j|a_i, \mathbf{x}_i, \mathbf{v}_i, \mathbf{x}_j, \mathbf{v}_j, \mathcal{D})$. It is assumed that a controller transmits a set of commands for a vehicle to follow a linear path $\mathbf{x}_i \rightarrow \mathbf{x}_j$, given $\mathbf{x}_i, \mathbf{v}_i, \mathbf{x}_j, \mathbf{v}_j$, and the objective is to authenticate command j , given prior commands, and $\mathcal{D}$. As discussed earlier, let $\Delta x \triangleq \|\mathbf{x} - \mathbf{x}_j\|$, where $\mathbf{x}$ is the instantaneous position of the vehicle between $\mathbf{x}_i \rightarrow \mathbf{x}_j$. In a similar way, let $\Delta v \triangleq \|\mathbf{v} - \mathbf{v}_j\|$, $\Delta x_i = \|\mathbf{x}_i - \mathbf{x}_j\|$, and $\Delta v_i = \|\mathbf{v}_i - \mathbf{v}_j\|$. The control objective is that $\Delta x \rightarrow 0$, and $\Delta v \rightarrow 0$, in a designated time $\Delta t_{i:j} = |j - i|T_s$ where T_s is the time period of a single time-step, and with optimal energy economics. From Equation (4.7) it follows that,

$$\Delta \dot{x} = \Delta v$$

$$\Delta \dot{v} = -\lambda_x \Delta x + \lambda_v \Delta v$$

since it was noted in Definition 8 that the motion consists of no lateral component, hence a uni-directional motion along the path $\mathbf{x}_i \rightarrow \mathbf{x}_j$, where $\lambda_x = \lambda_1 \lambda_2 > 0$, and $\lambda_v = \lambda_1 + \lambda_2 < 0$, and where $\lambda_1, \lambda_2 \in \mathbb{R}^-$. As discussed earlier, the objective is to find conditions for a dynamically optimal motion $\mathbf{x}_i \rightarrow \mathbf{x}_j$ in terms of λ_x and λ_v .

Theorem 12. *Given the set of commands $\mathbf{x}_i, \mathbf{x}_j \in \mathcal{S}$, $\mathbf{v}_i, \mathbf{v}_j$, and the dynamics $\mathcal{D}$, the optimal conditions for the motion $\mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ in terms of energy preservation where $\nu_f = 0$, and $|\mathbf{v}_i| > |\mathbf{v}_j|$ satisfies,*

$$\kappa_v v_j \Delta x_{i:j} + \frac{1}{2} m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i:j}^2 \approx \frac{1}{2} m \Delta v_{i:j}^2, \quad (4.17)$$

where $\Delta x_{i:j} \triangleq \|\mathbf{x}_j - \mathbf{x}_i\|$, and $\Delta v_{i:j} \triangleq \|\mathbf{v}_j - \mathbf{v}_i\|$.

Proof. Equation (4.7) can be written as,

$$\begin{bmatrix} \Delta \dot{x} \\ \Delta \dot{v} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\lambda_1 \lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix} \begin{bmatrix} \Delta x \\ \Delta v \end{bmatrix},$$

where it could be simply shown that,

$$\begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} \frac{\lambda_2}{\lambda_2 - \lambda_1} & \frac{-1}{\lambda_2 - \lambda_1} \\ \frac{-\lambda_1}{\lambda_2 - \lambda_1} & \frac{1}{\lambda_2 - \lambda_1} \end{bmatrix},$$

provided that $\lambda_1 \neq \lambda_2$, which results in a solution for Δx , and Δv , as,

$$\Delta x = (\lambda_2 e^{\lambda_1 t} - \lambda_1 e^{\lambda_2 t}) \frac{\Delta x_{i:j}}{\lambda_2 - \lambda_1} + (e^{\lambda_2 t} - e^{\lambda_1 t}) \frac{\Delta v_{i:j}}{\lambda_2 - \lambda_1}, \quad (4.18)$$

$$\Delta v = \lambda_1 \lambda_2 (e^{\lambda_1 t} - e^{\lambda_2 t}) \frac{\Delta x_{i:j}}{\lambda_2 - \lambda_1} + (\lambda_2 e^{\lambda_2 t} - \lambda_1 e^{\lambda_1 t}) \frac{\Delta v_{i:j}}{\lambda_2 - \lambda_1}. \quad (4.19)$$

Applying the standard control law as discussed in the literature [122], one will have the required horizontal thrust component according to Equation (4.4), and temporarily ignoring the disturbance ν_f as,

$$f \sin \theta = m \kappa_v v + m \lambda_v \Delta v - m \lambda_x \Delta x,$$

where $v = |\mathbf{v}_j| + \Delta v$ is the instantaneous speed magnitude of the vehicle along the direction of the motion, and the energy for an infinitesimally small displacement $i \rightarrow j$ could be derived as $dW = f \sin \theta dx$, where $dx = d\Delta x$, and $dW = m \kappa_v (v_j + \Delta v) d\Delta x + m \lambda_v \Delta v d\Delta x - m \lambda_x \Delta x d\Delta x$, where $\Delta v d\Delta x = \Delta v \frac{d\Delta x}{dt} dt = \Delta v^2 dt$, and the required energy for the horizontal motion would follow as,

$$\begin{aligned} \int_{\mathbf{x}_i}^{\mathbf{x}_j} dW &= \int_{\Delta x_{i:j}}^{\Delta x_{j:j}} m \kappa_v v_j d\Delta x \\ &+ m(\kappa_v \pm \lambda_v) \int_0^{\Delta t} \Delta v^2 dt - m \lambda_x \int_{\Delta x_{i:j}}^{\Delta x_{j:j}} \Delta x d\Delta x. \end{aligned} \quad (4.20)$$

It is worth noting that the term Δv^2 entails different formulations for the energy for a decelerating motion where $\Delta v > 0$, and an accelerating one, where $\Delta v < 0$. However, from Equation (4.19) it follows that,

$$\begin{aligned} (\Delta v)^2 &= (e^{2\lambda_1 t} + e^{2\lambda_2 t} - 2e^{(\lambda_1 + \lambda_2)t}) \left(\frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} \right)^2 \Delta x_{i:j}^2 \\ &+ (\lambda_2^2 e^{2\lambda_2 t} + \lambda_1^2 e^{2\lambda_1 t} - 2\lambda_1 \lambda_2 e^{(\lambda_1 + \lambda_2)t}) \left(\frac{1}{\lambda_2 - \lambda_1} \right)^2 \Delta v_{i:j}^2 \\ &+ (\lambda_2 e^{(\lambda_1 + \lambda_2)t} + \lambda_1 e^{(\lambda_1 + \lambda_2)t} - \lambda_1 e^{2\lambda_1 t} - \lambda_2 e^{2\lambda_2 t}) \frac{2\lambda_1 \lambda_2 \Delta x_i \Delta v_i}{(\lambda_2 - \lambda_1)^2}, \end{aligned}$$

where λ_1, λ_2 have to be selected such that $\int_0^{\Delta t} e^{\lambda_1 t} dt \approx \frac{-1}{\lambda_1}$, and $\int_0^{\Delta t} e^{\lambda_2 t} dt \approx \frac{-1}{\lambda_2}$. In this case,

$$\begin{aligned}
\int_0^{\Delta t} (\Delta v)^2 dt &\approx \left(\frac{-1}{2\lambda_1} + \frac{-1}{2\lambda_2} + \frac{2}{\lambda_1 + \lambda_2} \right) \left(\frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} \right)^2 \Delta x_{i:j}^2 \\
&+ \left(\frac{-\lambda_2}{2} + \frac{-\lambda_1}{2} + \frac{2\lambda_1 \lambda_2}{\lambda_1 + \lambda_2} \right) \frac{1}{(\lambda_2 - \lambda_1)^2} \Delta v_{i:j}^2, \\
&\approx -\frac{\lambda_x}{2\lambda_v} \Delta x_{i:j}^2 - \frac{1}{2\lambda_v} \Delta v_{i:j}^2,
\end{aligned}$$

and for the term $\int_{\mathbf{x}_i}^{\mathbf{x}_j} -m\lambda_x \Delta x \, d\mathbf{x}$ it follows that,

$$-m\lambda_x \int_{\Delta x_i}^{\Delta x_j} \Delta x \, d\Delta x = -\frac{1}{2}m\lambda_x (\Delta x_j^2 - \Delta x_i^2),$$

where $\Delta x_j = x_j - x_j = 0$, $\Delta x_i = \Delta x_{i:j}$. Consequently, for a decelerating motion one can write,

$$\begin{aligned}
W_{i:j}^D &\approx m\kappa_v v_j \Delta x_{i:j} - m(\kappa_v + \lambda_v) \frac{\lambda_x}{2\lambda_v} \Delta x_{i:j}^2 \\
&- m(\kappa_v + \lambda_v) \frac{1}{2\lambda_v} \Delta v_{i:j}^2 + \frac{1}{2}m\lambda_x \Delta x_{i:j}^2,
\end{aligned}$$

where $\kappa_v, \lambda_x > 0$, and $\lambda_v < 0$. Assuming that $\lambda_v \ll -\kappa_v$, $W_{i:j}^D$ can be further simplified as,

$$W_{i:j}^D \approx m\kappa_v v_j \Delta x_{i:j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i:j}^2 - \frac{1}{2}m \Delta v_{i:j}^2, \quad (4.21)$$

where it was denoted that $W_{i:j} \triangleq \int_{\mathbf{x}_i}^{\mathbf{x}_j} f \sin \theta \, d\mathbf{x}$, and where $m\kappa_v v_j \Delta x_{i:j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i:j}^2$ are positive energy components emerging from the thrust component $m\kappa_v(v_j + \Delta v)$ that acts along the direction of the motion, and $\frac{1}{2}m \Delta v_{i:j}^2$ is a negative energy component emerging from a resistive thrust $m\lambda_v \Delta v$ that acts against the direction of the motion as long as $|\mathbf{v}_i| > |\mathbf{v}_j|$, i.e., a decelerating motion. However, in an accelerating scenario where $|\mathbf{v}_i| < |\mathbf{v}_j|$, the thrust component $m\lambda_v \Delta v$ is positive and,

$$\begin{aligned}
W_{i:j}^A &\approx m\kappa_v v_j \Delta x_{i:j} - m(\kappa_v - \lambda_v) \frac{\lambda_x}{2\lambda_v} \Delta x_{i:j}^2 \\
&- m(\kappa_v - \lambda_v) \frac{1}{2\lambda_v} \Delta v_{i:j}^2 + \frac{1}{2}m\lambda_x \Delta x_{i:j}^2.
\end{aligned}$$

