

Cyber Security of Nonlinear Cyber-Physical Systems and Sensor Networks

Hamed Kazemi

A Thesis
in
The Department
of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy (Electrical and Computer Engineering) at
Concordia University
Montréal, Québec, Canada

October 2025

© Hamed Kazemi, 2025

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Mr. Hamed Kazemi**

Entitled: **Cyber Security of Nonlinear Cyber-Physical Systems and
Sensor Networks**

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

Doctor of Philosophy (Electrical and Computer Engineering)

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

Signed by the Final Examining Committee:

Dr. Chunjiang An Chair

Dr. Nasser Lashgarian Azad External Examiner

Dr. Shahin Hashtrudi Zad Examiner

Dr. Rastko Selmic Examiner

Dr. Fuzhan Nasiri Examiner

Dr. Khashayar Khorasani Supervisor

Approved by

Abdelwahab Hamou-Lhadj, Chair
Department of Electrical and Computer Engineering

2025

MOURAD DEBBABI, Dean
Faculty of Engineering and Computer Science

Abstract

Cyber Security of Nonlinear Cyber-Physical Systems and Sensor Networks

Hamed Kazemi, Ph.D.

Concordia University, 2025

Cyber-Physical Systems (CPS), characterized by the tight integration of computational algorithms and physical processes through networks of sensors and actuators, are foundational to modern technological ecosystems. However, the increasing interconnectivity and complexity of CPS introduce critical vulnerabilities, particularly to cyber-attacks and system faults. This thesis focuses on the cybersecurity of nonlinear CPS and distributed sensor networks, proposing robust, reliable, and resilient frameworks for real-time detection, isolation, and recovery from cyber threats and system anomalies.

The first major contribution of this thesis is a unified detection and isolation framework for nonlinear CPS affected by system faults and adversarial False Data Injection (FDI) attacks targeting both actuator and sensor networks, all in the presence of process and measurement noise. The proposed framework employs an Augmented Unscented Kalman Filter (AUKF) to jointly estimate system states and faults, enabling reliable discrimination between malicious attacks and unintentional failures. By incorporating model-based residual analysis alongside auxiliary filtering techniques, the framework facilitates multi-layered anomaly detection at both the command-and-control (C&C) level and within actuator channels.

The thesis then explores reinforcement learning (RL)-based methodologies for advanced cyber-attack and fault detection. A State-action-reward-state-action (SARSA) approach is introduced for online detection and isolation, in which an agent refines its policy through interaction with the system dynamics, aiming to ensure early detection while minimizing false alarms. This is further extended to a Deep Reinforcement Learning (DRL) framework using Deep Q -Networks (DQN), which addresses the scalability limitations of tabular methods in high-dimensional, nonlinear systems. The DRL-based approach leverages analytical insights from AUKF estimators and auxiliary filters, enhancing the agent's capability to detect subtle and stealthy attacks, including covert intrusions.

In the final part of the thesis, a resilient distributed state estimation framework is developed for sensor networks under cyber-attacks and sensor faults. Each node runs a local nonlinear estimator with an embedded detection mechanism. The architecture employs the Distributed Hybrid Information Fusion (DHIF) algorithm to ensure robust estimation through inter-node collaboration, even when FDI attacks compromise communication links.

A DRL-based detector at each node evaluates the trustworthiness of received data and dynamically reconfigures the fusion process upon detection of anomalies. The framework also accommodates switching communication topologies, commonly seen in practical CPS, and includes a rigorous stability analysis demonstrating the ultimate boundedness of the distributed estimation process under such conditions.

The proposed methodologies are validated through extensive simulation studies. A fixed-base inverted pendulum and a high-fidelity unmanned aerial vehicle (UAV) model are used to demonstrate the effectiveness of the frameworks in isolating cyber-attacks, detecting stealthy intrusions, and maintaining operational integrity in nonlinear environments. Simulation results on the UAV platform show that the proposed RL-based methods consistently outperform classical statistical techniques in terms of detection accuracy, isolation speed, and resilience—particularly in scenarios complicated by noise, system faults, and sophisticated attack strategies. Additionally, the distributed estimation and resilience framework is empirically validated through a UAV case study operating within a CPS sensor network characterized by limited sensing coverage and vulnerability to cyber-attacks and sensor faults, demonstrating reliable state recovery and robust path following across a range of challenging simulation scenarios.

Overall, this thesis presents a comprehensive cybersecurity framework for nonlinear CPS, combining model-based estimation, statistical detection, and learning-based strategies for robust fault and attack mitigation. By integrating estimation, detection, and isolation across both centralized and distributed settings, the proposed methodologies offer practical and scalable solutions for securing next-generation CPS against evolving cyber threats.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor, Professor Khashayar Khorasani, for his unwavering support, insightful guidance, and continuous encouragement throughout the course of my doctoral studies. His deep expertise, critical thinking, and high standards of research excellence have profoundly shaped my academic journey and professional development. I am truly fortunate to have had the opportunity to learn under his supervision.

I would also like to sincerely thank the members of my dissertation committee—Professor S. Hashtrudi-Zaad, Professor R. Selmic, Professor F. Nasiri, and Professor N. Lashgarian Azad—for their time, expert evaluation, and constructive feedback. Their thoughtful suggestions and valuable insights have significantly enriched the quality and rigor of this research.

A very special appreciation goes to my beloved wife, Parya, whose unwavering love, sacrifices, and constant encouragement paved the way for me to pursue and complete this journey. Her strength and patience have been a cornerstone of my success. I am also deeply grateful to my two wonderful children, Rayan and Aban, whose joy, laughter, and unconditional love have been a continuous source of motivation and inspiration, even in the most challenging moments.

I extend my heartfelt thanks to my parents, Seyed Ali and Monireh, for their endless support, love, and the values they instilled in me. Their lifelong encouragement and belief in my potential have been the foundation of all my achievements.

Finally, I would like to acknowledge the friendship and support of my colleagues and labmates, including Mohammad, Ali, Shadi, Mehdi, Mohammadreza, Anas, and Shahram. Their collaboration, thoughtful discussions, and camaraderie have made this journey both productive and enjoyable.

Contents

List of Figures	ix
List of Tables	xiii
List of Acronyms	xiii
1 Introduction	1
1.1 Motivation	1
1.2 Literature Review	2
1.2.1 Cyber-Attack Detection and Isolation in Nonlinear CPS	3
1.2.1.1 Model-Based Approaches	4
1.2.1.2 Data-Driven Approaches	7
1.2.2 Distributed State Estimation and System Resilience in CPS	10
1.2.2.1 System Resilience in CPS	12
1.3 General Problem Statement and Thesis Objectives	14
1.3.1 Topic 1: State and Fault Estimation and Cyber-Attack Detection and Isolation in Nonlinear CPS	14
1.3.2 Topic 2: Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation in Nonlinear CPS	15
1.3.3 Topic 3: Distributed State Estimation and System Recovery For Sensor Networks Under Faults and Cyber-Attacks	16
1.4 Contribution of Thesis	16
1.4.1 Topic 1: State and Fault Estimation and Cyber-Attack Detection and Isolation in Nonlinear CPS	16
1.4.2 Topic 2: Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation in Nonlinear CPS	17
1.4.3 Topic 3: Distributed State Estimation and System Recovery for Sensor Networks under Faults and Cyber-Attacks	17
1.5 Outline	18

2	Background: Cyber-Attacks in Nonlinear Cyber-Physical Systems (CPS)	20
2.1	Cyber-Attack Categorization	20
2.1.1	Categorization by Nature of Cyber-Attack	20
2.1.2	Categorization by Mechanism of Cyber-Attack	21
2.2	The Nonlinear State Estimation Problem Based on Unscented Kalman Filter (UKF)	22
2.3	Reinforcement Learning-Based Cyber-Attack Detection	24
2.4	Graph Theory and Topology Switching	25
3	Cyber-Attack and Fault Detection and Isolation of Sensors and Actuators in Nonlinear Cyber-Physical Systems	27
3.1	Problem Statement and Formulation	28
3.2	State and Fault Estimation Using Augmented Unscented Kalman Filters . .	30
3.2.1	Command and Control (C&C) Side Filter	32
3.2.2	Plant Side Filter	34
3.2.3	Stability of the AUKF	34
3.3	Sensor Cyber-attack and System Fault Detection and Isolation	39
3.3.1	Sensor Cyber-attack Detection and Isolation	39
3.3.2	Fault Detection and Isolation	40
3.4	Actuator Cyber-attack Detection and Isolation Using Auxiliary Filters . . .	41
3.5	Auxiliary Filter-Based Actuator and Sensor Attack Detection and Isolation in the Absence of Faults	44
3.6	Case Study Simulation Results	48
3.6.1	Fixed-base inverted pendulum	48
3.6.2	Unmanned Aerial Vehicle (UAV)	54
3.6.3	Auxiliary Filter-Based Actuator and Sensor Attack Detection for the UAV Case Study	66
3.7	CONCLUSIONS	68
4	Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation of Nonlinear Cyber-Physical Systems	70
4.1	Problem formulation	72
4.1.1	State and Fault Estimation Filter	73
4.2	The Q -table Reinforcement Learning-Based Anomaly Detection and Isolation	74
4.2.1	Optimal Detection Strategy	76
4.2.2	Detection Function	77
4.2.3	Observation Space Construction	78
4.2.4	Detection and Isolation Algorithms	78
4.3	Deep Reinforcement Learning-Based Sensor and Actuator Cyber-Attack Detection and Isolation	82

4.3.1	DRL-Based Cyber-Attack Detection and Isolation Formulation	84
4.3.2	Optimal Detection Strategy	86
4.3.3	Detection Functions and Observation Spaces	87
4.3.4	Detection and Isolation Algorithms	89
4.4	Case Study Simulations	93
4.4.1	Q-Table-Based UAV Cyber-Attack and Fault Detection and Isolation	94
4.4.2	DRL-Based Sensor and Actuator FDI Attack Detection and Isolation	100
4.4.3	Covert Attack Detection and Isolation	102
4.4.4	Performance Evaluation and Comparative Analysis	104
4.5	Conclusion	108
5	Resilient Distributed State Estimation for Nonlinear Cyber-Physical Systems with Sensor Networks under Cyber-Attacks	111
5.1	Problem Formulation	113
5.2	Resilient Distributed Data Fusion Approach	114
5.2.1	Sensor Fault Detection and Isolation	115
5.2.2	Propagation	116
5.2.3	Packing and Communication	117
5.2.4	Cyber-Attack Detection and Isolation	119
5.2.5	Update and System Recovery	120
5.3	Stability Analysis	122
5.3.1	Stability Under Switching Topologies	125
5.4	Case Study Simulations	127
5.4.1	Scenario 1: Sensor Network under Cyber-Attacks	129
5.4.2	Scenario 2: Simultaneous Sensor Fault and Cyber-Attacks	133
5.4.3	Scenario 3: UAV Path Following with Cyber-Attack Detection and Recovery	137
5.5	Conclusion	151
6	Conclusions and Future Work	152
6.1	Conclusions	152
6.2	Future Directions of Research	154
6.3	Accepted and Submitted Journal and Conference Papers	155
	References	157

List of Figures

Figure 2.1 Interactions between the agent and its environment in RL, characterized by state, action, and reward.	24
Figure 3.1 The CPS under faults and FDI attacks with the C&C and the plant side filters and detectors.	30
Figure 3.2 The CPS under actuator and sensor cyber-attacks with the C&C and the plant side auxiliary filters and detectors.	45
Figure 3.3 Cyber physical system including a fixed-base inverted pendulum and C&C center	48
Figure 3.4 System outputs under actuator fault.	49
Figure 3.5 Fault estimator and detector responses for the system under actuator fault.	50
Figure 3.6 Attack detector responses for the system under actuator fault. . . .	51
Figure 3.7 System outputs under fault and cyber-attack.	51
Figure 3.8 Fault estimator and detector responses for the system under actuator fault and attack.	52
Figure 3.9 Attack detector responses for the system under actuator fault & attack.	53
Figure 3.10 Angular positions and rates in the UAV body axis	54
Figure 3.11 The UAV's actual measurement outputs, and the AUKF estimates under the healthy condition.	57
Figure 3.12 Actuator fault estimator (AUKF) and detector responses for the system under actuator and sensor faults.	58
Figure 3.13 Sensor fault estimator (AUKF) and detector responses for the system under actuator and sensor faults.	59
Figure 3.14 The UAV's measurement values, and AUKF estimate under system faults and actuator and sensor cyber-attacks.	60
Figure 3.15 cyber-attack detector results for the sensor ϕ	61
Figure 3.16 cyber-attack detector results for the sensor Θ	61
Figure 3.17 Actuators cyber-attack detection results.	62
Figure 3.18 The UAV's measurement outputs, reference, and the received signals at the C&C center under covert attacks.	63
Figure 3.19 Covert attacks signals and the detection results.	64

Figure 3.20 The UAV's measurement outputs, reference values, and the received signals at the C&C center under actuator and sensor FDI attacks.	66
Figure 3.21 Actuator cyber-attack detection results, including actuator and auxiliary filter cyber-attacks, and residuals.	67
Figure 3.22 Sensor cyber-attack detection results, including sensor and auxiliary filter cyber-attacks and residuals.	68
Figure 4.1 The CPS under faults and FDI cyber-attacks in sensor network. . .	73
Figure 4.2 A state-machine diagram for the cyber-attack and fault detection and isolation problem, where $k = k_{ij}$ represents the transition time between hidden states, and r_{ij} denotes the received reward based on the corresponding actions.	75
Figure 4.3 The CPS under FDI cyber-attacks in actuator and sensor networks. . .	83
Figure 4.4 A state-machine diagram for actuator and sensor cyber-attack detection and isolation problem. $k = k_{ij}$ represents the transition time between hidden states, and r_{ij} denotes the received reward based on the corresponding actions.	85
Figure 4.5 DQN architecture with the target network technique.	86
Figure 4.6 Angular positions and rates in the UAV body axis	93
Figure 4.7 The UAV's measurement outputs and estimates and the sensor fault estimate under the the fault and cyber-attacks.	95
Figure 4.8 Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under nominal noise conditions. . . .	97
Figure 4.9 Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under various measurement noise. . .	98
Figure 4.10 Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under various cyber-attack noise. . .	99
Figure 4.11 Sensor and Actuator FDI cyber-attacks.	102
Figure 4.12 The UAV's measurement outputs and estimates under FDI sensor and actuator attacks.	103
Figure 4.13 Probability of FDI attack detection using the DRL detector for sensor and actuator cyber-attacks	104
Figure 4.14 Covert attack signals	105
Figure 4.15 The UAV's measurement outputs and estimates under covert attacks. .	106
Figure 4.16 Probability of covert attack detection using the DRL detector	107
Figure 4.17 Detection results of DRL, Q -table RL, χ^2 , and Euclidean-based approaches for cyber-attack detection under various noise conditions.	108

Figure 4.18 Performance comparison of the χ^2 , Euclidean-based, Q -table RL-based, and DRL-based cyber-attack detectors in terms of detection delay and false alarm probability under various noise conditions.	109
Figure 5.1 Cyber-Physical System (CPS) with a distributed sensor network. . .	115
Figure 5.2 UAV integrated with a distributed sensor network.	128
Figure 5.3 Distributed state estimation results for sensor network under healthy conditions.	130
Figure 5.4 Sensing status of each local node over time.	131
Figure 5.5 Detection results of the DRL-based cyber-attack detector for Attack21 and Attack67.	131
Figure 5.6 Switched graphs resulting from the recovery system under cyber-attacks: Attack21 (left) and both Attack21 and Attack67 (right).	132
Figure 5.7 Recovered distributed state estimation results under cyber-attacks on links 21 and 67.	132
Figure 5.8 Sensor fault at node 1 and cyber-attacks on links 12 and 45. The first subplot shows the faulty measurement and its estimation using AUKF. The second subplot highlights the attack signals initiated at $t = 30$ s and $t = 55$ s.	133
Figure 5.9 Comparison of detection and isolation results using DRL-based and χ^2 -based detectors under sensor fault and cyber-attacks.	134
Figure 5.10 Reconfigured communication topologies under the joint effects of sensor fault and cyber-attacks. The left graph shows the updated topology following Attack12; the right graph shows the configuration after Attack45. Node 1 is marked as faulty, and its measurements are excluded from estimation.	135
Figure 5.11 Recovered distributed state estimation results under a sensor fault and cyber-attacks on links 12 and 45.	136
Figure 5.12 Detection and isolation results based on DRL and χ^2 detectors under increased cyber-attack noise.	137
Figure 5.13 Sensing status of each local node over time.	138
Figure 5.14 State estimation results under healthy conditions.	139
Figure 5.15 UAV positions under healthy conditions.	140
Figure 5.16 3D UAV actual positions and distributed state estimates from local nodes at four different time snapshots under healthy conditions.	141
Figure 5.17 Attack signals injected into communication links x_{12} and x_{67}	142
Figure 5.18 3D UAV actual positions and estimation results under cyber-attacks affecting links 12 and 67.	143
Figure 5.19 UAV positions under cyber-attacks affecting links 12 and 67, initiated at $t = 20$ s and $t = 45$ s, respectively.	144
Figure 5.20 DRL-based attack detection results for Attack12 and Attack67. . . .	145

Figure 5.21 Network reconfiguration in response to the Attack12 (left) and both Attack12 and Attack67 (right).	145
Figure 5.22 State estimation results following recovery from Attack12 and Attack67. The attacks were initiated at $t = 20$ s and $t = 45$ s, detected at $t = 26$ s and $t = 58$ s, and recovered at $t = 28$ s and $t = 60$ s, respectively.	146
Figure 5.23 Mean estimation errors of the UAV's x , y , and z positions across three phases: healthy operation, under cyber-attacks, and after system recovery.	147
Figure 5.24 UAV positions under the recovery mechanism. The attacks were initiated at $t = 20$ s and $t = 45$ s, detected at $t = 26$ s and $t = 58$ s, and recovered at $t = 28$ s and $t = 60$ s, respectively.	149
Figure 5.25 3D UAV actual positions and estimation results after applying the recovery mechanism.	150

List of Tables

Table 3.1	Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under normal measurement noise.	65
Table 3.2	Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under measurement noise multiplied by 10.	65
Table 3.3	Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under measurement noise multiplied by 20.	65
Table 4.1	Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) and RL-based detector ($c = 0.01$) in detection of the faults (F.) and cyber-attacks (A.) under nominal noise.	100
Table 4.2	Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) and RL-based detector ($c = 0.01$) in detection of the faults (F.) and cyber-attacks (A.) under various measurement noise.	100
Table 4.3	Precision (Pr.), Recall (Rec.) , and F-Score (F-S.) for χ^2 , Euc. and RL detector ($c = 0.01 = c_1$ & $c = 0.15 = c_2$) in attack (A.) detection under various cyber-attack noise.	100
Table 4.4	Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under nominal noise.	110
Table 4.5	Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under various measurement noise.	110
Table 4.6	Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under various cyber-attack noise.	110
Table 5.1	Mean absolute estimation errors of rotational angles (Ang.) and position coordinates (Pos.) per node across different operational phases	148

List of Acronyms

ANN	Artificial Neural Network
AUKF	Augmented Unscented Kalman Filter
C&C	Command and Control
CNN	Convolutional Neural Network
CPS	Cyber-Physical System
DHIF	Distributed Hybrid Information Fusion
DNN	Deep Neural Network
DoS	Denial-of-Service
DQL	Deep Q-Learning
DQN	Deep Q-Network
DRL	Deep Reinforcement Learning
EKF	Extended Kalman Filter
FDI	False Data Injection
KF	Kalman Filter
KNN	K-Nearest Neighbors
ML	Machine Learning
POMDP	Partial Observable Markov Decision Process
PF	Particle Filters
RL	Reinforcement Learning
RNN	Recurrent Neural Network

SARSA State Action Reward State Action

SVM Support Vector Machines

UAV Unmanned Aerial Vehicle

UIO Unknown Input Observer

UKF Unscented Kalman Filter

UT Unscented Transform

ZDA Zero Dynamic Attack

Chapter 1

Introduction

1.1 Motivation

Cyber-Physical Systems (CPS) are complex infrastructures where cyber and physical components are tightly integrated to enable intelligent monitoring, control, and operation of critical subsystems [1–3]. While this integration significantly improves system efficiency and responsiveness, it also increases the system’s exposure to cyber-attacks—malicious actions that exploit vulnerabilities and may result in severe disruptions or physical damage [1]. Due to their interconnected nature and frequent remote accessibility, CPS are particularly vulnerable to cyber-attacks that can be launched through both cyber and physical channels [4].

Among the various types of cyber threats, False Data Injection (FDI) attacks are especially challenging to detect and mitigate. These attacks can alter sensor readings, system states, or control commands by introducing carefully crafted erroneous data. Moreover, FDI serves as the foundation for more advanced attack strategies such as replay attacks, covert attacks, and zero-dynamics attacks [5–7]. Real-world incidents—such as those documented in [8–14]—highlight the serious risks CPS face and reinforce the need for effective detection and isolation mechanisms. Timely identification of such attacks is crucial to limit their impact and maintain the safe and reliable operation of the overall system.

Furthermore, Machine-induced faults, such as parameter variations, structural changes, and faulty components, can degrade CPS performance [15]. Unlike basic detection, fault estimation identifies the fault’s nature and severity [16], and must be performed accurately and promptly to avoid system failures. The design of fault estimators depends on system dynamics and the fault signal’s characteristics [17, 18]. Additionally, accurate state estimation is vital for control and detection, by using methods such as Kalman Filters, observer-based techniques, and sliding mode observers [19–21].

To detect intrusions such as cyber-attacks or system faults, monitoring-based methods typically analyze audit data—such as application logs, network traffic flow, and user command activity—to distinguish between normal and abnormal behavior. However, as

network size increases, the volume of audit data grows rapidly, making manual detection increasingly impractical or even infeasible. Moreover, accurately distinguishing cyber-attacks from other anomalies, such as noise or benign disturbances, is critical to preventing stealthy attacks that may evade traditional detection mechanisms. To address these challenges, modern cybersecurity solutions increasingly leverage advanced machine learning (ML) and deep learning techniques. These data-driven approaches enable scalable, efficient, and adaptive threat detection by identifying complex patterns within large datasets, thereby improving both the accuracy and responsiveness of intrusion detection systems and making them essential components of contemporary cybersecurity defense strategies [22].

As another interesting related topic, distributed estimation, which aims to provide reliable local estimates of inaccessible system states or unknown parameters across distributed nodes (sensors) by using locally exchanged sensor data, has garnered significant interest across a variety of domains, including target tracking, region monitoring, area surveillance, industrial process monitoring, home automation, wildlife habitat observation, and traffic condition detection [23, 24]. Traditional centralized approaches typically rely on collecting measurements from all sensors in the network to compute an optimal global estimate. However, this imposes substantial communication and computational overhead. In contrast, distributed estimation strategies offer improved scalability and robustness by enabling each node to share information with its neighbors according to a fixed or dynamic communication topology. Such strategies generally enhance the reliability, accuracy, and flexibility of the overall estimation process [25].

Despite their advantages, distributed sensor networks are inherently vulnerable to cyber-attacks, particularly those targeting sensor measurements [23, 26–28]. False signals can be maliciously injected into the system, compromising the integrity of the data, degrading estimation accuracy, or even destabilizing the estimator. These vulnerabilities highlight the urgent need for secure distributed state estimation methods that are resilient to FDI attacks, ensuring reliable performance even in adversarial environments.

1.2 Literature Review

As the complexity and interconnectivity of modern CPS continue to grow, ensuring their reliability, robustness, and security against cyber threats has become a central research challenge. This literature review surveys the most relevant contributions across three critical dimensions: cyber-attack detection and isolation in nonlinear CPS, model-based and data-driven learning-based detection frameworks, and resilient distributed estimation strategies. For each of these themes, the review presents a structured analysis of the strengths, limitations, and recent innovations found in the literature, with an emphasis on nonlinear dynamics, partial observability, and the growing use of artificial intelligence techniques. Particular attention is given to attack detection in high-dimensional and

resource-constrained environments, the integration of estimation and detection, and the challenges of system resilience under sophisticated adversarial scenarios. Together, these insights lay the foundation for the methods developed in this thesis.

1.2.1 Cyber-Attack Detection and Isolation in Nonlinear CPS

Cyber-attack detection techniques—also referred to as intrusion detection methods—are critical components of secure CPS [29]. These techniques are generally divided into two broad categories: network-based approaches and physical-system-aware approaches, each with distinct assumptions, detection targets, and limitations.

Network-based approaches, rooted in the domain of conventional information security, emphasize packet-level analysis of network communication protocols. These methods often rely on statistical traffic profiling, rule-based analysis, or signature matching to detect deviations from normal behavior. Techniques such as Deep Packet Inspection (DPI), anomaly detection via time-series models, and graph-based traffic classification are common [30,31]. While these approaches can effectively detect attacks like Denial-of-Service (DoS), Man-in-the-Middle (MitM), and spoofing at the communication layer, they are often agnostic to the physics of the underlying system. As such, they may overlook critical indicators embedded in the system’s dynamics. Moreover, signature-based methods struggle against zero-day attacks or novel adversarial strategies, while anomaly-based detection methods are vulnerable to high false alarm rates in dynamic CPS environments.

To address these shortcomings, recent work has investigated hybrid approaches that fuse IT-layer monitoring with control-system models [32,33]. However, such integrations remain challenging due to the difference in timing, semantics, and abstraction levels between network traffic and physical process data. Furthermore, many network-based systems are designed for enterprise IT infrastructures and are difficult to adapt for real-time embedded CPS with strict latency constraints.

Physical-system-aware approaches, on the other hand, operate at the intersection of control theory and system modeling. These methods leverage analytical or data-driven models of the CPS to track deviations between expected and observed behavior. Specifically, they rely on residual generation—i.e., computing the difference between predicted and actual sensor measurements based on state estimation—and statistical evaluation to identify anomalies. This paradigm is more sensitive to system-specific attacks such as stealthy sensor spoofing or actuator tampering that bypass traditional IT-layer defenses [34,35].

Such methods typically employ estimation techniques (e.g., Kalman filters, observers, or nonlinear estimators) to infer hidden states of the system. A model of the expected system dynamics allows these techniques to detect inconsistencies introduced by adversarial manipulation. For instance, when an attacker injects false sensor data, the estimated system trajectory will gradually diverge from the actual measurements, triggering a residual threshold. These methods are particularly suited to CPS because they incorporate the

underlying physics and dynamics into the detection process, thereby reducing the likelihood of false alarms arising from benign network variations or transient faults.

A key advantage of physical-aware techniques is their ability to detect previously unknown or stealthy attacks, especially when the attacker has limited knowledge of the system dynamics. However, their performance depends heavily on the fidelity of the system model, the observability of system states, and the robustness of residual generation techniques under noise and uncertainty. Additionally, ensuring timely detection and localization of attacks in real-time applications remains a significant challenge.

Recent studies have recognized the complementary strengths of the two paradigms and proposed hybrid detection architectures that combine network-level and physical-layer insights [36–38]. For instance, hierarchical intrusion detection systems (IDS) may use low-level communication anomaly detection as a trigger for physical-model-based estimation, improving both sensitivity and specificity [39]. Another growing area is the integration of physical-aware detection within control loops, enabling resilient or attack-aware controllers that adapt based on estimated trust levels [40, 41].

Despite ongoing progress, the detection and isolation of cyber-attacks in nonlinear CPS remain open and active areas of research. One of the major challenges lies in developing detection strategies that can simultaneously handle: (i) nonlinear system dynamics, (ii) sensor and actuator faults, (iii) process and measurement noise, and (iv) adversarial uncertainty [42, 43]. Many existing works assume linear models, time-invariant structures, or full observability, which limits their applicability in real-world CPS such as unmanned vehicles, smart grids, and industrial automation networks [44].

To address these issues, researchers have increasingly focused on advanced filtering techniques, joint estimation-detection frameworks, and adaptive thresholding schemes that dynamically tune detection sensitivity based on system context and prior behavior [45]. Others explore attack-resilient observers and secure state estimators that embed attack-detection logic directly into estimation algorithms [46, 47]. Some works also investigate formal guarantees, such as input-to-state stability under attack or the convergence of estimation errors in partially observable networks [48].

In summary, cyber-attack detection in nonlinear CPS is evolving from static, siloed strategies to integrated, model-aware, and adaptive frameworks. The interplay between detection, estimation, and control is becoming central to achieving resilient CPS performance. In the following sections, model-based and data-driven detection approaches will be examined in greater detail, with a particular emphasis on their applicability to nonlinear, stochastic, and adversarial CPS environments.

1.2.1.1 Model-Based Approaches

Model-based approaches assume the availability of a sufficiently accurate mathematical representation of the CPS dynamics. These strategies rely on the structural integrity of

system models to infer internal states, monitor residuals, and detect inconsistencies that may indicate cyber intrusions or system faults. Generally, model-based detection frameworks consist of two key phases: estimation and detection. During the estimation phase, the system’s internal states are reconstructed from observed measurements using a model of the system dynamics, generating analytical redundancy. This redundancy enables prediction of expected behavior, which is compared to actual measurements in the detection phase to compute residuals. Decision-making strategies based on statistical thresholds, hypothesis testing, or optimization-based criteria are then used to flag anomalies indicative of malicious activity or sensor/actuator faults. Performance is assessed through standard metrics such as detection rate, isolation accuracy, false alarm rate, and detection latency.

The main advantage of model-based detection lies in its transparency and explainability: by leveraging physical laws or first-principles models, these methods offer interpretable detection results and structured performance guarantees. However, challenges arise when these models are nonlinear, time-varying, or uncertain—conditions that are common in realistic CPS.

A central research challenge in this area is the simultaneous estimation of system states and fault/attack signals, especially for nonlinear CPS. This problem becomes particularly complex under adversarial conditions where sensor and actuator channels may be selectively compromised. To distinguish between faults, noise, and cyber-attacks, high-fidelity models must be combined with robust estimation and detection algorithms. Traditional residual-based detectors, such as norm-based measures (e.g., L_1 , L_2 , or L_∞), χ^2 detectors, and Euclidean distance metrics, offer simplicity but may suffer from poor sensitivity in high-noise or stealthy attack environments.

To enhance robustness, Kalman filter-based approaches remain a foundational tool for estimation in model-based settings. These include the standard Kalman Filter (KF) for linear Gaussian systems [49], the Extended Kalman Filter (EKF) [50,51], and the Unscented Kalman Filter (UKF) [52–54]. The UKF, in particular, offers significant advantages in nonlinear systems by more accurately approximating the nonlinear transformations of the state distribution via sigma-point sampling. Further extensions, such as the Cubature Kalman Filter (CKF) [55] and the Interacting Multiple Model (IMM) filter [56], aim to handle model uncertainty, multimodal dynamics, or hybrid system behaviors, though they may increase computational overhead and are sensitive to initialization and noise characteristics.

Particle Filters (PF), which represent state distributions using random weighted samples, have also been applied to nonlinear and non-Gaussian environments, providing greater flexibility but at a high computational cost. This makes PFs less suitable for real-time CPS applications with limited processing resources [57]. Comparisons such as [58,59] show that UKF generally offers a good balance between computational tractability and accuracy, making it a favored choice in embedded detection systems.

Beyond Kalman filtering, observer-based methods offer a deterministic alternative. These approaches design observers—such as Luenberger observers, high-gain observers, or unknown input observers (UIOs)—to estimate system states and detect anomalies by examining deviations between measured and predicted outputs. For example, [60] uses a UIO to isolate FDI attacks based on adaptive thresholds, while [20] leverages nonlinear observer designs to handle systems with bounded disturbances. In recent years, enhanced observer structures with adaptive gains, disturbance decoupling, or sliding mode correction have been explored for better robustness under model mismatch and noise [61, 62].

Sliding Mode Observers (SMO) form a particularly robust class of observers for handling nonlinearities and bounded disturbances. These observers use a discontinuous control law to force the estimation error trajectory to a predefined sliding surface, thereby achieving strong convergence and insensitivity to model uncertainties [5]. However, practical implementations of SMO are often affected by chattering—rapid switching behavior—that may induce high-frequency oscillations, undesirable in hardware-in-the-loop CPS applications [63, 64]. To mitigate chattering, higher-order sliding mode designs and continuous approximations (e.g., super-twisting algorithms) have been proposed, though these trade off robustness for smoothness.

Addressing the challenge of nonlinear CPS under attack, recent work has generalized classical estimation frameworks. For instance, [65] proposes a linear UIO framework for fault/attack detection, showing limited applicability to nonlinear settings. In contrast, [66] advances the modeling framework to include bounded nonlinear dynamics and stochastic noise using encoding-decoding schemes for state recovery. Similarly, in [67], a fault detection scheme using finite-frequency performance criteria and event-triggered filtering is introduced, improving energy efficiency in networked systems. The authors formulate the detection task as an H_∞ filtering problem and derive sufficient conditions under stochastic disturbances, though they do not address actuator-side vulnerabilities. Related works such as [68, 69] have proposed robust designs by optimizing performance indices that explicitly trade off fault sensitivity and disturbance rejection in uncertain networked environments.

Another line of research explores secure state estimation and observer design with formal guarantees. In [70], secure estimators are developed for linear systems under sparse sensor attacks, where compromised measurements are filtered based on convex optimization criteria. These ideas have been extended to nonlinear systems using set-theoretic estimators or invariant set analysis, as shown in [71], though such methods often suffer from scalability issues in large-scale CPS.

Beyond detection, isolation is critical in CPS to localize which specific nodes or components have been compromised. However, isolation has received relatively limited attention in comparison to detection. In [72], a graph-based causality method is developed that exploits physical invariants to detect and locate coordinated FDI attacks. A similar goal is pursued in [73], which uses two-stage anomaly analysis for identifying suspicious

subcomponents in power systems based on load and flow metrics. In [74], a distributed attack isolation scheme is proposed using nonlinear UIOs and stage-wise inference across control areas. This work highlights the value of decentralized logic for scalable isolation but assumes accurate prior knowledge of subsystem models.

Recent approaches have begun integrating learning-based techniques with model-based frameworks to enhance isolation accuracy. For instance, [75] combines sensor correlation analysis with observability metrics to detect and localize stealthy attacks. Others have proposed dynamic Bayesian networks or graph neural networks to infer the most probable attack sources based on spatial-temporal evidence [76, 77].

Model-based approaches provide a principled and structured foundation for cyber-attack detection and isolation in CPS. They offer interpretability, statistical rigor, and physical consistency. However, their applicability may be constrained by model uncertainties, limited observability, nonlinear dynamics, or evolving attack strategies. To address these limitations, recent works increasingly emphasize hybrid designs that fuse model-based estimation with adaptive filtering, anomaly scoring, and learning-based refinement. These hybrid strategies are particularly well-suited to nonlinear CPS where purely model-driven or purely data-driven techniques fall short.

1.2.1.2 Data-Driven Approaches

Data-driven techniques for cyber-attack detection in CPS are increasingly regarded as indispensable, particularly in contexts where physical system models are difficult to construct, evolve rapidly, or are inherently uncertain. These methods capitalize on the rich, high-dimensional datasets generated by sensor and actuator networks in CPS to extract statistical or structural patterns, identify deviations from normative behavior, and recognize cyber threats in real time. The flexibility and scalability of data-driven approaches make them especially attractive for large-scale, dynamic, and heterogeneous CPS environments.

In the literature, data-driven methods have been categorized into regression-based, probabilistic, clustering, Markovian, and data-mining approaches [5, 34, 78]. Many of these techniques are unified under the broader umbrella of machine learning (ML), which includes a wide spectrum of algorithms that learn from data with minimal reliance on explicit system models. Depending on the availability of labeled data and the nature of the learning task, these methods are commonly divided into supervised, unsupervised, and reinforcement learning (RL), with more recent trends focusing on hybrid, deep, and transfer learning paradigms.

Supervised Learning: In supervised learning, models are trained on labeled datasets containing input-output pairs, allowing them to learn a direct mapping from features (e.g., sensor data, signal derivatives) to target labels (e.g., normal, compromised). In the CPS context, supervised classifiers are widely used for detecting FDI attacks, jamming signals, false alarms, and malware propagation.

Algorithms such as Artificial Neural Networks (ANN), Support Vector Machines (SVM), Random Forests (RF), K-Nearest Neighbors (KNN), and Decision Trees (DT) have been extensively applied. For example, [79] introduces a Hoeffding Adaptive Tree combined with instance selection for real-time intrusion detection in industrial control systems, demonstrating robustness under evolving data distributions. In [80], a hybrid detection system using One-Class SVM and supervised classification is proposed to detect stealthy attacks in mixed network-physical data. Likewise, [81] employs ensemble learning techniques to improve classification accuracy in Supervisory Control and Data Acquisition (SCADA) networks.

Despite their accuracy, supervised learning methods face a critical bottleneck: the need for extensive labeled datasets, which are expensive to generate, especially for rare or evolving attacks. In practice, datasets are often imbalanced, with very few positive samples (i.e., attacks), which complicates the training of reliable models.

Unsupervised Learning: In contrast, unsupervised methods operate without labeled data, making them suitable for exploratory tasks, anomaly detection, and systems where attack signatures are unknown or rapidly evolving. Techniques such as clustering (e.g., k -means, DBSCAN), Principal Component Analysis (PCA), Autoencoders, and Isolation Forests are often used to model the normal behavior of the system and detect statistical deviations.

Recent approaches have explored deep unsupervised architectures such as Variational Autoencoders (VAE), Generative Adversarial Networks (GANs), and Self-Organizing Maps (SOMs) for nonlinear feature extraction and anomaly scoring. In [82], a density-based clustering method is used to isolate cyber anomalies in multivariate sensor streams. Similarly, [83] demonstrates the efficacy of GANs in simulating CPS data distributions to detect previously unseen threats.

In high-dimensional and nonstationary CPS environments such as smart grids, autonomous vehicles, and sensor fusion platforms, unsupervised techniques are particularly attractive due to their minimal reliance on prior attack data. However, these methods often suffer from high false positive rates, requiring additional post-processing or ensemble frameworks [84]. In response, hybrid unsupervised-supervised pipelines are being explored to combine anomaly detection with pattern classification and context validation.

Reinforcement Learning (RL): RL methods operate under the paradigm of trial-and-error learning. Agents learn to make sequential decisions in a dynamic environment by interacting with it and receiving feedback in the form of scalar rewards. In the realm of CPS cybersecurity, RL is applied to develop active defense mechanisms such as adaptive firewall rules, intrusion response policies, and attack surface minimization.

A seminal contribution by [85] uses RL to devise a dynamic defense strategy against replay attacks modeled as a POMDP. In [86], a model-free RL framework is introduced to detect replay and data injection attacks through real-time interaction with the CPS.

Similarly, [87] proposes an adversarial training approach using RL agents to proactively mitigate coordinated attacks in simulated networked control systems.

RL is especially beneficial when labeled data is scarce or when the system evolves over time, as agents can adapt by continuously interacting with the environment. However, classical RL algorithms like SARSA or Q -learning struggle with continuous state spaces and long planning horizons, motivating the need for more expressive function approximators.

Deep Reinforcement Learning (DRL): DRL extends RL by integrating deep neural networks to approximate policies, value functions, or action models. DRL is capable of learning directly from high-dimensional input data (e.g., images, time series, or graphs), making it ideal for complex CPS environments where sensor fusion and spatiotemporal dynamics are involved.

In [88], a DRL-based intrusion detection system is deployed in a fog computing environment for IoT-based CPS. A decision agent classifies data streams in real time, achieving high detection accuracy with low latency. Another example, IoTWarden [89], uses a deep Q -network to learn optimal defense policies for false data injection attacks, with simulations showing robustness to varying attack profiles.

Recent DRL advancements include actor-critic methods such as A3C and PPO, which offer better convergence in continuous spaces. Furthermore, attention mechanisms and graph-based DRL architectures have been employed to improve reasoning over large-scale sensor-actuator networks [90].

Hybrid and Transfer Learning Approaches: To improve robustness and reduce training data requirements, hybrid techniques that integrate domain models with data-driven inference have become increasingly popular. For instance, [91] incorporates physical constraints into deep neural networks to ensure stability and reduce overfitting in anomaly detection tasks. Similarly, [92] explores model-informed RL, where known system dynamics are used to shape the agent’s learning space and improve convergence in safety-critical settings.

Transfer learning and continual learning frameworks allow models to generalize from one domain or task to another, which is crucial in rapidly changing CPS infrastructures. In [93], a transfer learning framework is proposed for anomaly detection in industrial CPS, showing significant gains in training efficiency and detection precision. Additionally, federated learning is being investigated to support decentralized model updates in privacy-sensitive CPS like smart cities and healthcare systems.

Emerging work also highlights the potential of self-supervised and contrastive learning techniques, where the learning objective is derived from the data structure itself rather than explicit labels. These approaches can be used to learn useful representations for downstream detection and classification tasks in data-scarce environments [94].

Data-driven approaches offer immense potential for enhancing CPS security through flexible, scalable, and adaptive learning frameworks. Supervised methods remain powerful

for well-annotated environments, while unsupervised methods and RL/DRL are better suited for dynamic or uncertain operating conditions. Hybrid techniques that combine first-principle knowledge with learning capabilities are currently the most promising direction for addressing the challenges of scalability, interpretability, and evolving threat landscapes in modern CPS.

1.2.2 Distributed State Estimation and System Resilience in CPS

Distributed state estimation plays a central role in the design and operation of CPS, where geographically dispersed sensors and controllers collaborate to monitor and control complex, nonlinear dynamical processes. By enabling local nodes in a sensor network to estimate global or shared state variables through limited-range communication, distributed estimation alleviates the bandwidth, computation, and fault-tolerance constraints associated with centralized approaches. This decentralized paradigm has found applications in a wide range of CPS domains, including but not limited to industrial automation, distributed robotics, power grids, intelligent transportation systems, environmental surveillance, and smart manufacturing [23, 25, 95].

Unlike centralized estimation frameworks—which rely on aggregating sensor data at a fusion center and are thus susceptible to single points of failure and communication bottlenecks—distributed methods improve scalability and robustness. Each node in the network processes local sensor measurements and exchanges information with neighbors defined by a communication graph, which can be static or dynamic. These features not only enhance system performance under communication and computation constraints but also allow resilience to node failures, network disturbances, and partial observability. For time-sensitive applications such as drone coordination, industrial fault detection, or traffic control, distributed estimation offers lower latency, better fault isolation, and real-time decision-making capabilities [96, 97].

A major contribution to this area is the Distributed Hybrid Information Fusion (DHIF) algorithm, introduced by Wang and Ren [98]. DHIF synergistically combines local filtering with neighbor information fusion while requiring only a single round of communication per time step. This stands in contrast to consensus-based approaches, such as those in [26, 99], which typically require multiple communication rounds per iteration to achieve convergence. As such, DHIF reduces communication overhead, energy consumption, and synchronization issues, making it suitable for sensor networks with dynamic or unreliable links.

In terms of estimation accuracy, DHIF employs unscented transformation-based fusion, which is more robust to nonlinearities than linear Kalman filter-based schemes. As shown in [100], DHIF can also be extended to handle unknown inputs and process disturbances through robust estimation strategies. Similarly, [101] proposes a dropout-resilient version of DHIF that maintains estimation performance under random sensor failures, and [102]

develops a version adapted to switching topologies, reflecting the practical needs of time-varying communication networks.

Diffusion strategies, introduced in [103], also aim to distribute the estimation process, but differ fundamentally in their reliance on local consensus and averaging. While diffusion schemes are communication-efficient, they may underperform in heterogeneous sensor networks or systems with complex nonlinear interactions. DHIF, by contrast, enables more principled integration of local observations and shared estimates and supports partial observability assumptions, which is more aligned with real-world CPS architectures [104].

Theoretical properties of DHIF include mean-square boundedness of estimation error under conditions of bounded noise, nonlinear dynamics, and time-varying directed graphs [98]. These robustness properties make it appealing for large-scale CPS such as multi-agent autonomous systems, water distribution networks, and power systems, where system dynamics are nonlinear, communication may be intermittent, and sensors exhibit heterogeneous quality.

Nevertheless, practical deployment of distributed estimation in CPS must also account for cyber threats. Distributed architectures increase the system’s attack surface, exposing vulnerabilities to attacks such as FDI, DoS, replay attacks, and coordinated sensor spoofing [23, 105, 106]. Even the compromise of a small subset of nodes can result in large-scale estimation errors due to the propagation of falsified data across the network, undermining the performance and safety of the entire system. This vulnerability has motivated extensive research into resilient estimation techniques.

To address these threats, numerous resilient filtering strategies have been proposed. In [107], a recursive filter for discrete-time nonlinear systems under hybrid attacks is introduced, integrating Bayesian inference for DoS detection with adaptive estimation. The method dynamically adjusts filtering parameters in response to anomaly scores, maintaining convergence under switching topologies. Similarly, [108] designs a resilient consensus-based estimator using distributed model predictive control (MPC), allowing agents to preserve formation control under spoofing attacks by embedding prediction models into the consensus loop. However, both approaches face limitations: [107] assumes perfect model knowledge, while [108] does not address fault or attack localization explicitly.

To improve attack awareness, machine learning-based intrusion detection systems (IDS) have been increasingly integrated with distributed estimators. For instance, [109] proposes using stochastic classifiers like Naive Bayes and SGD for anomaly detection in wireless sensor networks (WSNs), identifying cyber-attacks via changes in data distribution. In [110], adaptive thresholds are designed to detect attacks in real time under time-varying system behavior. These IDS frameworks offer increased detection sensitivity but often rely on extensive training data and may be ineffective against stealthy or low-amplitude attacks.

Fusion-centric and protocol-level solutions are also explored to enhance estimation resilience. In [111], a recursive fusion protocol is introduced to mitigate DoS and bandwidth

constraints in multi-sensor networks. This scheme utilizes dimensionality reduction and multiplicative noise models to maintain estimation stability under stochastic link failures. Despite its effectiveness, its current formulation is limited to linear dynamics. Extensions to nonlinear systems or inclusion of real-time diagnosis remain open problems.

An emerging line of work addresses secure distributed filtering for nonlinear systems with adversarial agents. In [112], a resilient nonlinear filter is designed to mitigate Byzantine attacks using reputation scoring and outlier detection. Nodes suspected of misbehavior are gradually excluded from the estimation process based on a time-weighted trust metric. Additionally, [113] explores federated learning in the context of distributed estimation, allowing agents to collaboratively train attack detection models without sharing raw data, thereby improving both security and privacy. These methods highlight the interplay between trust management, learning, and estimation in distributed CPS.

To further improve resilience, hybrid strategies have been proposed that combine anomaly detection, structural reconfiguration, and estimator redundancy. For example, in [114], a reconfigurable distributed estimator is introduced that adapts the communication topology upon detection of anomalies. Such approaches allow the estimator to dynamically isolate compromised nodes and preserve estimation accuracy, although their effectiveness depends on accurate and timely attack localization.

Distributed state estimation in CPS has evolved into a rich research area that intersects estimation theory, networked control, machine learning, and cybersecurity. While algorithms like DHIF provide foundational tools with strong theoretical guarantees, emerging threats necessitate additional capabilities, including attack detection, isolation, and reconfiguration. The next generation of estimation frameworks will likely be hybrid, combining physical-model-based inference, data-driven anomaly detection, and structural adaptation to ensure secure, resilient, and real-time estimation in dynamic and adversarial CPS environments.

1.2.2.1 System Resilience in CPS

Ensuring system resilience in CPS involves anticipating, absorbing, adapting to, and recovering from adversarial disruptions. This includes both proactive design strategies and reactive adaptation mechanisms that maintain performance and safety in the presence of cyber-attacks or physical faults. Three major design philosophies are commonly applied in resilient estimation and control: security by design, active countermeasures, and reconfiguration/redundancy strategies.

Security by Design: This principle emphasizes embedding robustness and attack tolerance from the earliest stages of system development, rather than retrofitting security into existing architectures. The goal is to co-design security policies alongside estimation and control algorithms. For instance, [115] provides a comprehensive overview of cyber-resilient architectures, including recommendations for integrating threat modeling, attack

surface minimization, authentication mechanisms, and post-attack recovery protocols during CPS design.

Security by design also promotes modular architectures and separation of critical and non-critical system functions. For example, [116] presents a layered observer design that isolates critical system dynamics from potentially compromised subsystems. Similarly, real-time operating systems and microkernel-based architectures have been explored to enforce secure task execution and reduce vulnerability footprints [117]. These approaches aim to ensure that core functionality is preserved even when parts of the system are under attack.

Active Countermeasures: Active countermeasures involve adaptive and reactive mechanisms that mitigate the impact of detected anomalies. These include observer-based fault isolation, learning-based adaptation, and resilient controllers. For instance, [118] proposes a switching sliding-mode controller that maintains closed-loop stability during DoS attacks by switching between control laws based on the communication status. Similarly, [119] introduces a distributed filtering strategy that compensates for corrupted measurements caused by FDI and jamming attacks.

Machine learning and reinforcement learning have also emerged as powerful tools for active mitigation. In [120], a DRL-based trust management scheme is used to dynamically reassign trust weights among nodes in a time-varying communication network. Each node learns to adaptively evaluate its neighbors' reliability and isolate compromised links without centralized oversight. Other strategies involve adaptive thresholding and residual weighting to reduce false alarms and improve sensitivity to stealthy or persistent attacks [110, 121].

Furthermore, recent developments in control-aware communication offer resilience under network constraints. For example, [122] proposes a joint control-communication framework that prioritizes data transmission based on control-criticality, thereby enhancing robustness against bandwidth-limiting attacks.

Reconfiguration and Redundancy: Redundancy and architectural flexibility are crucial in enabling CPS to reconfigure in response to localized failures or attacks. Redundant sensors, actuators, or communication paths can be selectively activated when primary channels are compromised. In [123], compromised agents are excluded from consensus protocols using a local verification score, allowing the rest of the network to maintain coordinated behavior.

Trust-based schemes and voting-based estimators are often used to isolate faulty nodes. For instance, [121] introduces a trust-based observer that down-weights information from low-reputation nodes based on residual analysis. Reconfiguration strategies also include graph rewiring, backup topology activation, and role reassignment within multi-agent systems.

Graph-theoretic formulations of resilience are gaining traction as tools to assess and optimize redundancy. [124] develops resilience metrics based on the number of independent paths between critical components, allowing for quantitative evaluation of

system robustness. These insights inform the design of CPS architectures with built-in tolerance to node or link failures.

Topology switching is another reconfiguration tool, particularly in wireless or mobile networks such as UAV swarms. In such scenarios, secure link scheduling and coordinated path planning can dynamically adapt the network structure to mitigate compromised routes while preserving global observability [125].

Hybrid Resilience Frameworks and Future Directions: In practice, effective CPS resilience often emerges from hybrid strategies that combine the above approaches. These include secure filtering algorithms, ML-based intrusion detection, reputation-aware fusion mechanisms, and dynamic controller switching. For example, [112] proposes a Byzantine-resilient filter that uses neighbor consensus scoring to exclude compromised agents, while [113] leverages federated learning to collaboratively train anomaly detectors across distributed nodes without sharing raw data.

Such integrated architectures are being explored in applications ranging from smart grids and water networks to autonomous vehicle systems and drone fleets. In these contexts, multi-layered detection and control hierarchies are employed to respond to both cyber and physical disruptions in real time.

Nevertheless, many open challenges remain. These include ensuring resilience in nonlinear and time-varying systems, detecting low-rate stealthy attacks, maintaining real-time operation under resource constraints, and formal verification of resilient behavior. There’s also growing interest in incorporating game-theoretic models, zero-trust architectures, and formal co-design frameworks that unify estimation, control, and cybersecurity guarantees.

In summary, system resilience in CPS is a multi-faceted challenge that requires the integration of secure design principles, adaptive defense mechanisms, and structural flexibility. Advances in distributed filtering, trust management, and machine learning are gradually enabling CPS to detect, isolate, and recover from sophisticated cyber-physical threats. However, achieving scalable, interpretable, and verifiable resilience in nonlinear, data-driven, and adversarial environments remains a central research direction in the years ahead.

1.3 General Problem Statement and Thesis Objectives

1.3.1 Topic 1: State and Fault Estimation and Cyber-Attack Detection and Isolation in Nonlinear CPS

This research investigates the critical challenge of secure and reliable state estimation in discrete-time nonlinear CPS subject to system faults, adversarial FDI attacks, and stochastic disturbances such as process and measurement noise. The focus lies on scenarios where data is exchanged across communication networks—specifically between sensors,

controllers, the command and control (C&C) center, and the plant—leaving communication channels vulnerable to malicious interference. Adversaries are assumed to have the ability to manipulate transmitted data in both measurement and actuation channels, complicating the distinction between normal system faults and intentional cyber-attacks. These challenges necessitate robust detection and isolation strategies that can operate effectively in nonlinear, noise-affected environments.

The primary objective of this thesis is to develop a robust estimation and detection framework for nonlinear CPS that can accurately estimate system states and isolate both system faults and cyber-attacks. This is achieved through the design and implementation of an augmented unscented Kalman filter (AUKF), complemented by fault and cyber-attack detectors placed at both the C&C center and the plant side. The approach includes stability analysis of the estimation dynamics and proposes auxiliary filtering strategies specifically for actuator attack detection. The effectiveness of the proposed framework is validated through extensive simulations using a high-fidelity unmanned aerial vehicle (UAV) model, demonstrating its capability to identify and isolate various types of faults and FDI attacks, including covert threats.

1.3.2 Topic 2: Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation in Nonlinear CPS

As CPS become increasingly interconnected and complex, they are more susceptible to sophisticated cyber-attacks that can compromise sensor and actuator signals. These attacks, often stealthy in nature, are difficult to distinguish from normal operational anomalies such as faults or noise. The key challenge lies in enabling early, accurate detection and isolation of these threats while minimizing false alarms. Traditional model-based techniques—though powerful—often rely on predefined thresholds and may fall short when faced with unknown or evolving attack strategies. This highlights the need for adaptive and intelligent detection mechanisms capable of learning from data and adapting to real-time conditions in nonlinear, noise-affected CPS.

This chapter aims to develop a hybrid detection and isolation framework for nonlinear CPS by integrating model-based estimation with data-driven reinforcement learning techniques. The proposed approach utilizes an AUKF for state estimation, while tabular RL and Deep Q-Network (DQN) algorithms are trained online to make real-time decisions regarding presence and type of anomalies. Auxiliary filters are incorporated to enhance sensitivity to actuator attacks. The resulting framework is designed to reduce detection delays and false alarm rates, enabling robust differentiation between faults and malicious cyber-attacks. The method’s effectiveness is validated through detailed simulations on a high-fidelity UAV model, with comparative analysis demonstrating its superiority over conventional detection strategies.

1.3.3 Topic 3: Distributed State Estimation and System Recovery For Sensor Networks Under Faults and Cyber-Attacks

Distributed state estimation is a powerful strategy for monitoring complex systems, where spatially dispersed sensor nodes cooperate to estimate the system's state by using local measurements and limited communication with neighboring nodes. However, in nonlinear CPS, the security of communication links between sensors is often overlooked, particularly in presence of cyber threats. These vulnerabilities are exacerbated by constraints in communication bandwidth, heterogeneous sensor capabilities, and the dynamic nature of wireless sensor networks. Ensuring the accuracy and robustness of distributed estimation under such conditions is a pressing and underexplored challenge.

This chapter aims to develop a resilient distributed state estimation framework for nonlinear CPS under cyber-attacks, by integrating advanced filtering, graph theory, and DRL. DRL is employed for online detection and isolation of cyber-attacks targeting communication links. The distributed estimation process leverages the DHIF strategy, while adapting to changes in network topology to maintain estimation performance. Theoretical analysis ensures the boundedness of the estimation error despite graph switching, and the framework's resilience is demonstrated through simulations by using a high-fidelity UAV model navigating within a constrained and attack-prone sensor network.

1.4 Contribution of Thesis

The main contributions of this thesis are as follows.

1.4.1 Topic 1: State and Fault Estimation and Cyber-Attack Detection and Isolation in Nonlinear CPS

- (i) Addressing the complex challenges associated with nonlinear CPS affected by process and measurement noise, machine-induced faults, and vulnerabilities to FDI attacks on sensor and actuator communication networks.
- (ii) Development of an Augmented Unscented Kalman Filter (AUKF) for joint state and fault estimation, along with stability analysis demonstrating bounded estimation error under nonlinear dynamics.
- (iii) Detection and isolation of sensor cyber-attacks within the command-and-control (C&C) center of the nonlinear CPS.
- (iv) Design of an auxiliary filter for actuator cyber-attack detection, along with formal methodology and performance evaluation under adversarial scenarios.

- (v) Differentiation between system faults and cyber-attacks by using the fault estimation capability of the AUKF, enabling attack detection even in presence of concurrent faults.
- (vi) Detection and isolation of stealthy cyber-attacks, including covert attacks that evade conventional detection mechanisms.
- (vii) Validation of the proposed methodologies through implementation on a nonlinear high-fidelity UAV model subjected to various faults and FDI/covert attacks.

1.4.2 Topic 2: Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation in Nonlinear CPS

- (i) Development of a RL-based online detection and isolation framework that enables the agent to learn optimal policies through direct interaction with the CPS environment, targeting both cyber-attacks and system faults in real time.
- (ii) Design of a DRL-based detection and isolation architecture specifically focused on identifying and localizing sensor and actuator cyber-attacks by leveraging high-dimensional state representations from the CPS environment.
- (iii) Development of learning-based strategies to derive optimal detection policies that prioritize early identification of anomalies while minimizing false alarms, ensuring suitability for real-time CPS deployment.
- (iv) Integration of model-based features—derived from an AUKF for joint state and fault estimation, and auxiliary filters for additional insight—into the RL-based detection mechanisms to enhance accuracy and robustness.
- (v) Achievement of robust detection and isolation capabilities for diverse anomalies and stealthy cyber-attacks, including covert attacks, by leveraging the capabilities of the trained online decision makers.
- (vi) Comparative analysis and validation of the proposed RL-based detection frameworks against conventional χ^2 -based, Euclidean-based, and tabular RL methods through simulation studies by using a nonlinear high-fidelity UAV model.

1.4.3 Topic 3: Distributed State Estimation and System Recovery for Sensor Networks under Faults and Cyber-Attacks

- (i) Development of a distributed state estimation framework for nonlinear CPS, where each sensing node employs a local estimator and cyber-attack detector, by using the DHIF algorithm and graph-theoretic methods to perform multi-step distributed estimation.

- (ii) Detection and isolation of local sensor faults within the distributed sensor network framework.
- (iii) Implementation of a cyber-attack detection and isolation mechanism to identify and mitigate FDI attacks on inter-sensor communication links.
- (iv) Introduction of a resilient estimation strategy capable of adapting to dynamic communication topologies to preserve estimation accuracy.
- (v) Stability analysis and theoretical proof of convergence for the proposed distributed estimation approach under switching network graphs.
- (vi) Validation of the proposed methodology through a UAV case study involving a CPS sensor network with limited sensing regions, demonstrating estimation recovery and robust path following under various fault and attack scenarios.

1.5 Outline

In Chapter 2, foundational concepts and background materials related to CPS and cyber-attacks are presented. Section 2.1 categorizes major types of cyber-attacks based on their mechanisms and impact on CPS. Section 2.2 introduces the nonlinear state estimation problem and highlights the use of UKF and their variants. Reinforcement learning-based approaches for cyber-attack detection are briefly reviewed in Section 2.3, while Section 2.4 presents relevant graph-theoretic tools and topology-switching concepts for sensor networks.

In Chapter 3, the detection and isolation of faults and cyber-attacks in nonlinear CPS is studied. Section 3.1 defines the problem setup and underlying system models. State and fault estimation by using AUKF, along with stability analysis, is detailed in Section 3.2. Section 3.3 develops detection and isolation strategies for sensor faults and cyber-attacks. Detection of actuator cyber-attacks by using auxiliary filters is described in the subsequent section. Section 3.5 addresses attack detection for both actuators and sensors. Finally, Section 3.6 presents simulation-based evaluations on a UAV system to validate the proposed approaches.

Chapter 4 develops online, learning-based cyber-attack and fault detection and isolation strategies. Section 4.1 presents the overall framework and design goals. Section 4.2 introduces a classical Q-table reinforcement learning method for anomaly detection and response. Section 4.3 extends this to DRL, leveraging state estimations and filter outputs for detecting and isolating sensor and actuator anomalies. Case study simulations in Section 4.4 demonstrate the adaptability and performance of the learning-based schemes under dynamic CPS environments.

In Chapter 5, a distributed approach to resilient state estimation in sensor networks under cyber-attacks is developed. Section 5.1 formulates the distributed estimation problem

for nonlinear CPS by using sensor networks. Section 5.2 describes the use of the Distributed Hybrid Information Fusion (DHIF) algorithm and graph-based techniques to achieve robust state estimation in presence of faults and attacks. Section 5.3 presents theoretical stability analysis under graph switching. Finally, Section 5.4 validates the distributed estimation and recovery strategy through simulations on a UAV operating within a partially observable sensor network.

Chapter 6 concludes the thesis by summarizing the main contributions and presenting potential directions for future research on resilient and intelligent CPS frameworks.

Chapter 2

Background: Cyber-Attacks in Nonlinear Cyber-Physical Systems (CPS)

In this chapter, essential background concepts relevant to this research are introduced. Section 2.1 presents a categorization of cyber-attacks commonly encountered in Cyber-Physical Systems (CPS), classified based on their nature and operational characteristics. Section 2.2 formulates the nonlinear state estimation problem using the Unscented Kalman Filter (UKF). Section 2.3 explores reinforcement learning-based approaches for online anomaly detection. Finally, Section 2.4 provides an overview of relevant graph-theoretical concepts and topology-switching mechanisms that serve as foundational tools for subsequent chapters on distributed estimation under network constraints and adversarial conditions.

2.1 Cyber-Attack Categorization

Cyber-attacks commonly encountered in CPS can be categorized based on their nature and the operational mechanisms used to compromise system behavior. These categorizations help guide the development of targeted detection and mitigation strategies.

2.1.1 Categorization by Nature of Cyber-Attack

According to the nature of cyber-attacks and the way they manifest in compromised systems, attacks can generally be classified into two main categories: *Denial of Service (DoS)* and *Deception* attacks [126].

DoS Attacks

DoS attacks aim to disrupt or entirely block the flow of information in CPS, often targeting communication channels between sensors, controllers, and actuators. Attackers may jam

signals, flood communication links with illegitimate traffic, or deliberately introduce delays. These actions can cause data loss or result in outdated information being reused (e.g., via zero-input or hold-input strategies), thereby degrading system performance or even leading to instability [127, 128].

Deception Attacks

Deception attacks manipulate legitimate system signals with falsified data to mislead controllers or observers. The attacker alters the integrity of measurements or control inputs without triggering immediate alarms, thereby subtly steering the system toward unsafe or undesirable states. These attacks are more insidious than DoS attacks because they actively undermine system objectives [129, 130]. Variants of deception attacks include replay, false data injection, zero-dynamics, and covert attacks, discussed in the next subsection.

2.1.2 Categorization by Mechanism of Cyber-Attack

Based on operational mechanisms, cyber-attacks in CPS can be categorized into specific strategies. Most of these are variations of FDI attacks, each leveraging different system vulnerabilities to stay undetected while manipulating system behavior.

Replay Attacks

Replay attacks involve capturing legitimate sensor measurements or control commands during normal operation and injecting them back into the system at a later time. Since the data is valid but outdated, replay attacks can bypass many anomaly detectors that assume temporal consistency but lack memory of previously transmitted values. These attacks can destabilize control or estimation processes without introducing obvious anomalies [?, 131]. Defense against replay attacks typically requires cryptographic time-stamping or watermarking.

FDI Attacks

FDI attacks are one of the most studied classes of deception attacks, where adversaries deliberately inject manipulated data into sensor measurements or control inputs to mislead estimators or controllers. The attacker’s goal is often to degrade system performance or cause physical damage. By exploiting model knowledge or measurement noise characteristics, attackers can craft data sequences that circumvent conventional detection schemes [132, 133]. FDI attacks pose a significant threat in critical infrastructures such as power systems and autonomous vehicles.

Zero-Dynamics Attacks (ZDAs)

Zero-dynamics attacks exploit the internal dynamics of a system to introduce undetectable disturbances. Specifically, these attacks construct false data inputs that excite the system's zero dynamics—unobservable modes that do not affect output trajectories under certain conditions. As a result, they can cause state divergence or instability while leaving measurement residuals unchanged, making detection extremely challenging [134–136]. ZDAs require precise system knowledge but are among the most stealthy attack strategies.

Covert Attacks

Covert attacks are designed to manipulate a system while remaining completely hidden from anomaly detectors. Unlike standard FDI or ZDA strategies, covert attacks explicitly account for the detection mechanism and aim to craft input sequences that maintain expected residual statistics. In some cases, attackers introduce decoupled inputs or bias signals that mimic nominal behavior from the detector's perspective [8, 137, 138]. This makes covert attacks particularly dangerous, as they exploit both system dynamics and detector models to remain invisible.

2.2 The Nonlinear State Estimation Problem Based on Unscented Kalman Filter (UKF)

We begin by formulating the general discrete-time nonlinear system used for state estimation:

$$\begin{aligned}x(k+1) &= f(x(k), u(k)) + w(k) \\ y(k) &= h(x(k)) + v(k),\end{aligned}\tag{1}$$

where k denotes the discrete-time index, $x(k) \in \mathbb{R}^n$ is the system state, $u(k) \in \mathbb{R}^p$ is the control input, and $y(k) \in \mathbb{R}^q$ is the measured output. The functions $f : \mathbb{R}^{n \times p} \rightarrow \mathbb{R}^n$ and $h : \mathbb{R}^n \rightarrow \mathbb{R}^q$ are nonlinear mappings. The terms $w(k) \in \mathbb{R}^n$ and $v(k) \in \mathbb{R}^q$ represent process and measurement noise, respectively. These noise terms are modeled as zero-mean, white Gaussian noise with known, time-invariant covariance matrices, and are assumed to be independent.

The objective of the state estimation problem is to recursively estimate $x(k)$ based on the sequence of output measurements $y_1, y_2, \dots, y_k$. In Bayesian terms, this corresponds to computing the posterior probability density function $p(x_k | y_{1:k})$ at each time step, given that the initial distribution $p(x_0 | y_0)$ is known. The estimation process involves two main steps: the prediction step and the update (correction) step.

The Unscented Kalman Filter (UKF) addresses this problem by approximating the distribution of the random variable $x(k)$ by using a set of deterministically selected sigma points. Specifically, the n -dimensional variable $x(k)$, characterized by its mean $\hat{x}(k)$ and covariance $\mathbf{P}(k)$, is represented by $2n + 1$ sigma points as follows:

$$\begin{aligned}
\mathcal{X}_0(k) &= \hat{x}(k) \\
W_0^m &= \frac{\kappa}{n + \kappa} \\
W_0^c &= \frac{\kappa}{n + \kappa} + (1 - \alpha_c^2 + \beta_c) \\
\mathcal{X}_i(k) &= \hat{x}(k) + \left(\sqrt{(n + \kappa)\mathbf{P}(k)} \right)_i, \quad i = 1, \dots, n \\
\mathcal{X}_{i+n}(k) &= \hat{x}(k) - \left(\sqrt{(n + \kappa)\mathbf{P}(k)} \right)_i, \quad i = 1, \dots, n \\
W_i^m &= W_i^c = \frac{1}{2(n + \kappa)}, \quad i = 1, \dots, 2n
\end{aligned} \tag{2}$$

Here, $\kappa \in \mathbb{R}$ is a scaling parameter such that $(n + \kappa) \neq 0$. The constants α_c and β_c determine the spread and higher-order moments of the sigma points around the mean. The term $\left(\sqrt{(n + \kappa)\mathbf{P}(k)} \right)_i$ denotes the i th column of the matrix square root (e.g., obtained via Cholesky decomposition). The sigma points generated by this scheme preserve the mean and covariance of the random variable $x(k)$ [139].

Given the set of sigma points generated by (2), the prediction step of the Unscented Kalman Filter proceeds as follows:

1. Each sigma point is propagated through the process model to yield a set of transformed samples:

$$\mathcal{X}_i(k + 1 | k) = f(\mathcal{X}_i(k), u(k))$$

2. The predicted state mean is computed as:

$$\hat{x}(k + 1 | k) = \sum_{i=0}^{2n} W_i^m \mathcal{X}_i(k + 1 | k)$$

3. The predicted state covariance is computed as:

$$\mathbf{P}(k + 1 | k) = \sum_{i=0}^{2n} W_i^c (\mathcal{X}_i(k + 1 | k) - \hat{x}(k + 1 | k)) (\mathcal{X}_i(k + 1 | k) - \hat{x}(k + 1 | k))^T$$

Compared to the Extended Kalman Filter (EKF), the UKF yields more accurate state predictions in nonlinear systems, as it avoids local linearization and instead preserves higher-order moment information through the unscented transformation. While Particle Filters (PF) are capable of handling a wider class of nonlinear and non-Gaussian systems, their

high computational burden often renders them impractical for real-time implementation, particularly in resource-constrained CPS environments [58]. In contrast, the UKF offers improved estimation accuracy with considerably lower computational complexity than PF, making it a suitable and scalable solution for real-time state estimation and cyber-attack detection in nonlinear CPS.

2.3 Reinforcement Learning-Based Cyber-Attack Detection

Unlike the more conventional branches of machine learning—namely supervised and unsupervised learning, which rely on available data—Reinforcement Learning (RL) enables an agent to learn through direct interaction with the environment. RL is characterized by the concepts of state, action, and reward, as shown in Fig. 2.1. It follows a trial-and-error approach, where the agent selects actions at each time step, resulting in two outcomes: the environment transitions to a new state, and the agent receives a corresponding reward or penalty. The reward serves as feedback that indicates the quality of the action. Over time, the agent learns to favor actions that yield higher rewards while avoiding detrimental ones. This iterative process of interaction between the agent and the environment forms the foundation of RL.

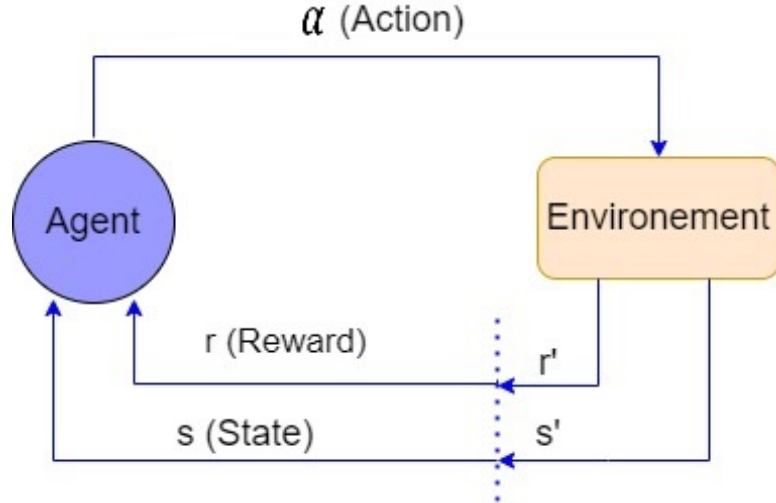


Figure 2.1: Interactions between the agent and its environment in RL, characterized by state, action, and reward.

Before introducing RL-based cyber-attack detection techniques that have been utilized in works such as [140, 141], we briefly review the Partially Observable Markov Decision Process (POMDP), which underpins these methods [142]. A discrete-time POMDP is defined by the tuple $(S, \mathcal{A}, T, \mathcal{R}, \mathcal{O}, \gamma)$, where:

- S is the set of (hidden) environment states,
- $\mathcal{A}$ is the set of possible agent actions,

- T is the state transition function, which defines the probability of transitioning from state s_k to s_{k+1} given action a_k ,
- $\mathcal{R} : S \times \mathcal{A} \rightarrow \mathbb{R}$ is the reward function mapping state-action pairs to rewards,
- $\mathcal{O}$ is the set of possible observations perceived by the agent, and
- $\gamma \in [0, 1]$ is the discount factor that determines the relative importance of immediate versus future rewards.

At each time step k , the environment is in a hidden state $s(k) \in S$, and the agent receives an observation $o(k) \in \mathcal{O}$, which depends probabilistically on $s(k)$. The agent then selects an action $a(k) \in \mathcal{A}$ and receives a reward $r(k) = \mathcal{R}(s(k), a(k))$ based on its action and the current state. Simultaneously, the environment transitions to a new state $s(k+1)$. This process repeats until a terminal state is reached. The goal of the agent is to determine an optimal policy $\pi : \mathcal{O} \rightarrow \mathcal{A}$ that maximizes the expected total discounted reward over time.

In RL-based cyber-attack detection frameworks, the underlying physical or cyber-physical system—whether modeled explicitly by a state-space representation or treated as a black box—is commonly considered as the environment, while the agent is tasked with learning to detect anomalies or cyber-attacks. The agent interacts with the system by receiving a sequence of observations (e.g., measurements, estimation errors, or statistical features), which it uses to infer the likelihood of malicious behavior. The goal of the agent is to learn a decision-making policy typically by maximizing a reward function that penalizes incorrect detection outcomes.

Depending on the availability and quality of observations, the RL formulation may rely on raw measurement data, state estimates from observers or filters, or latent feature representations learned through auxiliary models. After a sufficient training phase—often via simulation or historical attack data—the agent learns to issue alerts when anomalies are suspected. Studies, such as [143, 144], have demonstrated that such RL-based detectors can adapt to dynamic environments and uncover subtle attack patterns, making them a promising direction for resilient and adaptive anomaly detection in CPS.

2.4 Graph Theory and Topology Switching

This section provides an overview of key graph-theoretical concepts and topology-switching mechanisms that form the foundation for enhancing cybersecurity in distributed state estimation systems. A directed graph $\mathcal{G}(k) = \mathcal{G}(\mathcal{V}(k), \mathcal{E}(k))$ is used to represent the communication topology of a large-scale sensor network at time instant k , where $\mathcal{V}(k)$ denotes the set of vertices representing the local sensor nodes and $\mathcal{E}(k) \subseteq \mathcal{V}(k) \times \mathcal{V}(k)$ denotes the set of directed edges representing the communication links between nodes. We

assume that the communication topology is time-varying. Let $\mathcal{G}(k) = \{\mathcal{G}^1, \mathcal{G}^2, \dots, \mathcal{G}^{n_{\mathcal{G}}}\}$, with $n_{\mathcal{G}} \geq 1$, denote the set of all possible directed topologies. The switching signal $\sigma(k)$ is defined as a mapping $\sigma(k) : \{0, +\infty\} \rightarrow \{1, 2, \dots, n_{\mathcal{G}}\}$, where $0 = k_0 < k_1 < k_2 < \dots$ denote the switching instants. The communication topology at the switching instants is represented as $\mathcal{G}^{\sigma(k)}(\mathcal{V}^{\sigma(k)}, \mathcal{E}^{\sigma(k)}) \in \mathcal{G}(k)$, and for simplicity, it will be denoted as $\mathcal{G}^{\sigma(k)}$ unless otherwise specified. During each interval between consecutive switching instants, the topology remains fixed and corresponds to the graph $\mathcal{G}^{\sigma(k)}$.

An edge $ij \in \mathcal{E}(k)$ indicates that the node j can receive information from the node i at the time instant k , though this does not imply the reverse direction (i.e., i may not receive information from j). The sets of *in-neighbors* and *out-neighbors* of node i at the switching instant $\sigma(k)$ are defined by $N_{i,\text{in}}^{\sigma(k)} \triangleq \{j \mid ji \in \mathcal{E}^{\sigma(k)}, \forall j \neq i\}$, and $N_{i,\text{out}}^{\sigma(k)} \triangleq \{j \mid ij \in \mathcal{E}^{\sigma(k)}, \forall j \neq i\}$, respectively.

A *directed path* from the vertex i_0 to the vertex i_ℓ is defined as an ordered sequence of vertices $i_0, i_1, \dots, i_\ell$ such that $(i_{j-1}, i_j) \in \mathcal{E}(k)$ for $1 \leq j \leq \ell$. A graph $\mathcal{G}(k)$ is said to be *strongly connected* if there exists a directed path from every vertex to every other vertex in the graph. A *subgraph* of $\mathcal{G}(k)$, denoted by $\tilde{\mathcal{G}}(\tilde{\mathcal{V}}(k), \tilde{\mathcal{E}}(k))$, is a graph such that $\tilde{\mathcal{V}}(k) \subseteq \mathcal{V}(k)$ and $\tilde{\mathcal{E}}(k) \subseteq \mathcal{E}(k)$. When considering a subgraph under switching, it is represented by $\tilde{\mathcal{G}}^{\sigma(k)}(\tilde{\mathcal{V}}^{\sigma(k)}, \tilde{\mathcal{E}}^{\sigma(k)})$ or simply $\tilde{\mathcal{G}}^{\sigma(k)}$.

For a directed graph $\mathcal{G}(k)$, an associated *stochastic matrix* $\mathbf{D}(k) \in \mathbb{R}^{n \times n}$ is defined such that $\{\mathbf{D}(k)\}_{ij} > 0$ if $j \in J_i^{\sigma(k)}$, and $\{\mathbf{D}(k)\}_{ij} = 0$, otherwise. Additionally, the matrix is row stochastic, implying that for each $i \in \mathcal{V}(k)$, the condition $\sum_{j \in \mathcal{V}(k)} \{\mathbf{D}(k)\}_{ij} = 1$ holds, ensuring that each row sums up to 1.

A matrix is said to be *row stochastic* if each of its rows sums up to 1, and all its entries are non-negative. A row stochastic matrix is *primitive* if and only if the associated graph is strongly connected. If $\mathbf{A}$ is a primitive row stochastic matrix, the left eigenvector associated with the eigenvalue 1 (denoted by $\boldsymbol{\rho}$) has strictly positive entries, that is $\boldsymbol{\rho}^\top \mathbf{A} = \boldsymbol{\rho} > 0$ [145].

Chapter 3

Cyber-Attack and Fault Detection and Isolation of Sensors and Actuators in Nonlinear Cyber-Physical Systems

In this chapter, we address the challenges posed by discrete-time nonlinear Cyber-Physical Systems (CPS) operating under the influence of system faults, adversarial false data injection (FDI) attacks on both sensor and actuator networks, and the inevitable presence of process and measurement noise. We propose an integrated and robust framework aimed at enhancing the security, detection, and isolation capabilities of such systems. The approach is particularly relevant in environments where data is exchanged between sensors, controllers, and the plant—communication pathways that are susceptible to malicious intrusions. It is assumed that adversaries are capable of injecting falsified data into these communication links, prompting the need for distributed detection mechanisms on both the command and control (C&C) and plant sides.

To this end, the proposed method employs an augmented unscented Kalman filter (AUKF) for simultaneous estimation of system states and faults in nonlinear CPS. This framework includes a rigorous stability analysis of the estimation dynamics and addresses the crucial problem of distinguishing between system faults and cyber-attacks. Detection modules at the C&C center are used to identify anomalies in measurement channels, while auxiliary filters are introduced to detect and isolate actuator-side cyber-attacks. The performance and effectiveness of the proposed framework are validated through extensive simulations using both a fixed-base inverted pendulum and a high-fidelity unmanned aerial vehicle (UAV) model, demonstrating its ability to accurately detect and isolate faults, FDI threats, and covert attacks.

The main contributions of this chapter are as follows:

- (i) We address the complex challenges encountered in nonlinear CPS, including the presence of process and measurement noise, machine-induced faults, and vulnerabilities to false data injection (FDI) attacks targeting both sensor and actuator communication networks.
- (ii) We propose an Augmented Unscented Kalman Filter (AUKF) for joint state and fault estimation, and provide a formal stability analysis demonstrating the boundedness of estimation errors in nonlinear CPS.
- (iii) We develop and implement detection and isolation mechanisms for sensor cyber-attacks at the command and control (C&C) center.
- (iv) We design an auxiliary filter for actuator-side cyber-attack detection and establish its effectiveness through a rigorous design methodology and supporting simulation studies.
- (v) We demonstrate the ability to distinguish between the effects of faults and cyber-attacks by leveraging fault estimation via the AUKF, enabling robust cyber-attack detection even in the presence of system faults.
- (vi) We validate the proposed framework through comprehensive case studies involving a fixed-base inverted pendulum and a high-fidelity unmanned aerial vehicle (UAV), subject to various faults, FDI, and covert attacks.

The remainder of the chapter is organized as follows. Section 3.1 presents the mathematical modeling of the nonlinear CPS under cyber-attacks and faults, setting the stage for estimation and detection strategies. In Section 3.2, an AUKF is developed to jointly estimate system states and faults, and the stability of the estimation process is analyzed. Section 3.3 introduces a structured approach to detect and isolate both sensor faults and sensor-targeted cyber-attacks. The following section focuses on actuator-targeted cyber-attacks and proposes auxiliary filter-based detection mechanisms. Section 3.5 extends the auxiliary filter approach to distinguish between sensor and actuator cyber-attacks in the absence of physical faults. To validate the effectiveness of the proposed cyber-attack and fault detection and isolation framework, Section 3.6 presents detailed simulation results on a UAV system subjected to various cyber-attack and fault scenarios.

3.1 Problem Statement and Formulation

In this section, we present the mathematical formulation of the nonlinear CPS under consideration. The discrete-time nonlinear CPS dynamics, incorporating both system faults and stochastic disturbances, are described by the following equations:

$$\begin{aligned}
x(k+1) &= f(x(k)) + g(x(k))u^*(k) + \mathcal{L}_1(x(k))\theta(k) + w(k), \\
y(k) &= h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + v(k),
\end{aligned} \tag{3}$$

where $k \in \mathbb{Z}^{\geq 0}$ denotes the discrete time index. The vector $x(k) \in \mathbb{R}^n$ is the system state, $u^*(k) \in \mathbb{R}^p$ denotes the control input received at the plant, and $y(k) \in \mathbb{R}^m$ represents the system output measurement. The functions $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, $g : \mathbb{R}^n \rightarrow \mathbb{R}^{n \times p}$, and $h : \mathbb{R}^n \rightarrow \mathbb{R}^m$ are assumed to be continuously differentiable nonlinear functions that govern the nominal system dynamics, input mapping, and output equation, respectively. The term $\theta(k) \in \mathbb{R}^{n_\theta}$ denotes the fault vector, which aggregates plant, actuator, and sensor faults.

The mappings $\mathcal{L}_1 : \mathbb{R}^n \rightarrow \mathbb{R}^{n \times n_\theta}$ and $\mathcal{L}_2 : \mathbb{R}^n \rightarrow \mathbb{R}^{m \times n_\theta}$ are nonlinear matrix-valued functions that characterize how individual components of the fault vector $\theta(k)$ influence the system state and output, respectively. These functions encode the fault structure and its dependence on the current state, thereby enabling selective fault injection into the dynamics and measurements. The process noise $w(k) \in \mathbb{R}^n$ and measurement noise $v(k) \in \mathbb{R}^m$ are modeled as zero-mean, independent white Gaussian noise sequences with known covariance matrices Q and R , respectively. Throughout this study, it is assumed that both the system states and the fault vector are observable based on the available measurements, which ensures the feasibility of joint state and fault estimation.