As a result, Equation (4.21) modifies to,

$$\begin{aligned}
W_{i:j}^A &\approx m\kappa_v v_j \Delta x_{i:j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i:j}^2 + \frac{1}{2}m \frac{\kappa_v}{|\lambda_v|} \Delta v_{i:j}^2 \\
&+ m\lambda_x \Delta x_{i:j}^2 + \frac{1}{2}m \Delta v_{i:j}^2,
\end{aligned}$$

and since it was assumed that $|\lambda_v| \gg \kappa_v$, then $\frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \ll \lambda_x$, and $\frac{1}{2}m \frac{\kappa_v}{|\lambda_v|} \ll \frac{1}{2}m$, and it finally follows that,

$$W_{i:j}^A \approx m\kappa_v v_j \Delta x_{i:j} + m\lambda_x \Delta x_{i:j}^2 + \frac{1}{2}m \Delta v_{i:j}^2, \quad (4.22)$$

which constitutes the energy in accelerative piecewise linear motions. In order to demarcate the energy in decelerating modes designated by Equation (4.21) from the energy in the accelerating modes as presented in Equation (6) let the motion energy (from $i \rightarrow j$) in decelerating and accelerating modes, be denoted by $W_{i,j}^D$, and $W_{i,j}^A$, respectively. Clearly, the optimal condition for $W_{i,j}^D$ is where $m\kappa_v v_j \Delta x_{i,j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i,j}^2 = \frac{1}{2}m\Delta v_{i,j}^2$, implying $W_{i,j}^D = 0$, that is a condition where the kinetic energy of the vehicle is just enough to offset the drag. Under this optimal condition the legitimate remote controller deliberately issues commands $\mathbf{x}_i, \mathbf{v}_i, \mathbf{x}_j, \mathbf{v}_j$ such that $W_{i,j}^D = 0$, and the vehicle would traverse from $\mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ in a gliding mode with no horizontal thrust. However, in order for $W_{i,j}^D = 0$ a prior pre-accelerating stage is necessary to set the airspeed to $\mathbf{v}_i$ at i . On the other hand from Equation (6) it follows that an accelerative mode is optimal where $\Delta x_{i,j}$ is as small as possible given that λ_x is a gain that opposes disturbance forces ν_f , and is often much larger than 1 as will be justified shortly later in Lemma 7. As a conclusion, it can be indicated that the set of dynamic constraints denoted by $\mathcal{D}$ specifies optimal energy conditions for a motion $\mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$, where $|\mathbf{v}_i| > |\mathbf{v}_j|$, is to have $m\kappa_v v_j \Delta x_{i,j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i,j}^2 = \frac{1}{2}m\Delta v_{i,j}^2$, which completes the proof of the theorem. ■

Lemma 6. *Given $\mathbf{x}_k, \mathbf{v}_k$ at the present time-step k , the optimal energy condition for the motion $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ is to have a pre-accelerating motion $k \rightarrow i$ where $W_{k:i}^A \approx \frac{1}{2}m\Delta v_{k:i}^2$ and $|\mathbf{v}_j| = |\mathbf{v}_k|$.*

Proof. In the optimal case of Theorem 12, the energy for the motion $\mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ is $\frac{1}{2}m\Delta v_{i,j}^2$ that has to be initially supplied to the vehicle through prior speed acceleration of the vehicle to $\mathbf{v}_i$, since $\frac{1}{2}m\Delta v_{i,j}^2$ is the energy that is required to oppose the drag $m\kappa_v v_j \Delta x_{i,j} + \frac{1}{2}m \frac{\kappa_v \lambda_x}{|\lambda_v|} \Delta x_{i,j}^2$. Additionally, the optimal energy condition for the pre-accelerating phase $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i$ (k assumed to be the present time-step) is to minimize the displacement $\|\mathbf{x}_i - \mathbf{x}_k\|$ implying that $W_{k:i}^A \approx \frac{1}{2}m\Delta v_{k:i}^2$, which also follows that $\frac{1}{2}m\Delta v_{k:i}^2 \approx \frac{1}{2}m\Delta v_{i,j}^2$ or $|\mathbf{v}_j| = |\mathbf{v}_k|$, and this completes the proof of the lemma. ■

Theorem 12 and Lemma 6 are statements that can be used to assess the authenticity of new pairs of commands $\mathbf{x}_i, \mathbf{v}_i, \mathbf{x}_j, \mathbf{v}_j$ for piecewise linear motions $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ which comply $\mathcal{D}$, given the present state $\mathbf{x}_k, \mathbf{v}_k$. Furthermore, in order to accomplish the motion $\mathbf{x}_i, \mathbf{v}_i \rightarrow \mathbf{x}_j, \mathbf{v}_j$ in a specific amount of time $\Delta t_{i,j} \triangleq (j - i)T_s$, $j > i$, where $T_s \in \mathbb{R}^+$ is the time period of a single time-step, it would be sufficient to choose an arbitrary constant $\xi = |\lambda_1| \Delta t_{i,j}$ so that $e^{-\xi} \approx 0$, and $\lambda_2 < \lambda_1 < 0$. A typical range for ξ could be [4, 6]. In this case the following Lemma can be used to evaluate an appropriate range for λ_1, λ_2 .

Lemma 7. *Given System (4.7) and Equation (4.4), the sufficient condition for $\Delta x^2 + \Delta v^2 \leq \gamma_\nu^2 \|\nu_f\|_{max}^2$, $\forall \Delta x, \Delta v$, is to have,*

$$\lambda_1 < -1, \text{ and, } \lambda_2 + 1 < -\gamma_\nu^{-2},$$

where $\|\nu_f\|_{\max}$ is the maximum amplitude of the disturbance force, and $\gamma_\nu \in \mathbb{R}^+$ is an arbitrary small positive number.

The proof of the lemma is omitted as the focus of this chapter is not to discuss design aspects for controllers. However, it follows from Lemma 7 that one can choose $\lambda_2 < \lambda_1$, which also follows that $\lambda_x/|\lambda_v| = -\lambda_1\lambda_2/\lambda_1 + \lambda_2 \approx -\lambda_1$. Given that $-\lambda_1 = \xi/\Delta t_{i:j}$, Equation (4.17) reduces to,

$$m\kappa_v v_j \Delta x_{i:j} + \frac{1}{2}m \frac{\xi}{\Delta t_{i:j}} \Delta x_{i:j}^2 = \frac{1}{2}m \Delta v_{i:j}^2,$$

and finally,

$$W_{i:j}^D = m(\kappa_v v_j + \frac{\xi}{2} \bar{\mathbf{v}}_{i:j}) \Delta x_{i:j} - \frac{1}{2}m \Delta v_{i:j}^2, \quad (4.23)$$

where $\bar{\mathbf{v}}_{i:j} \triangleq \Delta x_{i:j}/\Delta t_{i:j}$, and where $W_{i:j}^D \approx 0$, optimally. In conclusion, given $\mathbf{x}_k, \mathbf{v}_k$ it could be concluded that the greater the absolute value of the energy $|W_{i:j}^D|$ of any decelerating motion from $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i$, the lower the probability of a_i , that is,

$$p(a_i|\mathbf{x}_i, |\mathbf{v}_i| < |\mathbf{v}_k|, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}, a_{0:k}, \mathcal{D}) = \gamma_d e^{-\gamma_d |W_{k:i}^D|}, \quad (4.24)$$

where $W_{k:i}^D$ could be derived from Equation (4.23), where $0 < \gamma_d < 1$ is an arbitrary weight factor to determine the weight factor of decelerating motions on the overall authenticity.

In a similar way, for any accelerating motion from $\mathbf{x}_k, \mathbf{v}_k \rightarrow \mathbf{x}_i, \mathbf{v}_i$, one can write,

$$p(a_i|\mathbf{x}_i, |\mathbf{v}_i| > |\mathbf{v}_k|, \mathcal{X}_{0:k}, \mathcal{V}_{0:k}, a_{0:k}, \mathcal{D}) = \gamma_a e^{-\gamma_a \|\mathbf{x}_i - \mathbf{x}_k\|}. \quad (4.25)$$

For the special case where $|\mathbf{v}_i| = |\mathbf{v}_k|$, the Δv^2 term in Equation (4.20) vanishes and the integration results in $W_{k:i}^E = m\kappa_v v_k \|\mathbf{x}_i - \mathbf{x}_k\| + \frac{1}{2}m\lambda_x \|\mathbf{x}_i - \mathbf{x}_k\|^2$.

4.5 Simulation Results

In what follows, it has been assumed that an updated map of the airspace $\mathcal{M}_k$ is periodically transmitted to aerial vehicles, where k is the present time-step. In every scenario a section of the airspace map is displayed, in which the center of the grids $\ell_i \in \mathcal{N}_m$ are marked by a dot and labeled with an indicating reference number i . Based on the methodologies discussed in this chapter the UAV calculates the authentication function $p(a_i|\mathbf{x}_i, \mathbf{v}_i, a_{0:k}, \mathcal{C}_k)$ at time k , and evaluates the trustworthiness function $p(\mathbf{x}_i|a_i, \mathbf{v}_i, a_{0:k}, \mathcal{C}_k)$ for all future points $\mathbf{x}_i$ in the airspace based on Equation (4.3), where $p(\mathbf{x}_i|\mathcal{M}_k)$ is 1 if an air-corridor from $\mathbf{x}_k \rightarrow \mathbf{x}_i$ is available in the map, and 0 if not. Depending on the trustworthiness function the legitimacy of the points in the map are

graded with a likelihood and a marker size proportional to the likelihood. The piecewise linear path illustrates the route already traversed to the present position. Note that the accuracy of the authentication process can be measured by the fraction of the unrestricted points in the map to the number of the points in the map. That is, zero-percent accuracy indicates that all the points in the map are trustworthy, which is equivalent to no authentication. Clearly, as the set of prior waypoints increases, the accuracy of authentication is also increased, since the UAV then has more information to rely on.

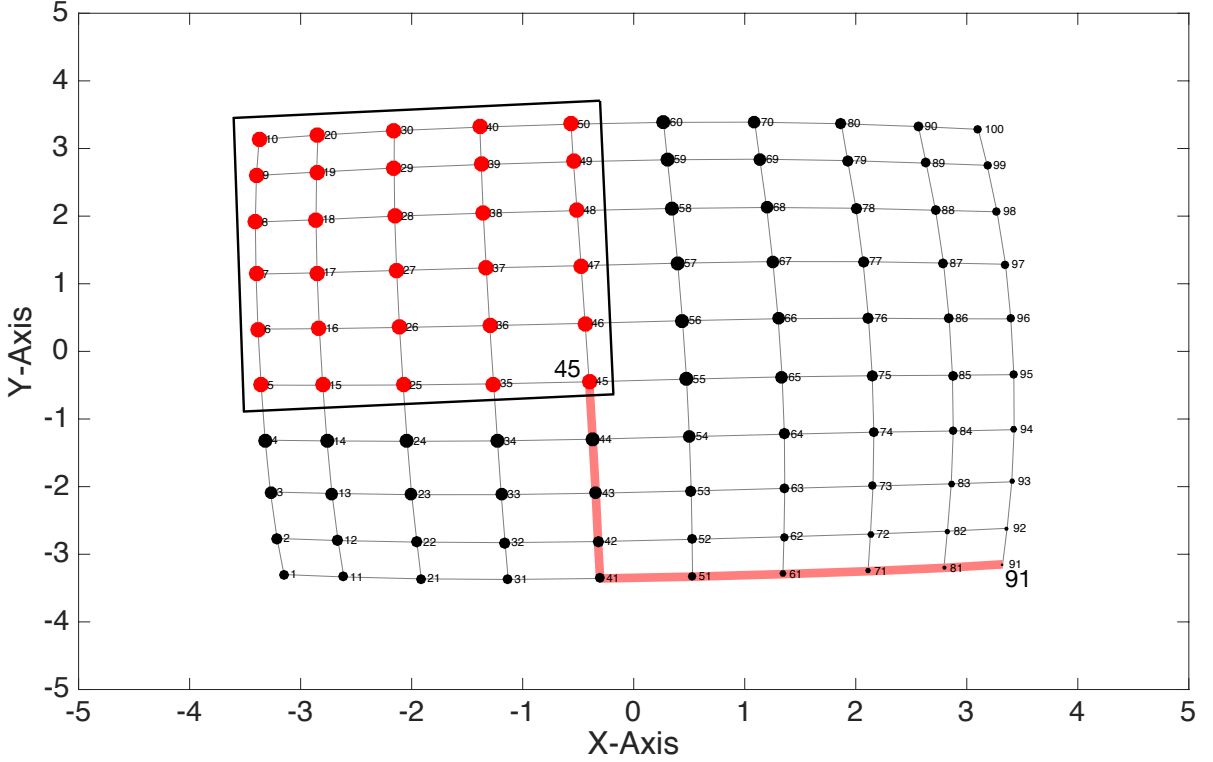


Figure 4.1: Simulated flight path of a vehicle from $\mathbf{x}_0 \rightarrow \mathbf{x}_k$, where $\mathbf{x}_0 \leftrightarrow 91 \in \mathcal{N}_m$, and $\mathbf{x}_k \leftrightarrow 45 \in \mathcal{N}_m$. The red path indicates the already taken path which is the most efficient route from the origin to the present position.