The control input for the plant and output of the CPS on the command and control (C&C) side, subject to cyber-attacks on the communication networks between the actuators and sensors, are expressed as follows:

$$\begin{aligned}
u^A(k) &= u^*(k) = u(k) + B^A A^u(k) \\
y^A(k) &= h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + D^A A^y(k) + v(k),
\end{aligned} \tag{4}$$

where $u(k)$ represents the control signal or reference signal generated on the C&C side, while $u^A(k) \in \mathbb{R}^p$ and $y^A(k) \in \mathbb{R}^m$ denote the control input received at the plant side and the outputs received at the C&C side, respectively. The signals $A^u(k) \in \mathbb{R}^{p_A}$ and $A^y(k) \in \mathbb{R}^{m_A}$ represent the cyber-attack signals, and the matrices B^A and D^A describe the actuator and sensor cyber-attack signatures, respectively. It is important to note that the signals $A^u(k)$ and $A^y(k)$ can be arbitrarily manipulated by a malicious adversary.

The presence of the network layer allows for observation of the CPS from both the plant and the C&C sides. The architecture of the CPS, along with the concept of observing it from both sides, is visually represented in Figure 3.1. In this figure, one can observe the inclusion of various components on the C&C and plant sides. Furthermore, communication networks are depicted in the diagram, illustrating communication channels between the controller, actuator, sensors, estimators, and auxiliary filters, each susceptible to cyber-attacks. In the

subsequent sections, we will provide specifics of these modules and their functionalities.

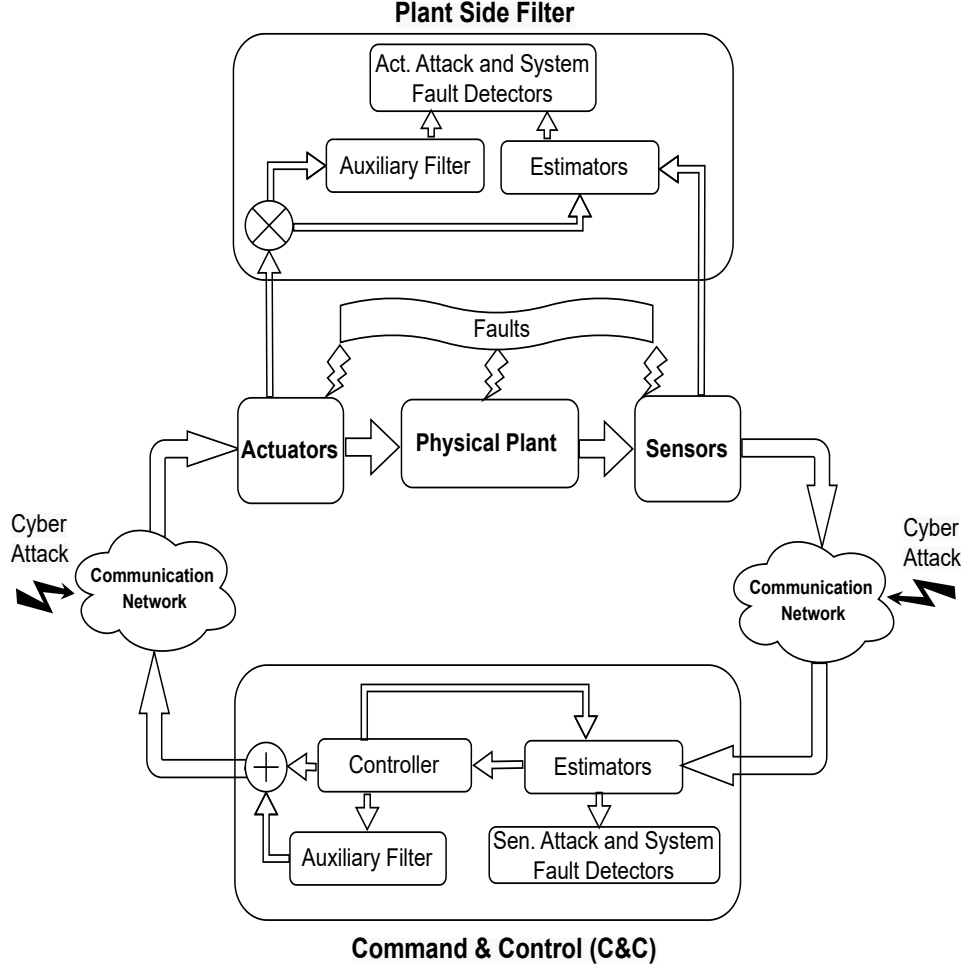


Figure 3.1: The CPS under faults and FDI attacks with the C&C and the plant side filters and detectors.

3.2 State and Fault Estimation Using Augmented Unscented Kalman Filters

To develop our methodology in the subsequent sections, we assume only the communication networks are vulnerable to be compromised and subject to cyber-attacks by malicious adversaries. Consequently, on the C&C side, we maintain access to the control signal denoted as $u(k)$. Additionally, all potential possible fault dynamics are assumed to be known *a priori* given the knowledge that one has regarding CPS sensors and actuators sources of fault characteristics, however their time of occurrence remains unknown. Given the fault properties and the fact that they stem from system anomalies and defects, this is a reasonable assumption that is also considered in notable works such as [146, 147]. Therefore,

the fault dynamics are described as follows:

$$\theta(k+1) = \theta(k) + f_\theta(x(k), \theta(k)), \quad (5)$$

where $f_\theta : \mathbb{R}^{n \times n_\theta} \rightarrow \mathbb{R}^{n_\theta}$ is a nonlinear differentiable function. However, the precise timing of fault occurrences is assumed to be unknown.

Therefore, one can consider the fault as an additional component of the system state. By augmenting the state variables of the system and the fault states into a single state vector, that is denoted as $X(k) = [x^T(k); \theta^T(k)]^T \in \mathbb{R}^N$, where $N = n + n_\theta$, one can rewrite the augmented state vector and the dynamics (3) as follows:

$$\begin{aligned} X(k+1) &= F(X(k)) + G(X(k))u^*(k) + \mathcal{W}(k) \\ y(k) &= H(X(k)) + v(k), \end{aligned} \quad (6)$$

where,

$$\begin{aligned} F(X(k)) &= \begin{bmatrix} f(x) + \mathcal{L}_1(x(k))\theta(k) \\ f_\theta(\theta(k), x(k)) + \theta(k) \end{bmatrix} \\ H(X(k)) &= h(x(k)) + \mathcal{L}_2(x(k))\theta(k) \\ G(X(k)) &= \begin{bmatrix} g(x(k)) \\ 0 \end{bmatrix} \end{aligned}$$

$$\mathcal{W}(k) = \begin{bmatrix} w(k) \\ 0 \end{bmatrix}.$$

The above representations allow us to treat the fault as an integral part of the augmented state vector and express the overall system dynamics accordingly.

Furthermore, the Unscented Transform (UT) [139] offers a numerical methodology that directly approximates the mean and covariance of the target distribution, in contrast to approximating the nonlinear function itself. This transformation utilizes sigma points, that are introduced in [148]. Transitioning to the objective of the estimation problem, this now involves the recursive estimation of system states based on output measurements. Following Bayes' theory, the recursive computation of state estimation at time k takes into account measurements up to time k . Unlike the standard UKF, which is focused on system state estimation, our proposed design extends its functionality to include fault estimation as well. This enhanced capability provides a more comprehensive understanding of system behavior. Furthermore, the AUKF is developed within the framework of nonlinear CPS, accompanied by a detailed stability analysis to ensure the robustness of the proposed method. This foundation supports the effectiveness of the proposed sensor cyber-attack and fault detection

and isolation approach, which will be introduced in the Section 3.3.

3.2.1 Command and Control (C&C) Side Filter

The CPS's states on the C&C side are estimated by the dynamic model (6) and the received signal $y^A(k)$, as represented in (4). In this section, we introduce the augmented uncensored Kalman filter (AUKF) scheme for fault and state estimation within the C&C of the CPS.

(1) Sigma Points Generation

First, the N -dimensional random variable $X(k)$ with mean $\bar{X}(k)$ and covariance $\mathbf{P}(k)$ is approximated by sigma points $\mathcal{X}_i(k)$ for $i = 1, \dots, N$, selected using the following equations:

$$\begin{aligned}\mathcal{X}_0(k) &= \bar{X}(k) \\ W_0^M &= \kappa/(N + \kappa) \\ W_0^c &= \kappa/(N + \kappa) + (1 - \alpha_c^2 + \beta_c) \\ \mathcal{X}_i(k) &= \bar{X}(k) + (\sqrt{(N + \kappa)\mathbf{P}(k)})_i \\ W_i &= 1/(2(N + \kappa)) \\ \mathcal{X}_{i+N}(k) &= \bar{X}(k) - (\sqrt{(N + \kappa)\mathbf{P}(k)})_i \\ W_{i+N} &= 1/(2(N + \kappa)),\end{aligned}\tag{7}$$

where $\kappa \in \mathbb{R}$ can be any number provided that $(N + \kappa) \neq 0$. The constants α_c and β_c determine the spread of the sigma points around the mean value, and $(\sqrt{(N + \kappa)\mathbf{P}(k)})_i$ denotes the i th column of the matrix square root of $(N + \kappa)\mathbf{P}(k)$. Also W_i , with different initial conditions W_0^M and W_0^c , denotes the weight associated with the i th point. The set of samples chosen using (7) has the same sample mean and covariance as the distribution of $X(k)$ [139].

(2) Propagation of the Sigma Points and Prediction

The sigma points presented in (7) are then propagated through the system dynamics:

$$\mathcal{X}_i^{CC}(k+1|k) = F(\mathcal{X}_i^{CC}(k)) + G(\mathcal{X}_i^{CC}(k))u(k),\tag{8}$$

where $\mathcal{X}_i^{CC}(k+1|k)$ denote the propagated sigma points. Here, and for other variables, the subscript CC indicates that the corresponding variable belongs to the C&C side. Given $Q(k)$, which denotes the covariance of the process noise, the prior state estimate $\hat{X}^{CC}(k+1|k)$, covariance estimate $\hat{\mathbf{P}}_X^{CC}(k+1|k)$, output propagated sigma points $\mathcal{X}_i^{CC}(k|k-1)$, and output estimate $\hat{y}^{CC}(k|k-1)$ are computed as follows:

$$\hat{X}^{CC}(k+1|k) = \sum_{i=0}^{2N} W_i^M \mathcal{X}_i^{CC}(k+1|k)\tag{9}$$

$$\begin{aligned}\hat{\mathbf{P}}_X^{CC}(k+1|k) &= \sum_{i=0}^{2N} W_i^c (\mathcal{X}_i^{CC}(k+1|k) - \hat{X}^{CC}(k+1|k)) \\ &\times (\mathcal{X}_i^{CC}(k+1|k) - \hat{X}^{CC}(k+1|k))^T + Q(k),\end{aligned}$$

$$\begin{aligned}\mathcal{Y}_i^{CC}(k|k-1) &= H(\mathcal{X}_i^{CC}(k|k-1)) \\ \hat{y}^{CC}(k|k-1) &= \sum_{i=0}^{2N} W_i^M \mathcal{Y}_i^{CC}(k|k-1).\end{aligned}\tag{10}$$

(3) Measurement Update

In the next step, we determine the measurement and cross-covariance matrices, denoted by $\hat{\mathbf{P}}_y^{CC}(k)$ and $\hat{\mathbf{P}}_{Xy}^{CC}(k+1)$, respectively, along with the Kalman filter gain vector $K^{CC}(k+1)$. Here, $R(k)$ denotes the covariance of the measurement noise. The computations required are as follows:

$$\begin{aligned}\hat{\mathbf{P}}_y^{CC}(k) &= \sum_{i=0}^{2N} W_i^c (\mathcal{Y}_i^{CC}(k|k-1) - \hat{y}^{CC}(k|k-1)) \\ &\times (\mathcal{Y}_i^{CC}(k|k-1) - \hat{y}^{CC}(k|k-1))^T + R(k),\end{aligned}\tag{11}$$

$$\begin{aligned}\hat{\mathbf{P}}_{Xy}^{CC}(k+1) &= \sum_{i=0}^{2n} W_i^c (\mathcal{X}_i^{CC}(k+1|k) - \hat{X}^{CC}(k+1|k)) \\ &\times (\mathcal{Y}_i^{CC}(k|k-1) - \hat{y}^{CC}(k|k-1))^T,\end{aligned}\tag{12}$$

$$K^{CC}(k+1) = \hat{\mathbf{P}}_{Xy}^{CC}(k+1) \hat{\mathbf{P}}_y^{CC}(k)^{-1}.\tag{13}$$

(4) Estimation

We compute estimates of the system states, outputs, and covariances, denoted by, $\hat{X}^{CC}(k+1)$, $\hat{y}^{CC}(k)$, and $\hat{\mathbf{P}}_X^{CC}(k+1)$, respectively, as follows:

$$\begin{aligned}\hat{X}^{CC}(k+1) &= \hat{X}^{CC}(k+1|k) + K^{CC}(k+1)(y^A(k) \\ &- \hat{y}^{CC}(k|k-1)),\end{aligned}\tag{14}$$

$$\hat{y}^{CC}(k) = H(\hat{X}^{CC}(k|k-1)),\tag{15}$$

$$\begin{aligned}\hat{\mathbf{P}}_X^{CC}(k+1) &= \hat{\mathbf{P}}_X^{CC}(k+1|k) \\ &- \hat{\mathbf{P}}_{Xy}^{CC}(k+1)\hat{\mathbf{P}}_y^{CC}(k)^{-1}\hat{\mathbf{P}}_{Xy}^{CC}(k+1)^T.\end{aligned}\tag{16}$$

3.2.2 Plant Side Filter

On the plant side, sensor measurements are taken before injection of sensor cyber-attacks. Consequently, the output of the CPS on this side can be expressed as follows:

$$y(k) = h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + v(k).\tag{17}$$

Furthermore, on the plant side, access is available to the potentially manipulated control signal $u^A(k) = u(k) + B^A A^u(k)$. Given the augmented state vector $X(k) = [x^T(k); \theta^T(k)]^T$ in the AUKF, the sigma points are propagated by using the following expression:

$$\mathcal{X}_i^p(k+1|k) = F(\mathcal{X}_i^p(k)) + G(\mathcal{X}_i^p(k))(u(k) + B^A A^u(k)),\tag{18}$$

where $\mathcal{X}_i^p(k)$ is obtained based on (7), and the index p denotes the corresponding variable on the plant side. In a manner similar to the C&C filter, the proposed filter on the plant side is expressed in the following form:

$$\hat{X}^p(k+1) = \hat{X}^p(k+1|k) + K^p(k+1)(y(k) - \hat{y}^p(k|k-1)),\tag{19}$$

$$\hat{y}^p(k) = H(\hat{X}^p(k|k-1)),\tag{20}$$

$$\hat{\mathbf{P}}_X^p(k+1) = \hat{\mathbf{P}}_X^p(k+1|k) - \hat{\mathbf{P}}_{Xy}^p(k+1)\hat{\mathbf{P}}_y^p(k)^{-1}\hat{\mathbf{P}}_{Xy}^p(k+1)^T.\tag{21}$$

3.2.3 Stability of the AUKF

In this section, we demonstrate stability of the state and fault estimations obtained through the AUKF in terms of the boundedness of the estimation errors, provided that the following assumption holds:

Assumption 3.1. *The sensor and actuator communication networks are not compromised by any cyber-attack.*

It should be noted that this assumption is made in order to show the boundedness of state and fault estimation in absence of cyber-attacks, and will be relaxed after Theorem 3.1 for cyber-attack detection and isolation.

Lemma 3.1. *For the CPS system described by (6) under Assumption 3.1, and based on the proposed AUKF algorithm, the state estimation error, prior state estimation error, and prior output estimation error are defined as follows: $\tilde{X}(k) = X(k) - \hat{X}(k)$, $\tilde{X}(k|k-1) = X(k) - \hat{X}(k|k-1)$, and $\tilde{y}(k|k-1) = y(k) - \hat{y}(k|k-1)$ respectively, where $\hat{X}$ and $\hat{y}$ can represent either $\hat{X}^{CC}$ and $\hat{y}^{CC}$ or $\hat{X}^p$ and $\hat{y}^p$. Then, the following hold:*

$$\tilde{X}(k+1|k) = \alpha(k)\mathcal{F}(k)\tilde{X}(k) + \mathcal{W}(k), \quad (22)$$

$$\tilde{y}(k|k-1) = \beta(k)\mathcal{H}(k)\tilde{X}(k|k-1) + v(k), \quad (23)$$

where $\alpha(k)$ and $\beta(k)$ are unknown diagonal matrices, and $\mathcal{F}(k) = \frac{\partial F}{\partial X}|_{X=\hat{X}(k)} + \frac{\partial G}{\partial X}|_{X=\hat{X}(k)}u(k)$ and $\mathcal{H}(k) = \frac{\partial H}{\partial X}|_{X=\hat{X}(k|k-1)}$.

Proof: Expanding $X(k+1)$ and $y(k)$ by using a Taylor series about $\hat{X}(k)$ yields:

$$\begin{aligned} X(k+1) &= F(\hat{X}(k)) + G(\hat{X}(k))u + \nabla(F(\hat{X}(k))) \\ &\quad + G(\hat{X}(k))u\tilde{X}(k) \\ &\quad + \frac{1}{2}\nabla^2(F(\hat{X}(k)) + G(\hat{X}(k))u)\tilde{X}^2(k) \\ &\quad + \dots + \mathcal{W}(k) \end{aligned} \quad (24)$$

$$\begin{aligned} y(k) &= H(\hat{X}(k)) \\ &\quad + \nabla H(\hat{X}(k))\tilde{X}(k) + \dots + v(k) \end{aligned} \quad (25)$$

On the other hand, by expanding $\hat{X}(k+1|k)$, as given in (9), using a Taylor series yields:

$$\begin{aligned} \hat{X}^{CC}(k+1|k) &= \frac{\kappa}{n+\kappa} \left(F(\hat{X}(k)) + G(\hat{X}(k))u \right) \\ &\quad + \frac{1}{2(N+\kappa)} \left(\sum_{i=0}^N F(\underbrace{(\hat{X}(k) + (\sqrt{(N+\kappa)\mathbf{P}(k)})_i)}_{arg_1}) \right. \\ &\quad \left. + G(arg_1)u + \sum_{i=N+1}^{2N} F(\underbrace{\hat{X}(k) - (\sqrt{(N+\kappa)\mathbf{P}(k)})_i}_{arg_2}) \right. \\ &\quad \left. + G(arg_2)u \right) = F(\hat{X}(k)) + G(\hat{X}(k))u \\ &\quad + \frac{1}{2}\nabla^2(F(\hat{X}(k)) + G(\hat{X}(k))u)\mathbf{P}(k) + \dots \end{aligned} \quad (26)$$

Substituting (24) and (26) into the prior state estimation error results in an approximate representation:

$$\tilde{X}(k+1|k) \approx \mathcal{F}(k)\tilde{X}(k) + \mathcal{W}(k). \quad (27)$$

Note that after removing the common terms, only the first term is shown in (27), and it is evident that there will always be residuals in the prior state estimation error. To account for these residuals and achieve exact equality, we introduce an unknown diagonal matrix that is denoted by $\alpha(k)$, such that

$$\tilde{X}(k+1|k) = \alpha(k)\mathcal{F}(k)\tilde{X}(k) + \mathcal{W}(k) \quad (28)$$

As for the prior output estimation error, following a similar approach, by substituting (25) in the output estimation error along with the expanded (10), and considering the diagonal matrix $\beta(k)$, one can obtain

$$\tilde{y}(k|k-1) = \beta(k)\mathcal{H}(k)\tilde{X}(k|k-1) + v(k). \quad (29)$$

This completes the proof of the lemma ■

Theorem 3.1. *Consider the nonlinear CPS described by (6). Let Assumption 3.1 hold, along with the following additional assumptions:*

- (1) *There exist real numbers $f_{min}, f_{max}, h_{min}, h_{max}, \alpha_{min}, \alpha_{max}, \beta_{min}, \beta_{max} \neq 0$ such that the following bounds on various matrices are satisfied for every $k \geq 0$, namely*

$$\begin{aligned} f_{min}^2 I &\leq \mathcal{F}(k)\mathcal{F}^T(k) \leq f_{max}^2 I \\ h_{min}^2 I &\leq \mathcal{H}(k)\mathcal{H}^T(k) \leq h_{max}^2 I \\ \alpha_{min}^2 I &\leq \alpha(k)\alpha^T(k) \leq \alpha_{max}^2 I \\ \beta_{min}^2 I &\leq \beta(k)\beta^T(k) \leq \beta_{max}^2 I \end{aligned} \quad (30)$$

- (2) *There are real numbers $p_{min}, p_{max}, q_{min}, q_{max}, r_{min}, r_{max}, \hat{q}, \hat{r}, \bar{\phi} \neq 0$ such that the following bounds are fulfilled,*

$$\begin{aligned} P_{min} I &\leq \hat{\mathbf{P}}_X(k+1) \leq p_{max} I \\ q_{min} I &\leq Q(k) \leq q_{max} I \\ \hat{q} I &\leq \hat{Q}(k+1) \\ r_{min} I &\leq R(k+1) \leq r_{max} I \\ \hat{r} I &\leq \hat{R}(k+1) \\ ||\phi(k)|| &< \bar{\phi} \end{aligned} \quad (31)$$

It now follows that the state and fault estimate error, $\tilde{X}(k) = X(k) - \hat{X}(k)$, and the prior output estimate error, defined as $\tilde{y}(k|k-1) = y(k) - \hat{y}(k|k-1)$ —where $\hat{X}(k)$ and $\hat{y}(k|k-1)$ represent filter estimate values from either the C&C side or the plant side—remain ultimately bounded in the mean square sense.

Proof: We choose the Lyapunov function candidate as follows:

$$V(\tilde{X}(k)) = \tilde{X}(k)^T (\hat{\mathbf{P}}_X(k))^{-1} \tilde{X}(k). \quad (32)$$

According to the conditions (30) and (31), we have

$$\frac{1}{P_{max}} \|\tilde{X}(k+1)\|^2 \leq V(\tilde{X}(k+1)) \leq \frac{1}{P_{min}} \|\tilde{X}(k+1)\|^2. \quad (33)$$

In the following, to ensure boundedness of $\tilde{X}$ as a stochastic variable, we need to compute $\hat{\mathbf{P}}_X(k+1)$. Taking into account the results of Lemma 3.1, the prior estimation error covariance matrix of the AUKF is denoted by $\mathbf{P}_X(k+1|k)$ and is computed as follows:

$$\begin{aligned} \mathbf{P}_X(k+1|k) &= E[\tilde{X}(k+1|k)\tilde{X}^T(k+1|k)] \\ &= E[(\alpha(k)\mathcal{F}(k)\tilde{X}(k) + \mathcal{W}(k)) \\ &\quad \times (\alpha(k)\mathcal{F}(k)\tilde{X}(k) + \mathcal{W}(k))^T] \\ &= \alpha(k)\mathcal{F}(k)\hat{\mathbf{P}}_X(k|k-1)\mathcal{F}^T(k)\alpha(k) \\ &\quad + \Delta\mathbf{P}_X(k+1) + Q(k). \end{aligned} \quad (34)$$

Let us define $\delta\mathbf{P}_X(k+1|k) = \hat{\mathbf{P}}_X(k+1|k) - \mathbf{P}_X(k+1|k)$, so that we can express $\hat{\mathbf{P}}_X(k+1|k)$ as follows:

$$\begin{aligned} \hat{\mathbf{P}}_X(k+1|k) &= \alpha(k)\mathcal{F}(k)\hat{\mathbf{P}}_X(k|k-1)\mathcal{F}^T(k)\alpha(k) \\ &\quad + \hat{Q}(k+1) \end{aligned} \quad (35)$$

where $\hat{Q}(k+1)$ is defined as:

$$\hat{Q}(k+1) = Q(k) + \Delta\mathbf{P}_X(k+1) + \delta\mathbf{P}_X(k+1|k) \quad (36)$$

and is guaranteed to be positive definite. Similarly, the following covariances are obtained:

$$\begin{aligned} \hat{\mathbf{P}}_{Xy}(k+1) &= \hat{\mathbf{P}}_X(k+1|k)(\beta(k)\mathcal{H}(k))^T \\ &\quad + \Delta\mathbf{P}_{Xy}(k+1) + \delta\mathbf{P}_{Xy}(k+1|k), \end{aligned} \quad (37)$$

and

$$\begin{aligned}\hat{\mathbf{P}}_y(k) &= \beta(k)\mathcal{H}(k)\hat{\mathbf{P}}_X(k|k-1)(\beta(k)\mathcal{H}(k))^T \\ &\quad + \hat{R}(k)\end{aligned}\tag{38}$$

where $\hat{R}(k)$ is defined as:

$$\hat{R}(k) = R(k) + \Delta\mathbf{P}_y(k) + \delta\mathbf{P}_y(k|k-1).\tag{39}$$

we now utilize the stochastic matrix $\Phi(k+1) \in \mathbb{R}^n$ introduced in [149]. To ensure that $\hat{\mathbf{P}}_{Xy}(k+1) = \hat{\mathbf{P}}_X(k+1|k)\Phi(k+1)(\beta(k)\mathcal{H}(k))^T$ where by utilizing the expression from (16), we can write:

$$\begin{aligned}\hat{\mathbf{P}}_X(k+1) &= \hat{\mathbf{P}}_X(k+1|k) \\ &\quad - \hat{K}(k+1)(\hat{\mathbf{P}}_X(k+1|k)\Phi(k+1)\mathcal{H}^T(k)\beta(k))^T,\end{aligned}\tag{40}$$

where,

$$\begin{aligned}\hat{K}(k+1) &= \hat{\mathbf{P}}_{Xy}(k+1)\hat{\mathbf{P}}_y^{-1}(k) \\ &= \hat{\mathbf{P}}_X(k+1|k)\Phi(k+1)\mathcal{H}^T(k)\beta(k) \\ &\quad \times [(\beta(k)\mathcal{H}(k))\hat{\mathbf{P}}_X(k+1|k)\beta(k)\mathcal{H}(k))^T \\ &\quad + \hat{R}(k)]^{-1}.\end{aligned}\tag{41}$$

Based on (14), one can obtain:

$$\begin{aligned}\tilde{X}(k+1) &= X(k+1) - (\hat{X}(k+1|k) + K(k+1)\tilde{y}(k|k-1)) \\ &= \tilde{X}(k+1|k) - K(k+1)\tilde{y}(k|k-1).\end{aligned}\tag{42}$$

The conditions outlined above are in line with those presented in [150], which were initially designed for nonlinear systems with linear output. By substituting the relevant quantities into the expression for $V(\tilde{X}(k+1))$, in a manner similar to the approach used in [150], and drawing upon established theorems related to the boundedness of stochastic processes [151], we can derive the following expression.

$$E[V(\tilde{X}(k+1)) - V(\tilde{X}(k))] \leq \mu - \lambda V(\tilde{X}(k)),\tag{43}$$

where $\mu > 0$ and $0 < \lambda \leq 1$ are given by:

$$\begin{aligned}
\lambda &= p_{min}(h_{min}\beta_{min}f_{min})^2[p_{max}(h_{max}\beta_{max}f_{max})^2 \\
&\quad + \hat{q}_{max}h_{max}^2 + r_{max}]^{-1} \\
\mu &= \frac{q_{max}}{\hat{q}_{min}}.n + \frac{h_{max}^2 p_{max}}{r_{min}}.m
\end{aligned} \tag{44}$$

This leads to the following inequality that:

$$\begin{aligned}
E\{\|\tilde{X}(k)\|^2\} &\leq \frac{P_{max}}{P_{min}}E\{\|\tilde{X}(0)\|^2\}(1-\lambda)^k \\
&\quad + \frac{\mu}{P_{min}} \sum_{i=1}^{k-1} (1-\lambda)^i
\end{aligned} \tag{45}$$

Regarding the prior output estimate error, it has been established that $\tilde{X}(k)$ is ultimately bounded; therefore, $\tilde{X}(k|k-1)$ is ultimately bounded as well. By applying Lemma 3.1 and equation (29), it follows that the prior output estimation error $\tilde{y}(k|k-1)$ remains ultimately bounded in the absence of cyberattacks. This concludes the proof of the theorem. ■

3.3 Sensor Cyber-attack and System Fault Detection and Isolation

A conventional approach to anomaly detection involves using an estimator to predict and estimate the system's output, followed by a comparison with the actual measurement. To demonstrate the estimation capability of the proposed filter in absence of cyber-attacks, earlier we have introduced Assumption 3.1. However, from this point onward, we relax this assumption. Our primary objective is to reliably detect and isolate sensor cyber-attacks and faults within the C&C module.

3.3.1 Sensor Cyber-attack Detection and Isolation

To detect sensor cyber-attacks at the C&C center, we utilize a χ^2 detector. This detector relies on the detection function, denoted by $g_A(k)$, computed as a weighted norm of the error between system output under potential cyber-attack and the estimator. Specifically, the sensor cyber-attack residual is defined as:

$$e_A(k) = \tilde{y}(k) = y^A(k) - \hat{y}^{CC}(k|k-1). \tag{46}$$

which is used to compute the detection function as follows:

$$g_A(k) = e_A^T(k) \mathbf{P}_{e_A}^{-1}(k) e_A(k), \tag{47}$$

where $\mathbf{P}_{e_A}(k) = E[e_A(k)e_A^T(k)]$ corresponds to the covariance matrix of $e_A(k)$.

According to Theorem 3.1, the residual (46) remains bounded in absence of cyber-attacks. However, based on equation (4) and assuming $D^a \neq 0$, the cyber-attack signal $A^y(k)$ will explicitly appear in the output that is received at the C&C, $y^A(k)$, and consequently in the residual (46) and the detection function (47). The detector issues an alarm if the detection function satisfies the condition $g_A(k) > \eta_A$, where η_A is a predefined threshold value that is obtained by Monte Carlo simulations for the healthy system. Concerning the stochastic behavior of the system due to noise and other uncertainties, the selection of η_A is made such that, under normal operating conditions (i.e., when the system is not compromised by anomalies), the probability of the detection function exceeding the threshold η_A is less than the threshold ϵ , i.e., $P(g_A(k) > \eta_A) \leq \epsilon$.

Regarding cyber-attack isolation problem, it is important to note that by incorporating fault dynamics into the augmented system dynamics, the estimation error and detection function $g_A(k)$ remain bounded despite the presence of faults. Since the fault dynamics are assumed to be known, this bounded value can be determined in a manner similar to the approach used for defining the cyber-attack detection threshold. Consequently, any deviations in the residual caused by a cyber-attack can be distinguished from those due to faults, allowing for the isolation of sensor cyber-attacks from system faults. The isolation of actuator cyber-attacks from sensor cyber-attacks will be discussed in Section 3.4.

3.3.2 Fault Detection and Isolation

In the previous section, we addressed fault estimation and established the boundedness of estimation errors, encompassing plant, actuator, and sensor faults. We now introduce a mechanism for detection of these faults. Given that $\hat{X}(k) = [\hat{x}^T(k); \hat{\theta}^T(k)]^T$, we can extract $\hat{\theta}(k)$ from $\hat{X}(k)$ as shown in (14). We define the fault residual $e_{\theta_l}(k)$ for each fault $\theta_l(k) \in \theta(k)$ as follows:

$$e_{\theta_l}(k) = \hat{\theta}_l(k) - \theta_l^m(k), \quad (48)$$

where $\theta_l^m(k) \in \theta^m(k)$ is a substitute for θ_l at the C&C, with $l \in 1, \dots, \mathbb{R}^{n_\theta}$, and $\theta^m(k)$ is generated by the following representation

$$\theta^m(k+1) = \theta^m(k) + f_\theta(\theta^m(k), x(k)), \quad (49)$$

Consequently, we employ a bank of AUKFs, each specifically designed for a corresponding fault $\theta_l \in \theta$. Note that $\theta_l^m(k)$ is unaffected by the actual fault occurrence, while $\hat{\theta}(k)$ is influenced by it.

According to (14), $\hat{\theta}(k)$ is a function of $y^A(k)$. The observability condition of the fault implies that the presence or absence of a fault affects $y^A(k)$, which in turn impacts $\hat{\theta}_l(k)$ and $e_{\theta_l}(k)$. Thus, the residual defined in (48) serves as an effective measure for fault detection.

In essence, a reduction in the residual indicates that the fault estimation is increasingly accurate, suggesting that the corresponding fault has indeed occurred in the main system.

Another χ^2 detector is employed for each fault θ_l for the purpose of fault detection. The fault detection function, denoted as $g_{\theta_l}(k)$, is defined as follows:

$$g_{\theta_l}(k) = e_{\theta_l}^T(k) \mathbf{P}_{e_{\theta_l}}^{-1}(k) e_{\theta_l}(k), \quad (50)$$

where $\mathbf{P}_{e_{\theta_l}}(k)$ corresponds to the covariance matrix of $e_{\theta_l}(k)$. The fault detector raises an alarm when the detection function meets the condition $g_{\theta_l}(k) < \eta_{\theta_l}$, where η_{θ_l} is a predetermined threshold value obtained by Monte Carlo simulations. The threshold η_{θ_l} is set to ensure that when the system is in a fault-free state, the probability of detecting a fault remains below a specified value, denoted by ϵ_{θ_l} ($P(g_{\theta_l}(k) < \eta_{\theta_l}) \leq \epsilon_{\theta_l}$).

By utilizing the outcomes of fault detectors, each corresponding to a specific fault $\theta_l \in \theta$ it becomes possible to differentiate and isolate the effects of individual faults. As previously explained, the presence of a cyber-attack can be identified at the C&C center, even in presence of faults. However, it is important to note that in the event of a cyber-attack on the sensor communication network, the AUKF within the C&C center may not produce a valid estimation of the system states and faults. Nevertheless, in such a scenario, the cyber-attack remains detectable in the C&C side, and the fault can be detected by the AUKF that is designed for the plant side.

3.4 Actuator Cyber-attack Detection and Isolation Using Auxiliary Filters

In this section we develop two auxiliary filters, one each on the C&C and plant sides. These auxiliary filters are designed to detect cyber-attacks on the actuator network. To enable this functionality, as explained for Figure 3.1, there are communication channels through the network between the C&C and plant sides, allowing the C&C auxiliary filter output to be transmitted to the plant side for comparison. However, it is important to note that this supplementary communication channel is also vulnerable to potential cyber-attacks.

Importantly, the role of these auxiliary filters is not to estimate the system's states, as this task is already accomplished by the AUKF that is proposed in the previous section. Instead, their primary function is detection of actuator cyber-attacks. The formulation of the auxiliary filter on the C&C side is provided as follows:

$$\begin{aligned} z_{Au}^{CC}(k+1) &= A_{Au} z_{Au}^{CC}(k) + F_{Au}(z_{Au}^{CC}(k)) + T_{Au} u(k) \\ &+ K_{Au} y^A(k), \end{aligned} \quad (51)$$

where $z_{Au}^{CC}(k) \in \mathbb{R}^n$ represents the state of the auxiliary filter at the C&C side. The nonlinear term and matrices $F_{Au}(\cdot)$, A_{Au} , T_{Au} , and K_{Au} are of appropriate dimensions and

will be designed and selected subsequently.

The proposed auxiliary filters on the plant side are expressed in the following form:

$$\begin{aligned} z_{Au}^p(k+1) &= A_{Au}z_{Au}^p(k) + F_{Au}(z_{Au}^p(k)) + T_{Au}u^A(k) + K_{Au}y(k) \\ &+ L_{Au}^p(z_{Au}^p(k) - (z_{Au}^{CC}(k) + D_{Au}^A A^{Au})). \end{aligned} \quad (52)$$

In the above expression, $z_{Au}^p(k) \in \mathbb{R}^n$ denotes the state of the auxiliary filter at the plant side, while $a^{Au} \in \mathbb{R}^{n_{a^{Au}}}$ illustrates the cyber-attack on the communication channels between the two filters with the signature D_{Au}^A . The error signals between the estimated states on both sides can be defined as $e_{Au}^{pc}(k) = z_{Au}^p - z_{Au}^{CC}$. The gain of the filter, L_{Au}^p , will be designed subsequently.

Assumption 3.2. *The malicious adversary does not have access to all the communication channels between the two side filters, i.e., $\text{rank}(D_{Au}^A) < n$. In other words, while all communication channels between sensors, actuators, and the C&C center may be vulnerable to cyber-attacks, at least one channel between the two auxiliary filters must remain inaccessible to the attacker.*

Assumption 3.3. *For $F_{Au}(x)$, there exists a positive constant δ for all x_1 and x_2 such that (Lipschitz condition)*

$$\|F_{Au}(x_1) - F_{Au}(x_2)\| \leq \delta \|x_1 - x_2\|, \quad (53)$$

The following will demonstrate how residual signals can be generated to detect actuator cyber-attacks, given by

$$res_{Au(k)} = L_{Au}^p(z_{Au}^p - {}^A z_{Au}^{CC}), \quad (54)$$

where, ${}^A z_{Au}^{CC}$ denotes the C&C-side auxiliary filter's output received at the plant side, which may also be vulnerable to cyber-attacks.

Theorem 3.2. *Under Assumptions 3.2 and 3.3 and if the following conditions hold, the residual $res_{Au(k)}$ is affected by the actuator cyber-attacks $A^u(k)$, and is decoupled from other cyber-attacks, faults and inputs, i.e. for $A^u(k) = 0$, e_{Au}^{pc} converges to zero asymptotically, provided that*

1. $K_{Au}D^A = 0$.
2. $L_{Au}^p D_{Au}^A = 0$.
3. $T_{Au}B^A \neq 0$.
4. *Given that the matrix L_{Au}^p satisfies the condition 2), we define the matrix $\mathbb{A}$ according to $\mathbb{A} = A_{Au} + L_{Au}^p$, such that $\mathbb{A}$ is Hurwitz by properly selecting the matrix A_{Au} that is at our disposal.*

Furthermore, if B^A is diagonal, each individual $res_{A_i^u(k)}$ is affected by the corresponding cyber-attack $A_i^u(k) \neq 0$ and is decoupled from the others.

Proof: By subtracting (51) from (52), one can derive the state-space representation of the error dynamics between the two filter states as follows:

$$\begin{aligned} e_{Au}^{pc}(k+1) &= \mathbb{A}e_{Au}^{pc}(k) + F_{Au}(z_{Au}^p(k)) \\ &\quad - F_{Au}(z_{Au}^{cc}(k)) + T_{Au}B^AA^u(k) \\ &\quad - K_{Au}D^AA^y(k) - L_{Au}^pD_{Au}^AA^{Au}(k). \end{aligned} \quad (55)$$

Under the Conditions that 1) and 2) hold, (55) can be simplified to:

$$\begin{aligned} e_{Au}^{pc}(k+1) &= \mathbb{A}e_{Au}^{pc}(k) + F_{Au}(z_{Au}^p(k)) \\ &\quad - F_{Au}(z_{Au}^{cc}(k)) + T_{Au}B^AA^u(k). \end{aligned} \quad (56)$$

To demonstrate the convergence of $e_{Au}^{pc}(k)$, let us first assume that $A^u(k) = 0$. We choose a Lyapunov function candidate $V(k) = e^{pc}(k)^T P e^{pc}(k)$, where the matrix P is symmetric positive definite (PD) that satisfies

$$\mathbb{A}^T P \mathbb{A} + (\delta^2 - 1)P + \delta P \mathbb{A} \mathbb{A}^T P + \delta I < 0. \quad (57)$$

It follows from (56) and (53) that:

$$\begin{aligned} V(k+1) - V(k) &= (\mathbb{A}e^{pc}(k) + F_{Au}(z_{Au}^p(k)) - F_{Au}(z_{Au}^{cc}(k)))^T \\ &\quad P(\mathbb{A}e^{pc}(k) + F_{Au}(z_{Au}^p(k)) - F_{Au}(z_{Au}^{cc}(k)) - e^{pc}(k)^T P e^{pc}(k)) \\ &= e^{pc}(k)^T \mathbb{A}^T P \mathbb{A} e^{pc}(k) + 2(\mathbb{A}e^{pc}(k))^T P (F_{Au}(z_{Au}^p(k)) \\ &\quad - F_{Au}(z_{Au}^{cc}(k)) + (F_{Au}(z_{Au}^p(k)) - F_{Au}(z_{Au}^{cc}(k)))^T P \\ &\quad (F_{Au}(z_{Au}^p(k)) - F_{Au}(z_{Au}^{cc}(k)) - e^{pc}(k)^T P e^{pc}(k)) \\ &\leq e^{pc}(k)^T (\mathbb{A}^T P \mathbb{A} - P) e^{pc}(k) + 2\delta \|e^{pc}(k)^T \mathbb{A}^T P\| \|e^{pc}(k)\| \\ &\quad + \delta^2 e^{pc}(k)^T P e^{pc}(k) \\ &\leq e^{pc}(k)^T (\mathbb{A}^T P \mathbb{A} - P) e^{pc}(k) + \delta (\|e^{pc}(k)^T \mathbb{A}^T P\|^2 \\ &\quad + \|e^{pc}(k)\|^2) + \delta^2 e^{pc}(k)^T P e^{pc}(k) \\ &= e^{pc}(k)^T (\mathbb{A}^T P \mathbb{A} + (\delta^2 - 1)P + \delta P \mathbb{A} \mathbb{A}^T P + \delta I) e^{pc}(k). \end{aligned} \quad (58)$$

Note that in view of (57), $\mathbb{A}^T P \mathbb{A} + (\delta^2 - 1)P + \delta P \mathbb{A} \mathbb{A}^T P + \delta I < 0$ in (58) implies $e^{pc}(k)$ tends to zero asymptotically for any initial condition $e(0)$, when $A^u(k) = 0$.

On the other hand, it follows from (56) that under the Condition 3), $e^{pc}(k)$ is affected by the actuator cyber-attack $A^u(k)$ for any $A^u(k) \neq 0$ and the impact of $e^{pc}(k)$ will appear in the residual $res_{A^u(k)}$. Consequently, by accounting for noise and other uncertainties, a

threshold value η_{ac} can be established. If $res_{Au(k)} > \eta_{ac}$, this serves as the decision logic to trigger an alarm, indicating the occurrence of an actuator cyber-attack. Furthermore, if B^A is diagonal, i.e., each individual cyber-attack only affects a communication channel in the actuator communication network, according to Equation (56), only the corresponding element of the vector $e_{Au}^{pc}(k)$ is affected, while it is decoupled from other channels' cyber-attacks. This completes the proof of the theorem. $\blacksquare$

In view of Theorem 3.2, we present below an algorithm for designing auxiliary filters. These filters are crucial for detecting and isolating actuator cyber-attacks. The algorithm provides a systematic approach to configuring these filters. For isolation, as demonstrated in Theorem 3.2, the residual $res_{Au(k)}$ is affected by the actuator cyber-attacks $A^u(k)$, and is decoupled from other cyber-attacks and faults. This approach thus enables the isolation of actuator cyber-attacks from other anomalies. Furthermore, if each individual cyber-attack affects only a specific communication channel, each actuator can be isolated from the others.

Algorithm 1 Auxiliary Filter Design Algorithm.

Inputs: Assumption 3.3 and conditions of Theorem 3.2

Output: $\mathbb{A}$ and A_{Au}

1. Compute K_{Au} according to the Condition 1). Setting $K_{Au} = 0$ is a valid selection.
 2. Compute the matrix L_{Au}^p to meet Condition 2). It is essential to note that L_{Au}^p cannot be zero due to the definition of $res_{Au(k)}$.
 3. Select a function F_{Au} that satisfies the Assumption 3.3 with a desired positive value of δ .
 4. Choose T_{Au} such that it does not nullify the potential cyber-attacks effect, i.e., $T_{Au}B^A \neq 0$.
 5. Given the matrix L_{Au}^p from the Step 2, then by properly selecting the matrix A_{Au} , one would select a new matrix $\mathbb{A}$ as $\mathbb{A} = A_{Au} + L_{Au}^p$, that is Hurwitz and satisfies $\mathbb{A}^T P \mathbb{A} + (\delta^2 - 1)P + \delta P \mathbb{A} \mathbb{A}^T P + \delta I < 0$ for a PD symmetric matrix P and the desired value of δ .
-

3.5 Auxiliary Filter-Based Actuator and Sensor Attack Detection and Isolation in the Absence of Faults

In this section, we aim to detect and isolate actuator and sensor cyber-attacks by employing the proposed auxiliary filters deployed on both the C&C side and the plant side, under the assumption that the system operates without faults.

Accordingly, by revisiting the original nonlinear system (3) and removing fault-related components, the mathematical model of the nonlinear CPS considered in this section is expressed as follows:

$$\begin{aligned} x(k+1) &= f(x(k)) + g(x(k))u^*(k) \\ y(k) &= h(x(k)). \end{aligned} \tag{59}$$

The control input delivered to the plant and the output received at the C&C side, both of which are subject to cyber-attacks on the communication networks between actuators and sensors, are represented by equation (4).

The architecture of the CPS with auxiliary filters is illustrated in Figure 3.2. In this figure, the communication links are vulnerable to cyber-attacks, and the auxiliary filters are shown as integral components of the detection and isolation framework.

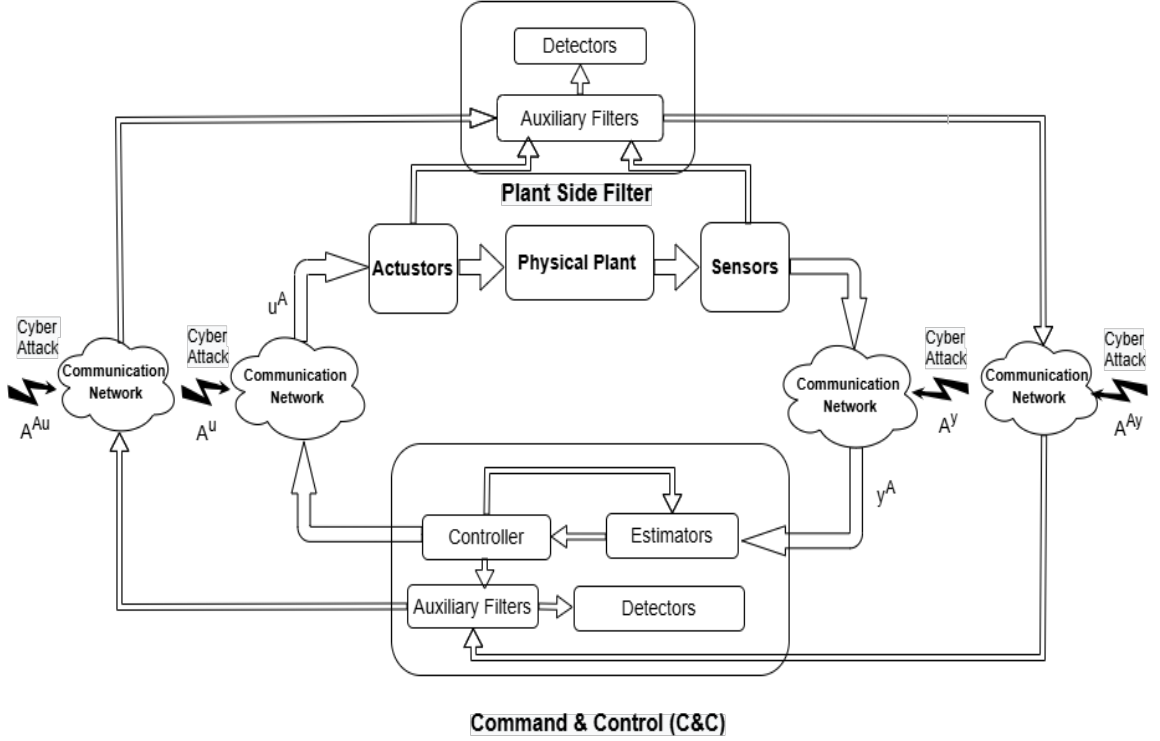


Figure 3.2: The CPS under actuator and sensor cyber-attacks with the C&C and the plant side auxiliary filters and detectors.

The structure for actuator cyber-attack detection and isolation follows the same principles outlined in Section 3.4. Accordingly, the residual signal used for actuator cyber-attack detection, denoted by $res_{A^u(k)}$, is computed using (54). We also assume that the same conditions specified in Assumptions 3.3 and 3.2 hold for both actuator and sensor attack detection.

For the sensor cyber-attack detection and isolation methodology, we first design the plant-side nonlinear auxiliary filter as follows:

$$\begin{aligned} z_{Ay}^p(k+1) &= A_{Ay}z_{Ay}^p(k) + F_{Ay}(z_{Ay}^p(k)) + T_{Ay}u^A(k) \\ &+ K_{Ay}y(k), \end{aligned} \quad (60)$$

where $z_{Ay}^p(k) \in \mathbb{R}^n$ represents the state of the sensor auxiliary filter at the plant side. The

nonlinear term $F_{Ay}(\cdot)$ and matrices A_{Ay} , T_{Ay} , and K_{Ay} are of appropriate dimensions and need to be designed.

On the C&C side, control inputs are obtained before the injection of actuator cyber-attacks. However, the measurement signal received at the C&C could be vulnerable to sensor cyber-attacks. Consequently, the proposed sensor auxiliary filters on the C&C side are formulated as follows:

$$\begin{aligned} z_{Ay}^{CC}(k+1) &= A_{Ay}z_{Ay}^{CC}(k) + F_{Ay}(z_{Ay}^{CC}(k)) + T_{Ay}y^A(k) \\ &+ K_{Ay}u(k) + L_{Ay}^{CC}(z_{Ay}^{CC}(k) - (z_{Ay}^p(k) + D_{Ay}^A A^{Ay})). \end{aligned} \quad (61)$$

where $z_{Ay}^{CC}(k) \in \mathbb{R}^n$ represents the state of the sensor auxiliary filter on the C&C side, and $A^{Ay} \in \mathbb{R}^{n_{Ay}}$ illustrates the cyber-attack occurring on the communication link between the two sensor filters, characterized by the signature D_{Ay}^A .

The error signals between the estimated states on both sides can be expressed as $e_{Ay}^{cp}(k) = z_{Ay}^{CC} - z_{Ay}^p$. Additionally, the residual of sensor cyber-attacks is defined as

$$res_{Ay}(k) = L_{Ay}^{CC}(z_{Ay}^{CC} - {}^A z_{Ay}^p) \quad (62)$$

Where ${}^A z_{Ay}^p$ indicates the output of the plant-side sensor auxiliary filter received at the C&C side, which could also be vulnerable to cyber-attacks.

Theorem 3.3. *Under Assumptions similar to 3.2 and 3.3 for D_{Ay}^A and F_{Ay} and provided that the following conditions hold, the residual $res_{Ay}(k)$ is affected by the sensor cyber-attack $A^y(k)$, and is decoupled from other cyber-attacks and inputs, i.e. for $A^y(k) = 0$, e_{Ay}^{cp} converges to zero asymptotically, provided that*

1. $K_{Ay}B^A = 0$.
2. $L_{Ay}^{CC}D_{Ay}^A = 0$.
3. $T_{Ay}D^A \neq 0$.
4. *Given that the matrix L_{Ay}^{CC} satisfies the condition 2), we define the matrix $\mathbb{A}$ according to $\mathbb{A} = A_{Ay} + L_{Ay}^{CC}$, such that $\mathbb{A}$ is Hurwitz by properly selecting the matrix A_{Ay} that is at our disposal.*

Furthermore, if D^A is diagonal, each individual $res_{Ay_i}(k)$ is affected by the corresponding cyber-attack $A_i^y(k)$ and is decoupled from the others.

Proof: The proof is similar to that of Theorem 3.2 and is omitted for brevity. ■

Furthermore, the parameters of the filters (60) and (61) can be determined by using an algorithm similar to the Algorithm 1.

In terms of isolating different cyber-attacks, as mentioned in the above theorems, actuator and sensor residuals are detected separately and are decoupled from each other. Furthermore, if there are various individual cyber-attacks, each affecting the corresponding channel in the actuator/sensor, then only the corresponding element of $res_{A^u(k)}/res_{A^y(k)}$ is affected. Therefore, by utilizing residuals (54) and (62), one can detect and isolate different actuator and sensor cyber-attacks.

Remark 3.1. *For simplicity in our analysis, the presence of noise was not considered in the auxiliary filter-based actuator and sensor cyber-attack detection and isolation procedure. However, in the simulation results presented in Section 3.6, we have incorporated noise and disturbances into both the control and measurement channels to emulate more realistic scenarios.*

Remark 3.2. *In Theorems 3.1, 3.2, and 3.3 no specific assumptions are made regarding the nature, characteristics, or types of sensor and actuator cyber-attacks, nor how attackers might compromise sensor and actuator communication channels. This flexibility implies that the proposed method is well-equipped to detect and isolate various types of deception attacks that are rooted in the FDI. These may include readily detectable attacks such as replay attacks, as well as more subtle forms of cyber-attacks, which might be considered undetectable according to some definitions [152]. These undetectable cyber-attacks encompass covert attacks and zero dynamics attacks. Typically, these cyber-attacks involve a component injected into the actuator communication network, where the effects caused by it are either unobservable or are compensated for at the outputs. Referring to (52), these components can be modeled as $A^u(k)$, which are shown to be detectable by utilizing our proposed actuator detectors. This matter will be illustrated in the next section, focusing on the detection and isolation of different FDI and covert attacks in nonlinear CPS. The proposed approach, therefore, provides a versatile solution to enhance system security against a wide range of cyber threats to nonlinear CPS.*

Remark 3.3. *The proposed framework encompasses two complementary detection strategies: the AUKF-based detection and the auxiliary filter-based detection. Each approach presents distinct advantages and trade-offs in terms of functionality, complexity, and implementation requirements.*

The AUKF-based method enables joint state and fault estimation, thereby facilitating both fault detection and isolation in addition to cyber-attack detection. This capability is especially valuable in environments where faults and cyber-attacks may simultaneously affect system performance. Moreover, the AUKF-based strategy does not require the deployment of additional communication links between the plant and the C&C center.

In contrast, the auxiliary filter-based approach is more computationally efficient, offering a lower implementation burden. While it does not include fault estimation and therefore cannot isolate faults, it effectively detects and isolates both sensor and actuator cyber-attacks. Notably, it enables the detection of actuator cyber-attacks even when such attacks do

not directly impact the measured system output—a limitation inherent to detection methods relying solely on AUKF-based residuals at the C&C center.

Overall, these two approaches are designed to complement each other, offering flexible and layered protection tailored to the specific detection and isolation needs of nonlinear CPS under varying cyber-attack and fault scenarios.

3.6 Case Study Simulation Results

3.6.1 Fixed-base inverted pendulum

In this section, simulations of a case study is presented. We consider a fixed-base inverted pendulum as a CPS equipped with AUKF to estimate the system states and faults. Using $x_1 = \phi$ and $x_2 = \dot{\phi}$, the inverted pendulum dynamics can be modeled as,

$$\begin{aligned}\dot{x}_1 &= x_2 \\ \dot{x}_2 &= \frac{g}{l} \sin x_1 - \frac{b}{ml^2} x_2 + \frac{T_m}{ml^2} + \frac{\theta}{ml^2}\end{aligned}\tag{63}$$

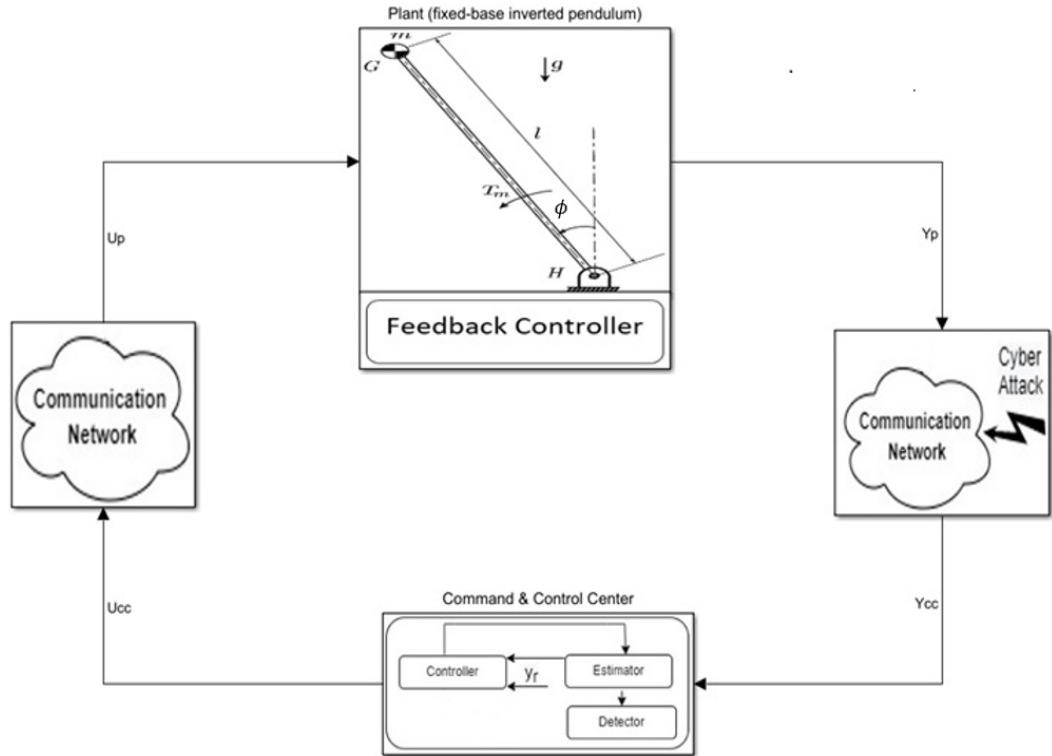


Figure 3.3: Cyber physical system including a fixed-base inverted pendulum and C&C center

where, ϕ denotes the angle of the pendulum rod from the vertical axis, measured counterclockwise; b is the viscous friction coefficient; l is the radius of inertia of the pendulum about a fixed point; m is the mass of the pendulum; g is the gravitational constant; and T_m represents the external torque applied at the fixed base. It is also assumed that the actuator fault is represented by θ , and both states are measured by sensors.

The model parameters are set as follows: $g = 9.8 \text{ m/s}^2$, $m = 0.2 \text{ kg}$, and $b = 0.1$. The model is discretized using a sampling period of $T_s = 10 \text{ ms}$, and the safe region for the angle around the equilibrium point is defined as $(-\frac{\pi}{3}, \frac{\pi}{3})$.

Furthermore, a feedback controller is implemented on the plant side to stabilize the pendulum rod in the vertical position. On the other hand, a tracking controller is implemented on the C&C side to follow the reference signal y_r . The sensor communication channel is assumed to be compromised by an attacker. To detect the presence of an attack, the proposed cyber-attack detector (47) is employed. Simultaneously, the fault is estimated using the AUKF on the C&C side. Moreover, to identify the time of fault occurrence, the fault detector (50) is utilized. The following figures illustrate the simulation results.

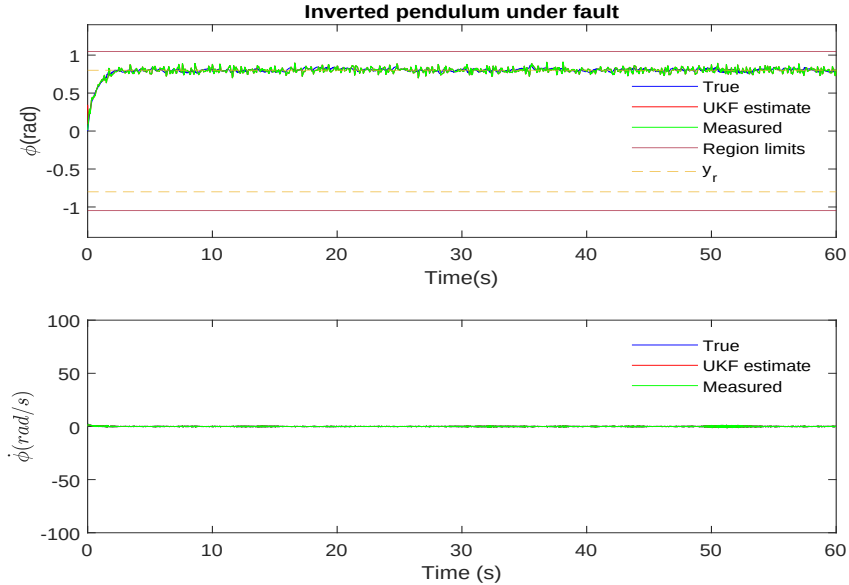


Figure 3.4: System outputs under actuator fault.

First, we assume that an actuator fault occurs at time $t = 20 \text{ s}$. Figure 3.4 illustrates the system outputs under this condition. The actual fault, its corresponding estimate, the estimation residual, the result of the fault detector, and the probability of fault occurrence are presented in Figure 3.5. Additionally, Figure 3.6 displays the results of the cyber-attack detector. As observed, the fault estimator and detector function correctly, whereas the cyber-attack detector is not triggered in this scenario.

It is important to note that in this example, the fault has no significant impact on the attack residual. However, even if the fault does influence the attack residual, the output of

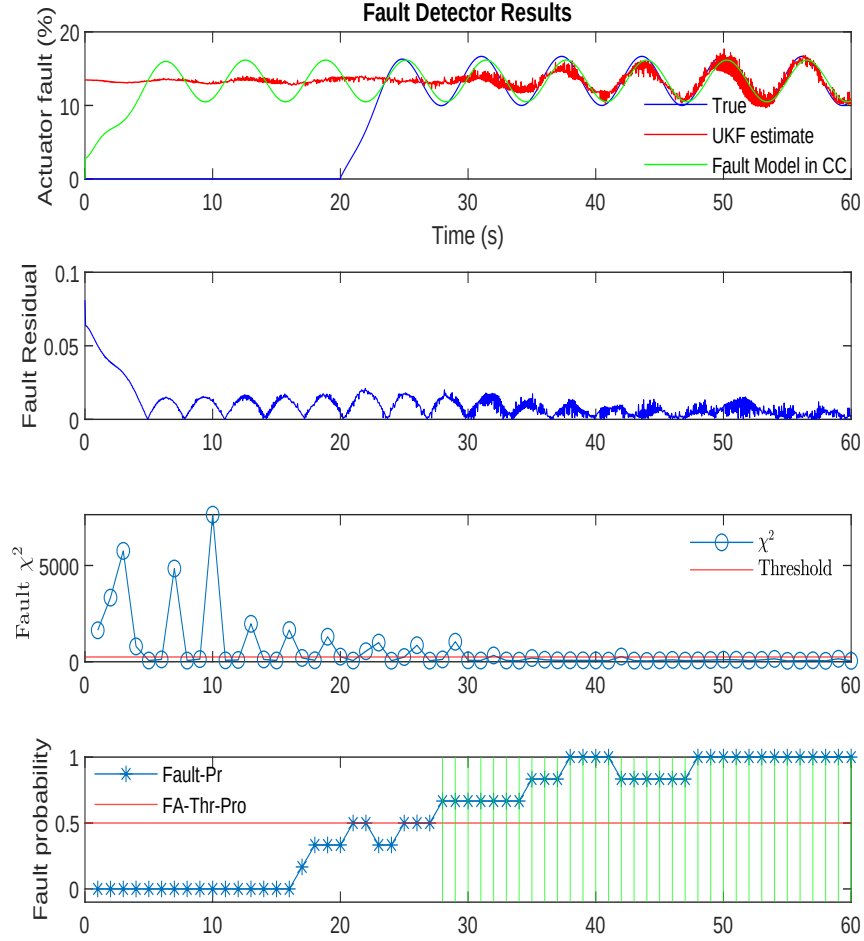


Figure 3.5: Fault estimator and detector responses for the system under actuator fault.

the fault detector—being sensitive only to the specific fault in a cyber-attack-free scenario—can still be used by the attack detector to disregard that effect appropriately.

In addition, as shown in Figures 3.8 and 3.9, under the simultaneous occurrence of a fault and a cyber-attack—corresponding to the system outputs depicted in Figure 3.7—the cyber-attack detector is still able to identify the presence of the attack. However, the fault detector does not perform reliably in the presence of a cyber-attack.

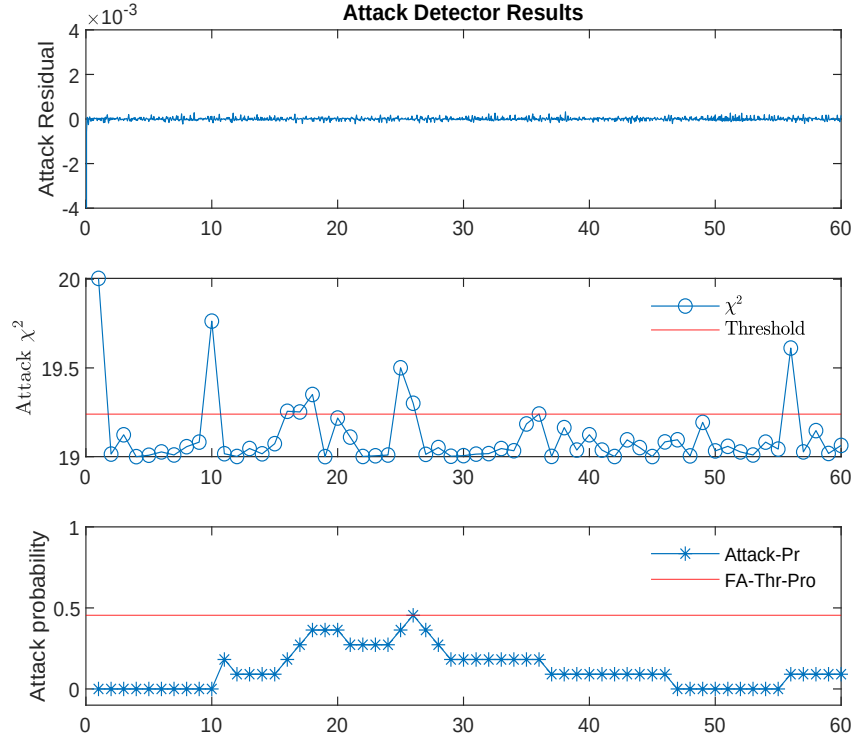


Figure 3.6: Attack detector responses for the system under actuator fault.

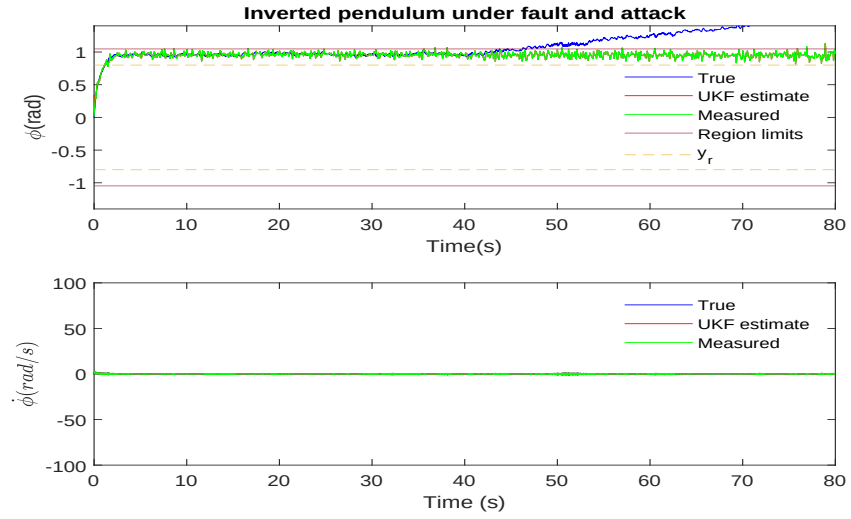


Figure 3.7: System outputs under fault and cyber-attack.

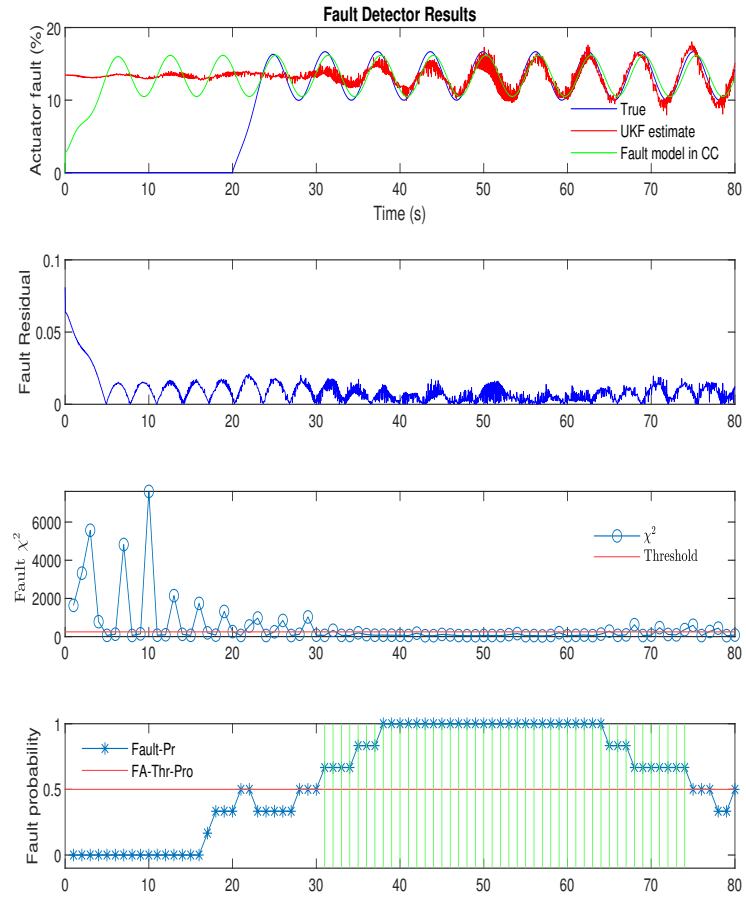


Figure 3.8: Fault estimator and detector responses for the system under actuator fault and attack.

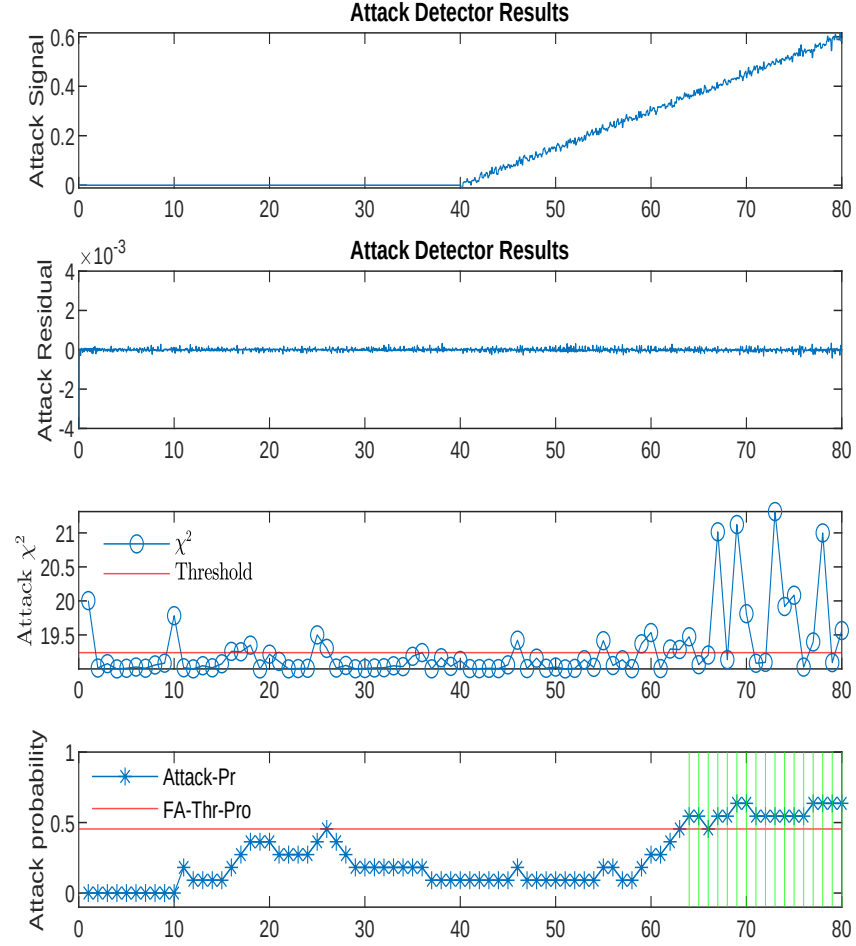


Figure 3.9: Attack detector responses for the system under actuator fault & attack.

3.6.2 Unmanned Aerial Vehicle (UAV)

In this section, we present a case study involving a mini UAV, specifically the commercial off-the-shelf Radio-controlled plane known as the Ultra Stick 25E [153]. This UAV, as shown in Figure 3.10, was developed by a group of researchers from the University of Minnesota. The UAV features a conventional design with horizontal and vertical tail surfaces, and is equipped with three primary control surfaces: the elevator, rudder, and ailerons, as depicted in Figure 3.10.

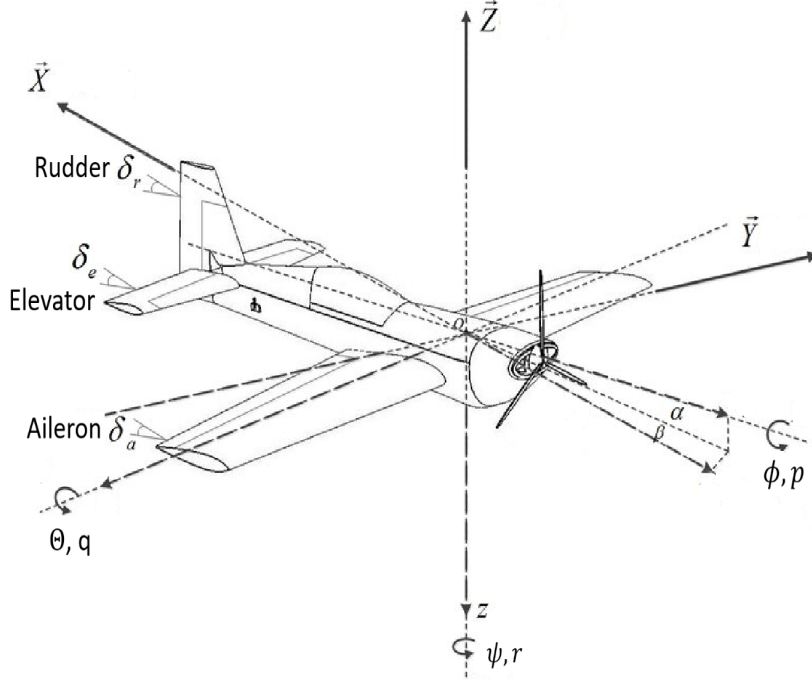


Figure 3.10: Angular positions and rates in the UAV body axis

All the control surfaces are actuated using Hitec servos. The UAV is further outfitted with a comprehensive set of avionics to support research and development in flight control system, and is equipped with a range of sensors, including those for measuring angular positions, rates, and linear accelerations. In this research, the controller's design is accomplished through the utilization of the backstepping method, as proposed in [154], involving the control of the roll, pitch, and yaw angles by using a total of six Lyapunov

functions. The angular rate dynamics can be expressed as follows [153]:

$$\begin{aligned}
p(k+1) - \frac{I_{xz}}{I_{xx}}r(k+1) &= p(k) - \frac{I_{xz}}{I_{xx}}r(k) + \frac{p_d S b}{I_{xx}}c_l \\
&\quad - \frac{I_{zz} - I_{yy}}{I_{xx}}q(k)r(k) + \frac{I_{xz}}{I_{xx}}q(k)p(k) \\
q(k+1) &= q(k) + \frac{p_d S \bar{c}}{I_{yy}}c_m - \frac{I_{xx} - I_{zz}}{I_{yy}}p(k)r(k) \\
&\quad - \frac{I_{xz}}{I_{yy}}(p^2(k) - r^2(k)) + \frac{I_p}{I_{yy}}w_p r(k) \\
r(k+1) - \frac{I_{xz}}{I_{zz}}p(k+1) &= r(k) - \frac{I_{xz}}{I_{zz}}p(k) + \frac{P_d S b}{I_{zz}}c_n \\
&\quad - \frac{I_{yy} - I_{xx}}{I_{zz}}p(k)q(k) - \frac{I_{xz}}{I_{zz}}q(k)r(k) - \frac{I_p}{I_{zz}}w_p q(k).
\end{aligned} \tag{64}$$

where p , q , and r represent the body axis angular rates, while ϕ , Θ , and ψ denote the body attitude Euler angles, specifically referred to as roll, pitch, and yaw, respectively. P_d stands for dynamic pressure, w_p represents the propeller rotation speed, and I_{xx} , I_{yy} , I_{zz} , I_{xz} , and I_p denote the moment of inertia coefficients. Moreover, c_l , c_m , and c_n represent non-dimensional moment coefficients [153].

The kinematics of the rotational motion, which links the body angular rates and the Euler angles is expressed as:

$$\begin{aligned}
\phi(k+1) &= \phi(k) + p(k) + \tan(\Theta(k))(q(k)\sin(\phi(k)) + r(k)\cos(\phi(k))) \\
\Theta(k+1) &= \Theta(k) + q(k)\cos(\phi(k)) - r(k)\sin(\phi(k)) \\
\psi(k+1) &= \psi(k) + \frac{q(k)\sin(\phi(k)) + r(k)\cos(\phi(k))}{\cos(\Theta(k))}
\end{aligned} \tag{65}$$

Additional equations describing the kinematics of the rotational motion, along with the parameter values, can be found in [153]. Referring to the dynamical model in (3), we consider $x(k) = [\phi(k), p(k), \Theta(k), q(k), \psi(k), r(k)]^T$, where $\phi(k)$, $\Theta(k)$, and $\psi(k)$ are measured and represent the system outputs.

Additionally, as mentioned above, a backstepping controller has been integrated into the plant side to stabilize the roll, pitch, and yaw angles. The desired (reference) values for these angles are denoted as $\bar{\phi}$, $\bar{\Theta}$, and $\bar{\psi}$, while $\bar{p}$, $\bar{q}$, and $\bar{r}$ are determined based on the system parameters. The corresponding errors are denoted as e_x , with x representing each of the system states. The designed control system has been implemented in the Matlab/Simulink environment, and its effectiveness has been evaluated through a series of numerical simulations.

Within the framework of the CPS as illustrated in Figure 3.1, we make the assumption that the UAV serves as the plant. Meanwhile, the C&C center receives the UAV's outputs and determines reference values for the corresponding actuators on the UAV. Consequently,

the communication networks for sensors and actuators, as well as the actuator cyber-attack auxiliary filter, may be compromised by cyber-attacks. To assess the effectiveness of proposed detection and isolation methodologies within the context of the introduced CPS system, we consider two distinct simulation scenarios, as detailed in the following subsections.

Sensor and Actuator FDI Attack and System Fault Detection and Isolation

We consider two FDI attacks in the sensor network, impacting ϕ and Θ , and two additional FDI attacks in the actuator networks, targeting $\bar{\Theta}$ and $\bar{\psi}$. Details of these cyber-attacks will be discussed subsequently. In addition to these cyber-attacks, we also investigate practical system faults. According to [155], one common fault that can occur in this UAV is elevator servo degradation, as servos tend to degrade over time and with usage. Here, we assume that an oscillatory mode fault occurs in the elevator actuator δ_e . Another potential fault in this UAV is sensor bias, as described in [156], which we consider for the ϕ sensor.

Thus, the system output is represented as

$$y(k) = [\phi(k), \Theta(k), \psi(k)]^T + \mathcal{L}_2(x(k))\theta(k) + v(k),$$

where $\theta(k)$ is a fault vector encompassing both actuator and sensor faults. The assumed actuator fault in the elevator δ_e affects the coefficient c_m , with the relationship between δ_e and c_m detailed in [153]. This impact propagates to $q(k)$ as described in (64). Accordingly, in reference to (3), $\mathcal{L}_1(k)$ is a matrix with all rows set to zero except for the one corresponding to the state $q(k)$. For the sensor fault, $\mathcal{L}_2(k)$ is a matrix with all rows zeroed except for the row corresponding to the faulty sensor $\phi(k)$.

In summary, for the Scenario A, we address the detection and isolation of six anomalies, encompassing two faults and four cyber-attacks, through various scenarios, all of which are addressed by using the proposed methodology.

To detect the presence of a sensor cyber-attack, the proposed cyber-attack detector (47) is utilized. Meanwhile, the fault is estimated using the AUKF on the C&C side. Additionally, to determine the time of fault occurrence, the fault detector (50) is applied. The following figures illustrate the simulation results.

First, let us assume that the CPS is operating under normal, healthy conditions. In this scenario, the UAV follows various reference values issued by the C&C center, as depicted in Figure 3.11. The system actual outputs, along with their estimated values achieved by the proposed AUKF and their desired references values, are accessible in the C&C center. The other three system states are estimated by the proposed filter as well.

In the following, we analyze the system behavior under faults. We assume that the actuator and sensor faults occur at times $t = 7$ seconds and $t = 15$ seconds, respectively. Figures 3.12 and 3.13 provide detailed information regarding the faults and their estimates,

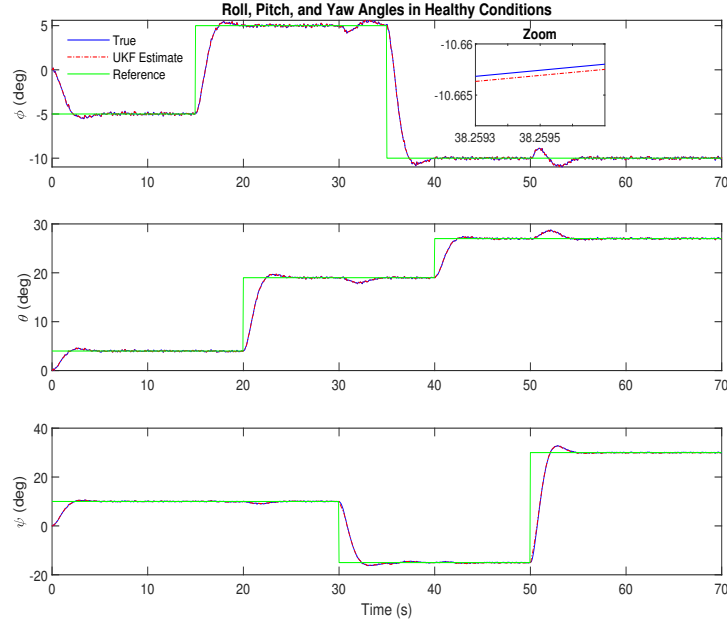


Figure 3.11: The UAV's actual measurement outputs, and the AUKF estimates under the healthy condition.

the estimation residuals, the results of fault detectors, and probabilities of occurrence of actuator and sensor faults, respectively.

To address faults, we employ two separate AUKFs in the C&C center, each designed for the specific fault type. As observed in the above figures, the proposed AUKFs effectively estimate the faults, and the corresponding detectors accurately determine the time of fault occurrence, which aligns with the real-time occurrence of the fault in the plant. Consequently, the AUKF produces very accurate estimations, and the residuals remain below the predefined thresholds. It should be noted that in this work, for all thresholds, we conducted multiple Monte Carlo simulation runs for the healthy system under various noise levels to determine the thresholds.