Figure 4.1 is an example depicting part of the map without considering the geo-fencing rule $p(\mathbf{x}_i|\mathcal{M}_k) \in \{0, 1\}$, where an aerial vehicle begins at the origin $\mathbf{x}_0 \leftrightarrow 91$ and follows a path to grid 45. In the absence of geo-fencing constraints and preserved paths for priority service vehicles, there is an available corridor to all adjacent grids of 45. At $k = 9$, $\mathbf{x}_k \leftrightarrow 45$, and the vehicle determines all trustworthy future positions, i.e., points enclosed in the rectangle (marked by red colour). Therefore, if a future waypoint $\mathbf{x}_i$ is inside the enclosed box the command is obliged and passed to the autopilot.

Figure 4.2 depicts a case example where geo-fencing rules $p(\mathbf{x}_i|\mathcal{M}_k)$ are implemented

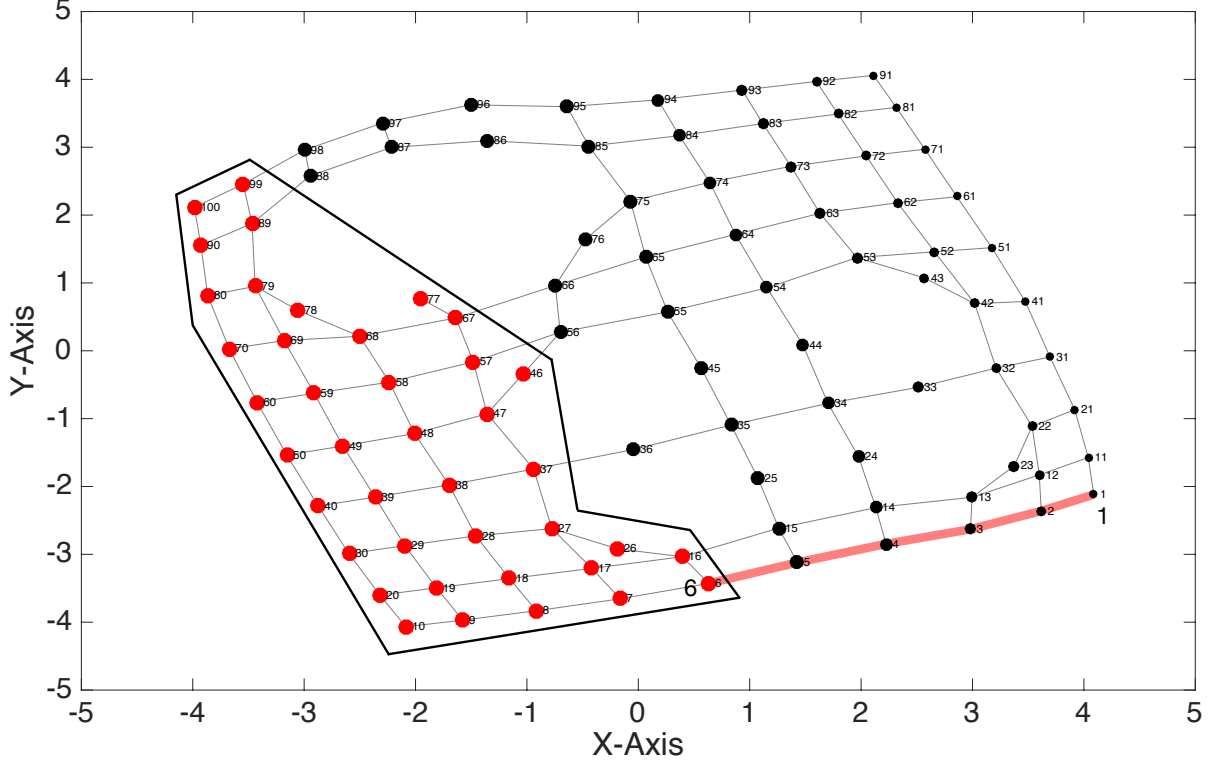


Figure 4.2: A relatively short flight path of a vehicle from $\mathbf{x}_0 \rightarrow \mathbf{x}_k$, where $\mathbf{x}_0 \leftrightarrow 1 \in \mathcal{N}_m$, and $\mathbf{x}_k \leftrightarrow 6 \in \mathcal{N}_m$. As the prior set of the prior waypoints $\{1, \dots, 6\}$ is relatively small, the authentication of the future waypoints embraces a large set of trustworthy possibilities, hence, relatively non-restricted, i.e., inaccurate.

in the map and certain air-corridors are wiped out from the map. As a result the available future routes for the vehicle is restricted. At $k = 5$ the vehicle evaluates all future trustworthy points $\mathbf{x}_6$ in the map where there is an available air-corridor and generates $p(\mathbf{x}_6 | a_6, \mathbf{x}_{0:5}, \mathcal{M}_5)$ for some certain $\gamma_s \in \mathbb{R}^+$, and marks them by “red” (enclosed by a polygon).

A future waypoint $\mathbf{x}_5$ if inside the polygon is authenticated, and obliged for the autopilot to follow. Otherwise, the waypoint will not be passed to the autopilot. Figure 3.4 is the repeated case study of Figure 4.2, except with more prior waypoints for the computation of $p(a_{k+1} | \mathbf{x}_{k+1}, \cdot)$, hence, more restricted. Clearly, the points in the polygon of Figure 4.3 are inside the polygon of Figure 4.2 which is due to the fact that all trustworthy waypoints authenticated at $k = 9$ have to be authentic at $k = 5$ too.

Finally, Figure 4.4 depicts the flight path of the aerial vehicle in Figures 4.2 and 4.3 at $k = 12$, where the vehicle has traversed through more waypoints. The accuracy of the authentication is increasing from 61% at $k = 5$, to 76% at $k = 9$, and

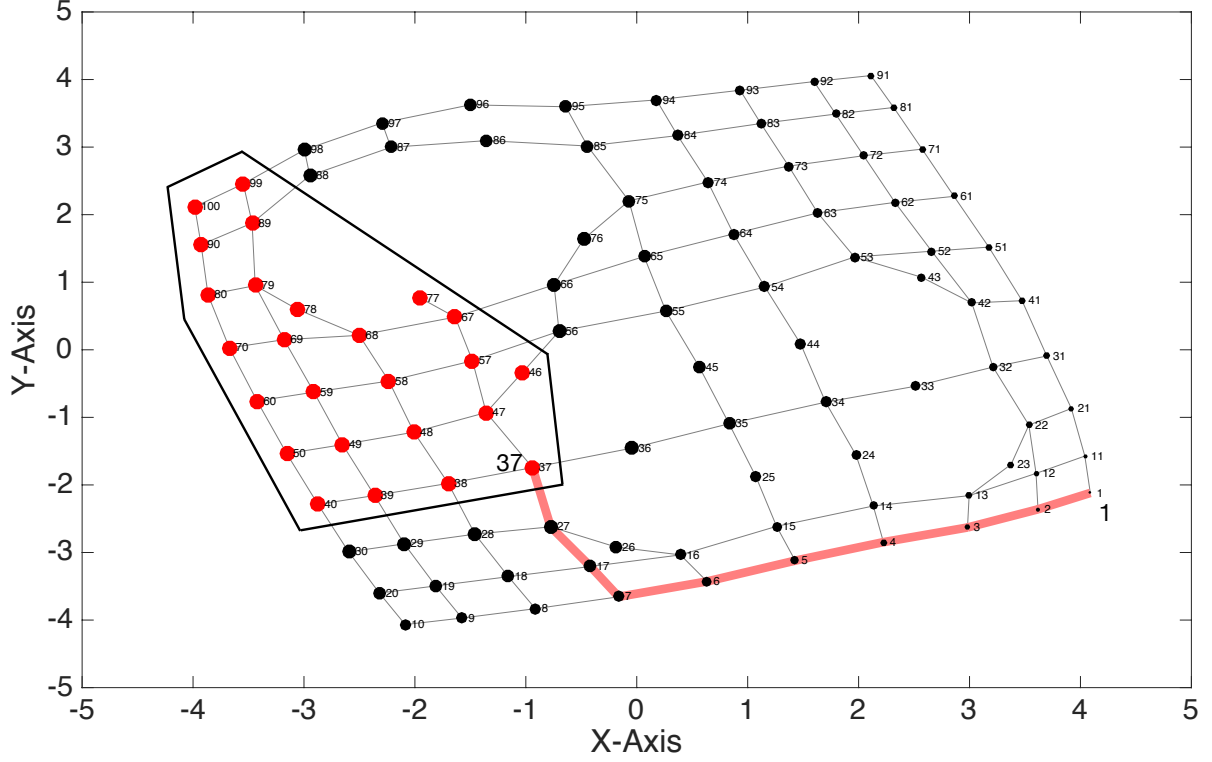


Figure 4.3: A similar case study to Figure 4.2 with the exception that the set of prior waypoints in this example are $\mathcal{X}_{0:9}$ are greater in the number of elements. This entails $p(a_{10}|\mathbf{x}_{10}, \cdot)$ to be evaluated based on a larger set of conditions, hence a smaller set of trustworthy options as future waypoints. Clearly the number of trustworthy points $\mathbf{x}_9$ in this figure has decreased to 24, in comparison to 39 trustworthy points in Figure 4.2, implying an increased accuracy.

finally to 89% at $k = 12$. Clearly, Equation (4.1) indicates that $p(a_{i:i+n}|\mathbf{x}_{i:i+n}, \cdot) = p(a_{i+n}|\mathbf{x}_{i+n}, \cdot) p(a_{i:i+n-1}|\mathbf{x}_{i:i+n-1}, \cdot)$ implying that trustworthy waypoints at every time-step encompasses all trustworthy points at prior waypoints, excluding all backup motions.