Note that in this example the fault does not significantly impact the cyber-attack residual. However, even if the fault was to affect the cyber-attack residual, the output of the fault detector, in a attack-free system, is only sensitive to the corresponding fault. In such cases, the cyber-attack detector could rely on the outcomes of the fault detector, simply disregarding any associated effects, or the cyber-attack threshold could be adjusted accordingly by considering the effect in the Monte Carlo procedure explained earlier. This principle applies to other cyber-attack detectors as well. Consequently, the separation of system faults from cyber-attacks can be successfully accomplished within the C&C framework.

Next, we consider occurrence of four FDI attacks, comprising two sensor cyber-attacks

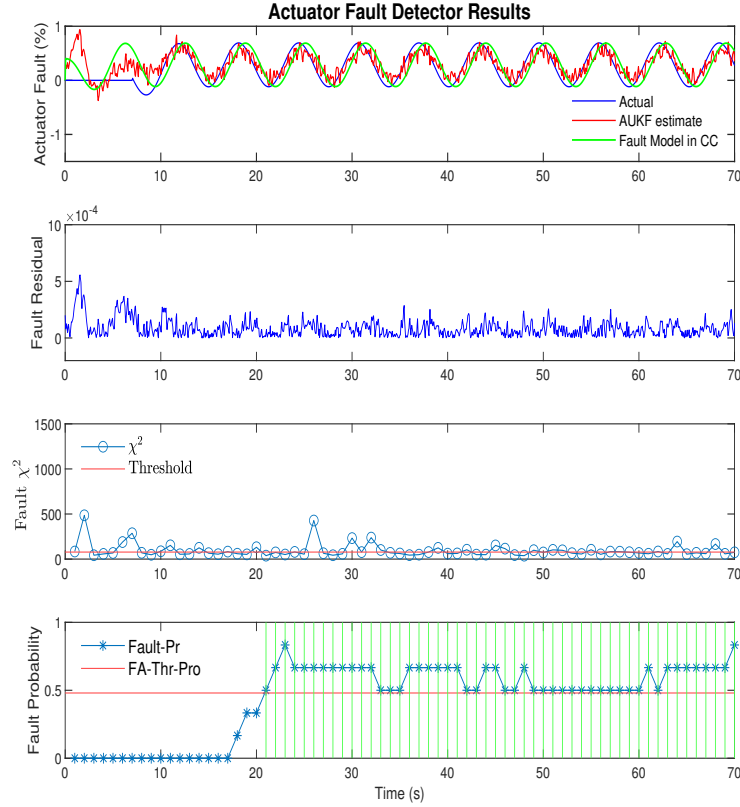


Figure 3.12: Actuator fault estimator (AUKF) and detector responses for the system under actuator and sensor faults.

and two actuator cyber-attacks. The characteristics of these cyber-attacks are illustrated in the initial sub-figures of Figures 3.15 and 3.16 for two sensor cyber-attacks on ϕ and ψ , respectively. Similarly, the first sub-figure of Figure 3.17 displays the actuator cyber-attacks affecting $\bar{\Theta}$ and $\bar{\psi}$. The sensor cyber-attacks on ϕ and ψ are introduced at $t = 35$ s and $t = 45$ s, respectively, while actuator cyber-attacks impacting $\bar{\Theta}$ and $\bar{\psi}$ occur at $t = 55$ s and $t = 60$ s, respectively. Additionally, we assume the attacker simultaneously compromises two communication channels between auxiliary filters in the actuator network. These two cyber-attacks are depicted in the second sub-figure of Figure 3.17. In Figure 3.14, we present the system actual values, estimated values, and reference values. Unlike faults, cyber-attacks lead to significant deviations in the filter output and system states from normal conditions. In the case of sensor cyber-attacks, the system states remain within normal bounds, however the measurements received at the corresponding C&C and, consequently, the estimation results will be affected. This situation could potentially mislead the monitoring system or decision-makers in the C&C. Actuator cyber-attacks, on the other hand, can push the plant into an unstable condition, as evident in the second and third sub-figures in Figure 3.14.

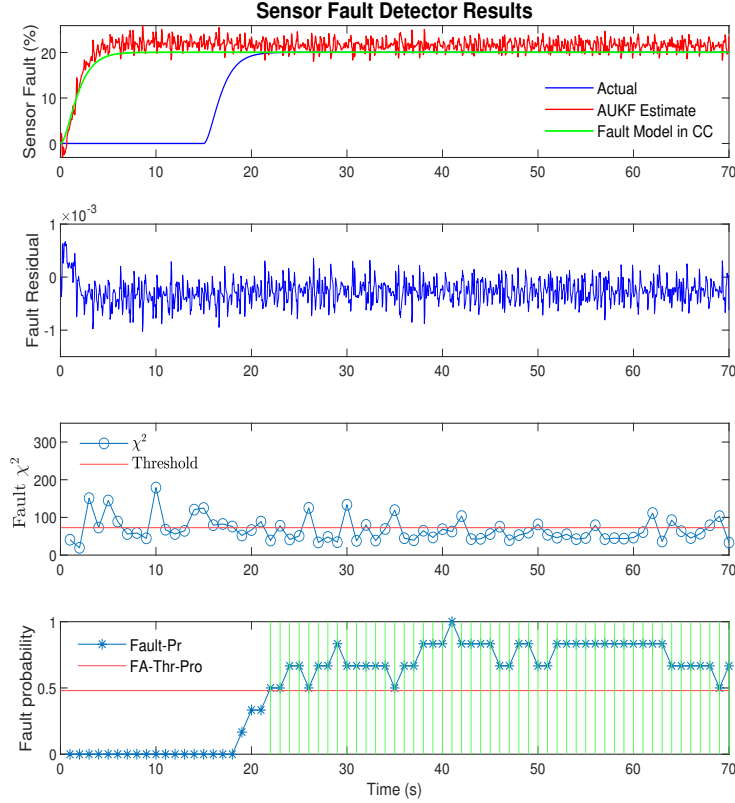


Figure 3.13: Sensor fault estimator (AUKF) and detector responses for the system under actuator and sensor faults.

Therefore, our objective is to promptly detect and isolate these anomalies.

Figures 3.15 and 3.16 demonstrate that the AUKF-based χ^2 cyber-attack detectors effectively detects the corresponding sensor cyber-attacks for the sensor communications of ϕ and ψ under both fault and cyber-attack scenarios. In theses figures after occurring cyber-attacks on sensor communication channels, the corresponding residuals and χ^2 detectors changes and when the values of χ^2 values pass the predefined thresholds, then according to the behavior of the detector output the last sub-figures show probability of occuring the cyber-attacks. Whenever this probability is greater than its assigned threshold, green lines, it implies the cyber-attack has been detected.

Next, we address the detection of actuator cyber-attacks. In contrast to the previous AUKF-based χ^2 detectors, actuator cyber-attacks are detected and isolated by using the proposed auxiliary filter that is provided in Algorithm 1. The following values represent the

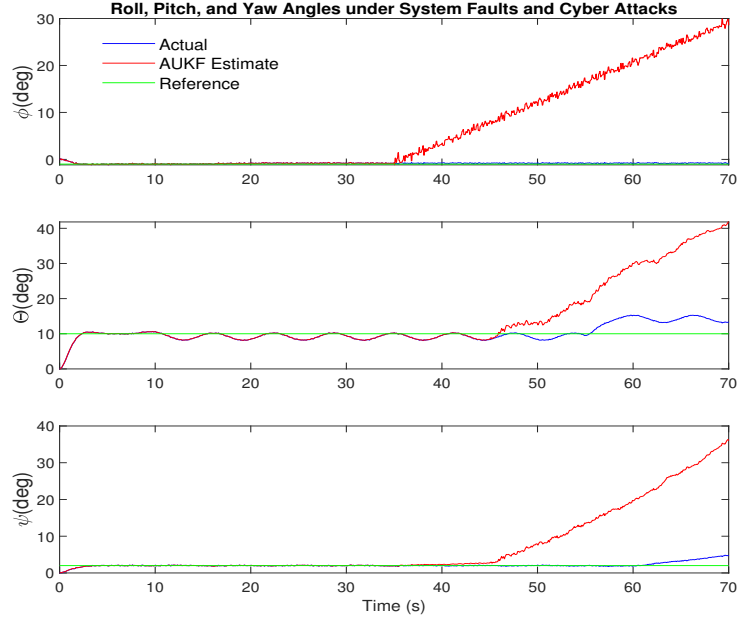


Figure 3.14: The UAV's measurement values, and AUKF estimate under system faults and actuator and sensor cyber-attacks.

designed parameters of the auxiliary filters, which are included in (51) and (52), that is,

$$\begin{aligned}
 A_{Au} &= [-2 \ 0 \ 0; 0 \ 0 \ 0; 0 \ 0 \ 0], F_{Au}(x) = \sin(x)\mathbf{I}_3 \\
 T_{Au} &= \mathbf{I}_3, L_{Au}^p = [1.5 \ 0 \ 0; 0 \ 0 \ 0; 0 \ 0 \ 0] \\
 K_{Au} &= 0, D_{Au}^a = B^a = [0 \ 0 \ 0; 0 \ 1 \ 0; 0 \ 0 \ 1] \\
 B^a &= [0 \ 0 \ 0; 0 \ 1 \ 0; 0 \ 0 \ 1].
 \end{aligned}$$

As depicted in Figure 3.17, the detectors effectively detect the corresponding actuator cyber-attacks, as evidenced by their corresponding residuals that are changing from zero in the last sub-figure of Figure 3.17. Due to the different structure of these detectors as compared to the AUKF-based detectors for sensor cyber-attacks and AUKF for system faults, the actuator cyber-attack detector results are not influenced by other anomalies.

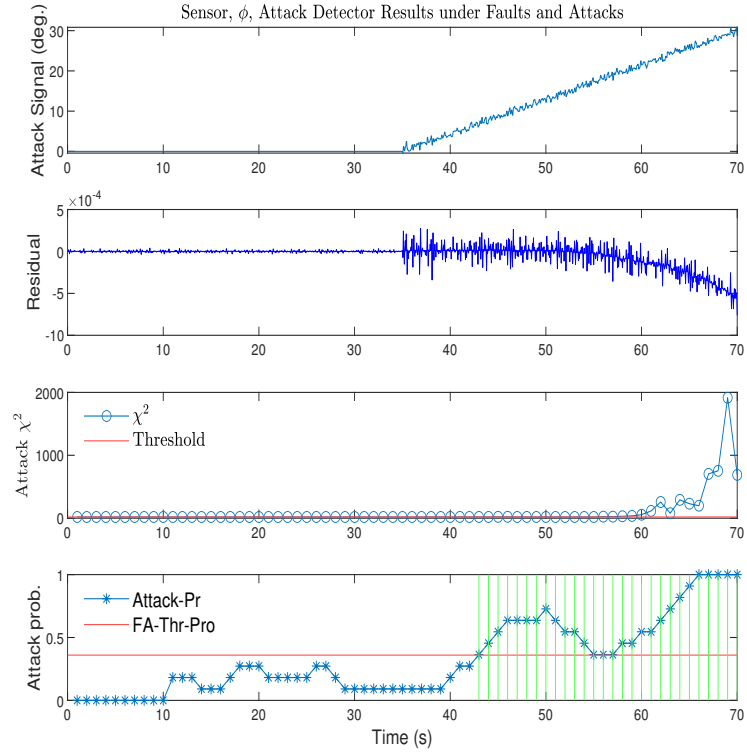


Figure 3.15: cyber-attack detector results for the sensor ϕ .

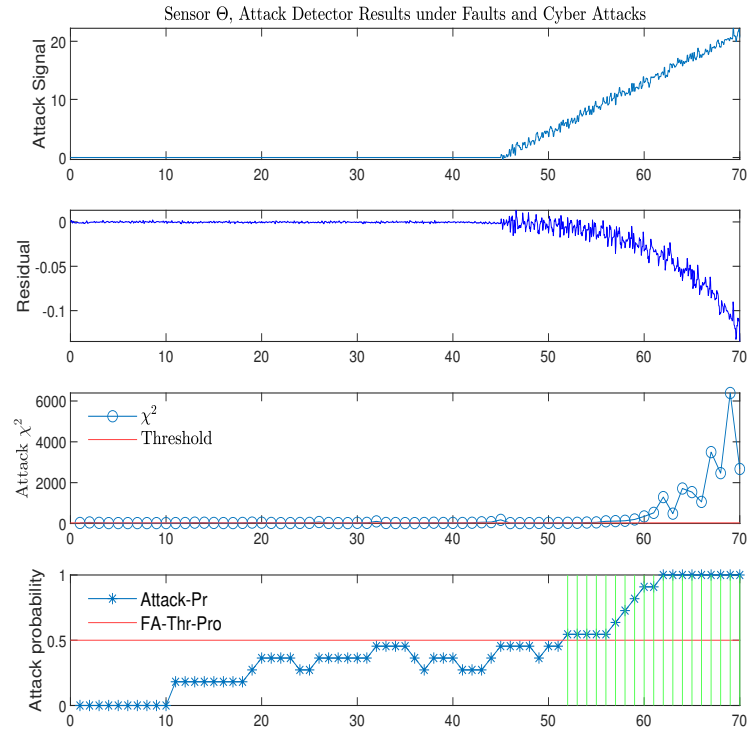


Figure 3.16: cyber-attack detector results for the sensor Θ .

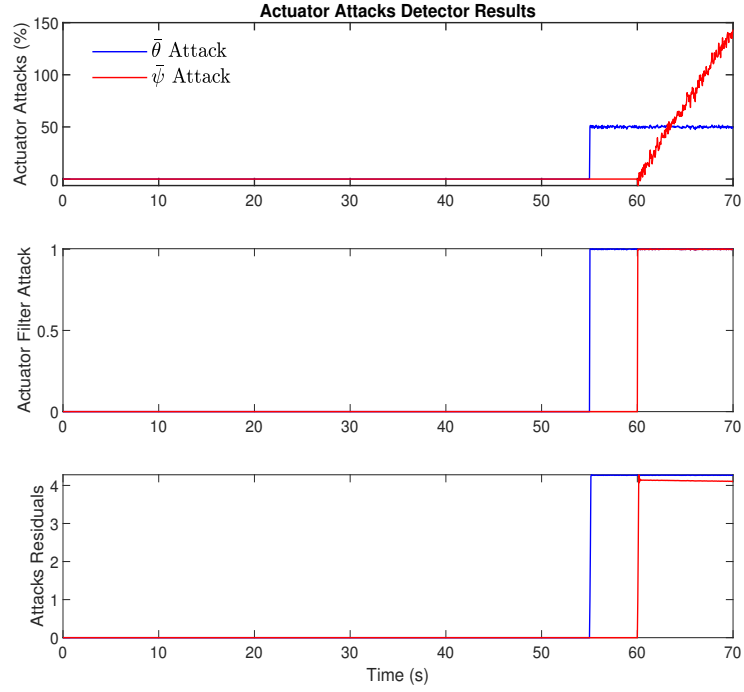


Figure 3.17: Actuators cyber-attack detection results.

Covert Attack Detection and Isolation

In the second simulation scenario for the UAV case study, we consider two covert attacks occurring on the CSP communication networks. The first one impacts $\bar{\Theta}$ and Θ simultaneously at time 25 seconds, and the second addresses $\bar{\psi}$ and ψ simultaneously at time 45 seconds. Figure 3.18 illustrates the impact of these cyber-attacks on the system output. Given that attackers have system knowledge, they aim to generate stealthy cyber-attacks by compensating for the effect of actuator cyber-attacks on the sensor communication network.

The covert attacks signals are represented in the first two sub-figures of Figure 3.19. Consequently, as shown in Figure 3.18, the signals received at C&C follow the issued references. However, the actual values for Θ and ψ alter significantly on the plant side, contrary to the C&C's desire. Due to our proposed methodology, the actuator auxiliary filter can detect and isolate these covert attacks, as depicted in the last sub-figure of Figure 3.19. These findings demonstrate that each proposed detector effectively diagnoses the corresponding cyber-attacks, and other anomalies do not affect their detection performance. Consequently, regarding provided simulation scenarios, all faults and cyber-attacks are successfully detected and isolated.

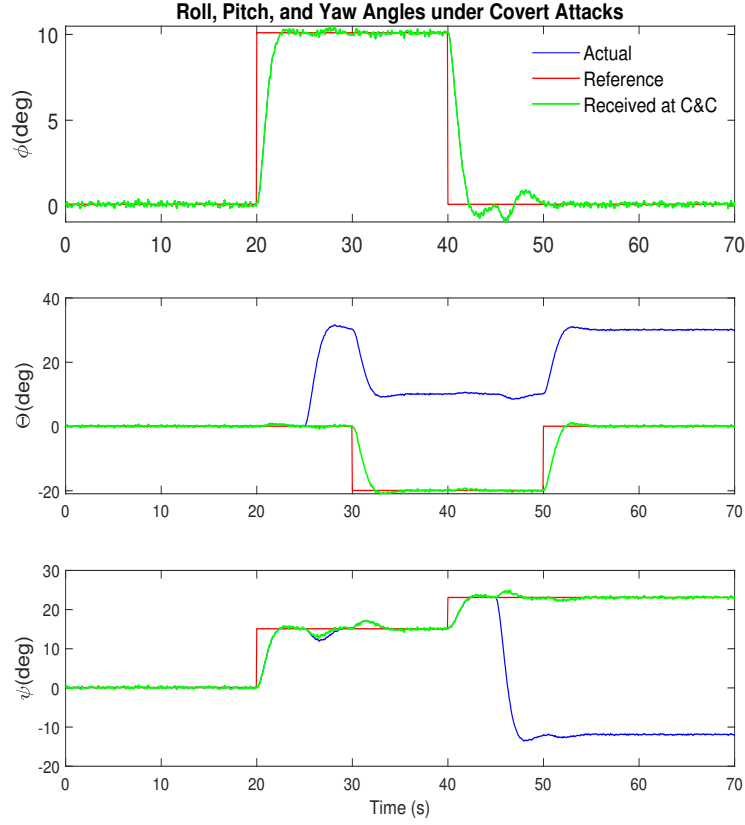


Figure 3.18: The UAV’s measurement outputs, reference, and the received signals at the C&C center under covert attacks.

Performance Evaluations and Comparisons

To investigate false alarm rates and verify the performance of our detection methodology for both cyber-attacks and fault detection, we have obtained confusion matrices that compare the performance of the χ^2 detector with the Euclidean detector [157] across 100 Monte Carlo simulation runs. By manipulating noise amplitudes, thresholds, and varying the time occurrence of anomalies, we have computed precision, recall, and F-score metrics for fault detectors and sensor cyber-attack detectors. To make the detection process practical, we define a “miss trial” as a failure to identify a cyber-attack or fault within the maximum acceptable detection delay, that is denoted by T_{ACC} . Based on simulation results and criteria such as the simulation period and the minimum time required for an anomaly to fully impact the UAV system, we set $T_{ACC} = 20$ seconds. Precision, recall, and F-score were also computed across all trials to evaluate detector performance [140], as follows,

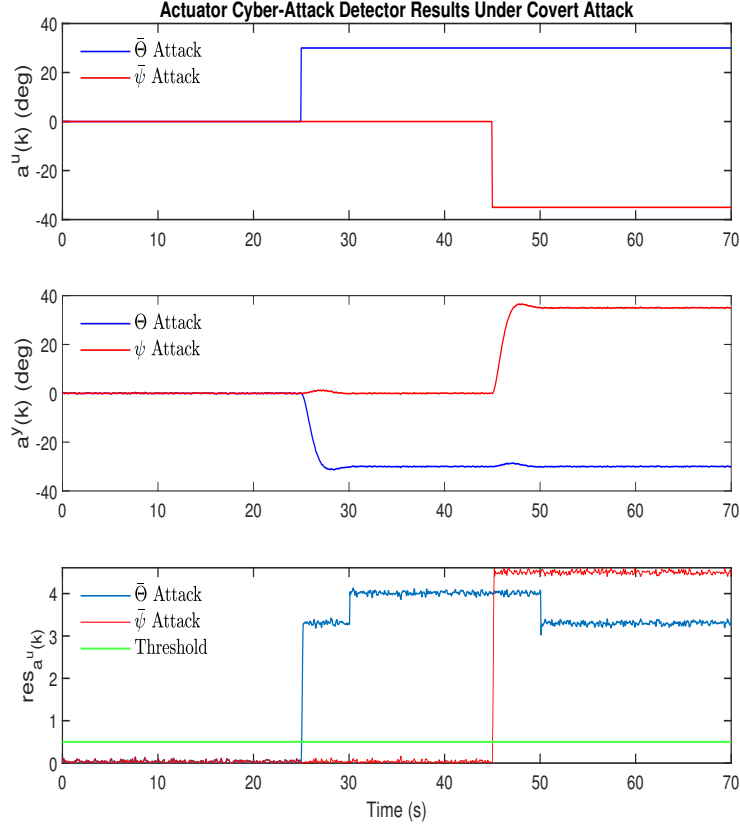


Figure 3.19: Covert attacks signals and the detection results.

$$\begin{aligned}
 precision &= \frac{num(\tau \leq T_s \leq \tau + T_{ACC})}{num(\tau \leq T_s \leq \tau + T_{ACC}) + num(T_s \leq \tau)}, \\
 Recall &= \frac{num(\tau \leq T_s \leq \tau + T_{ACC})}{num(\tau \leq T_s \leq \tau + T_{ACC}) + num(T_s \geq \tau + T_{ACC})}, \\
 F-score &= 2 \times \frac{precision \times Recall}{precision + Recall}
 \end{aligned} \tag{66}$$

where τ denotes the actual fault/cyber-attack occurrence time, T_s denotes the anomaly detection time announced by detectors, and $num(\cdot)$ represents the number of trials in which the detection time is the specific period. For instance, $num(T_s \leq \tau)$ denotes the number of trials leading to a false alarm. Table 3.1 presents the confusion matrix for the normal case of faults and cyber-attacks for χ^2 and Euclidean detectors. A normal range of measurement noise is provided for the fault detector under normal conditions when the system is free from cyber-attacks. A similar scenario is provided for the cyber-attack detector assuming faults have occurred in the system.

Due to accurate threshold selection, both detectors result in low false alarm rates. However, the χ^2 methodology shows superior performance regarding the above metrics.

Table 3.1: Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under normal measurement noise.

Metrics	$\chi^2(Fault)$	ED (Fault)	$\chi^2(Attack)$	ED (Attack)
Precision	0.95	0.91	0.98	0.92
Recall	0.92	0.93	1	0.98
F-score	0.93	0.92	0.96	0.95

Table 3.2: Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under measurement noise multiplied by 10.

Metrics	$\chi^2(Fault)$	ED (Fault)	$\chi^2(Attack)$	ED (Attack)
Precision	0.91	0.75	0.94	0.78
Recall	0.95	0.96	0.95	0.98
F-score	0.93	0.84	0.95	0.87

Table 3.3: Precision, recall, and F-score for χ^2 and Euclidean detectors (ED) in fault and cyber-attack detection under measurement noise multiplied by 20.

Metrics	$\chi^2(Fault)$	ED (Fault)	$\chi^2(Attack)$	ED (Attack)
Precision	0.88	0.63	0.89	0.65
Recall	1	0.98	1	1
F-score	0.94	0.77	0.94	0.79

We increase the magnitude of noise first by 10 times and then by 20 times the nominal condition. We investigate precision, recall, and F-score metrics in Tables 3.2 and 3.3, respectively.

Across these scenarios, the Euclidean-based detector experiences significant performance fluctuations, leading to higher false alarm rates and consequently lower overall performance. In contrast, the χ^2 detector remains relatively stable due to the fact that its detection function includes the estimation error covariance. For both detectors, it can be concluded that as the magnitude of noise increases, their precision decreases. Additionally, the presence of a fault does not significantly impact the cyber-attack detector performance since the effects of known faults have been taken into account to obtain the cyber-attack thresholds.

3.6.3 Auxiliary Filter-Based Actuator and Sensor Attack Detection for the UAV Case Study

In this section, we aim to detect and isolate actuator and sensor cyber-attacks using the proposed auxiliary filters implemented on both the plant and C&C sides. Within the CPS framework illustrated in Figure 3.2, the communication networks associated with sensors and actuators, as well as the auxiliary filters themselves, are assumed to be vulnerable to FDI attacks. Furthermore, it is assumed that no faults occur in this scenario.

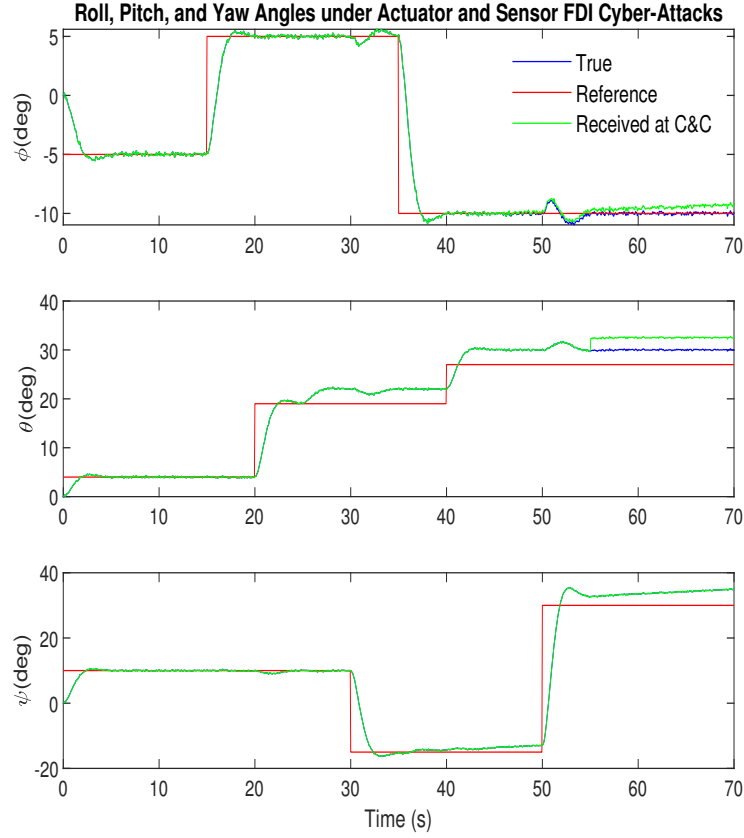


Figure 3.20: The UAV's measurement outputs, reference values, and the received signals at the C&C center under actuator and sensor FDI attacks.

We consider two FDI attacks in the actuator network, targeting the control of $\bar{\theta}$ and $\bar{\psi}$, and two FDI attacks in the sensor network, affecting the measurements of ϕ and θ . All of these attacks are addressed using the proposed auxiliary filter-based methodology.

Although the proposed theorems guarantee that the residuals converge to zero in the absence of cyber-attacks, it is still necessary to define detection thresholds due to the presence of noise in the simulation. These thresholds are established by running the system multiple times under varying conditions, ensuring that each residual remains below its corresponding threshold in the absence of cyber-attacks and exceeds it when the respective

cyber-attack occurs.

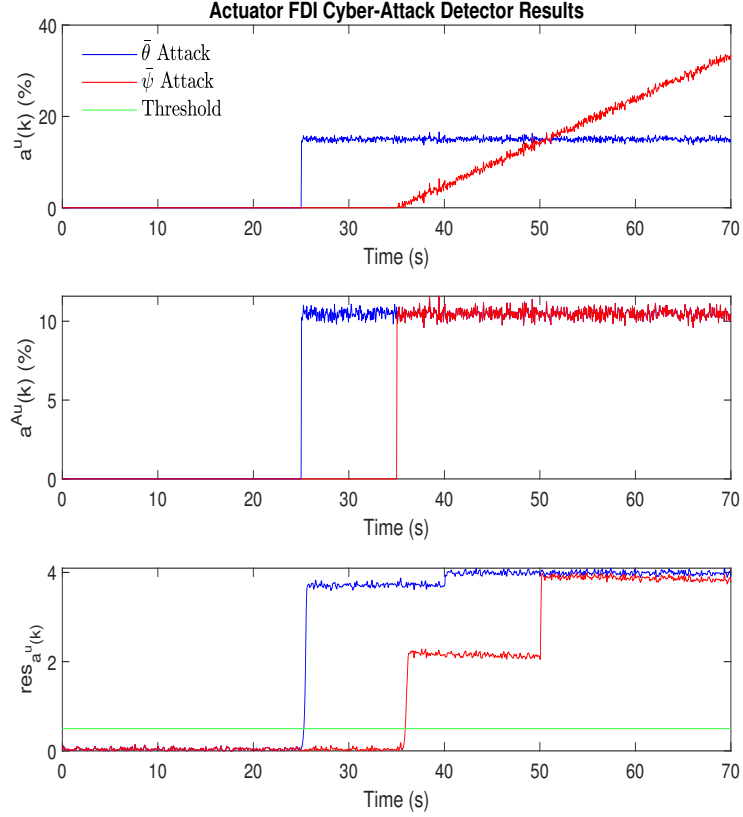


Figure 3.21: Actuator cyber-attack detection results, including actuator and auxiliary filter cyber-attacks, and residuals.

Initially, the CPS operates under normal, healthy conditions and adheres to reference values issued by the C&C center, as shown in the first 25 seconds of Figure 3.20. Subsequently, actuator FDI attacks corresponding to $\bar{\theta}$ and $\bar{\psi}$ occur at times 25 seconds and 35 seconds, respectively. Additionally, sensor cyber-attacks ϕ and θ are assumed to occur at times 45 seconds and 55 seconds, respectively. The impact of these cyber-attacks on system outputs is depicted in Figure 3.20. The models of actuator and sensor cyber-attacks, including auxiliary filters cyber-attacks, are represented in the first two subfigures of Figures 3.21 and 3.22, respectively. Actuator cyber-attacks can cause the system states (true values) to diverge from the reference values issued by the C&C center, while sensor cyber-attacks have the potential to mislead the monitoring system in the C&C by altering the received signals. By leveraging the proposed cyber-attack detection methodology, we are able to recognize the cause of the divergence and the alteration.

To detect and isolate actuator cyber-attacks, the auxiliary filters given in (51) and (52) are utilized. Similar to the design outlined in (66), appropriate auxiliary filter parameters

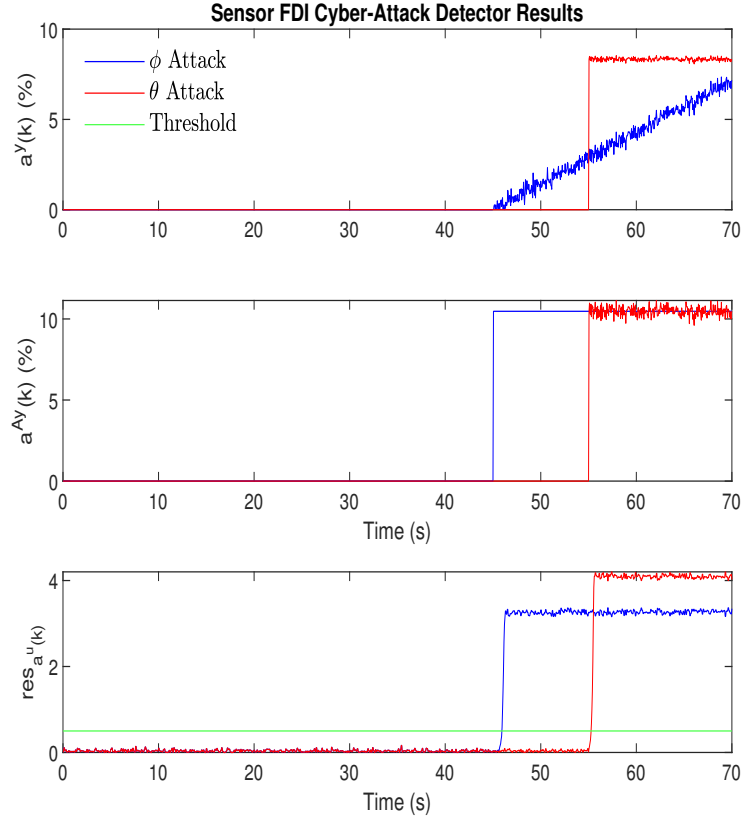


Figure 3.22: Sensor cyber-attack detection results, including sensor and auxiliary filter cyber-attacks and residuals.

are selected for both actuator and sensor cyber-attack detection.

Figure 3.21 illustrates the FDI attacks occurring on the communication networks of $\bar{\theta}$ and $\bar{\psi}$, along with the auxiliary filters and the residuals of actuator cyber-attacks. Moreover, Figure 3.22 presents the FDI attacks of the communication networks of ϕ and θ , along with the auxiliary filters and the residuals of sensor cyber-attacks. Each residual is defined particularly for each network channel, and they are only sensitive to the corresponding cyber-attack and are decoupled from others. Consequently, isolating among different cyber-attacks is possible; this can be illustrated in the last subfigures of Figures 3.21 and 3.22.

3.7 CONCLUSIONS

In conclusion, this chapter presents a comprehensive approach to enhance the security of cyber-physical systems (CPS), offering several significant contributions and innovations. First, we have effectively addressed the challenges posed by cyber-attacks on sensors and actuators network, along with system faults. Moreover, the introduction of an Augmented

Unscented Kalman Filter (AUKF) for state and fault estimation, including a thorough stability analysis, in conjunction with the AUKF-based and auxiliary filters for cyber-attack detection, empowers the system to adeptly detect and isolate cyber-attacks, even in presence of system faults. This approach provides clear differentiation between faults and cyber-attacks in the cyber-attack detector. Furthermore, the systematic design of auxiliary filters improves the method's feasibility for detecting actuator cyber-attacks. Ultimately, validation through simulations in a high-fidelity UAV model scenario underscores the methodology's effectiveness in monitoring the CPS security and reliability.

Chapter 4

Reinforcement Learning-Based Cyber-Attack and Fault Detection and Isolation of Nonlinear Cyber-Physical Systems

In this chapter, we explore advanced reinforcement learning (RL)-based methodologies for the detection and isolation of faults and cyber-attacks in nonlinear cyber-physical systems (CPS). As CPS become increasingly complex and networked, they are more exposed to stealthy cyber threats and unexpected system faults, which can significantly degrade performance and compromise safety. Addressing the challenge of distinguishing between cyber-attacks, faults, and noise is therefore critical for ensuring secure operation.

We first present a Q -table reinforcement learning-based approach for the joint detection and isolation of actuator and sensor faults and cyber-attacks. This method combines model-based and data-driven techniques by leveraging the Augmented unscented Kalman filter (AUKF) for accurate state and fault estimation, alongside a State-action-reward-state-action (SARSA) learning module that enables online decision-making. The proposed framework is designed to provide early detection with a low false alarm rate by continuously updating the Q -table based on observed system behavior. An online decision-making module is introduced to distinguish and isolate various anomalies, including machine-induced faults and cyber-attacks, in real-time.

To further enhance the detection capability, we introduce a deep reinforcement learning (DRL)-based hybrid framework that builds on the limitations of tabular RL in high-dimensional nonlinear systems. This advanced method employs Deep Q -Networks (DQN) to train a detector that not only accelerates the detection process but also improves robustness against stealthy and covert cyber-attacks that traditional detectors may fail to identify. The DRL-based detector is supported by auxiliary filters and the AUKF, which together

provide analytical insights that enhance the learning agent’s decision-making accuracy. This integration allows for a more comprehensive understanding of system behavior under various operating conditions.

Extensive simulations on the UAV platform show that the proposed RL-based methodologies outperforms classical χ^2 -based and Euclidean-based schemes in terms of detection speed, accuracy, and reliability, establishing it as a powerful tool for real-time security monitoring in nonlinear CPS.

The main contributions of this chapter are summarized as follows:

- (i) **RL-Based Online Detection and Isolation:** We develop a Q -table RL method for real-time detection and isolation of system faults and sensor cyber-attacks. The approach enables an agent to learn optimal detection policies through direct interaction with the CPS environment, addressing both faults and attacks dynamically.
- (ii) **Design of a DRL-Based Detection and Isolation Architecture:** We design a DQN architecture tailored to detect and isolate cyber-attacks targeting both sensors and actuators. The framework leverages high-dimensional state representations extracted from the CPS environment to enable accurate and scalable anomaly localization.
- (iii) **Optimal Policy Learning for Timely and Reliable Detection:** We propose learning-based algorithms that enable the agent to discover optimal detection policies, emphasizing early detection while minimizing false alarms and supporting real-time implementation in CPS environments.
- (iv) **Integration of State and Fault Estimation Techniques:** We incorporate an AUKF for joint state and fault estimation, along with auxiliary filters for deeper analytical insight. These model-based signals are used as informative features for the RL-based detection systems, significantly improving accuracy and robustness.
- (v) **Capability to Distinguish Among Different Anomalies and Detect Stealthy Attacks:** By integrating auxiliary filters and the AUKF within an online decision-making framework, the proposed methodologies exhibit a strong ability to differentiate between sensor and actuator cyber-attacks and system faults. Furthermore, they effectively detect and isolate stealthy cyber-attacks, including covert attacks that are designed to bypass conventional detection mechanisms.
- (vi) **Comprehensive Validation through High-Fidelity UAV Simulations:** The proposed methodologies are validated via detailed case study simulations using a high-fidelity UAV model. We perform comparative analyses against conventional χ^2 -based, Euclidean-based, and Q -table RL-based schemes, showing superior performance in detection and isolation speed, accuracy, and reliability.

The remainder of the chapter is organized as follows. Section 4.1 formally defines the anomaly detection problem in the RL context, highlighting the integration of estimated state and fault information into the learning environment. Section 4.2 introduces a classical tabular RL method to detect and isolate sensor and actuator anomalies based on system observations and estimation residuals. In Section 4.3, a DRL approach is proposed to overcome the scalability limitations of Q-table methods. The DRL agent is trained to process high-dimensional inputs, including outputs from the AUKF and auxiliary filters, thereby improving accuracy and generalization in detecting complex anomalies. Section 4.4 presents simulation results demonstrating the adaptability and robustness of the proposed RL-based strategies under diverse cyber-attack and fault scenarios in UAV systems.

4.1 Problem formulation

The mathematical model of the nonlinear CPS, including fault signals and additive noise is considered as follows:

$$\begin{aligned} x(k+1) &= f(x(k)) + g(x(k))u(k) + \mathcal{L}_1(x(k))\theta(k) + w(k) \\ y(k) &= h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + v(k), \end{aligned} \quad (67)$$

where k denotes the discrete-time sample, $x(k) \in \mathbb{R}^n$ represents the state, $u(k) \in \mathbb{R}^p$ denotes the control input, and $y(k) \in \mathbb{R}^q$ denotes the measured output. The functions $f(x(k))$, $g(x(k))$, and $h(x(k))$ denote nonlinear terms having appropriate dimensions. The fault vector at time k is denoted by $\theta(k) \in \mathbb{R}^{n_\theta}$, $\mathcal{L}_1$ and $\mathcal{L}_2$ denote the dynamic matrices of differentiable functions depending on the system states that model anomalies as fault vectors. Additionally, $w(k) \in \mathbb{R}^n$ and $v(k) \in \mathbb{R}^q$ represent zero-mean white Gaussian noise for the process and measurements, respectively. The system states and the fault signals are assumed to be observable.

First, we consider the case where the system is affected by the fault vector and the attacker compromises the sensor communication network. In Section 4.3, we shift our focus to a fault-free CPS that is compromised by both actuator and sensor cyber-attacks. The initial CPS architecture is illustrated in Figure 4.1, where the command and control (C&C) center may be geographically distant from the plant and is connected to it solely through communication networks. When the sensor communication channels are compromised by a cyber-attack, the output received at the C&C side becomes:

$$y^A(k) = h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + D^A A^y(k) + v(k). \quad (68)$$

where $y^A(k) \in \mathbb{R}^q$ denotes the output received at the C&C, $A^y(k) \in \mathbb{R}^{q_A}$ denotes the FDI cyber-attack signal, and D^A describes the sensor attack signature, determining which

communication channels are compromised by the attackers. Both $A^y(k)$ and D^A can be arbitrarily changed and selected by the attacker.

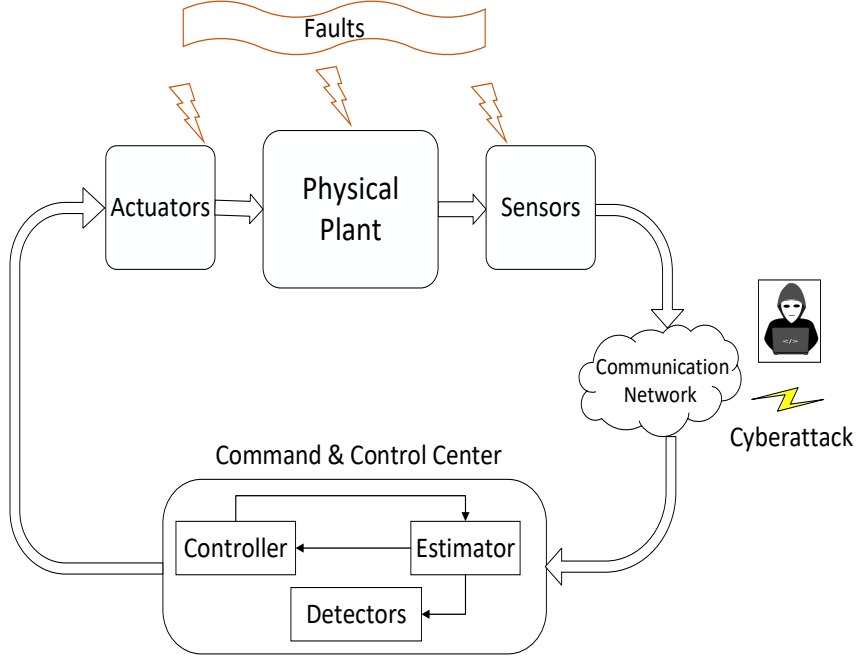


Figure 4.1: The CPS under faults and FDI cyber-attacks in sensor network.

4.1.1 State and Fault Estimation Filter

Given that the fault dynamics are described by

$$\theta(k+1) = \theta(k) + f_\theta(x(k), \theta(k)), \quad (69)$$

where f_θ is a nonlinear differentiable function, the fault is treated as an additional system state. By augmenting the system state and fault variables into a single vector $X(k) = [x^T(k); \theta^T(k)]^T \in \mathbb{R}^N$, where $N = n + n_\theta$, and defining the system output as $y(k) = H(X(k)) = h(x(k)) + \mathcal{L}_2(x(k))\theta(k)$, the overall state-space representation of the CPS is derived by combining both models (67) and (69).

To perform augmented state estimation, we adopt the Augmented Unscented Kalman Filter (AUKF) scheme, as detailed in Chapter 3. The estimates of the augmented state vector $\hat{X}(k)$, the system output $\hat{y}(k)$, and the state covariance $\hat{\mathbf{P}}_X(k)$ are computed as follows:

$$\begin{aligned} \hat{X}(k) &= \hat{X}(k|k-1) + K(k)(y^A(k) - \hat{y}(k|k-1)) \\ \hat{y}(k) &= H(\hat{X}(k|k-1)) \\ \hat{\mathbf{P}}_X(k) &= \hat{\mathbf{P}}_X(k|k-1) - K(k)\hat{\mathbf{P}}_y(k)K(k)^T \end{aligned} \quad (70)$$

where $\hat{X}(k|k-1)$ and $\hat{y}(k|k-1)$ represent the prior estimates of the state and output, respectively. Additional implementation details can be found in section 3.2.

In the following, we present two reinforcement learning-based frameworks: a Q -table RL method tailored for the detection and isolation of system faults and sensor cyber-attacks, and a DRL approach aimed at detecting and isolating both actuator and sensor cyber-attacks.

4.2 The Q -table Reinforcement Learning-Based Anomaly Detection and Isolation

Drawing from RL principles, we model the detection problem as a partially observable Markov decision process (POMDP), where the defender (agent) interacts with the environment, which consists of the system model and the observation space. A POMDP is defined by the tuple $(\mathcal{S}, \mathcal{A}, \mathcal{O}, \mathcal{T}, \mathcal{R})$, where $\mathcal{S}$ represents the overall system states that might be hidden, $\mathcal{A}$ is the set of actions, $\mathcal{O}$ is the set of observations, $\mathcal{T}$ defines the transition probabilities between states, and $\mathcal{R}$ is the reward function. The defender makes decisions based on a sequence of observations and actions, aiming to detect and isolate cyber-attacks and faults while accounting for uncertainties in attack strategies, system dynamics, and measurement noise. The objective is to minimize both detection delay and false alarms, ensuring timely and reliable system protection.

Each anomaly introduces two hidden states, namely: pre-occurrence and post-occurrence. The combination of a fault and a cyber-attack is depicted in Figure 4.2. At each time instant, the agent (defender) can choose between two available actions: “stop” to declare a cyber-attack/fault or “continue” to gather additional information. The hidden states and transitions between them that occur at time $k = k_{ij}$ are illustrated with dashed circles and lines, respectively. The defender receives the reward r_{ij} based on the corresponding actions.

The agent’s goal is to achieve an optimal policy as denoted by $\pi : \mathcal{O} \rightarrow \mathcal{A}$, where $\mathcal{A}$ and $\mathcal{O}$ represent the sets of actions and observations, respectively. This optimal policy aims to efficiently map observations to actions while maximizing the agent’s expected total discounted reward. In our approach, the agent updates a Q -table indexed by observation-action pairs, enabling it to learn the optimal policy based on its experiences during the detection process.

Value-based RL algorithms estimate the quality of a policy π using a state-action value function within a given state-action pair (s_k, a_k) [158]. In our setup, the latent states s_k are depicted in Figure 4.2, and the agent selects actions $a_k \in \{\text{stop}, \text{continue}\}$. The state-action value function, also known as the Q -function, is formally defined as:

$$Q(s_k, a_k) = \mathbb{E}[R_k | s_k, a_k], \quad (71)$$

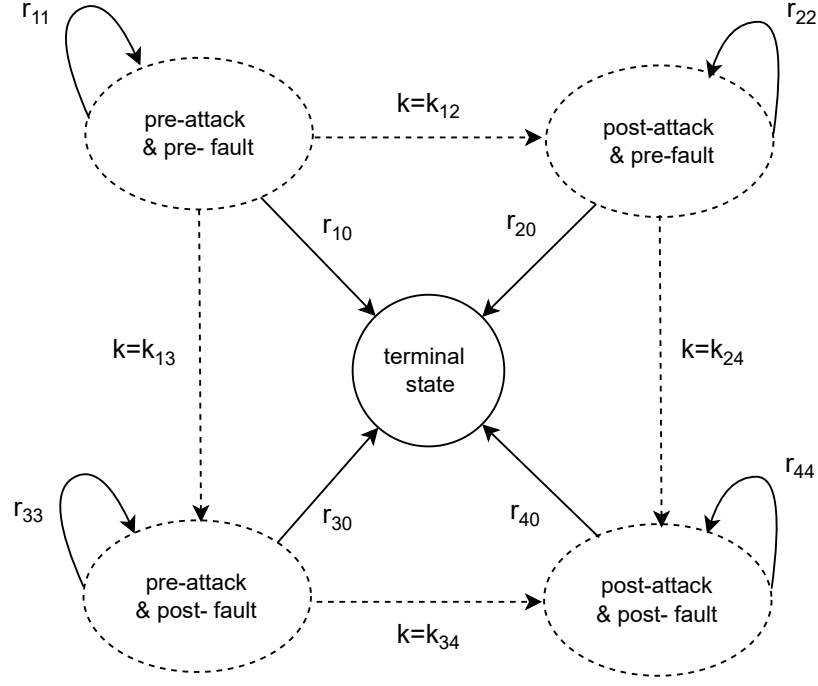


Figure 4.2: A state-machine diagram for the cyber-attack and fault detection and isolation problem, where $k = k_{ij}$ represents the transition time between hidden states, and r_{ij} denotes the received reward based on the corresponding actions.

where R_k denotes the long-term cumulative reward:

$$R_k = \sum_{t=0}^{\infty} \gamma^t r_{k+t+1}, \quad (72)$$

with r representing the immediate reward and $\gamma \in [0, 1)$ the discount factor. The agent updates its policy π in order to maximize the expected return captured by the Q -function.

In our implementation, we adopt the SARSA (State-Action-Reward-State-Action) algorithm, which updates the Q -value based on the actual action taken in the next time step. The SARSA update rule is given by:

$$Q(s_k, a_k) \leftarrow Q(s_k, a_k) + \alpha [r_{k+1} + \gamma Q(s_{k+1}, a_{k+1}) - Q(s_k, a_k)], \quad (73)$$

where α is the learning rate and a_{k+1} is the action selected in the next state s_{k+1} following the current policy.

Since the underlying system states s_k are hidden and only indirectly inferred through observations, we reformulate the value function using observations o_k instead of states. Consequently, we approximate the action-value function as $Q(o_k, a_k)$, where the observation

space will be defined in the following sections. The policy is then obtained as:

$$a_k = \arg \max_a Q(o_k, a). \quad (74)$$

Finally, since our objective is to minimize a long-term cost rather than maximize a reward, the cumulative reward R_k can be reinterpreted as a cumulative cost J_k , and the optimization becomes minimizing J_k . This cost-oriented formulation remains consistent with the reinforcement learning framework.

4.2.1 Optimal Detection Strategy

We develop an optimal detection approach for nonlinear CPS under cyber-attacks and faults by using a very prompt detection framework. Let T_s denote the stopping time chosen by the defender, while τ represents the unknown cyber-attack or fault initiation time. The probability measure of the cyber-attack/fault initiation at the time k is denoted by P_k , and the expectation operator is E_k .

Since τ is unknown, it can, for instance, follow a geometric distribution. Therefore, the stopping problem is formulated as a trade-off between false alarms (premature stopping) and detection delay (delayed stopping). This structure aligns with classical most prompt (quickest) detection problems [159].

To formalize the detection cost, we define the expected total discounted cost in a form analogous to [140]:

$$E\left[\sum_{k=0}^{\infty} \gamma^k r_k\right] = P_{\tau}(\{T_s < \tau\}) + E_{\tau}\left[\sum_{k=\tau}^{T_s} \gamma^k c\right], \quad (75)$$

where the first term represents the false-alarm probability, capturing the event where the stopping time T_s occurs before the attack/fault occurs ($T_s < \tau$). The second term accounts for the detection delay, with each delay step incurring a cost c . The expectation is taken over the attack initiation time τ . In quickest detection problems, the false-alarm penalties are often weighted based on the prior distribution of τ , typically geometric or exponential. This can be explicitly incorporated into our formulation by considering the expected false-alarm rate under a geometric prior on τ , leading to:

$$\begin{aligned} \min_{T_s} \quad & \{P_{\tau}(\{T_s < \tau\}) + E_{\tau}\left[\sum_{k=\tau}^{T_s} \gamma^k c\right]\} \equiv \\ \min_{T_s} \quad & \{P_{\tau}\{T_s^-\} + cE_{\tau}[T_s^+]\}, \end{aligned} \quad (76)$$

where $T_s^- \equiv T_s < \tau$ denotes the premature stopping, and $T_s^+ \equiv \sum_{k=\tau}^{T_s} \gamma^k$ captures

the cumulative discounted delay. By adjusting the cost parameter c , one can balance between minimizing false alarms and reducing the detection delay, thus optimizing detection reliability according to the system requirements.

Given uncertainties in the POMDP model, such as the cyber-attack initiation time τ and the attacker's strategy, a model-free RL approach [160] can be used to optimize the detection policy. Our goal is to establish a direct mapping between observations and actions, determining the optimal stopping time T_s based on the system's pre- or post-attack state. The defender receives measurements at each time step, that are processed for cyber-attack and fault detection objectives by using the previously introduced AUKF estimator.

4.2.2 Detection Function

The defender's goal is to solve (76) by using a RL approach where P_k is unknown. However, this is related to the detection function $\eta(k)$, defined for cyber-attacks as,

$$\eta_A(k) = \tilde{y}(k)^T \tilde{y}(k). \quad (77)$$

where $\tilde{y}(k) = y^A(k) - \hat{y}(k|k-1)$ represents the output estimation error that is obtained in the C&C center and $\hat{y}(k)$ represents the output estimation that is derived from the AUKF.

Theorem 4.1. *Consider the CPS system governed by (67), subject to the cyber-attack $A^y(k)$ and the fault vector θ as defined in (68) and (69), respectively. Given that the system states and fault signals are observable, and assuming that the process and measurement noise covariances are bounded, the estimation error $\tilde{y}(k)$ and, consequently, the detection function (77), remain bounded in absence of a cyber-attack. However, in presence of a cyber-attack, this error is distinctly affected, even when faults are present.*

Proof: Referring to the Theorem 3.1, the state estimation error $\tilde{X}(k)$ and the output estimation error $\tilde{y}(k)$ remain ultimately bounded in the mean square sense, provided no cyber-attack is present. This boundedness holds under the assumptions of Lipschitz continuity of the system dynamics and bounded process and measurement noise covariances.

The capability to distinguish between cyber-attacks and faults relies on the augmented state estimation framework, which explicitly incorporates the fault dynamics. Unlike the system faults that adhere to physical characteristics of sensors and actuators, cyber-attacks introduce anomalies that deviate from these inherent dynamics. Given that cyber-attacks exhibit distinct dynamic behavior, their effects can be isolated and identified through residual analysis and anomaly detection techniques. This distinction enables the system to differentiate between naturally occurring faults and adversarial manipulations, improving the detection reliability.

From (68) and (77), assuming $D^A \neq 0$, the cyber-attack signal $A^y(k)$ directly influences the received output y^A at the command and control (C&C) center, thereby impacting the detection function $\eta_A(k)$. Specifically, since the fault dynamics are explicitly modeled within

the augmented state estimation framework, the resulting estimation error and detection function $\eta_A(k)$ remain bounded despite the presence of faults. Given that the fault-induced residual is consistent with the modeled system dynamics, any additional deviations in the estimation error—caused by a cyber-attack—can be distinguished from those originating from faults.

Moreover, the reinforcement learning (RL)-based detector is trained across a range of fault conditions and cyber-attack scenarios. Consequently, even in the presence of faults, the detector can reliably identify cyber-attacks at the C&C center. This completes the proof. ■

On the other hand, during normal system operation, it is expected that the probability P_k will be low. Consequently, small values of $\eta_A(k)$ (close to zero) may indicate normal system operation. Conversely, during injection of a cyber-attack, when the system deviates from its normal state, an increase in P_k is anticipated. Thus, as stated in Theorem 4.1, sustained elevated values of $\eta_A(k)$ over a window of time may indicate presence of a cyber-attack, potentially aiding in reducing the uncertainty about the system's state.

4.2.3 Observation Space Construction

To tackle the computational complexity in continuous spaces such as $\eta_A(k)$, we employ observation quantization, dividing the observation space into I intervals by using predefined quantization thresholds. Each interval $\beta_{i-1} \leq \eta_A(k) < \beta_i$ corresponds to an observation representation ρ_i at time k . Additionally, a finite observation history of size M is utilized, resulting in I^M possible observation windows. I and M are selected based on the performance of the detection function and the desired memory allocation for storing the Q -table. At any time step k , the sliding window comprises quantized versions of observations within the window, forming the observation space $\mathcal{O}$. For instance, if $I = M = 2$, then $\mathcal{O} = [\rho_1, \rho_1], [\rho_1, \rho_2], [\rho_2, \rho_1], [\rho_2, \rho_2]$.

For each conceivable observation-action pair (o, a) , we propose learning a $Q(o, a)$ value, that is denoted by $Q_A(o, a)$ for cyber-attack detection, representing the expected future cost, through an RL algorithm. All $Q(o, a)$ values are stored in a Q -table of size $I^M \times 2$. Following the learning phase, the defender's policy involves selecting the action a with the minimum $Q(o, a)$ for each observation o .

4.2.4 Detection and Isolation Algorithms

The proposed RL-based detection scheme comprises of two primary phases, namely, (a) the learning phase, and (b) the online detection and isolation phase. In the learning phase, the defender undergoes training by using the SARSA, that is recognized for its effectiveness in POMDP settings [160]. During the training process, the defender accumulates experience through numerous episodes with different given τ values, representing various FDI attacks/faults, leading to the acquisition of a Q -table. A simulation environment

is established where the defender takes actions based on observations and receives corresponding costs. Using this experience, the defender iteratively updates and refines the Q -table.

In the Algorithm 2 presented below, E_n represents the number of learning episodes, T denotes the maximum length of a learning episode, α indicates the learning rate, and ϵ represents the exploration rate. Under the ϵ -greedy policy, an action is chosen with the minimum Q value with a probability of $1 - \epsilon$, while the alternative action is selected with a probability of ϵ for exploration during the learning process. The learning phase does not require storing large amounts of training data, only a sliding observation window of size M needs to be retained at each time.

For the presence of fault detection, a corresponding algorithm similar to the Algorithm 2 is required. In this algorithm, (78) is employed instead of (77) to compute $\eta_{\theta_l}; l \in 1 \dots \mathbb{R}^{n_\theta}$ for each fault, as follows:

$$\eta_{\theta_l}(k) = \tilde{\theta}_l(k)^T \tilde{\theta}_l(k) \quad (78)$$

where $\tilde{\theta}_l(k) = (\theta_l^m(k) - \hat{\theta}_l(k))$. Here, $\theta_l^m(k)$ represents the fault model, considering the known fault dynamics given in (69), and $\hat{\theta}_l(k)$ represents the output of an AUKF. Consequently, there is a bank of AUKFs, each designed for the corresponding fault parameter $\theta_l \in \theta$. It should be pointed out that $\theta_l^m(k)$ is not affected by the actual fault occurrence, while $\hat{\theta}_l(k)$, in accordance with the fault observability condition and the presence of $y^A(k)$ in the AUKF equation (70), is impacted by the occurrence of the corresponding fault. Consequently, this signal can be used in an RL-based detection and decision-making process.

In the online detection or decision-making phase, as outlined in Algorithm 3, actions are determined based on observations. The defender selects the action with the lowest expected future cost (Q value) at each time, by using the previously learned Q -tables for cyber-attacks and faults. The online detection phase continues until the defender selects the stop action, indicating the declaration of a cyber-attack or a fault and termination of the process. It should be noted that following the declaration of a cyber-attack or a fault and subsequent restoration of the system to normal operating conditions, the online detection phase can be recommenced. In other words, once a defender is trained, no further training is necessary.

The proposed RL-based detection algorithm is implemented using the SARSA algorithm, which enables stable decision-making through iterative updates of the Q -value function. As an on-policy method, SARSA ensures convergence under standard conditions such as sufficient exploration of the observation-action space and a properly decaying learning rate [160]. Operating in an online learning framework, SARSA inherently adapts to variations in system dynamics while preserving robustness in decision outcomes. This

Algorithm 2 Learning Phase cyber-attack Detection

```
Initialize  $Q_A(o, a)$  arbitrarily,  $\forall o \in \mathcal{O}$  and  $\forall a \in \mathcal{A}$ .
for  $ep = 1$  to  $E_n$  do
   $k \leftarrow 0$ ,  $o \in \{\mathcal{O} | s = \text{pre-cyber-attack}\}$ 
   $s \leftarrow \text{pre-cyber-attack}$ ,  $a \leftarrow \text{continue}$ 
  while  $k < T$  do
     $k \leftarrow k + 1$ 
    if  $a = \text{stop}$  then
       $s \leftarrow \text{terminal}$ 
      if  $k < \tau$  then
         $r \leftarrow 1$ 
      else
         $r \leftarrow 0$ 
      end if
       $Q_A(o, a) \leftarrow Q_A(o, a) + \alpha(r - Q_A(o, a))$ 
    else if  $a = \text{continue}$  then
      if  $k \geq \tau$  then
         $r \leftarrow c$ 
         $s \leftarrow \text{post-cyber-attack}$ 
      else
         $r \leftarrow 0$ 
      end if
      Compute  $\eta_A(k)$  using (77) and quantize it.
      Update observation window  $o$  with recent  $\rho_i$  and get  $o'$ .
      Choose  $a'$  randomly (probability  $\epsilon$ ) or as:
       $a' \leftarrow \text{argmin}_a Q(o', a)$  with probability  $1 - \epsilon$ .
       $Q_A(o, a) \leftarrow Q_A(o, a) + \alpha(r + \gamma Q_A(o', a') - Q_A(o, a))$ 
       $o \leftarrow o'$ ,  $a \leftarrow a'$ 
    end if
  end while
end for
Output:  $Q$ -table  $Q_A(o, a)$ ,  $\forall o \in \mathcal{O}$ ,  $\forall a \in \mathcal{A}$ 
```

robustness is further enhanced by a reward structure that penalizes both premature stopping (false alarms) and excessive detection delays, thereby enforcing an optimal balance between responsiveness and reliability. Moreover, the use of a sliding observation window helps attenuate the effects of transient disturbances, enabling the algorithm to generalize across diverse operating scenarios.

The SARSA algorithm updates the Q -table gradually, one step at a time, over a fixed number of episodes, each with a known time duration limit. The time complexity of SARSA does not depend on the size of the action or observation spaces. Moreover, the corresponding space complexity stays constant by using a sliding observation window, which reduces the need for storing large training datasets.

Algorithm 2 is designed for cyber-attack detection, while a similar algorithm based on

Algorithm 3 Decision Maker: Online Cyber-Attack and Fault Detection and Isolation.

```
1:  $Q$ -tables learned in Algorithm 1 for sensor cyber-
   attack and faults detection.
2:  $o \in \{\mathcal{O} | s = \text{pre-attack}\}$ ,  $a \leftarrow \text{continue}$ ,  $k \leftarrow 0$ 
3: while  $a \neq \text{stop}$  do
4:    $k \leftarrow k + 1$ 
5:   Collect the measurements  $y(k)$ 
6:   Compute  $\eta_A(k)/\eta_{\theta_i}(k)$  using (77)/(78) and
   quantize it to obtain  $\rho_i$  if  $\beta_{i-1} \leq \eta_A(k)/\eta_{\theta_i}(k) < \beta_i$ , for  $i = 1, \dots, I$ 
7:   Update the sliding observation window with the
   recent entry  $\rho_i$  and obtain new  $o$ .
8:   Compute  $Q_A(o, a)$  and  $Q_F(o, a)$  for all  $a$ 
9:    $a_{AS} \leftarrow \arg \min_a Q_A(o, a)$ 
10:   $a_F \leftarrow \arg \min_a Q_F(o, a)$ 
11:  if  $a_{AS} = \text{stop}$  then
12:     $s \leftarrow \text{Sensor cyber-attack detected}$ 
13:     $a \leftarrow \text{stop}$ 
14:  else if  $a_F = \text{stop}$  then
15:     $s \leftarrow \text{System fault detected}$ 
16:     $a \leftarrow \text{stop}$ 
17:  else
18:     $s \leftarrow \text{System is healthy}$ 
19:     $a \leftarrow \text{continue}$ 
20:  end if
21: end while
22: Terminate the procedure
```

(78) instead of (77) is trained for each fault. Although cyber-attacks can influence the fault estimation process, and thus impact the fault detection and isolation performance, they remain detectable and isolatable even under presence of system faults.

Remark 4.1. *The RL methodology proposed above can potentially be applied to detect other types of anomalies, such as actuator cyber-attacks, as long as they affect the system output, and thus influence the detection function that is governed by (77). However, similar to many detection methods, our approach has limitations. If a cyber-attack does not affect the measurement signals received at the C&C center or closely mimics a system fault for which the detector is trained, it may be challenged to detect the cyber-attack or differentiate between the origin of it (isolating actuator vs. sensor).*

4.3 Deep Reinforcement Learning-Based Sensor and Actuator Cyber-Attack Detection and Isolation

The mathematical model of the nonlinear CPS considered in this section is given by:

$$\begin{aligned} x(k+1) &= f(x(k)) + g(x(k))u^*(k) + w(k) \\ y(k) &= h(x(k)) + v(k), \end{aligned} \quad (79)$$

where k represents the discrete-time sample, $x(k) \in \mathbb{R}^n$ denotes the state, $u^*(k) \in \mathbb{R}^p$ represents the control input received at the plant side, and $y(k) \in \mathbb{R}^m$ denotes the measured output. The functions $f(x(k))$, $g(x(k))$, and $h(x(k))$ denote nonlinear terms having appropriate dimensions. Additionally, $w(k) \in \mathbb{R}^n$ and $v(k) \in \mathbb{R}^m$ represent zero-mean white Gaussian noise for the process and measurements, respectively. The system states are assumed to be observable.

The architecture of the CPS is illustrated in Figure 4.3, where the C&C center is connected to the plant exclusively via communication networks. Both the control inputs to the plant and the measured outputs received at the C&C side may be affected by cyber-attacks on the communication links between the actuators and sensors. The control and output signals, under such attacks, are represented as:

$$\begin{aligned} u^A(k) &= u^*(k) = u(k) + B^A A^u(k) \\ y^A(k) &= h(x(k)) + \mathcal{L}_2(x(k))\theta(k) + D^A A^y(k) + v(k), \end{aligned} \quad (80)$$

where $u(k)$ is the control or reference signal generated at the C&C center. The signals $u^A(k) \in \mathbb{R}^p$ and $y^A(k) \in \mathbb{R}^m$ represent the control input and output received at the plant and C&C sides, respectively. The vectors $A^u(k) \in \mathbb{R}^{p_A}$ and $A^y(k) \in \mathbb{R}^{m_A}$ denote the cyber-attack signals introduced into the actuator and sensor channels. The matrices B^A and D^A characterize the corresponding cyber-attack signatures. These attack signals can be arbitrarily manipulated by a malicious adversary.

To perform state estimation, which will later be utilized for sensor cyber-attack detection, we employ the AUKF scheme as outlined in (70). Since the presence of faults is not considered in this section (as indicated by the system model in (79)), the AUKF is used to estimate only the system states x .

For DRL-based actuator cyber-attack detection, we employ the two auxiliary filters proposed in Section 3.4, under their corresponding assumptions. The formulation of the auxiliary filter on the C&C side is given as follows,

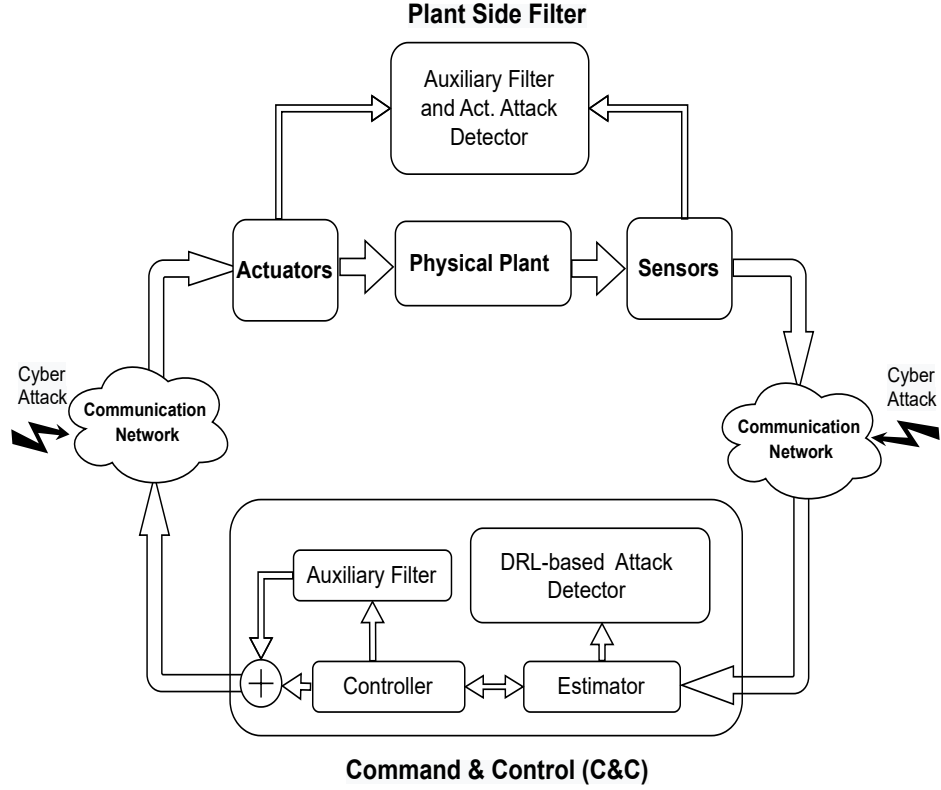


Figure 4.3: The CPS under FDI cyber-attacks in actuator and sensor networks.

$$\begin{aligned}
 z_{Au}^{CC}(k+1) &= A_{Au}z_{Au}^{CC}(k) + F_{Au}(z_{Au}^{CC}(k)) + T_{Au}u(k) \\
 &+ K_{Au}y^A(k),
 \end{aligned} \tag{81}$$

where $z_{Au}^{CC}(k) \in \mathbb{R}^n$ represents the state of the auxiliary filter at the C&C side. The nonlinear term and matrices $F_{Au}(\cdot)$, A_{Au} , T_{Au} , and K_{Au} are of appropriate dimensions and have been designed and selected in Section 3.4. The corresponding auxiliary filter on the plant side is expressed as:

$$\begin{aligned}
 z_{Au}^p(k+1) &= A_{Au}z_{Au}^p(k) + F_{Au}(z_{Au}^p(k)) + T_{Au}u^A(k) + K_{Au}y(k) \\
 &+ L_{Au}^p(z_{Au}^p(k) - (z_{Au}^{CC}(k) + D_{Au}^A A_{Au})).
 \end{aligned} \tag{82}$$

where, $z_{Au}^p(k) \in \mathbb{R}^n$ denotes the state of the auxiliary filter at the plant side, while $a^{Au} \in \mathbb{R}^{n_{a^{Au}}}$ illustrates the cyber-attack on the communication channels between the two filters with the signature D_{Au}^a . Additionally, the residual signal used for attack detection is defined as:

$$res_{Au(k)} = L_{Au}^p(z_{Au}^p - {}^A z_{Au}^{CC}), \quad (83)$$

The parameters and terms used in these filters, as well as the gain of the filter, L_{Au}^p , have been introduced and described in detail in Section 3.4.

The proposed AUKF-based state estimator and the auxiliary filter-based residual both serve as critical inputs to the DRL-based detection and isolation framework introduced in the following subsection.

4.3.1 DRL-Based Cyber-Attack Detection and Isolation Formulation

Similar to the Q -table-based detection method presented in Subsection 4.2, the detection problem is formulated as a POMDP problem, where the detector is modeled as an agent that interacts with the system model and the observation space within its environment. However, rather than storing state-action values in a Q -table, the Q -function is approximated using a DRL approach. The primary objective is to promptly detect and isolate actuator and sensor cyber-attacks while minimizing both detection delay and false alarms. This enables a reliable and timely response, addressing the challenges of real-time anomaly detection in nonlinear cyber-physical systems.

Each anomaly is modeled with two hidden states: pre-occurrence and post-occurrence. The combination of actuator and sensor cyber-attacks is illustrated in Figure 4.4. At each time step, the agent (defender), located at the C&C center, can choose one of two actions: “stop” to declare the presence of a cyber-attack, or “continue” to collect additional observations. The hidden states and their transitions, which occur at time $k = k_{ij}$, are depicted using dashed circles and lines, respectively. Based on the selected action, the defender receives a corresponding reward r_{ij} .

The agent’s objective is to determine an optimal policy, denoted by $\pi : \mathcal{O} \rightarrow \mathcal{A}$, which maps observations to actions in a manner that maximizes the expected cumulative discounted reward.

Value-based RL algorithms employ the state-action value function to evaluate a policy π for a given state-action pair (s_k, a_k) [158]. In this context, the hidden states s_k correspond to the discrete pre- and post-anomaly conditions illustrated in Figure 4.4, while the actions a_k consist of either declaring an attack (“stop”) or continuing the observation (“continue”). The optimal action is selected according to:

$$\begin{aligned} a_k &= \underset{a}{\operatorname{argmax}} Q(s_k, a) \\ Q(s_k, a_k) &= \mathbb{E}[R_k \mid s_k, a_k] = \mathbb{E}[r_{k+1} + \gamma r_{k+2} + \gamma^2 r_{k+3} + \cdots \mid s_k, a_k], \end{aligned} \quad (84)$$

where R_k represents the long-term cumulative reward, r_k denotes the immediate reward at

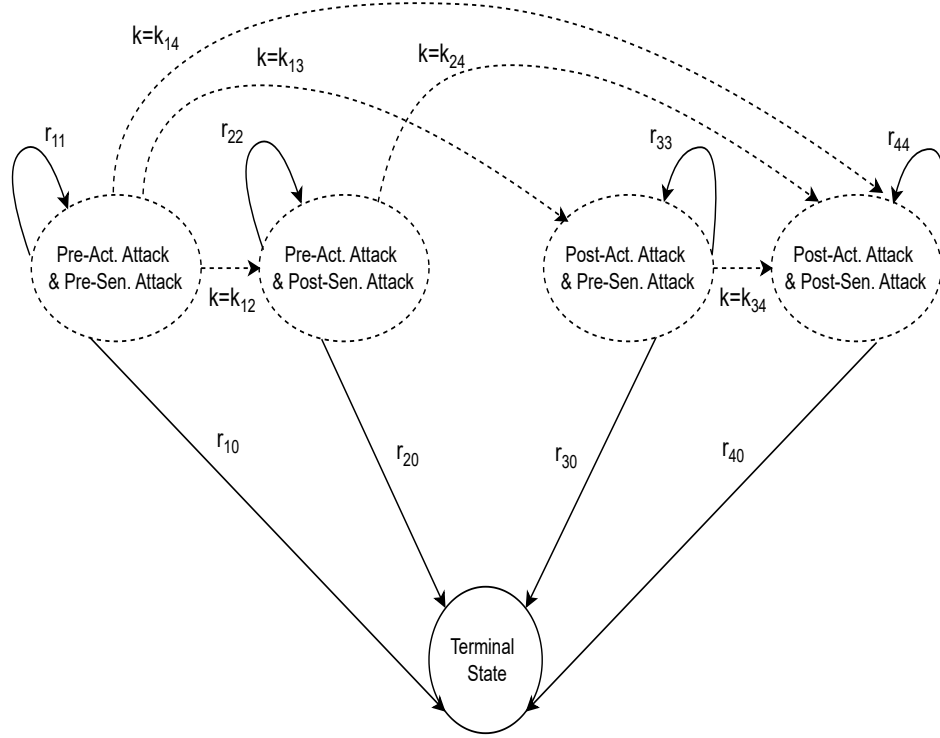


Figure 4.4: A state-machine diagram for actuator and sensor cyber-attack detection and isolation problem. $k = k_{ij}$ represents the transition time between hidden states, and r_{ij} denotes the received reward based on the corresponding actions.

time step k , and $\gamma \in [0, 1]$ is the discount factor that prioritizes immediate rewards over distant ones.

Tabular reinforcement learning relies on a lookup table or Q -table to store expected rewards (Q -values) for each state-action pair. However, as the sizes of the state and action spaces increase, this approach requires substantial memory and computation, rendering it impractical for large-scale or high-dimensional problems. In many real-world applications, the state and action spaces are continuous, making tabular methods such as SARSA and Q -learning inefficient and often infeasible. In contrast, deep learning has emerged as a powerful enhancement to traditional RL approaches. By leveraging function approximation and representation learning, deep neural networks can extract compact, low-dimensional features from raw high-dimensional inputs, thereby significantly improving learning efficiency and enabling reinforcement learning to scale to complex environments [161].

Training a DQN with deep neural networks (DNNs) for Q -function approximation can be unstable due to strong correlations between sequential observations and between the Q -values, $Q(s, a)$, and their corresponding target values $Q(s', a')$. This instability may result in inefficient learning and potential divergence during training [162].

To mitigate this issue, two essential techniques, namely experience replay memory and target networks were introduced for DQN in [163]. Experience replay memory allows the

agent to store a collection of past experiences and sample them randomly during training, preventing the correlations that arise from consecutive experiences. In contrast, the target network acts as a static copy of the estimation network, with its parameters remaining unchanged for a fixed number of updates before being refreshed. A schematic representation of the target network technique, as implemented in this work, is shown in Figure 4.5. This stabilization strategy helps disrupt the direct feedback loop between predicted and target Q -values, reducing harmful correlations. As demonstrated in [163], DQN updates the target network only after large number of updates to the estimation network, leading to more stable and reliable learning.

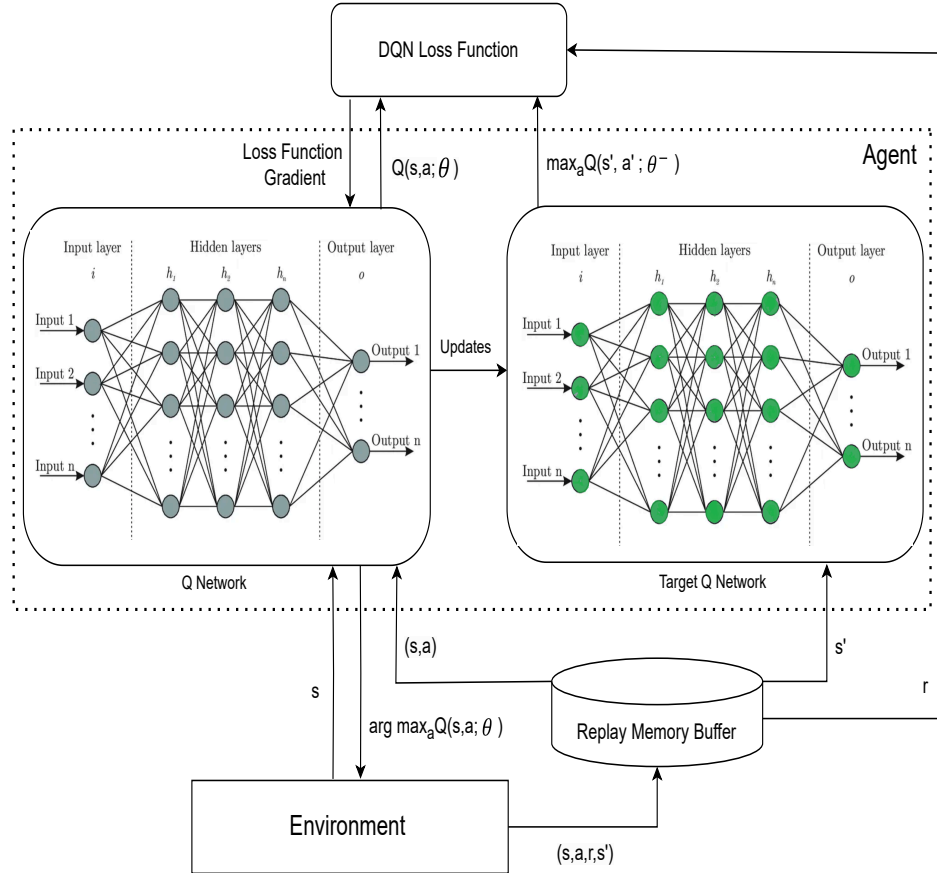


Figure 4.5: DQN architecture with the target network technique.

4.3.2 Optimal Detection Strategy

The optimal detection strategy developed in this section follows the same principles as the Q -table-based strategy in Section 4.2, with a key distinction: rather than minimizing a cost function, we aim to maximize the expected cumulative reward using DRL. This reward-based formulation allows the agent to make optimal decisions by learning from the environment through interaction and feedback.

We consider the problem of detecting and isolating actuator and sensor cyber-attacks in nonlinear CPS. Let T_s denote the stopping time selected by the defender, and τ be the unknown time at which a cyber-attack is launched. The defender's challenge lies in selecting T_s to balance the trade-off between early and delayed detection. If $T_s < \tau$, a false alarm occurs, whereas if $T_s > \tau$, detection latency increases. Since the cyber-attack strategy and the associated probability distribution P_k over time are unknown, the decision must be made based on partial and uncertain observations.

Due to the system's partially observable nature, the hidden system states cannot be directly measured. Instead, the agent receives an observation vector at each time step, which depends on system dynamics and previous actions. The system states remain hidden but are directly linked to the observation values and influenced by various actions. Thus, in our pursuit of an optimal policy π , we define the Q -value as a function of the observation $o_k \in \mathcal{O}$ and action a_k , denoted by $Q(o_k, a_k)$. The agent utilizes this Q -value function to evaluate the expected return of taking action a_k given observation o_k and subsequently following policy π . In the DQN framework, this function is approximated by a deep neural network parameterized by θ , such that

$$Q(o_k, a_k; \theta) \approx \mathbb{E}[R_k \mid o_k, a_k], \quad (85)$$

The optimal policy $\pi : \mathcal{O} \rightarrow \mathcal{A}$ is then defined as

$$\pi(o_k) = \arg \max_{a \in \mathcal{A}} Q(o_k, a; \theta), \quad (86)$$

selecting actions that maximize the expected long-term return given the current observation.

The primary objective is to determine an optimal policy that allows for timely detection and isolation by estimating whether the system resides in a pre- or post-attack state. This involves learning a reliable mapping from observations to actions that minimizes decision uncertainty and enhances detection performance. The observation space, which plays a central role in this mapping, will be formally introduced in the subsequent subsection.

To support this decision-making process, the defender employs the AUKF-based state estimator and auxiliary filters to extract informative features. These outputs—namely, the estimated system states and residual signals—form the inputs to the DRL agent, enabling accurate and robust cyber-attack detection and isolation.

4.3.3 Detection Functions and Observation Spaces

The defender's objective is to determine the optimal stopping time (T_s) for both actuator and sensor cyber-attacks using a DRL-based approach. Although P_k is unknown, it is closely related to the detection functions $\eta_{A^y}(k)$ and $\eta_{A^u}(k)$, that are defined for sensor and

actuator cyber-attacks, respectively, as follows:

$$\begin{aligned}\eta_{Ay}(k) &= \tilde{y}(k)^T \tilde{y}(k), \\ \eta_{Au}(k) &= res_{Au(k)}.\end{aligned}\tag{87}$$

where $\tilde{y}(k) = y^A(k) - \hat{y}(k|k-1)$ represents the output estimation error obtained at the C&C center, and $\hat{y}(k)$ is the output estimate derived from the AUKF. The term $res_{Au(k)}$ is obtained from Equation (83).

Theorem 4.2. *Consider the CPS system described by (79), subject to actuator and sensor cyber-attacks $A^u(k)$ and $A^y(k)$, as defined in (80). Assume that the system states are observable and that the covariances of the process and measurement noise are bounded. Then, in the absence of cyber-attacks, the output estimation error $\tilde{y}(k)$, and consequently the detection function $\eta_{Ay}(k)$, remain bounded.*

In contrast, under the presence of a sensor cyber-attack, $\eta_{Ay}(k)$ exhibits a significant deviation, enabling effective detection. Moreover, the detection function $\eta_{Au}(k)$ is primarily influenced by actuator cyber-attacks $A^u(k)$ and is structurally decoupled from other types of attacks and control inputs.

Proof: By the standard convergence properties of the AUKF, as established in Theorem 3.1, the state estimation error $\tilde{x}(k)$ and the output estimation error $\tilde{y}(k)$ remain ultimately bounded in the mean-square sense in the absence of cyber-attacks, provided that the system states are observable and the process and measurement noise covariances are bounded.

In the presence of a sensor cyber-attack $A^y(k)$, from (80) and (87), the attack signal directly affects the received system output at the C&C center, $y^A(k)$, as long as $D^A \neq 0$. This alteration propagates to the detection function $\eta_{Ay}(k)$, resulting in a measurable deviation from its nominal (attack-free) behavior. Therefore, $\eta_{Ay}(k)$ serves as an effective indicator for distinguishing between normal and compromised system states.