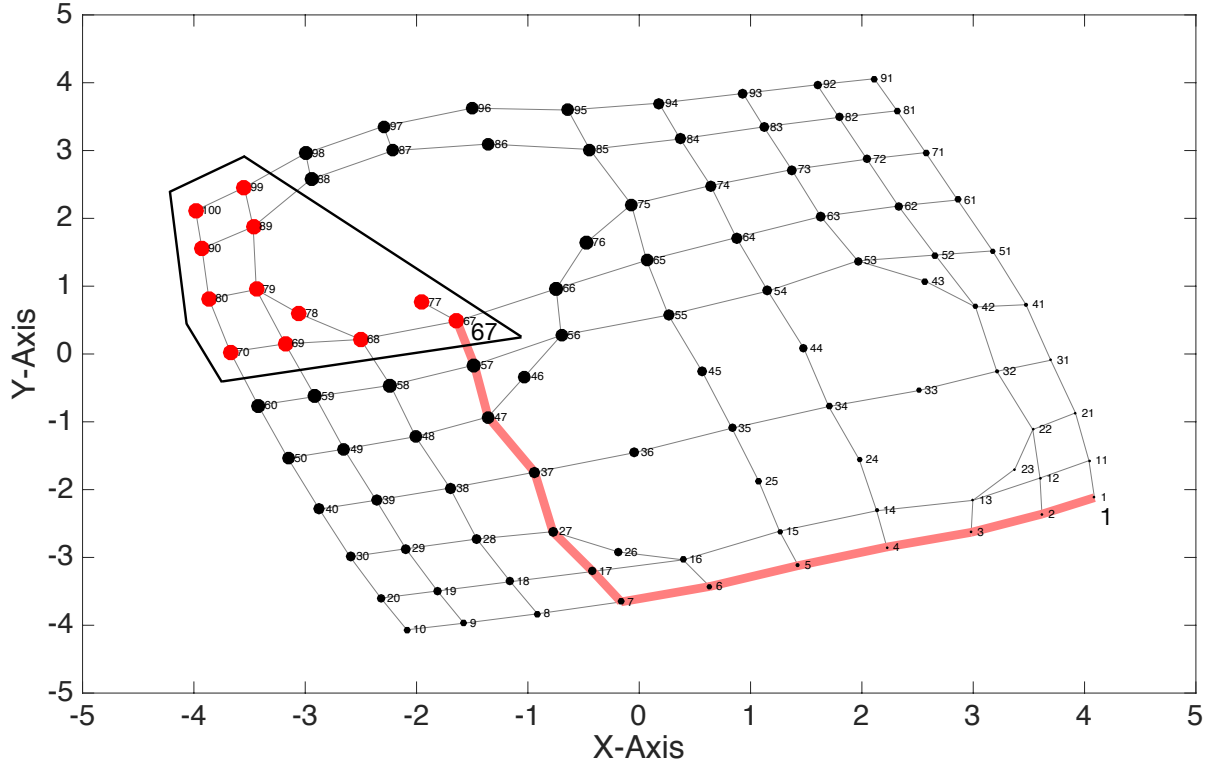


Figure 4.4: Flight path of the aerial vehicle in Figures 4.2 and 4.3 at $k = 12$. As the prior path is increasing in size, authentication of future waypoints narrows to less waypoints, indicating the accuracy of the authentication process.

4.6 Chapter Conclusion and Future Works

In this chapter the author has introduced a novel learning algorithm for onboard authentication of autonomous aerial vehicles, that is independent from the features and characteristics of transmitted signals. This method is expectedly more applicable in network controlled applications where there is no peer-to-peer communication between the GCC and the UAV, such as in UAM where transmitted signals are relayed multiple times from the sender to the receiver. The proposed methodology models a probabilistic function that gauges the consistency of received waypoint commands with respect to the prior flight path in order to verify that a coherent optimal path could be constructed from the origin to the new waypoint. If there is no coherent path that corroborates prior waypoints to the new commands, the authentication function returns the likelihood of a static cyberattack. In a similar manner, commands that could not corroborate an acceptable energy conservation practice in their motion toward future waypoints would be detectable by the authentication function through a response value that indicates the likelihood of a dynamic cyberattack. Moreover, commands that violate geo-fencing rules or traffic control commands could be verified and omitted, ensuring only secure commands to be obliged and passed to the autopilot.

The present results of this chapter do not reflect the right of a change-in-destination that a legitimate Ground Control Station may have during the mission of its slave UAV. This sudden change-in-destination is currently perceived by the authentication process (onboard the UAV) as an act of intrusion, although this might not be the case. It is recommendable for the present work to be extended in the future so that the controller onboard the UAV may also differentiate between a “true” change-in-destination, versus a “false” change-in-destination that is an act of an adversarial attacker.

Chapter 5

Conclusion of the Thesis and Future Works

5.1 Cooperative Filters

The majority of the present thesis involves application of “cooperative filters” in CPS security issues, and particularly for resiliency against time-delay and spoofing cyberattacks. Cooperative filters are identical Linear and Time-Invariant (LTI) filters formulated for CPS tele-communication systems, and designed to be installed immediately after the transceivers of the constituting subsystems in a CPS, in a Multi-Agent System (MAS) framework. The inputs and outputs of the cooperative filters are scalar CPS states that are transported from one subsystem (referred to as the source) to one or multiple other subsystems (referred to as destinations) through tele-communication links, where the objective is to protect the source states against Man-in-the-Middle adversarial intrusions on the tele-communication links. Corresponding to each and every scalar state a separate filter has to be employed, implying that protecting a vector of states requires a multi-channel filter for each subsystem. The filters are interconnected in a MAS to exchange state information between neighbouring agents in a way that the output of each filter is the input of an adjacent filter, so that the entire network can form a connected bi-directional graph where nodes indicate filters and the edges indicate the tele-communication links between the agents (i.e., the filters), hence “cooperative filters”.

Cooperative filters are designed in such a fashion to achieve output consensus, despite of intruding cyberattacks. In other words, after lapse of a negligible and controllable transient time, the outputs of all the filters in the entire CPS settle down at a consensus value. The transient time of the filters can be arbitrarily adjusted through variation of the filter gains, which implies that the settling time of the filters can be arbitrarily controlled

to support the operational speed of the applications. In particular, in high-speed applications (e.g., applications in which the frequency bandwidth of the CPS states are relatively high) a higher filter gain would be required, as opposed to low-speed applications where the filter gain could be reduced in order to economize the tele-communication bandwidths.

However, output consensus in cooperative filters imply that one could recovery of the source state information at the destination nodes, despite of disruptive cyberattacks on the interconnecting tele-communication links. This could be achieved by removing in-degree edges at the source node, and allowing other filters to follow the source as in a conventional leader-follower MAS framework. Chapters 2 and 3 of the present thesis discuss theoretical aspects of cooperative filters under certain cyberattack scenarios.

5.1.1 Future Works for Improving the Efficiency of Cooperative Filters

It follows that the performance of the cooperative filters in the recovery of the cyberthreats is directly related to the filter gains. The gain of the cooperative filters can also be shown to have proportional relationship with the bandwidth of the tele-communication channels as well as the topology of the graph. This further implies that cooperative filters require sufficient tele-communication bandwidths for stable operation. The study of the impact could be the basis of a future work, where the objective would be achieving efficient cooperative filters with most affordable communication bandwidths. Additionally, the cooperative filter scheme discussed in Chapters 2 and 3 can be shown to be ineffective where compound cyberattacks inflict the CPS. It is advisable to study the effect of such compound cyberattacks and try to administer resilient policies under these circumstances through a separate research work.

5.2 Authentication of Ground Control Station Commands

Authentication of Ground Control Station Commands in Urban Air Mobility has been the subject of Chapter 4 of the thesis. In this chapter the author has introduced a novel learning algorithm for onboard authentication of autonomous aerial vehicles, that is independent from the features and characteristics of transmitted signals. This method is expectedly more applicable in network controlled applications where there is no peer-to-peer communication between the GCC and the UAV, such as in UAM where transmitted

signals are relayed multiple times from the sender to the receiver. The proposed methodology models a probabilistic function that gauges the consistency of received waypoint commands with respect to the prior flight path in order to verify that a coherent optimal path could be constructed from the origin to the new waypoint. If there is no coherent path that corroborates prior waypoints to the new commands, the authentication function returns the likelihood of a static cyberattack. In a similar manner, commands that could not corroborate an acceptable energy conservation practice in their motion toward future waypoints would be detectable by the authentication function through a response value that indicates the likelihood of a dynamic cyberattack. Moreover, commands that violate geo-fencing rules or traffic control commands could be verified and omitted, ensuring only secure commands to be obliged and passed to the autopilot.

5.2.1 Future Works in Authentication of Ground Control Station Commands

The results obtained in the chapter do not reflect the right of a change-in-destination that a legitimate Ground Control Station may have during the mission of its slave UAV. This sudden change-in-destination is currently perceived by the authentication process (onboard the UAV) as an act of intrusion, although this might not be the case. It is recommendable for the present work to be extended in the future so that the controller onboard the UAV may also differentiate between a “true” change-in-destination, versus a “false” change-in-destination that is an act of an adversarial attacker.

Appendix A

List of Publications

1. A Resilient Control Against Time-Delay Switch and Denial of Service Cyber Attacks on Load Frequency Control of Distributed Power Systems, 4th IEEE Conference on Control Technology and Applications (CCTA 2020), Montréal, Canada, August 24-26, 2020.
2. A Multidimensional Bayesian Methodology for Diagnosis, Prognosis, and Health Monitoring of Electro-Hydraulic Servo Valves, in IEEE Transactions on Control Systems Technology, vol. 30, no. 3, pp. 931-943, doi: 10.1109/TCST.2021.3079198, May 2022.
3. Optimization of Localization Error in Multi-Agent Systems through Cooperative Positioning: Autonomous Navigation in Partially Denied GNSS, The 10th IEEE International Symposium on Inertial Sensors and Systems, Kaua'i, Hawaii, USA, March 27 to 31, 2023.
4. Cooperative Localization of Multi-Agent Autonomous Aerial Vehicle (AAV) Networks in Intelligent Transportation Systems, in IEEE Journal of Intelligent Transportation Systems, vol. 6, pp. 49-66, doi: 10.1109/OJITS.2025.3531363, 2025.
5. Anti-Spoofing Aided Solutions for Urban Air Mobility: Ground Command Authentication, 64th IEEE Conference on Decision and Control (CDC), Dec. 9 to Dec. 12, 2025.
6. Time-Delay Resilient Cooperative Filters for Cyber-Physical Systems, MDPI Journal of Electronics, Accepted with comments in July 2025.

Bibliography

- [1] M. S. Mahmoud, M. M. Hamdan, U. A. Baroudi, Modelling and Control of Cyber-Physical Systems Subject to Cyberattacks: A Survey of Recent Advances and Challenges, *Neurocomputing* 338, Pages 101-115, 2019.
- [2] Y. Liu, Y. Peng, B. Wang, S. Yao, Z. Liu, Review on Cyber-Physical Systems, *IEEE/CAA Journal of Automatica Sinica*, Vol. 4, No. 1, January 2017.
- [3] A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge, Cyberattack Vulnerabilities Analysis for Unmanned Aerial Vehicles, *Infotech at Aerospace 2012, AIAA*, Pages 1-30, 2012.
- [4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, *IEEE Internet Things J.* 4 (5) 1125-1142, 2017.
- [5] Y. Ashibani, Q. H. Mahmoud, Cyber-Physical Systems Security: Analysis, Challenges and Solutions, *Computer Security* 68, 81-97, 2017.
- [6] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, K. P. Chow, Security Issues and Challenges for Cyber-Physical System, *Proc. IEEE/ACM International Conference Green Computer Communication, Cyber-Physical Society Computer*, Pages 733-738, 2010.
- [7] Q. Jing, A. V. Vasilakos, J. Wan, Security of the Internet of Things: Perspectives and Challenges, *Wireless Networks* 20 (8): 2481-501, 2014.
- [8] J. A. Stankovic, Research Directions for the Internet of Things, *IEEE Internet of Things Journal* No. C, 3-9, 2014.
- [9] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, F. Xie, Cyber-Physical System Risk Assessment, *9th International Conference on Intelligent Information, Signal Processing*, Pages 442-447, 2013.