Furthermore, according to Theorem 3.2, the residual $res_{Au(k)}$ is solely influenced by the actuator cyber-attack signal $A^u(k)$ and remains decoupled from other cyber-attack signals and control inputs. Consequently, as shown in (87), the detection function $\eta_{Au}(k)$ is affected only by actuator cyber-attacks and is structurally independent of other system anomalies.

This completes the proof of the theorem. ■

The ability to distinguish between sensor and actuator cyber-attacks hinges on the fact that, the residual $res_{Au(k)}$ is exclusively influenced by A^u and remains decoupled from other cyber-attacks. Consequently, we assume that the binary result of the actuator attack detector—introduced in the next section—is transmitted to the C&C center. The DRL-based sensor attack detector is then trained under diverse conditions to effectively differentiate between these cyber-attacks.

Despite the effectiveness of the proposed detection functions in improving observability and providing insight into system anomalies, the actual probability of cyber-attack

occurrence, P_k , remains unknown. This uncertainty persists due to various factors such as process and measurement noise, modeling inaccuracies, bounded estimation errors, and challenges in determining reliable detection thresholds. These complexities hinder the design of a deterministic rule-based detection scheme. In this context, DRL offer a promising alternative by learning optimal detection and isolation policies directly from interaction with the system environment.

As for the observation space, we adopt the same quantization structure introduced in Subsection 4.2.3 for both detection functions, $\eta_{A^u}(k)$ and $\eta_{A^y}(k)$. Although DQN are capable of handling continuous observation spaces via function approximation, feeding raw continuous values directly into the network can result in increased computational complexity and slower convergence. Observation quantization addresses this issue by discretizing the input space, thereby reducing dimensionality and enhancing training efficiency. This discretization also contributes to improved policy interpretability and robustness against minor variations in the detection function values.

Unlike traditional reinforcement learning approaches that rely on explicit construction of a Q -table, our method utilizes DRL to approximate the Q -function implicitly. The proposed DRL algorithms and implementation details are presented in the following subsection.

4.3.4 Detection and Isolation Algorithms

The proposed DRL-based detection scheme consists of two main phases, namely (a) the learning phase, and (b) the online detection and isolation phase. The learning phase, as presented in Algorithm 4, leverages Deep Q -Network to detect cyber-attacks in a dynamic environment. It follows a reinforcement learning framework where an agent interacts with an observation space $\mathcal{O}$ and selects actions from an action space $\mathcal{A}$ using an ϵ -greedy policy. The agent trains a Q -network with parameters θ to approximate the optimal action-value function while utilizing a target Q -network θ^- to stabilize training. By storing past experiences in a replay buffer D , the algorithm enables batch updates, reducing temporal correlation and improving convergence. The reward function is designed based on the accuracy of attack declarations relative to actual attack occurrences, ensuring effective learning. Through iterative updates using gradient descent and periodic soft updates to the target network, the algorithm optimizes its policy for detecting cyber threats.

By integrating experience replay and target networks, the algorithm enhances stability and efficiency, addressing key challenges in reinforcement learning. The use of exploration-exploitation trade-offs ensures that the agent generalizes well to unseen attack scenarios. As compared to traditional RL, this approach benefits from deep learning’s capability to approximate complex state-action relationships, enabling robust cyber-attack detection in high-dimensional spaces. This algorithm may be used for both actuator and sensor attack detection, where in the former case, the observation space is obtained based on the quantized $\eta_{A_u}(k)$, while in the latter, the quantized $\eta_{A_y}(k)$ forms the observation space.

Algorithm 4 Learning Phase – DQN-Based Cyber-Attack Detection

Input:

- Quantized observation space $\mathcal{O}$, Action space $\mathcal{A}$.
- Replay buffer D with capacity C .
- Neural network parameters θ (Q -network) and θ^- (target Q -network).
- Hyperparameters:
 - Learning rate α , discount factor γ , exploration rate ϵ .
 - Soft update factor σ , batch size BS , update frequency N_{target} .
 - Episode count E_n , and maximum steps T .

Output: Trained Q -network with parameters θ^* .

Environment Setup:

- States: *Pre-attack*, *Post-attack*.
 - Rewards: Based on accuracy of attack declarations relative to attack time τ .
 - Actions ($\mathcal{A}$): Decide to declare an attack or continue monitoring.
-

1: Initialize:

- Q -network with random weights θ .
- Target Q -network: $\theta^- = \theta$.
- Replay buffer $D = \emptyset$.

2: For $ep = 1 : E_n$ **do** (Episodes)

3: Reset environment to initial state $s_0 = \textit{pre-cyber-attack}$.

4: Initialize observation o_0 , set $k = 0$.

5: While $k < T$ **do** (Steps within an episode)

6: Increment $k = k + 1$.

7: Compute action probabilities from Q -network:

$$p(a_k|o_k; \theta) = \text{softmax}(Q(o_k, \cdot; \theta)).$$

8: Select action a_k using ϵ -greedy policy:

- With probability ϵ , select random action $a_k \sim \mathcal{A}$.

- Otherwise, select action a_k based on action probabilities $p(a_k|o_k; \theta)$.

9: Execute action a_k , observe reward r_k , and next state o_{k+1} .

10: Store transition (o_k, a_k, r_k, o_{k+1}) in D .

11: If $|D| > C$, discard oldest entry.

12: If $k \bmod N_{target} = 0$:

13: Sample minibatch of size BS from D .

14: Compute target Q -values using target network:

$$y_i = r_i + \gamma \max_{a'} Q(o_{i+1}, a'; \theta^-).$$

15: Compute Q -value estimate: $\hat{Q}_i = Q(o_i, a_i; \theta)$.

16: Update θ via gradient descent:

$$\theta \leftarrow \theta - \alpha \nabla_{\theta} (\hat{Q}_i - y_i)^2.$$

17: Update target network:

$$\theta^- \leftarrow \sigma \theta + (1 - \sigma) \theta^-.$$

18: Terminate episode if $a_k = \textit{stop}$ or o_k is terminal.

19: Decrease ϵ (exploration rate decay).

20: End While**21: End For**

22: Return trained Q -network θ^* .

Regarding the cyber-attack isolation problem, as discussed in the previous section, the actuator cyber-attack detection results remain unaffected by other anomalies. This is due to the distinct structure of the auxiliary filter-based actuator detector compared to the AUKF-based sensor detector, as well as the transmission of actuator detection results to the decision-making process, that is described next. This structural separation allows for accurate and reliable isolation of actuator and sensor cyber-attacks.

Algorithm 5 Online Decision-Maker – DQN-Based Cyber-Attack Detection and Isolation

Input:

- Trained deep Q -network parameters θ^* .
- Observation space $\mathcal{O}$.
- States: $s_0 = \text{Pre-cyber-attacks/ healthy system}$, $s_1 = \text{Pre-Act Attack}$ & Post-Sen Attack , $s_2 = \text{Post-Act Attack}$.
- Initial state s_0 .
- Quantization levels $\{\beta_i\}$.
- Maximum time window T .
- The binary result of actuator attack detection: B_{Au}
- Probability threshold Th .

Output:

- cyber-attack detection result (healthy, actuator attack, or sensor attack).
-

1: Initialize:

- Observation o_0 , action $a = \text{continue}$, and step counter $k = 0$.

2: While $k < T$ **and** $a \neq \text{stop}$ **do:**

- 3: Increment $k = k + 1$.
- 4: Observe system outputs $y(k)$ and output estimate $\hat{y}(k)$.
- 5: Compute detection metric $\eta_{Ay}(k)$ and quantize:
 $\rho_i = \text{Quantize}(\eta_{Ay}(k), \{\beta_i\})$.
- 6: Update observation o_k with ρ_i .
- 7: Compute action probabilities using the trained Q -network:
 $p = \text{softmax}(Q(o_k, \cdot; \theta^*))$.
- 8: Select action a_k based on probability threshold:

$$a_k = \begin{cases} 1, & \text{if } p > Th \\ 0, & \text{otherwise.} \end{cases}$$

9: Decision-making:

- If $a_k = \text{stop}$ and $B_{Au} = 0$:
 - Report $s = s_1$.
 - Exit loop.
- If $D_{Au} = 1$:
 - Report $s = s_2$.
 - Exit loop.
- Else:
 - Continue monitoring.

10: End While.

- 11: If $k = T$ without detection, report $s = s_0$.
-

The online detection and isolation phase, presented in Algorithm 5, utilizes the trained deep Q -network to classify the system state as either healthy, under actuator attack, or under sensor attack. This algorithm, embedded in the C&C center detector, begins by observing system outputs and their estimates, which are processed to compute the quantized detection function $\eta_{A_y}(k)$. The trained Q -network evaluates the current observation and assigns action probabilities. The algorithm selects an action based on a probability threshold, where a sufficiently high probability prompts the termination of monitoring and an attack declaration. Specifically, a separate online cyber-attack detection algorithm, similar to the Algorithm 5, is implemented at the plant side for actuator attack detection, where $\eta_{A_u}(k)$ forms the observation space. To avoid redundancy, this aspect is not detailed here. The output of the actuator cyber-attack detection algorithm, a binary signal, is transmitted to the C&C center for use in Algorithm 5, enabling the decision-making process to distinguish between different types of cyber-attacks.

Following the declaration of a cyber-attack and subsequent system restoration, the online detection phase can be recommenced without requiring additional training, as the defender remains pre-trained. This approach facilitates real-time decision-making by leveraging the learned policy from the training phase. By considering various system conditions under both healthy and cyber-attack scenarios, the trained model determines the optimal stopping time T_s in the online detection phase, minimizing false alarms and detection delays. This advantage will be demonstrated in the next section through case study simulations, comparing the proposed approach with other detection methods such as RL, χ^2 , and Euclidean-based techniques.

Remark 4.2. *In Theorem 4.2, that contributes to constructing the observation space for the proposed detection and isolation framework, as well as in the training and online detection algorithms, no specific assumptions are imposed on the nature, characteristics, or types of actuator and sensor cyber-attacks, nor on the methods attackers may use to compromise sensor and actuator communication channels. This generality ensures that the proposed approach is capable of detecting and isolating a wide range of deception attacks based on FDI detection performed by the decision maker. These include not only straightforward attacks like replay attacks but also more sophisticated cyber threats that are often considered stealthy under certain definitions [152], such as covert and zero dynamics attacks. Typically, these cyber-attacks involve adversarial components injected into the actuator communication network, designed to either remain unobservable or be counteracted at the system outputs. As described in (82), such adversarial components can be modeled as $A^u(k)$ and are demonstrated to be detectable using the proposed DRL-based detection scheme. This will be further examined in the next section through case studies on the detection and isolation of various FDI and covert attacks in nonlinear CPS. Ultimately, the proposed approach provides a flexible and robust security mechanism, strengthening nonlinear CPS against a broad spectrum of cyber threats.*

4.4 Case Study Simulations

In this section, similar to Chapter 4, we consider a case study involving a mini UAV, shown in Figure 4.6, named the Ultra Stick 25E [153]. The UAV is equipped with three primary control surfaces: elevator, rudder, and ailerons. It is equipped with sensors measuring angular positions, rates, and linear accelerations. The control design utilizes the backstepping method that is proposed in [154], involving six Lyapunov functions to control the roll, pitch, and yaw angles.

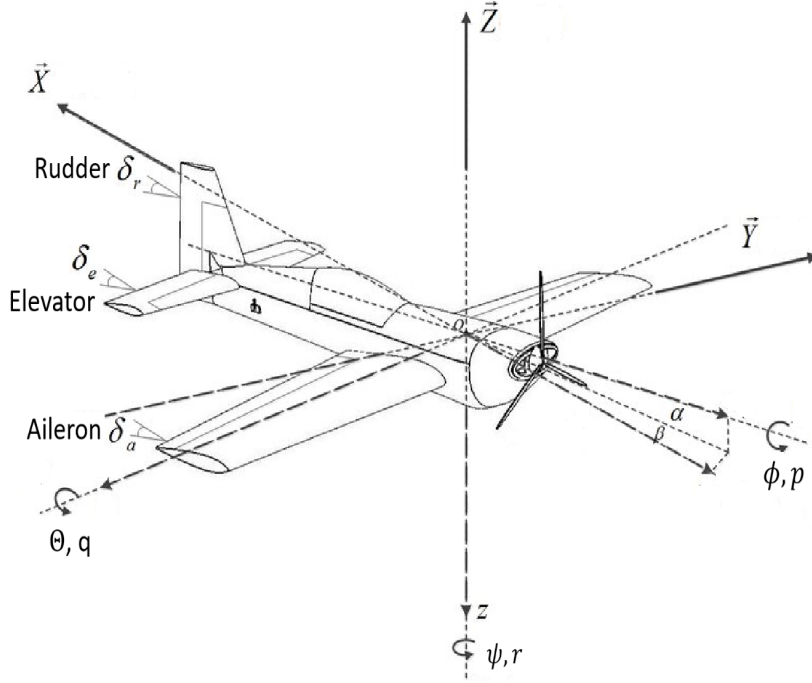


Figure 4.6: Angular positions and rates in the UAV body axis

The angular rate dynamics can be expressed as follows [153]:

$$\begin{aligned}
 p(k+1) - \frac{I_{xz}}{I_{xx}}r(k+1) &= p(k) - \frac{I_{xz}}{I_{xx}}r(k) + \frac{p_d S b}{I_{xx}}c_l \\
 &\quad - \frac{I_{zz} - I_{yy}}{I_{xx}}q(k)r(k) + \frac{I_{xz}}{I_{xx}}q(k)p(k) \\
 q(k+1) &= q(k) + \frac{p_d S \bar{c}}{I_{yy}}c_m - \frac{I_{xx} - I_{zz}}{I_{yy}}p(k)r(k) \\
 &\quad - \frac{I_{xz}}{I_{yy}}(p^2(k) - r^2(k)) + \frac{I_p}{I_{yy}}w_p r(k) \\
 r(k+1) - \frac{I_{xz}}{I_{zz}}p(k+1) &= r(k) - \frac{I_{xz}}{I_{zz}}p(k) + \frac{p_d S b}{I_{zz}}c_n \\
 &\quad - \frac{I_{yy} - I_{xx}}{I_{zz}}p(k)q(k) - \frac{I_{xz}}{I_{zz}}q(k)r(k) - \frac{I_p}{I_{zz}}w_p q(k).
 \end{aligned} \tag{88}$$

where p , q , and r represent the body axis angular rates, while ϕ , Θ , and ψ denote the body attitude Euler angles, specifically referred to as roll, pitch, and yaw, respectively. P_d stands for dynamic pressure, w_p represents the propeller rotation speed, and I_{xx} , I_{yy} , I_{zz} , I_{xz} , and I_p denote the moment of inertia coefficients. Moreover, c_l , c_m , and c_n represent non-dimensional moment coefficients.

The kinematics of the rotational motion, which links the body angular rates and the Euler angles is expressed as:

$$\begin{aligned}\phi(k+1) &= \phi(k) + p(k) + \tan(\Theta(k))(q(k)\sin(\phi(k)) + r(k)\cos(\phi(k))) \\ \Theta(k+1) &= \Theta(k) + q(k)\cos(\phi(k)) - r(k)\sin(\phi(k)) \\ \psi(k+1) &= \psi(k) + \frac{q(k)\sin(\phi(k)) + r(k)\cos(\phi(k))}{\cos(\Theta(k))}\end{aligned}\quad (89)$$

Additional equations describing the kinematics of the rotational motion, along with the parameter values, can be found in [153].

4.4.1 Q-Table-Based UAV Cyber-Attack and Fault Detection and Isolation

Referring to the dynamical model in (67), we consider

$$x(k) = [\phi(k), p(k), \Theta(k), q(k), \psi(k), r(k)]^T$$

and

$$y(k) = [\phi(k), \Theta(k), \psi(k)]^T + \mathcal{L}_2(x(k))\theta(k) + v(k),$$

where $\mathcal{L}_2(k)$ and $\theta(k)$ will be detailed later. We have implemented a high-fidelity model of the system in the Matlab/Simulink environment, along with the designed backstepping control law [154] in the plant side. Their effectiveness has been evaluated through a series of numerical case study simulations.

Within the CPS framework as illustrated in Figure 4.1, we assume that the UAV serves as the plant, while the C&C center receives system outputs and determines reference values for the corresponding actuators of the UAV. Communication networks for sensors are assumed to be compromised by cyber-attacks, with two cyber-attacks in the sensor network affecting ϕ and Θ . For each case, we assume that the cyber-attack $A^y(k) = [A_1^y(k); A_2^y(k)]^T$, introduced in (68) as an arbitrary FDI signal, consists of ramp functions having different values and noise as follows:

$$A_i^y(k) = K_{Ai}r_i(k) + v_{Ai}(k); i \in \{1, 2\}, \quad (90)$$

where K_{Ai} , $r_i(k)$, and $v_{Ai}(k)$ denote attack gain, ramp function, and additive cyber-attack noise, respectively. Since $v_{Ai}(k)$ is under the attacker's control and is distinct from the

measurement noise $v(k)$, the attacker can leverage it to enhance the effectiveness of the cyber-attack.

Moreover, we investigate a sensor bias fault in the UAV, as described in [156], that is specifically affecting the ϕ sensor. We assume that the fault dynamics is known and is described as follows:

$$\begin{aligned}\theta_1(k+1) &= \theta_1(k) + \theta_2(k) \\ \theta_2(k+1) &= -\theta_2(k) - \theta_1(k) + C_\theta,\end{aligned}\tag{91}$$

where $\theta(k) = [\theta_1(k), \theta_2(k)]^T$ and C_θ is a constant that represents the bias value. Considering the CPS model (67), we have, $\mathcal{L}_1(x(k)) \equiv 0$ and $\mathcal{L}_2(x(k))$ is a matrix with all rows zero except the one corresponding to the faulty sensor (ϕ) that is $[1, 1]$.

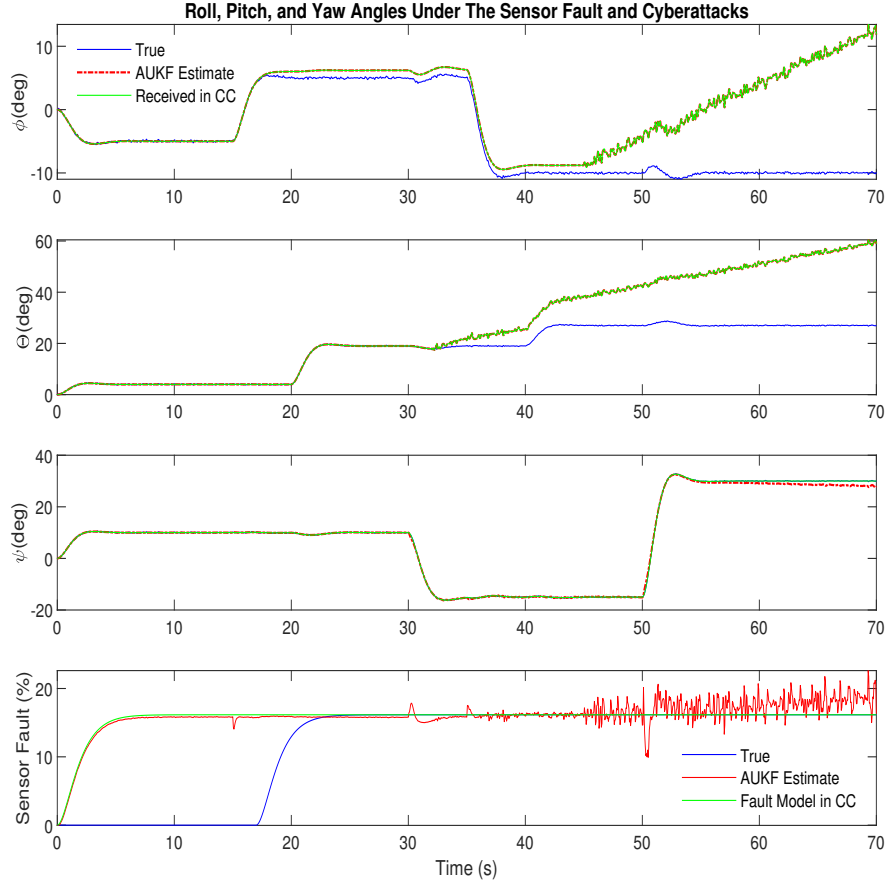


Figure 4.7: The UAV's measurement outputs and estimates and the sensor fault estimate under the the fault and cyber-attacks.

First, to observe the system behavior under fault and cyber-attacks, we assume that

the sensor fault ϕ , presented in (91), and cyber-attacks affecting Θ and ϕ , presented in (90), occur at times $\tau = 18s$, $\tau = 33s$, and $\tau = 45s$, respectively. These three anomalies are addressed and investigated by using the proposed methodology of this chapter. The system states and faults are estimated by using the AUKF on the C&C side. The first three sub-figures of Figure 4.7 depict the actual values at the plant side, the signals received at the C&C, and the estimated values for the roll, pitch, and yaw angles of the UAV under fault and cyber-attack conditions. The fourth sub-figure shows the fault estimation, its actual value, and the model developed on C&C side. The estimated values demonstrate the filters function correctly in absence of cyber-attacks, however they are affected when cyber-attacks occur.

After obtaining the state and fault estimates, we proceed to the detection and isolation step. In the proposed RL-based online cyber-attack detection scheme, we select the number of quantization levels as $I = 4$, and the quantization thresholds are determined through an off-line simulations by monitoring η_A and η_θ during the learning phase for both cyber-attacks and faults. Moreover, we choose $M = 3$, indicating that the sliding observation window comprises of 3 entries. Furthermore, the learning parameters are set to $\alpha = 0.2$ and $\epsilon = 0.1$, while the episode length is designated as $T = 70$ for both cyber-attacks (ϕ and Θ) and sensor fault.

During the learning phase, the defender and fault detector undergo extensive training under both healthy and cyber-attack conditions. The training is conducted in various scenarios to ensure comprehensive exploration of the observation space, including different attack and fault conditions. Additionally, the system is trained under varying noise levels to account for uncertainties. To illustrate the tradeoffs between average detection delay and false alarm probability, the proposed algorithm is trained for both $c = 0.01$ and $c = 0.15$.

Performance Evaluation and Comparative Analysis

In this section, we evaluate and compare the performance of the proposed RL-based attack detection and isolation scheme with existing methods such as χ^2 [164] and Euclidean-based approaches [157]. We simulate faults and cyber-attacks, then assess performance metrics including false alarm probability and average detection delay.

To compute the probability of false alarm, we choose τ as a geometric random variable with the parameter σ such that the probability density function (PDF) is defined as $P(\tau = k) = \sigma(1 - \sigma)^{(k-1)}$, where $k = 1, 2, 3, \dots$ and σ follows a uniform distribution in the range $[10^{-4}, 10^{-3}]$. The probability of false alarm is computed by summing the PDF, considering various values for T_s and τ . More specifically, it is determined as the ratio of summation of PDF from zero to the announced attack/fault time, over summation of PDF from zero to the actual occurrence time.

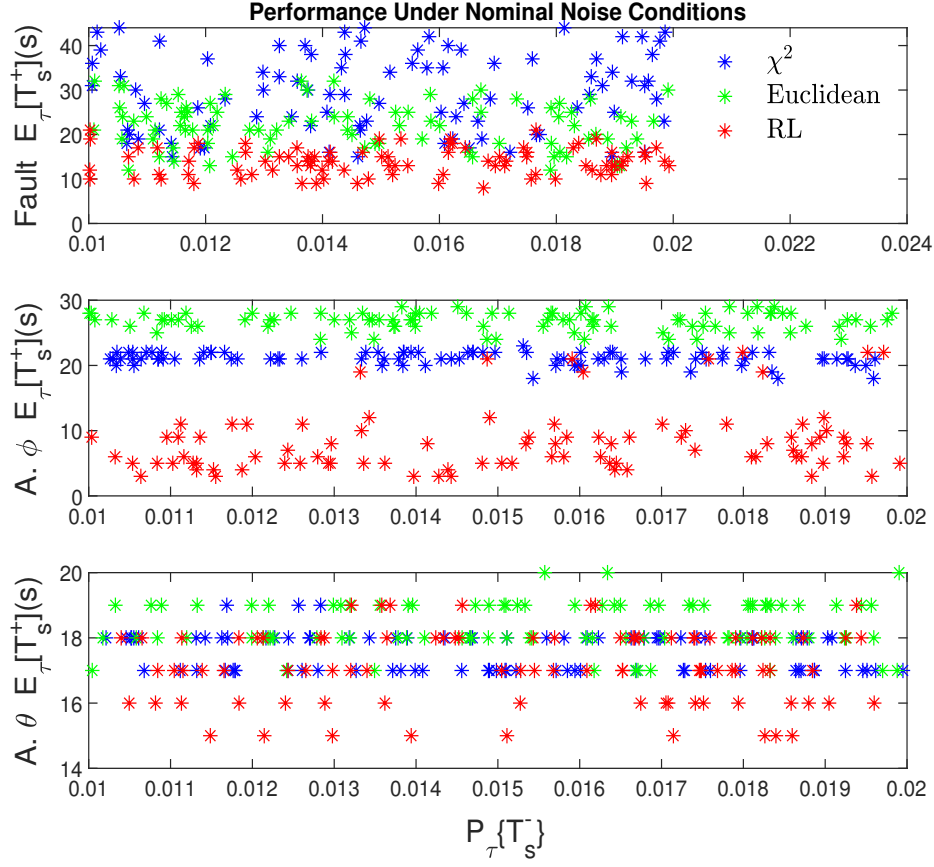


Figure 4.8: Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under nominal noise conditions.

The performance plots shown in Figures 4.8, 4.9, and 4.10 compare the proposed RL-based algorithm with the χ^2 and Euclidean-based detectors under fault and sensor cyber-attacks. In these figures, the y -axis represents the detection delay, while the x -axis shows the false alarm probability. Each point corresponds to a simulation run under different attack/fault scenarios. In Figure 4.8 that is under nominal noise, despite low false alarm rates across all detectors, due to accurate threshold selection, the RL-based defender shows superior performance with consistently lower detection delays. Expanding the comparison to various noise conditions, Figure 4.9 evaluates the detector performance under increasing measurement noise. While the Euclidean-based detector experiences significant performance fluctuations, leading to higher false alarm rates, the χ^2 detector remains relatively stable. In contrast, the RL-based defender consistently outperforms both, maintaining low false alarms and low detection delays.

In another scenario, increased noise level in the injected cyber-attacks accentuates the χ^2 detector's sensitivity, as demonstrated in [164]. Figure 4.10 illustrates a significant

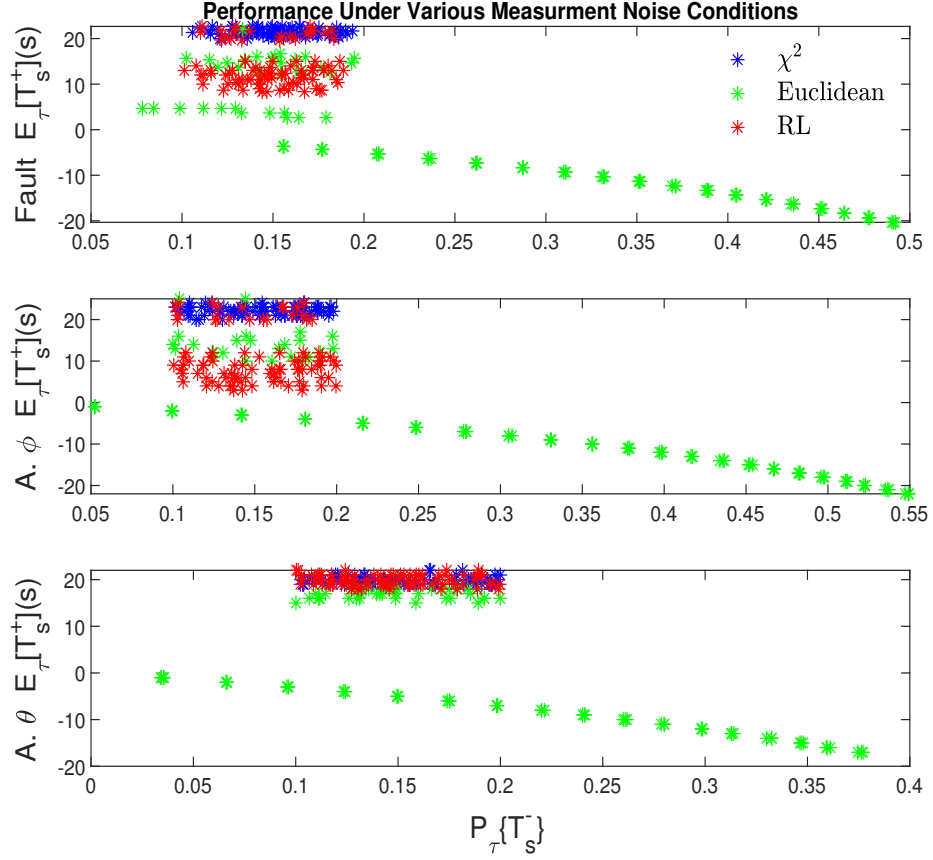


Figure 4.9: Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under various measurement noise.

increase in the false alarms for the χ^2 detector. In contrast, the RL defender’s robustness, as highlighted by its diverse training conditions, ensures consistent high performance even under elevated noise levels.

Through extensive Monte Carlo simulation runs conducted over 10,000 runs, we comprehensively assess the performance of our proposed detector alongside the χ^2 and Euclidean-based detectors. Manipulating noise amplitudes, thresholds, and varying parameter c for our proposed algorithm, we generate performance plots and compute precision, recall, and F-score metrics for all the simulation scenarios. To make the detection process practical, we define a “miss trial” as a failure to identify a cyber-attack or fault within the maximum acceptable detection delay, that is denoted by T_{ACC} . Precision, recall, and F-score are computed across all trials to evaluate the detector performance [140], as follows:

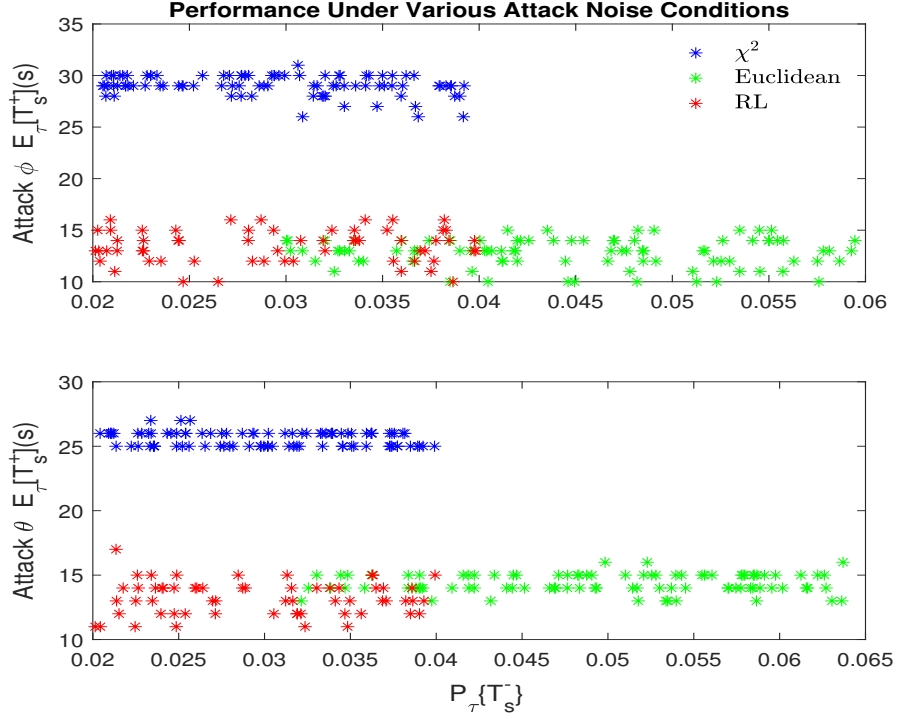


Figure 4.10: Performance comparison of the χ^2 , Euclidean-based, and RL-based fault and cyber-attack (A) detectors in terms of detection delay ($E_\tau[T_s^+]$) and false alarm probability ($P_\tau\{T_s^-\}$) under various cyber-attack noise.

$$\begin{aligned}
 precision &= \frac{num(\tau \leq T_s \leq \tau + T_{ACC})}{num(\tau \leq T_s \leq \tau + T_{ACC}) + num(T_s \leq \tau)}, \\
 Recall &= \frac{num(\tau \leq T_s \leq \tau + T_{ACC})}{num(\tau \leq T_s \leq \tau + T_{ACC}) + num(T_s \geq T_{ACC})}, \\
 F-score &= 2 \times \frac{precision \times Recall}{precision + Recall}.
 \end{aligned} \tag{92}$$

Based on the simulation results, we set $T_{ACC} = 20$ seconds for the RL-based fault detector and 30 seconds for the χ^2 - and Euclidean-based fault detectors. For attack detection, T_{ACC} was set to 15 seconds for the RL detector and 25 seconds for the χ^2 - and Euclidean-based detectors. Increasing T_{ACC} would allow anomalies more time to affect the system, potentially improving the above metrics. Conversely, reducing T_{ACC} could decrease performance, as it limits the window for detecting anomalies. Tables 4.1, 4.2, and 4.3 summarize the precision, recall, and F-score results for the χ^2 , Euclidean-based, and our proposed RL-based detectors, respectively, under different parameter settings ($c = 0.01$ and $c = 0.15$) across various simulation scenarios. Across these scenarios, the RL-based detection scheme consistently outperforms the other detectors, demonstrating its notable

Table 4.1: Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) and RL-based detector ($c = 0.01$) in detection of the faults (F.) and cyber-attacks (A.) under nominal noise.

Meth.	$\chi^2(F.)$	Euc. (F.)	RL (F.)	$\chi^2(A.)$	Euc. (A.)	RL(A.)
Pr.	0.94	0.95	0.98	0.98	0.94	0.99
Rec.	0.70	0.85	0.95	0.95	0.7	0.96
F-S.	0.80	0.90	0.96	0.96	0.80	0.97

Table 4.2: Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) and RL-based detector ($c = 0.01$) in detection of the faults (F.) and cyber-attacks (A.) under various measurement noise.

Meth.	$\chi^2(F.)$	Euc. (F.)	RL (F.)	$\chi^2(A.)$	Euc. (A.)	RL (A.)
Pr.	0.94	0.65	0.96	0.96	0.71	0.99
Rec.	0.83	0.99	0.97	0.95	0.99	0.95
F-S.	0.88	0.79	0.97	0.95	0.83	0.97

Table 4.3: Precision (Pr.), Recall (Rec.) , and F-Score (F-S.) for χ^2 , Euc. and RL detector ($c = 0.01 = c_1$ & $c = 0.15 = c_2$) in attack (A.) detection under various cyber-attack noise.

Methods	$\chi^2(A.)$	Euc. (A.)	RL (A., c_1)	RL (A., c_2)
Pr.	0.93	0.89	0.96	0.91
Rec.	0.7	0.95	0.92	0.94
F-S.	0.8	0.92	0.94	0.92

superiority. This advantage can be attributed to the training process, where the defender effectively learns to distinguish between transient system noise and sustained cyber-attacks, resulting in a significant reduction in the false alarm rates and detection delays.

4.4.2 DRL-Based Sensor and Actuator FDI Attack Detection and Isolation

In another simulation benchmark, we consider the same UAV within the CPS framework illustrated in Figure 4.3. The UAV is modeled using the nonlinear system defined in (79), where the C&C center receives system outputs and generates reference values for the UAV's actuators. The system output is represented as:

$$y(k) = [\phi(k), \Theta(k), \psi(k)]^T + v(k),$$

where $\phi(k)$, $\Theta(k)$, and $\psi(k)$ denote the roll, pitch, and yaw angles, respectively, and $v(k)$ is the measurement noise.

A high-fidelity model of the UAV has been implemented in the MATLAB/Simulink environment, incorporating the backstepping control strategy from [154]. This controller is embedded on the plant side to stabilize the roll, pitch, and yaw angles. The reference angles are denoted by $\bar{\phi}$, $\bar{\Theta}$, and $\bar{\psi}$, while the corresponding angular rates $\bar{p}$, $\bar{q}$, and $\bar{r}$ are computed based on system parameters. The proposed detection and isolation approach has been evaluated through extensive numerical simulations.

The actuators and sensors communication networks are assumed to be compromised by cyber-attacks, with two attacks targeting the sensor network and two affecting the actuator network. In each case, we define the cyber-attack as $A(k) = [A_1(k); A_2(k)]^T$, introduced in (80) as $A^y(k)$ and $A^u(k)$. This arbitrary FDI signal consists of ramp functions with different values and added noise, formulated in (90).

The characteristics of the sensor and actuator FDI cyber-attacks are illustrated in the first and second sub-figures of Figure 4.11. The sensor cyber-attacks on ϕ and Θ are introduced at $t = 35$ s and $t = 46$ s, respectively, while actuator cyber-attacks impacting $\bar{\Theta}$ and $\bar{\psi}$ occur at $t = 55$ s and $t = 66$ s, respectively. Additionally, we assume the attacker simultaneously compromises two communication channels between auxiliary filters in the actuator network. These two cyber-attacks are depicted in the third sub-figure of Figure 4.11.

In Figure 4.12, we present the system's actual values, estimated values, and reference values. cyber-attacks lead to significant deviations in the AUKF output and system states from normal conditions. In the case of sensor cyber-attacks, the system states remain within normal bounds; however, the measurements received at the corresponding C&C and, consequently, the estimation results will be affected. This situation could potentially mislead the monitoring system or decision-makers in the C&C. Actuator cyber-attacks, on the other hand, can push the plant into an unstable condition, as evident in Figure 4.12. Therefore, our objective is to promptly detect and isolate these anomalies.

For sensor attack detection, once the state estimate is obtained using the AUKF, the sensor detection function $\eta_{A^y}(k)$ is computed, allowing us to proceed with the DRL-based detection approach. Similarly, for actuator attack detection, the detection function $\eta_{A^u}(k)$ is derived using the proposed auxiliary filters, as outlined in Algorithm 1. The designed parameters of the auxiliary filters, which are incorporated into (81) and (82), are given as follows:

$$\begin{aligned} A_{Au} &= [-2 \ 0 \ 0; 0 \ 0 \ 0; 0 \ 0 \ 0], F_{Au}(x) = \sin(x)\mathbf{I}_3 \\ T_{Au} &= \mathbf{I}_3, L_{Au}^p = [1.5 \ 0 \ 0; 0 \ 0 \ 0; 0 \ 0 \ 0] \\ K_{Au} &= 0, D_{Au}^a = B^a = [0 \ 0 \ 0; 0 \ 1 \ 0; 0 \ 0 \ 1] \\ B^a &= [0 \ 0 \ 0; 0 \ 1 \ 0; 0 \ 0 \ 1]. \end{aligned}$$

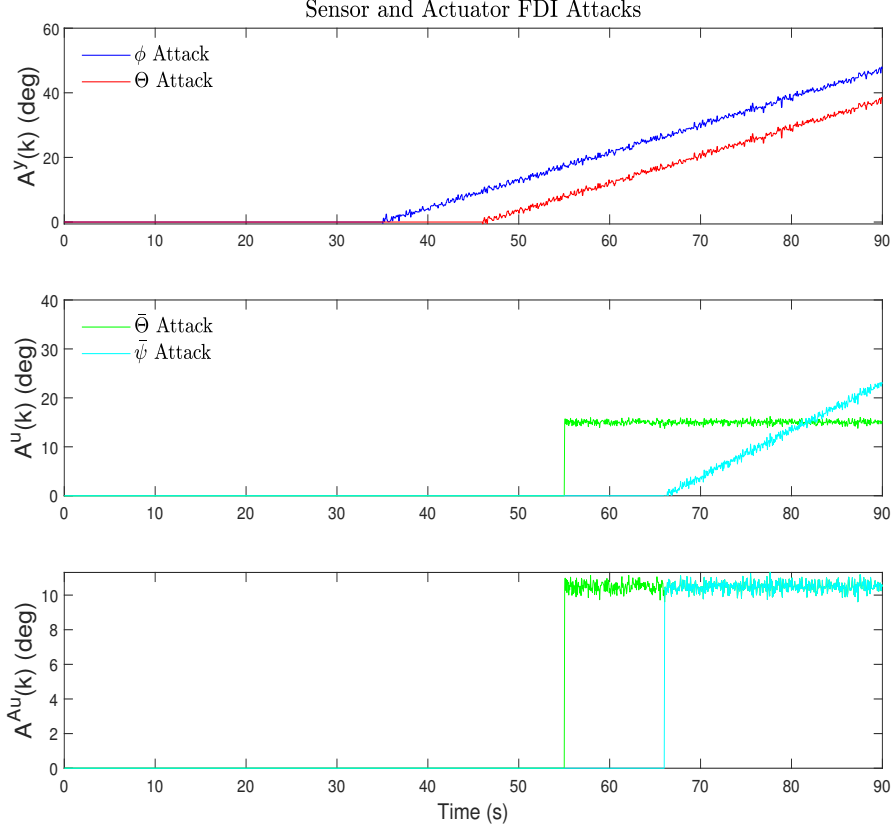


Figure 4.11: Sensor and Actuator FDI cyber-attacks.

In the proposed DRL-based online cyber-attack detection scheme, for both sensor and actuator detectors, we select the number of quantization levels as $I = 4$, and the quantization thresholds are determined through offline simulations by monitoring $\eta_{Ay}(k)$ and $\eta_{Au}(k)$ for each one separately during the learning phase. Moreover, we choose $M = 4$, indicating that the sliding observation window comprises 4 entries. Furthermore, the learning parameters are set to $\alpha = 0.2$ and $\epsilon = 0.1$, while the episode length is designated as $T = 90$.