- [10] Q. Gou, L. Yan, Y. Liu, Y. Li, Construction and Strategies in IoT Security System, Proceedings IEEE Int. Conf. Green Comput. Commun. IEEE Internet of Things, IEEE Cyber-Physical Society Computer Green Com-iThings-CPS Com. Pages 1129-1132, 2013.
- [11] K. Zhao, L. Ge, A Survey on the Internet of Things Security, 9th Int. Conference on Computer Intelligent Security, Pages 663-667, 2013.
- [12] S. Ali, R. W. Anwar, O. K. Hussain, Cyber Security for Cyber-Physical Systems: A Trust Based Approach, Journal of Theory Applications Information Technology 71 (2) : Pages 144-152, 2015.
- [13] R. Mahmoud, T. Yousuf, F. Aloul, I. Zuolkernan, Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures, 10th International Conference on Internet Technology Security Trans. IEEE, Pages 336-341, 2015.
- [14] Q. Shafi, Cyber-Physical Systems Security: A Brief Survey, Computer Science and Its Applications (ICCSA), 12th International Conference, IEEE, Pages 146-150, 2012.
- [15] J. Kao, R. Marculescu, Eavesdropping Minimization via Transmission Power Control in Ad-hoc Wireless Networks, Sensor Ad-Hoc Communication Networks 2 : Pages 707-714, 2006.
- [16] A. Rawnsley, Iran's Alleged Drone Hack: Tough, but Possible, <http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/>, Dec. 2011.
- [17] V. Hassani, N. Crasta, A.M. Pascoal, Cyber Security Issues in Navigation Systems of Marine Vessels from a Control Perspective, Proceedings of the ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering OMAE2017, June 25-30, 2017.
- [18] D. Ding, Q. L. Han, Y. Xiang, X. Ge, X. M. Zhang, A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems, Neurocomputing, 275 1674-1683, 2018.
- [19] E. J. Byres, J. Lowe, The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems, Proceedings of the VDE Kongress, Vol. 116, Pages 1-6, 2004.
- [20] A. A. Cardenas, S. Amin, S. S. Sastry, Research Challenges for the Security of Control Systems, <https://www.usenix.org/legacy/event/hotsec08/tech/fullpapers/cardenas/cardenas.html/>, Mar. 2008.

- [21] A. A. Cardenas, S. Amin, S. S. Sastry, Secure Control: Towards Survivable Cyber-Physical Systems, Proc. 28th ICDCS, Pages 495-500, 2008.
- [22] H. Sandberg, A. Teixeira, and K. H. Johansson, On Security Indices for State Estimators in Power Networks, Proceedings of the 1st Workshop on Secure Control Systems (CPSWEEK 2010), 2010.
- [23] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, Quantifying Cyber-Security for Networked Control Systems, Control of Cyber-Physical Systems, Ser. Lecture Notes in Control and Information Sciences, D. C. Tarraf, Ed. Springer International Publishing, Vol. 449, Pages 123-142, 2013.
- [24] I. Shames, F. Farokhi, T.H. Summers, Security Analysis of Cyber-Physical Systems Using H2 Norm, IET Control Theory Applications 11 (11), Pages 1749-1755, 2017.
- [25] D. Ding, Z. Wang, G. Wei, F.E. Alsaadi, Event-Based Security Control for Discrete-Time Stochastic Systems, IET Control Theory Applications, 10 (15), Pages 1808-1815, 2016.
- [26] V.S. Dolk, P. Tesi, C.D. Persis, W.P.M.H. Heemels, Event-Triggered Control Systems Under Denial-of-Service Attacks, IEEE Transactions on Control Network Systems, 4 (1), Pages 93-105, 2017.
- [27] C. De Persis and P. Tesi, On Resilient Control of Nonlinear Systems under Denial-of-Service, Proc. of the IEEE Conference on Decision and Control, Los Angeles, CA, USA, 2014.
- [28] S. Feng, P. Tesi, C.D. Persis, Towards Stabilization of Distributed Systems under Denial of Service, Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), IEEE, Pages 5360-5365, 2017.
- [29] G. C. Walsh, H. Ye, L. G. Bushnell, Stability Analysis of Networked Control Systems, IEEE Transactions on Control Systems Technology, Vol. 10, No. 3, MAY 2002.
- [30] G. C. Walsh, O. Beldiman, L. G. Bushnell, Asymptotic Behaviour of Nonlinear Networked Control Systems, IEEE Transactions on Automatic Control, Vol. 46, No. 7, JULY 2001.
- [31] M. Semerci, A.T. Cemgil, B. Sankur, An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks, Computer Networks 136, Pages 137-154, 2018.

- [32] Y. Ali, Y. Xia, L. Ma, A. Hammad, Secure Design for Cloud Control System Against Distributed Denial of Service Attack, *Control Theory Technology* 16 (1), Pages 14-24, 2018.
- [33] J. Hao, R.J. Piechocki, D. Kaleshi, W.H. Chin, Z. Fan, Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids, *IEEE Transactions on Industrial Informatics*, Vol. 11, No. 5, Pages 1-12, 2015.
- [34] J. Wang, Y. Song, S. Liu, S. Zhang, Security in H2 Sense for Polytopic Uncertain Systems with Attacks Based on Model Predictive Control, *J. Franklin Institute* 353 (15) Pages 3769-3785, 2016.
- [35] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, S. S. Sastry, Kalman Filtering with Intermittent Observations, *IEEE Transactions on Automatic Control*, Vol. 49, No. 9, Pages 1453-1464, Sep. 2004.
- [36] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, S. S. Sastry, Foundations of Control and Estimation Over Lossy networks, *Proceedings IEEE*, Vol. 95, No. 1, Pages 163-187, Jan. 2007.
- [37] G. Hug, J.A. Giampapa, Vulnerability Assessment of AC State Estimation with Respect to False Data Injection cyber-attacks, *IEEE Transactions on Smart Grid* 3 (3), Pages 1362-1370, 2012.
- [38] C.H. Lo, N. Ansari, A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid, *IEEE Transactions on Emerging Topics in Computing*, 1 (1), Pages 33-44, 2013.
- [39] L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, Z. Han, Detecting False Data Injection Attacks on Power Grid by Sparse Optimization, *IEEE Transactions on Smart Grid* 5 (2), Pages 612-621, 2014.
- [40] Y. Huang, J. Tang, Y. Cheng, H. Li, K.A. Campbell, Z. Han, Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis, *IEEE Systems Journal*, 10 (2), Pages 532-543, 2016.
- [41] Y. Mo, R. Chabukswar, B. Sinopoli, Detecting Integrity Attacks on SCADA Systems, *IEEE Transactions on Control Systems Technology*, 22 (4), Pages 1396-1407, 2014.
- [42] D. Ding, Z. Wang, D.W. Ho, G. Wei, Observer Based Event Triggering Consensus Control for Multi-Agent Systems with Lossy Sensors and cyber-attacks, *IEEE Transactions on Cybernetics*, 47 (8) Pages 1936-1947, 2017.

- [43] J. Milosevic, T. Tanaka, H. Sandberg, K.H. Johansson, Analysis and Mitigation of Bias Injection Attacks Against a Kalman Filter, *IFAC-PapersOnLine* 50 (1), Pages 8393-8398, 2017.
- [44] H. Fang, R. A. De Callafon, J. Cortes, Simultaneous Input and State Estimation for Nonlinear Systems with Applications to Flow Field Estimation, *Automatica*, Vol. 49, No. 9, Pages 2805-2812, 2013.
- [45] S. Yong, M. Zhu, E. Frazzoli, A Unified Filter for Simultaneous Input and State Estimation of Linear Discrete-Time Stochastic Systems, *Automatica*, Vol. 63, No. 1, Pages 321-329, 2016.
- [46] N. Forti, G. Battistelli, L. Chisci, B. Sinopoli, A Bayesian Approach to Joint Attack Detection and Resilient State Estimation, in: *IEEE 55th Conference on Decision and Control (CDC)*, IEEE, Pages 1192-1198, 2016.
- [47] F. Guo, Q. Xu, C. Wen, L. Wang, P. Wang, Distributed Secondary Control for Power Allocation and Voltage Restoration in Islanded DC Micro-grids, *IEEE Trans. Sustain. Energy*, Vol. 9, No. 4, Pages 1857-1869, doi: 10.1109/TSTE.2018.2816944, Oct. 2018.
- [48] S. E. Tuna, LQR-Based Coupling Gain for Synchronization of Linear Systems [Online]. Available: <http://arxiv.org/abs/0801.3390>.
- [49] C. Ma, J. Zhang, Necessary and Sufficient Conditions for Consensusability of Linear Multi-Agent Systems, *IEEE Transactions on Automatic Control*, Vol. 55, No. 5, May 2010.
- [50] A. Abdessameud, A. Tayebi, Cooperative Output Regulation of Linear Multi-Agent Systems with Communication Constraints, *IEEE 55th Conference on Decision and Control (CDC)*, December 2016.
- [51] A.Y. Lu, G.H. Yang, Distributed Consensus Control for Multi-Agent Systems Under Denial-of-Service, *Information Science*, Vols. 439-440, Pages 95-107, May 2018.
- [52] R. P. S. Mahler, *Statistical Multi-Source Multi-Target Information Fusion*, Norwood, MA, USA: Artech House, Inc., 2007.
- [53] D. Carnevale, A. Teel, and D. Nesic, A Lyapunov Proof of an Improved Maximum Allowable Transfer Interval for Networked Control Systems, *IEEE Transactions on Automation and Control*, Vol. 52, No. 5, Pages 892-897, May 2007.

- [54] S. Dashkovskiy, H. Ito, and F. Wirth, On a Small Gain Theorem for ISS Networks in Dissipative Lyapunov Form, *European Journal of Control*, Vol. 17, No. 4, Pages 357-365, 2011.
- [55] K. Ding, Y. Li, D.E. Quevedo, S. Dey, L. Shi, A Multi-Channel Transmission Schedule for Remote State Estimation Under DoS Attacks, *Automatica* 78, Pages 194-201, 2017.
- [56] Y. Yuan, H. Yuan, L. Guo, H. Yang, S. Sun, Resilient Control of Networked Control System Under DoS Attacks: A Unified Game Approach, *IEEE Transactions Ind. Inf.* 12 (5) Pages 1786-1794, 2016.
- [57] S. Liu, P.X. Liu, A.E. Saddik, A Stochastic Game Approach to the Security Issue of Networked Control Systems Under Jamming Attacks, *J. Franklin Inst.* 351 (9), Pages 4570-4583, 2014.
- [58] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, Control of nonlinear heartbeat models under time-delay switched feedback using emotional learning control, *Int. J. Recent Trends Eng. Technol.*, Vol. 10, no. 2, pp. 85-91, 2014.
- [59] Y. Yuan, Z. Li, and K. Ren, Modelling load redistribution attacks in power systems, *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382-390, Jun. 2011.
- [60] H. Bevrani, *Robust Power System Frequency Control*, Power Electronics and Power Systems, New York, NY, USA: Springer, 2009.
- [61] Y. Wei Law, T. Alpcan, Security Games for Risk Minimization in Automatic Generation Control, *IEEE Transactions on Power Systems*, vol. 30, No. 1, Jan 2015.
- [62] P. Kundur, *Power System Stability and Control*, New York, NY, USA: McGraw-Hill Professional, 1994.
- [63] F. Wu, K. Moslehi, and A. Bose, Power System Control Centers: Past, Present, and Future, *Proc. IEEE*, vol. 93, no. 11, pp. 1890-1908, Nov. 2005.
- [64] S. Aunga, Z.M. Htikeb, Modelling and Simulation of Load Frequency Control for Three Area Power System Using Proportional Integral Derivative (PID) Controller, *American Scientific Research Journal for Engineering, Technology, and Sciences (AS-RJETS)*, ISSN 2313-4410, ISSN (Online) 2313-4402, 2016.
- [65] R. Dey, S. Ghosh, G. Ray, A. Rakshit, H_∞ Load Frequency Control of Interconnected Power Systems with Communication Delays, *Electrical Power and Energy Systems* 42 672-684 (2012).

- [66] A. Sargolzaei, Kang K. Yen, Mohamed N. Abdelghani, Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems, *IEEE Transactions on Smart Grid*, Vol. 7, No. 2, March 2016.
- [67] D. Dotta, A. S. E. Silva, and I. C. Decker, Wide-Area Measurement Based Two-Level Control Design Considering Signal Transmission Delay, *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 208-216, Feb. 2009.
- [68] Q. Yang, D. An, and W. Yu, On Time Desynchronization Attack Against IEEE 1588 Protocol in Power Grid Systems, in *Proc. IEEE Energytech*, Cleveland, OH, USA, pp. 1-5, May 2013.
- [69] A. Sargolzaei, K. Yen, and M. N. Abdelghani, Delayed Inputs Attack on Load Frequency Control in Smart Grid, in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, pp. 1-5, Feb. 2014.
- [70] A. Sargolzaei, K. Yen, and M. N. Abdelghani, Time-Delay Switch Attack on Load Frequency Control in Smart Grid, *J. Adv. Commun. Technol.*, Vol. 5, pp. 55-64, Nov. 2014.
- [71] S. Amin, A. A. Cardenas, and S. S. Sastry, Safe and Secure Networked Control Systems under Denial-of-Service Attacks, paper presented at the *Proc. 12th Int. Conf. Hybrid Syst. Comput. Control*, San Francisco, CA, USA, 2009.
- [72] Y. Sun, Y. Wang, Z. Wei, G. Sun, and X. Wu, Robust H_∞ Load Frequency Control of Multi-Area Power System with Time Delay: A Sliding Mode Control Approach, *IEEE/CAA Journal of Automatica Sinica*, Vol. 5, No. 2, March 2018.
- [73] X. Yu, K. Tomsovic, Application of Linear Matrix Inequalities for Load Frequency Control with Communication Delay, *IEEE Transactions on Power Systems*, Vol. 19, No. 3, August 2004.
- [74] T. Mori, Criteria for Asymptotic Stability of Linear Time-Delay Systems, *IEEE Trans. Automatic Control*, Vol. AC-30, Pages 158-160, 1985.
- [75] Y. Mi, Y. Fu, C. Wang, Decentralized Sliding Mode Load Frequency Control for Multi-Area Power Systems, *IEEE Transactions on Power Systems*, Vol. 28, No. 4, November 2013.
- [76] Y. Li, P. Zhang, L. Ma, Denial of Service Attack and Defence Method on Load Frequency Control System, *Journal of the Franklin Institute*, Volume 356, Issue 15, Pages 8625-8645, October 2019.

- [77] A. Almulhem, Threat Modelling of a Multi-UAV System, *Transportation Research Part A* 142, Pages 290-295, 2020.
- [78] M. Yeasir Arafat, S. Moh, Routing Protocols for Unmanned Aerial Vehicle Networks: A Survey, doi: 10.1109/ACCESS.2019.2930813, 2019.
- [79] O. K. Sahingoz, Mobile Networking with UAVs: Opportunities and Challenges, in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Pages 933-941, doi: 10.1109/icuas.2013.6564779, May 2013.
- [80] K. Zhang, W. Zhang, J.-Z. Zeng, Preliminary Study of Routing and Data Integrity in Mobile adhoc UAV Network, in *Proc. Int. Conf. Apperceiving Comput. Intell. Anal.*, Pages 347-350, doi: 10.1109/icacia.2008.4770039, Dec. 2008.
- [81] D. Jung, P. Tsiotras, Inertial Attitude and Position Reference System Development for a Small UAV, in *Proc. AIAA Infotech@Aerosp. Conf. Exhibit*, Pages 1-15. doi: 10.2514/6.2007-2763, 2007.
- [82] G. Mao, S. Drake, B. D. O. Anderson, Design of an Extended Kalman Filter for UAV Localization, in *Proc. Inf., Decis. Control*, Pages 224-229. doi: 10.1109/idc.2007.374554, 2007.
- [83] H.S. Ahn, C.H. Won, DGPS/IMU Integration-Based Geolocation System: Airborne Experimental Test Results, *Aerospace Science and Technology*, Vol. 13, No. 6, Pages 316-324, doi: 10.1016/j.ast.2009.06.003, 2009.
- [84] A. K.S. Wong, T.K. Woo, A.T.L. Lee, X. Xiao, V.W.H. Luk, K.W. Cheng, An AGPS-Based Elderly Tracking System, in *Proc. 1st International Conference on Ubiquitous Future Network*, pp. 100-105. doi: 10.1109/icufn. 2009.5174293, 2009.
- [85] Bora Ly, Romny Ly, Cybersecurity in Unmanned Aerial Vehicles (UAVs), *Journal of Cyber Security Technology*, DOI: 10.1080/23742917.2020.1846307, Nov. 2020.
- [86] R. Filjar, S. Kos, David Brcic, Jamming-Spoofing-Meaconing-Resilient GNSS Performance at the Open Sea, <https://www.researchgate.net/publication/333802169>, May 2014.
- [87] SASC Wants Alternative GPS by 2023, Available online: <https://breakingdefense.com/2020/06/sasc-wants-alternative-gps-by-2023>.
- [88] Strategy for the Department of Defence, Positioning, Navigation, and Timing (PNT) Enterprise, Department of Defence, Office of Prepublication and Security Review, August 2019.

- [89] The War Zone (Journal), June 29, 2021.
- [90] O. Walker, F. Vanegas, F. Gonzalez, A Framework for Multi-Agent UAV Exploration and Target-Finding in GPS-Denied and Partially Observable Environments, *Sensors*, 20, 4739; doi:10.3390/s20174739, 2020.
- [91] Y. Zhang, A Fusion Methodology to Bridge GPS Outages for INS/GPS Integrated Navigation System, *IEEE Access*, doi: 10.1109/ACCESS.2019.2911025, 2019.
- [92] F. Vanegas, J. Roberts, K. J. Gaston, F. Gonzalez, A Framework for UAV Navigation and Exploration in GPS-denied Environments, *IEEE Aerospace Conference*, DOI: 10.1109/AERO.2019.8741612, June 2019.
- [93] F. J. Perez-Grau, R. Ragel, F. Caballero, A. Viguria, A. Ollero, An Architecture for Robust UAV Navigation in GPS-Denied Areas, *J Field Robotics*, 35:121-145, DOI: 10.1002/rob.21757, 2018.
- [94] H. Qin, Z. Meng, W. Meng, X. Chen, H. Sun, F. Lin, M. H. Ang Jr, Autonomous Exploration and Mapping System Using Heterogeneous UAVs and UGVs in GPS-Denied Environments, *IEEE Transactions on Vehicular Technology*, DOI: 10.1109/TVT.2018.2890416, January 2018.
- [95] H. A. Hashim, GPS-Denied Navigation: Attitude, Position, Linear Velocity, and Gravity Estimation with Nonlinear Stochastic Observer, in *Proceedings of the 2021 American Control Conference (ACC)*, New Orleans, LA, USA, 2021, Pages 1146-1151, doi: 10.23919/ACC50511.2021.9482995, 2021.
- [96] W. Youn, H. Ko, H. Choi, I. Choi, J. Baek, H. Myung, Collision-Free Autonomous Navigation of A Small UAV Using Low-Cost Sensors in GPS-Denied Environments, *International Journal of Control, Automation and Systems* 19(2) 953-968, <http://dx.doi.org/10.1007/s12555-019-0797-7>, 2021.
- [97] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Lagkas, I. Moscholios, A Compilation of UAV Applications for Precision Agriculture, *Computer Networks*, 172 107148, 2020.
- [98] H. Shakhathreh, A.H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N.S. Othman, A. Khreishah, M. Guizani, Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges, *IEEE Access* 7 48572-48634, 2019.

- [99] A. Androjna, T. Brcko, I. Pavic, H. Greidanus, Assessing Cyber Challenges of Maritime Navigation, *Journal of Marine Science and Engineering*, doi:10.3390/jmse8100776, March 2020.
- [100] Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, Aaron A. Fansler, Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks, *Ion GNSS Conference* Nashville, TN, September, 2012.
- [101] A. Rawnsley, Iran's Alleged Drone Hack: Tough, but Possible, <http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/>, Dec. 2011.
- [102] N. Gyagenda, J. V. Hatilima, H. Roth, V. Zhmud, A Review of GNSS-Independent UAV Navigation Techniques, *Robotics and Autonomous Systems* 152 104069, 2022.
- [103] G. Schmidt, GPS Based Navigation Systems in Difficult Environments, *Gyroscopy Navigation* 10 (2) 41-53, 2019.
- [104] R. Opromolla, G. Fasano, G. Rufino, M. Grassi, A. Savvaris, LiDAR-Inertial Integration for UAV Localization and Mapping in Complex Environments, *International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, pp. 649-656, 2016.
- [105] Y. Lin, F. Gao, T. Qin, W. Gao, T. Liu, W. Wu, Z. Yang, S. Shen, Autonomous Aerial Navigation Using Monocular Visual-Inertial Fusion, *J. Field Robotics* 35 (1) 23-51, 2018.
- [106] H. Qin, Y. Bi, K.Z. Ang, K. Wang, J. Li, M. Lan, M. Shan, F. Lin, A Stereo and Rotating Laser Framework for UAV Navigation in GPS-Denied Environment, *IECON 42nd Annual Conference of the IEEE Industrial Electronics Society*, IEEE, pp. 6061-6066, 2016.
- [107] E. Lopez, R. Barea, A. Gomez, A. Saltos, L.M. Bergasa, E.J. Molinos, A. Nemra, Indoor SLAM for Micro-Aerial Vehicles Using Visual and Laser sensor fusion, *Robot 2015: Second Iberian Robotics Conference*, Springer, pp. 531-542, 2016.
- [108] C. Sampedro, A. Rodriguez-Ramos, H. Bavle, A. Carrio, P. de la Puente, P. Campoy, A Fully-Autonomous Aerial Robot for Search and Rescue Applications in Indoor Environments using Learning-Based Techniques, *Journal of Intelligent Robot. Systems* 95 (2) 601-627, 2019.
- [109] Y. Bi, M. Lan, J. Li, K. Zhang, H. Qin, S. Lai, B.M. Chen, Robust Autonomous Flight and Mission Management for Mavs in GPS-Denied Environments, *11th Asian Control Conference (ASCC)*, IEEE pp. 67-72, 2017.

- [110] D. Hahnel, R. Triebel, W. Burgard and S. Thrun, Map Building with Mobile Robots in Dynamic Environments, IEEE International Conference on Robotics and Automation (Cat. No.03CH37422), Taipei, Taiwan, 2003, Pages 1557-1563 Vol.2, doi: 10.1109/ROBOT.2003.1241816, 2003.
- [111] A.R. Kuroswiski, N.M.F. de Oliveira, E.H. Shiguemori, Autonomous Long-Range Navigation in GNSS-Denied Environment with Low-Cost UAV Platform, 2018 Annual IEEE International Systems Conference (SysCon), IEEE, pp. 1-6, 2018.
- [112] Y. Tang, Y. Hu, J. Cui, F. Liao, M. Lao, F. Lin, R.S. Teo, Vision-Aided Multi-UAV Autonomous Flocking in GPS-Denied Environment, IEEE Transactions on Industrial Electronics 66 (1), 616-626, 2018.
- [113] F. Valenti, D. Giaquinto, L. Musto, A. Zinelli, M. Bertozzi, A. Broggi, Enabling Computer Vision-Based Autonomous Navigation for Unmanned Aerial Vehicles in Cluttered GPS-Denied Environments, 21st International Conference on Intelligent Transportation Systems (ITSC), IEEE, pp. 3886-3891, 2018.
- [114] R.C. Leishman, T.W. McLain, R.W. Beard, Relative Navigation Approach for Vision-Based Aerial GPS-Denied Navigation, Journal of Intelligent Robotic Systems, 74 (1-2) 97-111, 2014.
- [115] M. Nieuwenhuisen, D. Droschel, M. Beul, S. Behnke, Autonomous Navigation for Micro Aerial Vehicles in Complex GNSS-Denied Environments, Journal of Intelligent Robotic Systems 84 (1-4), 199-216, 2016.
- [116] Q. Li, D.C. Li, Q.F. Wu, L.W. Tang, Y. Huo, Y.X. Zhang, N. Cheng, Autonomous Navigation and Environment Modelling for MAVs in 3-D Enclosed Industrial Environments, Compututer Ind. 64 (9), 1161-1177, 2013.
- [117] A. Bachrach, S. Prentice, R. He, N. Roy, Range-Robust Autonomous Navigation in GPS-denied Environments, J. Field Robotics 28 (5), 644-666, 2011.
- [118] K. Schmid, P. Lutz, T. Tomic, E. Mair, H. Hirschmuller, Autonomous Vision-Based Micro Air Vehicle for Indoor and Outdoor Navigation, J. Field Robotics 31 (4), 537-570, 2014.
- [119] H. Oleynikova, C. Lanegger, Z. Taylor, M. Pantic, A. Millane, R. Siegwart, J. Nieto, An Open-Source System for Vision-Based Micro-Aerial Vehicle Mapping, Planning, and Flight in Cluttered Environments, J. Field Robotics 37 (4), 642-666, 2020.

- [120] K. Mohta, M. Watterson, Y. Mulgaonkar, S. Liu, C. Qu, A. Makineni, K. Saulnier, K. Sun, A. Zhu, J. Delmerico, et al., Fast Autonomous Flight in GPS-Denied and Cluttered Environments, *J. Field Robotics* 35 (1), 101-120, 2018.
- [121] P. Lutz, M.G. Muller, M. Maier, S. Stoneman, T. Tomic, I. Von Bargen, M.J. Schuster, F. Steidle, A. Wedler, W. Sturzl, et al., ARDEA-An MAV with Skills for Future Planetary Missions, *J. Field Robotics* 37 (4), 515-551, 2020.
- [122] Y. Gu, X. Yu, K. Guo, J. Qiao, L. Guo, Detection, Estimation, and Compensation of False Data Injection Attack for UAVs, *Information Sciences* 546, Pages 723-741, 2021.
- [123] Y. Gu, K. Guo, L. Guo, J. Qiao, J. Jia, X. Yu, L. Xie, An Enhanced UAV Safety Control Scheme Against Attacks on Desired Trajectory, *Aerospace Science and Technology*, Vol. 119, 107212, December 2021.
- [124] D. Muniraj, M. Farhood, Detection and Mitigation of Actuator Attacks on Small Unmanned Aircraft Systems, *Control Eng. Pract.* 83, Pages 188-202, 2019.
- [125] A. Sargolzaei, K. Yazdani, A.R. Abbaspour, C.D. Crane, W.E. Dixon, Detection and Mitigation of False Data Injection Attacks in Networked Control Systems, *IEEE Trans. Ind. Inform.* 16 (6), Pages 4281-4292, 2020.
- [126] H. Sedjelmaci, S.M. Senouci, N. Ansari, A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyberattacks in UAV Networks, *IEEE Trans. Syst. Man Cybern. Syst.* 48 (9), Pages 1594-1606, 2018.
- [127] H.Z. Wang, J.Q. Ruan, B. Zhou, C.B. Li, Q.W. Wu, M.Q. Raza, G.Z. Cao, Dynamic Data Injection Attack Detection of Cyberphysical Power Systems with Uncertainties, *IEEE Trans. Ind. Inform.* 15 (10), Pages 5505-5518, 2019.
- [128] J.J.Q. Yu, Y.H. Hou, V.O.K. Li, Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks, *IEEE Trans. Ind. Inform.* 14 (47), Pages 3271-3280, 2018.
- [129] M.L. Corradini, A. Cristofaro, Robust Detection and Reconstruction of State and Sensor Attacks for Cyberphysical Systems Using Sliding Modes, *IET Control Theory Appl.* 11 (11), Pages 1756-1766, 2017.
- [130] Y.D. Song, W. Ao, C.Y. Wen, Adaptive Cyberphysical System Attack Detection and Reconstruction with Application to Power Systems, *IET Control Theory Appl.* 10 (12), Pages 1458-1468, 2016.

- [131] A. Ameli, A. Hooshyar, E.F. El-Saadany, A.M. Youssef, An Intrusion Detection Method for Line Current Differential Relays, *IEEE Trans. Inf. Forensics Security*, 15, Pages 329-344, 2020.
- [132] Thrun, Burgard, Fox, *Probabilistic Robotics*, MIT Press, 2005.
- [133] Sun, Yan, Li, Faxu., Algebraic Connectivity and Disjoint Vertex Subsets of Graphs. *Mathematical Problems in Engineering*, 1-6, 10.1155/2020/5763218, 2020.
- [134] D. Ding, Z. Wang, Q.L. Han, G. Wei, Security Control for Discrete Time Stochastic Nonlinear Systems Subject to Deception Attacks, *IEEE Transactions on System Man and Cybernetics Systems* 48 (5), Pages 779-789, 2018.
- [135] C. Deng, C. Wen, MAS-Based Distributed Resilient Control for a Class of Cyber-Physical Systems with Communication Delays Under DoS Attacks, *IEEE Transactions on Cybernetics*, doi: 10.1109/TCYB.2020.2972686, March 2020.
- [136] M. Meng, L. Liu, G. Feng, Output Consensus for Heterogeneous Multiagent Systems with Markovian Switching Network Topologies, *International Journal of Robust and Nonlinear Control*, DOI: 10.1002/rnc.3918, Feb. 2018.
- [137] M. Meng, G. Xiao, C. Zhai, G. Li, Z. Wang, Distributed Consensus of Heterogeneous Multi-Agent Systems Subject to Switching Topologies and Delays, *Journal of the Franklin Institute* 357, 6899-6917, 2020.
- [138] A.H. Tahoun, M. Arafa, Cooperative Control for Cyber-Physical Multi-Agent Networked Control Systems with Unknown False Data Injection and Replay Cyber-Attacks, *ISA Transactions* 110, Page 1-14, 2021.
- [139] Z. Feng, G. Wen, and G. Hu, Distributed Secure Coordinated Control for Multiagent Systems under Strategic Attacks, *IEEE Trans. Cybern.*, Vol. 47, No. 5, Pages 1273-1284, May 2017.
- [140] C. Deng, C. Wen, MAS Based Distributed Resilient Control for a Class of Cyber-Physical Systems With Communication Delays Under DoS Attacks, *IEEE Transactions on Cybernetics*, Early Access DOI: 10.1109-TCYB.2020.2972686, March 2020.
- [141] D. Zhang, G. Feng, A New Switched System Approach to Leader-Follower Consensus of Heterogeneous Linear Multiagent Systems With DoS Attack, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, DOI:10.1109/TSMC.2019.2895097, February 2019.

- [142] Z. Ahmed, M.M. Khan, M.A. Saeed, W. Zhang, Consensus Control of Multi-Agent Systems with Input and Communication Delay: A Frequency Domain Perspective, *ISA Transactions* 101, Pages 69-77, 2020.
- [143] T. Qi, L. Qiu, J. Chen, Fellow, MAS Consensus and Delay Limits Under Delayed Output Feedback, *IEEE Transactions on Automatic Control*, Vol. 62, No. 9, Sep. 2017.
- [144] M. Zhanga, A. Saberla, A. A. Stoorvogel, Synchronization in the Presence of Unknown, Nonuniform and Arbitrarily Large Communication Delay, *European Journal of Control* 38, Pages 63-72, 2017.
- [145] Z. Liu, D. Nojavanzadeh, A. Saberi, A. A. Stoorvogel, Scale-Free Collaborative Protocol Design for Output Synchronization of Heterogeneous Multi-Agent Systems With Nonuniform Communication Delays, *IEEE Transactions on Network Science and Engineering*, Vol. 9, No. 4, August 2022.
- [146] C. Wang, C. Wen, L. Guo, Adaptive Consensus Control for Nonlinear Multiagent Systems With Unknown Control Directions and Time-Varying Actuator Faults, *IEEE Transactions on Automatic Control*, Vol. 66, No. 9, September 2021.
- [147] S. Xiong, Z. Hou, L. Fan, Consensus Control of Unknown Nonlinear Discrete-Time Multi-Agent Systems with Nonuniform Time-Delays, *IEEE 12th Data Driven Control and Learning Systems Conference*, Xiangtan, China, May 12-14, 2023.
- [148] L. Yuan, J. Li, Consensus of Discrete-Time Nonlinear Multiagent Systems Using Sliding Mode Control Based on Optimal Control, *IEEE Access*, Vol.10, 2022.
- [149] X. J. Peng, Y. He, Consensus of Multi-Agent Systems With Time-Varying Delays and Switching Topologies Based on Delay-Product-Type Functionals, *IEEE Transactions on Cybernetics*, Digital Object Identifier 10.1109/TCYB.2022.3200686, 2022.
- [150] F. Sun, X. Wu, J. Kurths, W. Zhu, Group Consensus for Heterogeneous Multi-Agent Systems With Time Delays Based on Frequency Domain Approach, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 53, No. 5, May 2023.
- [151] L. Solyman, A. Elbadawy, A. Meroth, Single Model Scheme Based Smith Predictor for the Mitigation of the Effects of Network Imperfections in Consensus Control of Multi Agent Systems, *10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2024.

- [152] J. C. Geromel, P. Colaneri, Stability and Stabilization of Continuous-Time Switched Linear Systems, SIAM J. Control Optimization, Vol. 45, No. 5, Pages 1915-1930, 2006.
- [153] Z. M. Kassas, J. Khalife, A. A. Abdallah and C. Lee, I Am Not Afraid of the GPS Jammer: Resilient Navigation Via Signals of Opportunity in GPS-Denied Environments, in IEEE Aerospace and Electronic Systems Magazine, vol. 37, no. 7, pp. 4-19, 1 July 2022, doi: 10.1109/MAES.2022.3154110.
- [154] W. Liu, Z. Li, S. Sun, R. Malekian, Z. Ma and W. Li, Improving Positioning Accuracy of the Mobile Laser Scanning in GPS-Denied Environments: An Experimental Case Study, in IEEE Sensors Journal, vol. 19, no. 22, pp. 10753-10763, 15 November, 2019, doi: 10.1109/JSEN.2019.2929142.
- [155] R. Aparna, H. T. Sai Ruchitha, N. Pranavi, A. G. keskar, IMU based Tracking of a Person using Nonlinear Autoregressive Exogenous (NARX) Algorithm in GPS-denied Areas, 2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA), 2020, pp. 1-4, doi: 10.1109/ICMICA48462.2020.9242732.
- [156] H. Lezki and I.S. Yetik, Localization Using Single Camera and LiDAR in GPS-Denied Environments, 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302512.
- [157] F. Ahmed, J.C. Mohanta, A. Keshari, P.S. Yadav, Recent Advances in Unmanned Aerial Vehicles: A Review, Arabian Journal for Science and Engineering 47, 7963-7984, 2022.
- [158] T. T. Mac, C. Copot, D. T. Tran, R. De Keyser, Heuristic Approaches in Robot Path Planning: A survey, Robot. Auto. Syst., Vol. 86, Pages 13-28, Dec. 2016.
- [159] A.G. Pires, P.A.F. Rezeck, R.A. Chaves, et al., Cooperative Localization and Mapping with Robotic Swarms, Journal of Intelligent Robot Systems 102, 47, <https://doi.org/10.1007/s10846-021-01397-z>, 2021.
- [160] M. Basso, D. Stocchero, P. Schnarndorf, E. Pignaton de Freitas, Merging Three-Dimensional Occupancy Grid Maps to Support Multi-UAVs Cooperative Navigation Systems. Journal of Field Robotics. 40. 10.1002/rob.22143, 2022.
- [161] F. Bouali et al., 5G for Vehicular Use Cases: Analysis of Technical Requirements, Value Propositions and Outlook, IEEE Open Journal of Intelligent Transportation Systems, Vol. 2, pp. 73-96, doi: 10.1109/OJITS.2021.3072220, 2021.

- [162] T. Bouzid, N. Chaib, M. Bensaad, O. Oubbati, 5G Network Slicing with Unmanned Aerial Vehicles: Taxonomy, Survey, and Future Directions, *Transactions on Emerging Telecommunications Technologies*. 34. 10.1002/ett.4721, 2022.
- [163] M. Kiraz, F. Sivrikaya, S. Albayrak, A Survey on Sensor Selection and Placement for Connected and Automated Mobility, *IEEE Open Journal of Intelligent Transportation Systems*, Vol. 5, pp. 692-710, doi: 10.1109/OJITS.2024.3481328, 2024.
- [164] L. Gao et al., Cooperative Localization in Transportation 5.0, *IEEE Transactions on Intelligent Vehicles*, Vol. 9, No. 3, pp. 4259-4264, doi: 10.1109/TIV.2024.3377163, March 2024.
- [165] Z. M. Kassas et al., Aircraft Navigation in GNSS-Denied Environments via Radio SLAM With Terrestrial Signals of Opportunity, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 10, pp. 14164-14182, Oct. 2024.
- [166] Q. Zhang, Y. Dai, T. Zhang, C. Guo and X. Niu, Road Semantic Enhanced Land Vehicle Integrated Navigation in GNSS Denied Environments, *IEEE Transactions on Intelligent Transportation Systems*, Sep. 2024.
- [167] A. I. Ameer, O. S. Oubbati, A. Lakas, A. Rachedi, M. B. Yagoubi, Efficient Vehicular Data Sharing using Aerial P2P Backbone, *IEEE Transactions on Intelligent Vehicles*, doi: 10.1109/TIV.2024.3414140, 2024.
- [168] K. Messaoudi, A. Baz, O. Sami Oubbati, A. Rachedi, T. Bendouma, M. Atiquzzaman, UGV Charging Stations for UAV-Assisted AoI-Aware Data Collection, *IEEE Transactions on Cognitive Communications and Networking*, Vol. 10, no. 6, pp. 2325-2343, doi: 10.1109/TCCN.2024.3394859, Dec. 2024.
- [169] Z. Huang, S. Chen, Y. Pian, Z. Sheng, S. Ahn and D. A. Noyce, Toward C-V2X Enabled Connected Transportation System: RSU-Based Cooperative Localization Framework for Autonomous Vehicles, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 10, pp. 13417-13431, Oct. 2024.
- [170] Z. Wang, P. Keo, M. Saberi, Real-Time Traffic State Measurement Using Autonomous Vehicles Open Data, *IEEE Open Journal of Intelligent Transportation Systems*, Vol. 4, pp. 602-610, doi: 10.1109/OJITS.2023.3298893, 2023.
- [171] M. Yu, K. Gong, W. Zhao, R. Liu, LiDAR and IMU Tightly Coupled Localization System Based on Ground Constraint in Flat Scenario, *IEEE Open Journal of Intelligent Transportation Systems*, Vol. 5, pp. 296-306, doi: 10.1109/OJITS.2024.3406390, 2024.

- [172] Concept of Operations of Unmanned Aircraft System (UAS) Traffic Management (TM) v2.0, Federal Aviation Administration (FAA), March 2020.
- [173] J. Zhou, D. Sun, I. Hwang and D. Sun, Control Protocol Design and Analysis for Unmanned Aircraft System Traffic Management, in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 9, pp. 5914-5925, doi: 10.1109/TITS.2021.3083675, Sept. 2021.
- [174] R. Faria, L. Brito, K. Baras and J. Silva, Smart mobility: A survey, International Conference on Internet of Things for the Global Community (IoTGC), Funchal, Portugal, pp. 1-8, doi: 10.1109/IoTGC.2017.8008972, 2017.
- [175] E. C. Pinto Neto, D. M. Baum, J. R. de Almeida, J. B. Camargo, P. S. Cugnasca, A Trajectory Evaluation Platform for Urban Air Mobility (UAM), in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9136-9145, doi: 10.1109/TITS.2021.3091411, July 2022.
- [176] Cotton, B. William, David J. Wing, Airborne Trajectory Management for Urban Air Mobility, In 2018 Aviation Technology, Integration, and Operations Conference, Page 3674, 2018.
- [177] Global Air Traffic Management Operational Concept, 1st edition, document 9854, ICAO, Montreal, QC, Canada, 2005.
- [178] F. Ho et al., Decentralized Multi-Agent Path Finding for UAV Traffic Management, IEEE Transactions on Intelligent Transportation Systems, Vol. 23, No. 2, Pages 997-1008, doi: 10.1109/TITS.2020.3019397, Feb. 2022.
- [179] Y. I. Jenie, E.-J. van Kampen, J. Ellerbroek, and J. M. Hoekstra, Taxonomy of Conflict Detection and Resolution Approaches for Unmanned Aerial Vehicle in an Integrated Airspace, IEEE Trans. Intelligent Transportation Systems, Vol. 18, No. 3, Pages 558-567, Mar. 2017.
- [180] R. Stern, N.R. Sturtevant, A. Felner, S. Koenig, H. Ma, T. T. Walker, J. Li, D. Atzmon, L. Cohen, T. K. Satish Kumar, E. Boyarski, R. Bartak, Multi-Agent Pathfinding: Definitions, Variants, and Benchmarks, Proceedings of the International Symposium on Combinatorial Search, 2019.
- [181] F. Ho, A. Salta, R. Geraldès, A. Goncalves, M. Cavazza, and H. Prendinger, Multi-Agent Path Finding for UAV Traffic Management, in Proc. 18th Int. Conf. Auto. Agents Multi-Agent Syst. (AAMAS), Pages 131-139, 2019.

- [182] W. B. Cotton, R. Hilb, S. Koczko, D. J. Wing, A Vision and Roadmap for Increasing User Autonomy in Flight Operations in the National Airspace, 16th AIAA Aviation Technology, Integration, and Operations Conference, Washington, DC, 2016.
- [183] W. B. Cotton, R. Hilb, S. Koczko, D. J. Wing, Preliminary Assessment of Operational Hazards and Safety Requirements for Airborne Trajectory Management (ABTM) Roadmap Applications, NASA/TM-2016-219176, Hampton, VA, 2016.
- [184] N. Samir Labib, G. Danoy, J. Musial, M.R. Brust, P. Bouvry, Internet of Unmanned Aerial Vehicles - A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management. *Sensors*, 19(21), 4779, 2019.
- [185] K. W. Huang, H. M. Wang, Combating the Control Signal Spoofing Attack in UAV Systems, in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7769-7773, doi: 10.1109/TVT.2018.2830345, Aug. 2018.
- [186] Q. Wu, W. Mei, and R. Zhang, Safeguarding wireless network with UAVs: A physical layer security perspective, *IEEE Wireless Communication*, vol. 26, no. 5, pp. 12-18, Oct. 2019.
- [187] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, Efficient Certificate-Less Aggregate Signature with Conditional Privacy Preservation in IoV, *IEEE Systems Journal*, vol. 15, no. 1, pp. 245-256, Mar. 2021.
- [188] H. Tan, W. Zheng, P. Vijayakumar, Secure and Efficient Authenticated Key Management Scheme for UAV-Assisted Infrastructure-less IoVs, *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6389-6400, Jun. 2023.
- [189] C. Fan, H. Liu, B. Li, C. Zhao, S. Mao, Adversarial Game Against Hybrid Attacks in UAV Communications With Partial Information, in *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 2204-2208, doi: 10.1109/TVT.2021.3132934, Feb. 2022.
- [190] Yulin Teng, Pinchang Zhang, Yangyang Liu, Jiankuo Dong, Fu Xiao, Exploiting Carrier Frequency Offset and Phase Noise for Physical Layer Authentication in UAV-Aided Communication Systems, *IEEE Transactions on Communications*, vol.72, no.8, pp.4708-4724, 2024.
- [191] A. V. Savkin, H. Huang, W. Ni, Securing UAV Communication in the Presence of Stationary or Mobile Eavesdroppers via Online 3D Trajectory Planning, *IEEE Wireless Communication Letter*, vol. 9, no. 8, pp. 1211-1215, Aug. 2020.

- [192] Yi Zhou, Zheng Ma, Heng Liu, Phee Lep Yeoh, Yonghui Li, Branka Vucetic, Pingzhi Fan, A UAV-Aided Physical Layer Authentication Based on Channel Characteristics and Geographical Locations, *IEEE Transactions on Vehicular Technology*, vol.73, no.1, pp.1053-1064, 2024.
- [193] Yapei Gu, Kexin Guo, Lei Guo, Jianzhong Qiao, Jindou Jia, Xiang Yu, Lihua Xie, An Enhanced UAV Safety Control Scheme Against Attacks on Desired Trajectory, *Aerospace Science and Technology*, vol. 119, 107212, ISSN 1270-9638, <https://doi.org/10.1016/j.ast.2021.107212>, 2021.
- [194] Yuge Zhang, Physical Layer Authentication Based on Gaussian Mixture Model Under Unknown Number of Attackers, 2021 IEEE/CIC International Conference on Communications in China (ICCC), pp.70-74, 2021.
- [195] Yichao Chen, Guanbang Liu, Zhen Zhang, Lidong He, Secure Remote Control for Multi-UAV Systems: A Physical Layer Security Perspective, *IEEE International Conference on Unmanned Systems (ICUS)*, pp.916-921, 2022.
- [196] Yi Zhou, Phee Lep Yeoh, Kyeong Jin Kim, Zheng Ma, Yonghui Li, Branka Vucetic, Game Theoretic Physical Layer Authentication for Spoofing Detection in UAV Communications, *IEEE Transactions on Vehicular Technology*, vol.71, no.6, pp.6750-6755, 2022.
- [197] Yapei Gu, Kexin Guo, Chenlong Zhao, Xiang Yu, Lei Guo, Fast Reactive Mechanism for Desired Trajectory Attacks on Unmanned Aerial Vehicles, *IEEE Transactions on Industrial Informatics*, vol.19, no.8, pp.8976-8984, 2023.
- [198] Huangwenqing Shi, Mu Niu, Yulin Teng, Pinchang Zhang, Privacy-Preserving Physical Layer Authentication Exploiting Carrier Frequency Offset in UAV-aided Communication Systems, 2024 International Conference on Networking and Network Applications (NaNA), pp.247-251, 2024.
- [199] Yichao Chen, Guanbang Liu, Zhen Zhang, Lidong He, Shibo He, Improving Physical Layer Security for Multi-UAV Systems Against Hybrid Wireless Attacks, *IEEE Transactions on Vehicular Technology*, vol.73, no.5, pp.7034-7048, 2024.