As depicted in Figure 4.13, the proposed detectors effectively identify the corresponding sensor and actuator cyber-attacks. Due to the distinct structure of the auxiliary filter-based actuator detector compared to the AUKF-based sensor detector, the actuator cyber-attack detection results remain unaffected by other anomalies, allowing for accurate isolation of these cyber-attacks.

4.4.3 Covert Attack Detection and Isolation

In the second simulation scenario, we consider two covert attacks targeting the CPS communication networks. The first attack simultaneously affects $\bar{\Theta}$ and Θ at 25 seconds,

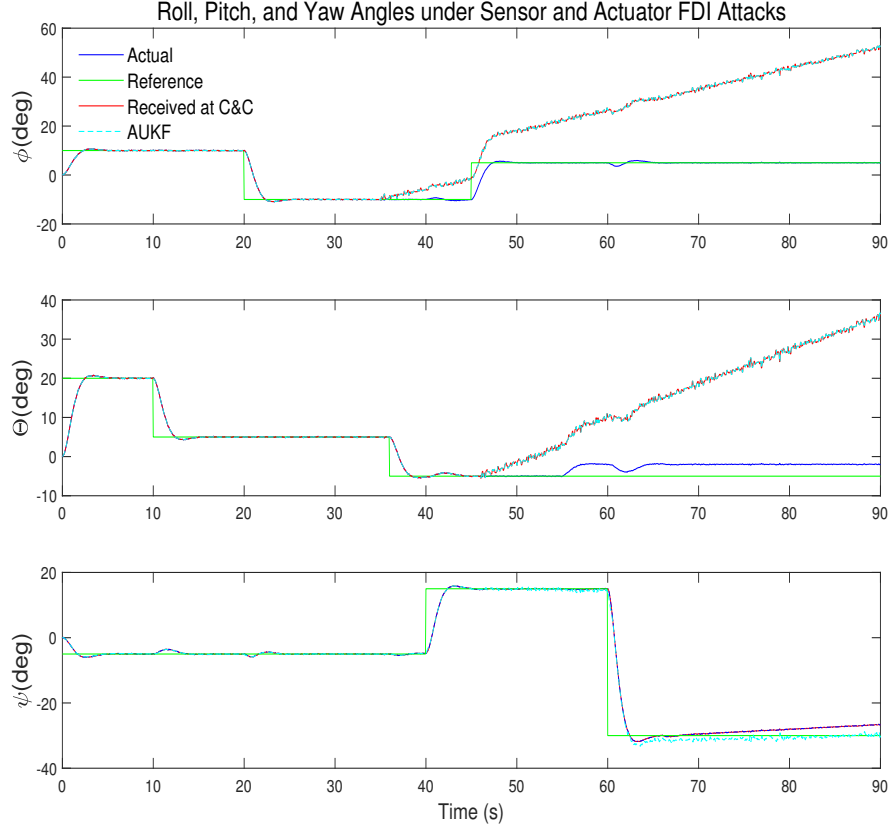


Figure 4.12: The UAV's measurement outputs and estimates under FDI sensor and actuator attacks.

while the second impacts $\bar{\psi}$ and ψ at 45 seconds. The covert attack signals are illustrated in Figure 4.14, where, in addition to simultaneous actuator and sensor cyber-attacks, we also assume the presence of auxiliary filter cyber-attacks, as shown in the last subfigure. Figure 4.15 demonstrates the impact of these cyber-attacks on the system output. Given that the attackers possess system knowledge, they attempt to craft stealthy cyber-attacks by compensating for the effects of actuator cyber-attacks within the sensor communication network.

Consequently, Figure 4.15 shows that the signals received at the C&C follow the issued reference values, while the actual plant-side values of Θ and ψ deviate significantly from the intended behavior. Despite this, our proposed methodology enables the trained actuator detector to successfully detect and isolate these covert attacks, as illustrated in Figure 4.16.

The above results confirm that each proposed detector effectively identifies its corresponding cyber-attacks without being influenced by other anomalies. Therefore, across all simulated scenarios, the proposed approach successfully detects and isolates all cyber-attacks.

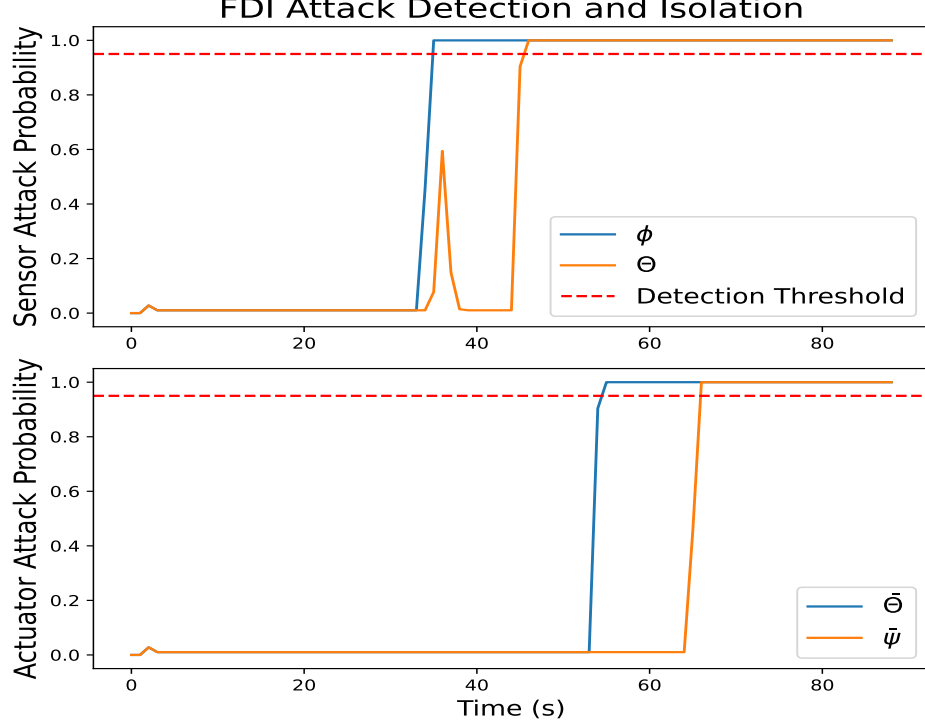


Figure 4.13: Probability of FDI attack detection using the DRL detector for sensor and actuator cyber-attacks

4.4.4 Performance Evaluation and Comparative Analysis

In this section, we evaluate the effectiveness of the proposed DRL-based cyber-attack detection and isolation scheme by comparing it against traditional Q -table RL, χ^2 -based, and Euclidean-based detection methods [157, 164]. For the Q -table RL approach, we maintain a similar agent-environment structure. However, instead of employing a DNN to approximate the Q -function, the method relies on a discrete Q -table of size $I^M \times 2$, where all $Q(o, a)$ values are explicitly stored. The learning process follows the SARSA algorithm, which is recognized for its effectiveness in POMDP [160].

The evaluation is conducted through cyber-attack simulations to assess the detection performance against a FDI attack in Θ , under three different conditions: (i) standard noise levels, (ii) increased measurement noise, and (iii) increased cyber-attack noise. The detection results for each method are illustrated in Figure 4.17, where the attack is introduced at $t = 43$ s.

Unlike other methods that provide binary outputs—indicating either a healthy state (0) or the presence of a cyber-attack (1)—the DRL-based detection approach leverages the probabilistic nature of deep reinforcement learning. Specifically, the proposed algorithms output a probability of cyber-attack detection, yielding values between 0 and 1. This probabilistic assessment offers a more nuanced interpretation of the system's security state,

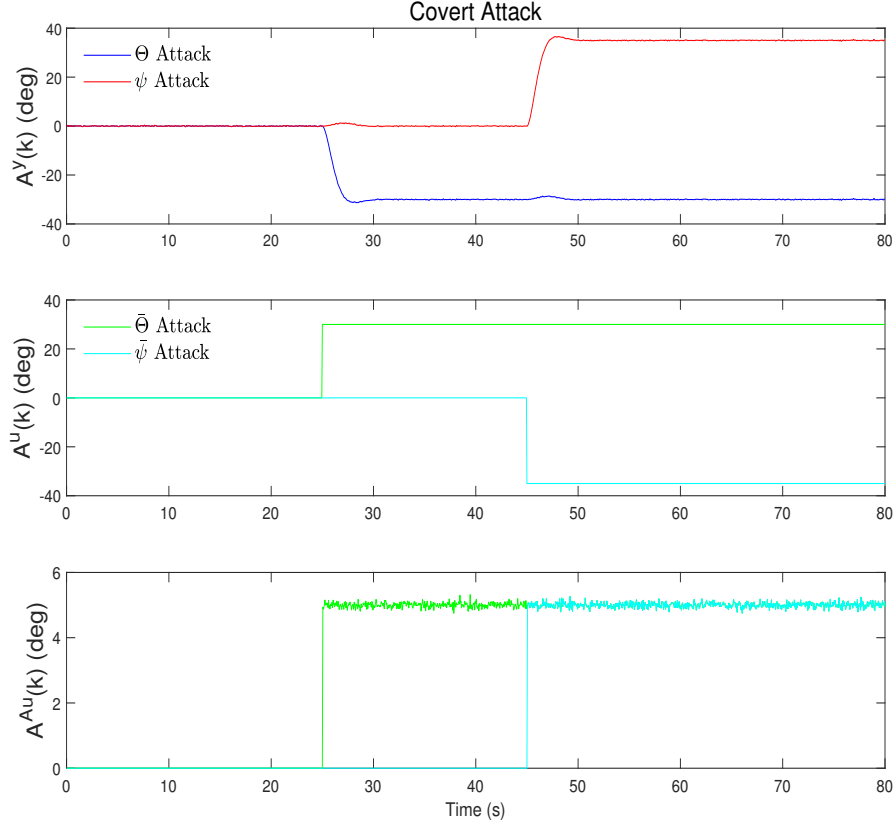


Figure 4.14: Covert attack signals

enhancing detection reliability and robustness.

In all scenarios, the DRL-based detector outperforms the other approaches, demonstrating superior accuracy and faster detection times. The Q -table RL detector also performs well, though slightly less effectively than DRL. The χ^2 and Euclidean-based methods, however, struggle under specific conditions. Under normal noise conditions, both exhibit higher detection delays due to their threshold design, which aims to minimize false alarms. When measurement noise increases, the Euclidean-based detector produces false alarms, reducing its reliability. Under increased attack noise, the χ^2 detector fails to detect the cyber-attack within the episode length, a known limitation discussed in previous research [164]. These findings highlight the robustness of the proposed DRL-based detection scheme, particularly in challenging and noisy environments, where traditional detection methods may struggle.

To compare the performance of the proposed DRL-based detectors with other detection methods in terms of false alarm probability and detection delay, we conduct simulations under various noise conditions, cyber-attack timings, and detection thresholds. Key performance metrics, including false alarm probability and average detection delay, are

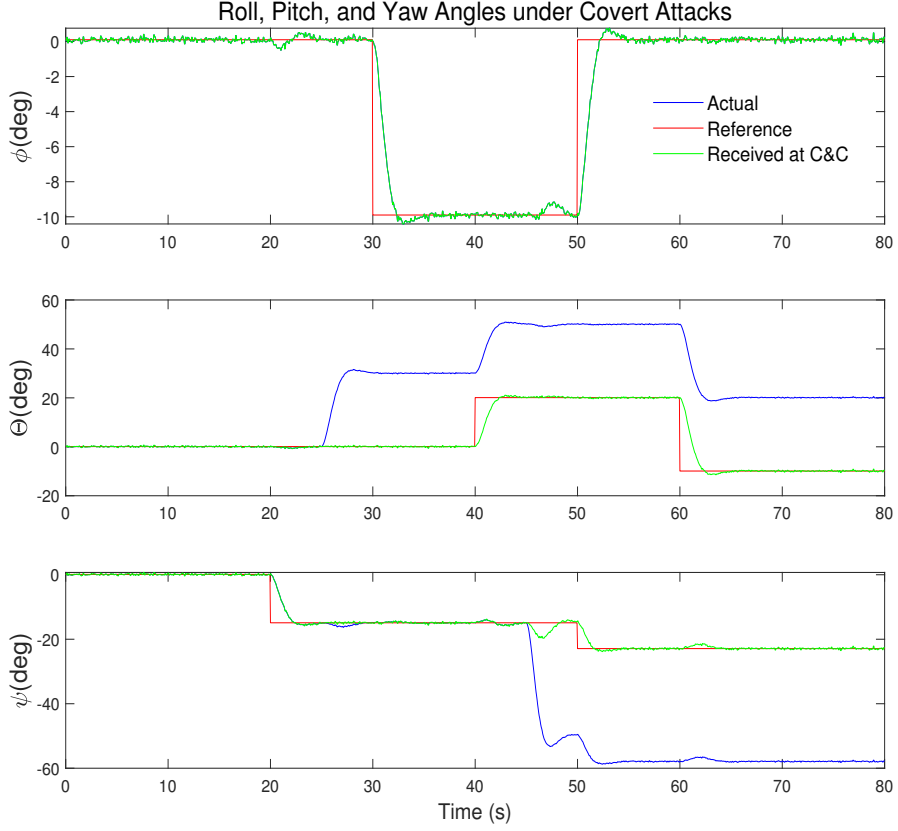


Figure 4.15: The UAV's measurement outputs and estimates under covert attacks.

analyzed. To compute the false alarm probability, we model τ , the time of attack occurrence, as a geometric random variable with parameter σ . Its probability density function (PDF) is given by:

$$P(\tau = k) = \sigma(1 - \sigma)^{(k-1)}, \quad k = 1, 2, 3, \dots$$

where σ is uniformly distributed within the range $[10^{-4}, 10^{-3}]$. The false alarm probability is then determined by integrating the PDF over different values of T_s and τ . Specifically, it is computed as the ratio of the integral of the PDF from zero to the declared attack time to the integral of the PDF from zero to the actual attack occurrence time.

The performance plots shown in Figure 4.18, compare the proposed DRL-based algorithm with the Q -table RL-based, χ^2 and Euclidean-based detectors under sensor cyber-attacks. In these figures, the y -axis represents the detection delay, while the x -axis shows the false alarm probability. Each point corresponds to a simulation run under different cyber-attack scenarios. In the first sub-figure that is under nominal noise, despite low false alarm rates across all detectors, due to accurate threshold selection, DRL and RL-based defenders shows superior performance with consistently lower detection delays. Expanding

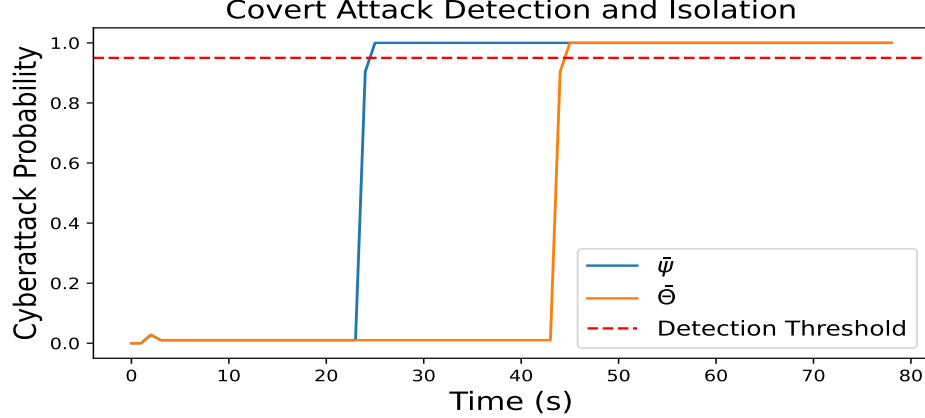


Figure 4.16: Probability of covert attack detection using the DRL detector

the comparison to various noise conditions, the second sub-figure evaluates the detector performance under increasing measurement noise. While the Euclidean-based detector experiences significant performance fluctuations, leading to higher false alarm rates, the χ^2 detector remains relatively stable. In contrast, the DRL and RL-based defenders consistently outperform both, maintaining low false alarms and low detection delays.

In another scenario, increased noise level in the injected cyber-attacks accentuates the χ^2 detector's sensitivity, as demonstrated in [164]. The third sub-figure illustrates a significant increase in the detection delay for the χ^2 detector. In contrast, the DRL and RL defender's robustness, as highlighted by its diverse training conditions, ensures consistent high performance even under elevated noise levels.

Through extensive Monte Carlo simulations conducted over 10,000 trials, we comprehensively evaluate the performance of the proposed detector in comparison with the RL-based, χ^2 , and Euclidean-based detection schemes. By varying noise amplitudes and detection thresholds, we compute the precision, recall, and F-score metrics for all simulation scenarios using the formulation in (92), where the maximum acceptable detection delay T_{ACC} is set to 15 for the RL-based and DRL-based detectors and 25 seconds for the χ^2 - and Euclidean-based detectors based on simulation results. Increasing T_{ACC} allows more time for anomalies to manifest and influence the system dynamics, potentially enhancing detection metrics. Conversely, a smaller T_{ACC} narrows the detection window and may reduce performance. Tables 4.4, 4.5, and 4.6 present the precision, recall, and F-score results for the χ^2 , Euclidean-based, Q-table RL-based, and proposed DRL-based detectors across diverse simulation settings.

Overall, both DRL- and Q-table RL-based approaches deliver strong performance, with the DRL method demonstrating slightly better results. This advantage stems from its training process, where the detector effectively learns to differentiate between transient system noise and sustained cyber-attacks, leading to a significant reduction in false alarm

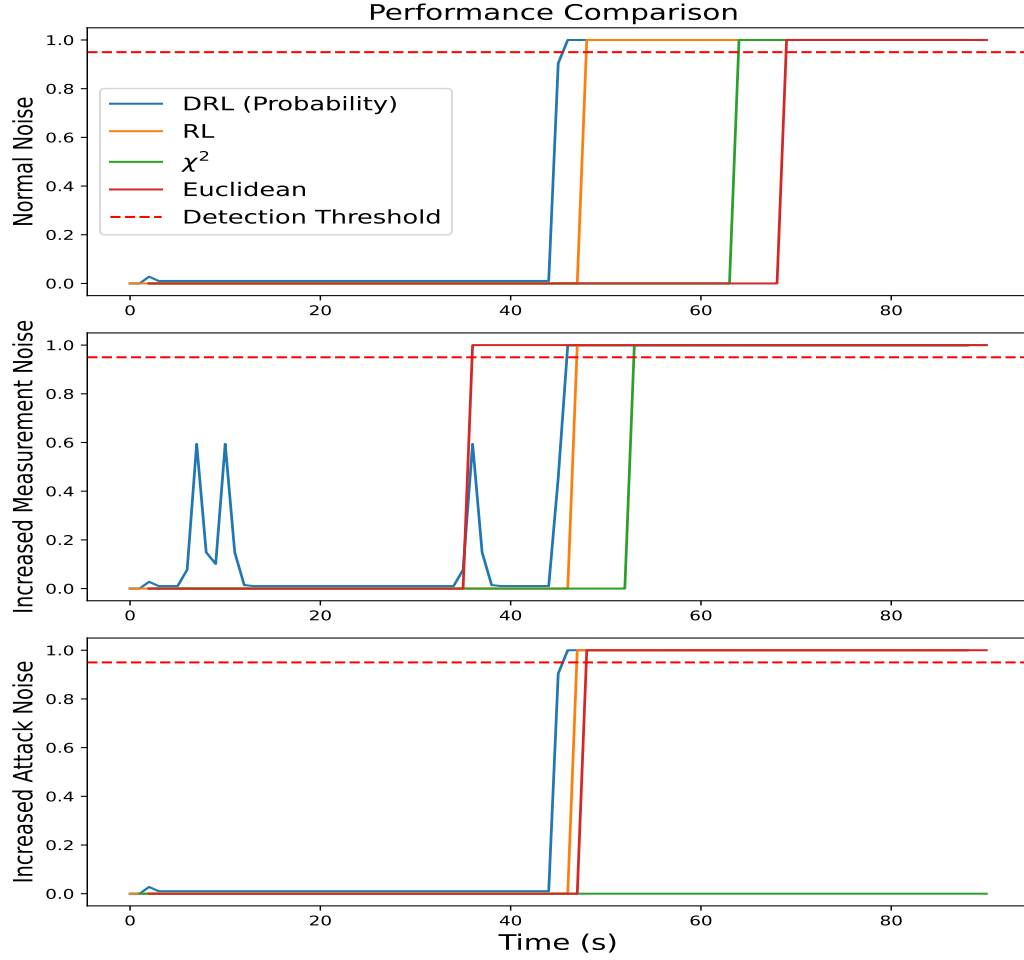


Figure 4.17: Detection results of DRL, Q -table RL, χ^2 , and Euclidean-based approaches for cyber-attack detection under various noise conditions.

rates and detection delays. Furthermore, unlike the Q -table RL approach, the DRL method does not require storing values in a lookup table, making it a more scalable and adaptable solution.

4.5 Conclusion

In this chapter, we addressed the problem of real-time cyber-attack and fault detection and isolation in nonlinear cyber-physical systems (CPS) by formulating it as a partially observable Markov decision process (POMDP). We explored both classical reinforcement learning (RL) approaches, such as Q -table-based methods, and more advanced deep reinforcement learning (DRL) techniques. In the RL-based framework, the detector was modeled as an intelligent agent tasked with optimizing its detection policy to achieve early response with minimal false alarms.

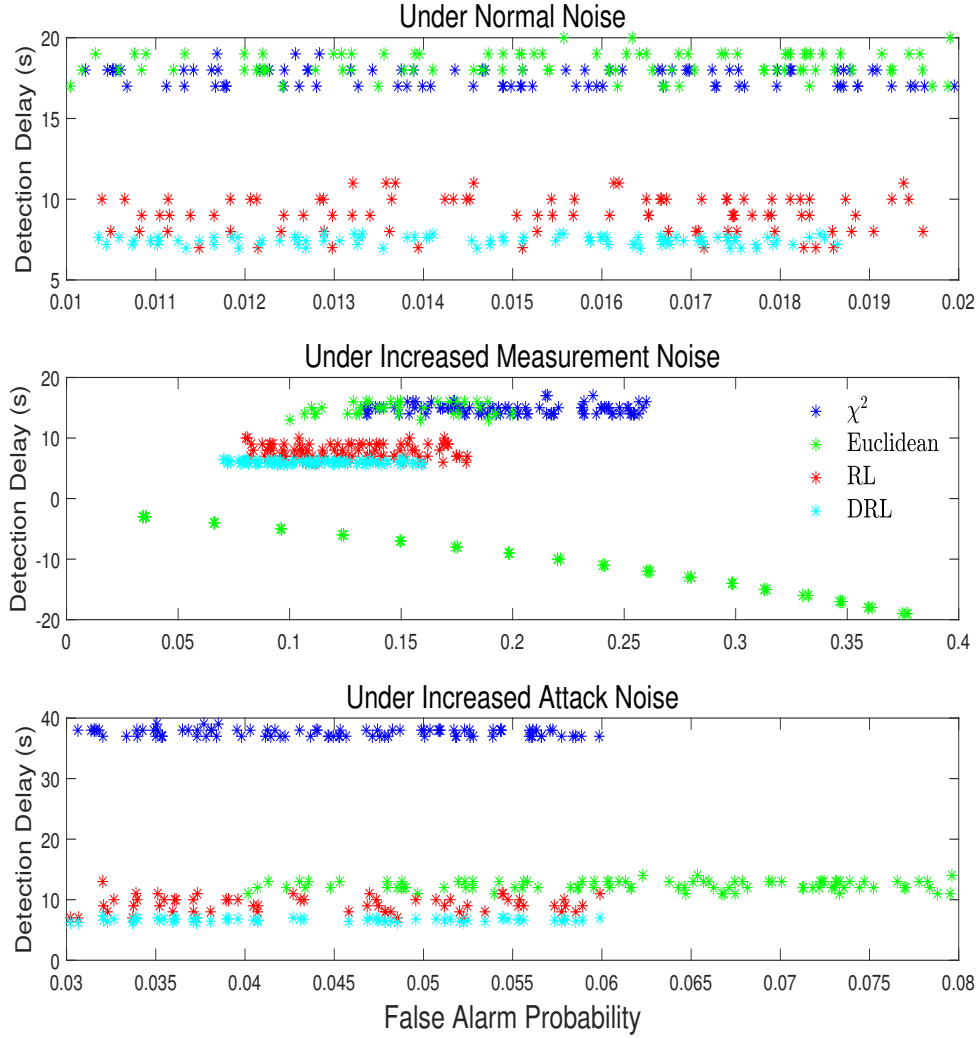


Figure 4.18: Performance comparison of the χ^2 , Euclidean-based, Q -table RL-based, and DRL-based cyber-attack detectors in terms of detection delay and false alarm probability under various noise conditions.

To enhance detection accuracy and robustness in the presence of nonlinear dynamics, noise, and uncertainties, we proposed a hybrid DRL-based framework that integrates model-based techniques—namely, the Augmented unscented Kalman filter (AUKF) and auxiliary residual filters—with deep Q -network. This synergy between model-based filtering and data-driven learning enables the framework to detect and isolate various types of cyber-attacks both effectively and optimally, including stealthy and covert attacks that often evade traditional FDI mechanisms.

The proposed approaches were validated through extensive case study simulations on a high-fidelity UAV model within CPS frameworks. Comparative analyses demonstrated the

Table 4.4: Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under nominal noise.

Meth.	χ^2	Euc.	RL	DRL
Pr.	0.94	0.89	0.98	0.99
Rec.	0.96	0.81	0.96	0.97
F-S.	0.95	0.85	0.97	0.98

Table 4.5: Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under various measurement noise.

Meth.	χ^2	Euc.	RL	DRL
Pr.	0.89	0.62	0.94	0.97
Rec.	0.95	0.99	0.96	0.96
F-S.	0.92	0.76	0.95	0.97

Table 4.6: Precision (Pr.), Recall (Rec.), and F-Score (F-S.) for χ^2 , Euclidean-based (Euc.) Q -table RL-based (RL) and DRL detectors under various cyber-attack noise.

Meth.	χ^2	Euc.	RL	DRL
Pr.	0.92	0.85	0.96	0.98
Rec.	0.59	0.97	0.95	0.95
F-S.	0.72	0.91	0.96	0.96

superior performance of the DRL-based method over traditional χ^2 -based and Euclidean-based schemes, as well as the Q -table RL-based approach in terms of detection speed, accuracy, and reliability. While the Q -table method also yielded promising results. These findings underscore the potential of reinforcement learning, particularly DRL, as a powerful and adaptive tool for enhancing the security and resilience of next-generation CPS.

Chapter 5

Resilient Distributed State Estimation for Nonlinear Cyber-Physical Systems with Sensor Networks under Cyber-Attacks

This chapter presents a resilient distributed state estimation framework tailored for nonlinear cyber-physical systems (CPS) operating under the persistent threat of cyber-attacks. Cyber-physical systems integrate computation, communication, and physical processes, often distributed across interconnected subsystems and sensor networks. While these systems offer increased flexibility, efficiency, and automation, they also introduce complex vulnerabilities—particularly when reliant on wireless or networked communication channels for real-time monitoring and control. Among the most critical challenges in CPS is ensuring the accuracy and reliability of state estimation under adverse conditions, such as cyber-attacks or faults that compromise sensor data integrity.

The proposed framework leverages a network of spatially distributed sensor nodes, each equipped with a local nonlinear state estimator and an embedded cyber-attack detection mechanism. This decentralized architecture not only improves scalability and reduces reliance on centralized infrastructure but also enhances resilience by allowing each node to contribute independently to the global state awareness. Central to our approach is the integration of the Distributed Hybrid Information Fusion (DHIF) algorithm with graph-theoretic tools, enabling robust multi-step estimation in environments with time-varying and potentially unreliable network topologies.

In particular, this work addresses the detection and isolation of False Data Injection (FDI) attacks that compromise communication links between sensor nodes. These attacks

can significantly impair estimation accuracy by injecting deceptive data into the network, thereby corrupting the global state awareness and potentially destabilizing the system. To counteract this threat, we employ a Deep Reinforcement Learning (DRL)-based detection and isolation mechanism that operates locally at each node, leveraging distributed state estimation information to assess the trustworthiness of incoming data. Upon identifying an attack, the framework activates a resilient estimation protocol that dynamically reconfigures the information fusion process and modifies the communication topology to bypass compromised links, thereby preserving estimation accuracy and maintaining system integrity.

This chapter further extends the analysis to consider switching communication graphs, reflecting realistic scenarios where network connectivity changes over time due to link failures or environmental factors. We rigorously prove that the proposed distributed estimation remains ultimately bounded under these conditions, ensuring long-term stability and robustness even when subject to adversarial interventions.

To validate the effectiveness of the proposed scheme, we conduct a comprehensive case study involving an unmanned aerial vehicle (UAV) operating in a partially observable environment monitored by a distributed sensor network with limited sensing regions. The UAV relies on the network for situational awareness and navigation. Simulation results demonstrate that our framework successfully detects cyber-attacks, isolates affected communication links, and maintains reliable state estimation despite both cyber and topological disruptions.

The main contributions of this chapter are summarized as follows:

- (i) Development of a distributed state estimation framework for nonlinear CPS, where each sensing node integrates a local state estimator and a cyber-attack detector. The framework employs the DHIF algorithm and graph-theoretic methods to achieve accurate and robust multi-step state estimation objective.
- (ii) Detection and isolation of local sensor faults within the distributed sensor network framework.
- (iii) Implementation of a cyber-attack detection and isolation mechanism, where these mechanisms enable identification and mitigation of FDI attacks on inter-node communication links.
- (iv) Proposed a resilient estimation strategy that dynamically reconfigures the fusion process and adapts to variations in network topology, thereby maintaining estimation accuracy under compromised conditions.
- (v) Theoretical analysis and proof of the ultimate boundedness and stability of the proposed distributed estimation framework, even under switching graph topologies and adversarial conditions.

- (vi) Empirical validation of the proposed methodology by using a UAV case study operating within a CPS sensor network characterized by limited sensing coverage and vulnerabilities due to cyber-attacks and sensor faults, where we have demonstrated effective estimation recovery and robust path following under various simulation scenarios.

The remainder of the chapter is organized as follows. Section 5.1 presents the distributed estimation problem formulation, including network assumptions, sensor models, and potential adversarial scenarios. Section 5.2 details a multi-step distributed estimation strategy using the DHIF algorithm, where each node is equipped with a local estimator and an attack detector. Graph-theoretic tools are employed to ensure robustness against topology changes and compromised nodes. Section 5.3 provides a rigorous theoretical analysis of the stability of the proposed estimator under switching communication graphs. Section 5.4 concludes the chapter by presenting simulation results from a UAV application in a distributed sensing environment, demonstrating estimation recovery and resilience to cyber-attacks on the network.

5.1 Problem Formulation

In this section, we provide a formal description of the nonlinear CPS under investigation and define the mathematical models governing its physical dynamics and distributed sensing architecture. The physical plant is modeled as a discrete-time nonlinear system:

$$x(k+1) = f(x(k)) + w(k), \quad (93)$$

where k denotes the discrete-time index, and $x(k) \in \mathbb{R}^n$ is the system state vector at the time instant k . The function $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ describes the nonlinear state transition and is assumed to be known to all sensing nodes. The process noise $w(k) \in \mathbb{R}^n$ is modeled as zero-mean Gaussian noise with covariance $Q(k)$.

The measurement model at each sensor node $i \in \mathcal{V}$ is given by:

$$y_i(k) = h_i(x(k)) + \mathcal{L}_i(x(k))\theta_i(k) + v_i(k), \quad (94)$$

where $y_i(k) \in \mathbb{R}^{m_i}$ denotes the local observation at the node i at time k . The function $h_i : \mathbb{R}^n \rightarrow \mathbb{R}^{m_i}$ represents the nominal nonlinear sensing process, while $\theta_i(k) \in \mathbb{R}^{n_{\theta_i}}$ denotes the sensor fault vector, and $\mathcal{L}_i(x(k))$ is a nonlinear matrix-valued function that models the fault distribution over the measurement channels. The additive measurement noise $v_i(k) \in \mathbb{R}^{m_i}$ is assumed to be zero-mean Gaussian with the covariance $R_i(k)$, and uncorrelated with the process noise. For notational simplicity, the measurement dimension m_i is assumed constant over time and fixed per node.

Not all sensors have full access to the entire system state. In particular, sensing nodes

are remotely and geographically distributed throughout the spatial domain of the CPS. Consequently, a given sensor node i can only acquire informative measurements when the plant enters or operates within its effective sensing region. This reflects real-world CPS deployments, where sensing coverage is inherently spatiotemporally sparse, as in aerial surveillance with UAVs, distributed environmental monitoring, or fault detection in smart grids. Therefore, achieving reliable state estimation necessitates cooperation among nodes through structured information exchange and fusion.

The overall CPS architecture is depicted in Figure 5.1. The system comprises a nonlinear physical plant interfacing with a distributed network of sensor nodes that communicate via a dedicated, potentially time-varying communication graph. This graph allows nodes to exchange data required for distributed estimation, but it is also vulnerable to adversarial manipulation such as FDI attacks on communication links. Each sensing node is equipped with a local state estimator and integrated cyber-attack and fault detection mechanisms, thereby supporting both decentralized inference and resilient operation.

To compensate for limited local observability and to counteract the effects of faults and adversarial threats, the nodes employ a cooperative estimation strategy based on the Distributed Hybrid Information Fusion (DHIF) algorithm. This strategy enables each node to fuse its local measurements with the filtered estimates received from neighboring nodes while taking into account the possibility of compromised data. The objective of the proposed framework is to ensure that the global system state can be estimated in a robust and bounded manner, even in presence of sensor faults, cyber-attacks, and incomplete sensing coverage.

5.2 Resilient Distributed Data Fusion Approach

An enhanced version of the DHIF algorithm is presented that explicitly addresses the challenges posed by sensor faults, cyber-attacks, and the need for resilient operation in the CPS. Building on the foundational distributed fusion framework that is proposed in [98], we assume that at each time step k , every sensor node $i \in \mathcal{V}$ maintains an estimate of the global system state, denoted by $\hat{x}_i(k)$, along with an associated error covariance matrix $\mathbf{P}_i(k)$. The proposed resilient data fusion procedure is carried out locally at each node and consists of five major steps. These include sensor fault detection, propagation, packing and communication, cyber-attack detection and isolation, and update and system recovery.

A key feature of our proposed approach is that the communication network between the nodes is potentially vulnerable to FDI attacks, whereby malicious actors may compromise the exchanged information. Consequently, the framework must ensure robustness to both malicious data and local sensing faults while maintaining estimation accuracy through accomplishing collaboration among nodes.

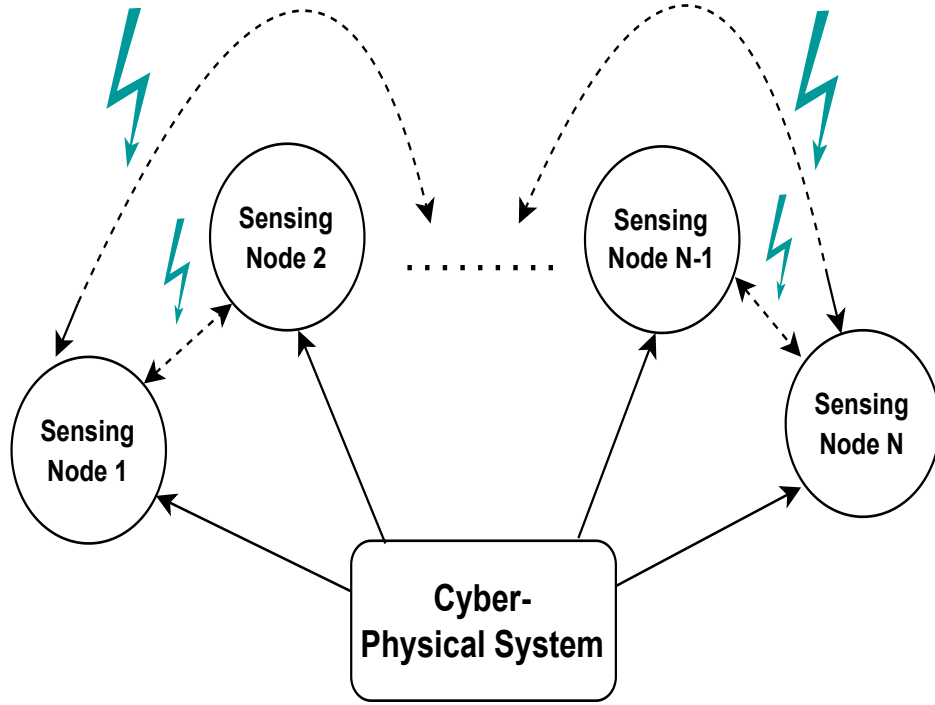


Figure 5.1: Cyber-Physical System (CPS) with a distributed sensor network.

5.2.1 Sensor Fault Detection and Isolation

As a prerequisite for reliable collaboration, each sensing node performs a local sensor fault detection procedure before sharing its information with neighbors. To guarantee that the shared data originates from a trustworthy and fault-free source, we employ a local fault detection mechanism based on the Augmented Unscented Kalman Filter (AUKF) developed in Chapter 3. We assume that the dynamics of the fault affecting each sensor node are known and can therefore be modeled as part of an augmented system state.

This approach allows the fault to be treated as an additional component of the estimated state vector. Thus, in each sensor node, we incorporate an independent AUKF instance that estimates the fault vector using the local measurement model. The fault detection metric η_{θ_i} for node i is defined as:

$$\eta_{\theta_i}(k) = \tilde{\theta}_i(k)^T \tilde{\theta}_i(k), \quad (95)$$

where $\tilde{\theta}_i(k) = \theta_i^m(k) - \hat{\theta}_i(k)$, and $\theta_i^m(k)$ represents the expected fault signal derived from known fault dynamics, while $\hat{\theta}_i(k)$ is the fault estimate obtained from the AUKF. It is important to note that $\theta_i^m(k)$ evolves according to known dynamics and is unaffected by presence of an actual fault, whereas $\hat{\theta}_i(k)$, through its dependence on the measurement $y_i(k)$ in (94), is sensitive to fault manifestations.

We employ the DRL-based detection module introduced in Chapter 4, specifically Algorithms 4 and 5, adapting it to operate based on the detection function $\eta_{\theta_i}(k)$. This detector determines whether the local sensor node is operating reliably. Only nodes that pass the fault detection test are allowed to participate in the collaborative state estimation process. For these qualified nodes, we revert to the original system dynamics defined by equations (93) and (94), excluding the augmented state.

5.2.2 Propagation

Each sensing node i propagates its local posterior estimate from the previous time step to the current one by using the Unscented Transformation (UT), which is particularly well-suited for capturing the effects of nonlinear dynamics without requiring linear approximations. This propagation step is critical in ensuring that each node maintains an accurate local prediction of the system state based on its past information, independent of communication with other nodes at this stage.

In the distributed filtering framework, the UT is performed by generating a set of $2n+1$ deterministic sigma points around the current posterior mean estimate. These sigma points, denoted by $\mathcal{X}_{i,r}(k-1)$ for $r = 0, \dots, 2n$, are constructed to capture the first two moments (mean and covariance) of the state distribution, that is:

$$\begin{aligned}\mathcal{X}_{i,0}(k-1) &= \hat{x}_i(k-1), \\ \mathcal{X}_{i,r}(k-1) &= \hat{x}_i(k-1) + (\sqrt{(n+\kappa)\mathbf{P}_i(k-1)})_r, \\ \mathcal{X}_{i,r+n}(k-1) &= \hat{x}_i(k-1) - (\sqrt{(n+\kappa)\mathbf{P}_i(k-1)})_r,\end{aligned}\tag{96}$$

where $\kappa \in \mathbb{R}$ denotes a tuning parameter used to control the spread of the sigma points, ensuring that the scaled covariance matrix is positive definite. The matrix square root is typically computed via Cholesky decomposition, and $(\sqrt{(n+\kappa)\mathbf{P}_i(k-1)})_r$ represents the r th column of this square root matrix. Parameters α_c and β_c are used to further fine-tune the sigma point distribution, where α_c controls the overall spread and β_c incorporates prior knowledge about the distribution.

The weights that are used for computing the propagated mean and covariance are defined as follows:

$$\begin{aligned}W_{i,0}^m &= \kappa/(n+\kappa), \\ W_{i,0}^c &= \kappa/(n+\kappa) + (1 - \alpha_c^2 + \beta_c), \\ W_{i,r}^m &= W_{i,r}^c = \frac{1}{2(n+\kappa)}, \quad \forall r = 1, \dots, 2n.\end{aligned}\tag{97}$$

Once the sigma points are generated, each point is propagated through the nonlinear system dynamics that are defined by the function $f(\cdot)$, that is:

$$\mathcal{X}_{i,r}(k|k-1) = f(\mathcal{X}_{i,r}(k-1)). \quad (98)$$

The prior local estimate of the state $\hat{x}_i(k|k-1)$ and its corresponding error covariance $\hat{\mathbf{P}}_i(k|k-1)$ for the node i are then reconstructed by using the weighted sum of the transformed sigma points, as follows:

$$\begin{aligned} \hat{x}_i(k|k-1) &= \sum_{r=0}^{2n} W_{i,r}^m \mathcal{X}_{i,r}(k|k-1), \\ \hat{\mathbf{P}}_i(k|k-1) &= \sum_{r=0}^{2n} W_{i,r}^c (\mathcal{X}_{i,r}(k|k-1) - \hat{x}_i(k|k-1)) \\ &\quad \times (\mathcal{X}_{i,r}(k|k-1) - \hat{x}_i(k|k-1))^T + Q_i(k), \end{aligned} \quad (99)$$

where $Q_i(k)$ denotes the process noise covariance matrix associated with the node i . This prediction step equips each node with a prior state estimation that will be refined through local sensing and collaborative fusion with neighboring agents under the subsequent steps.

5.2.3 Packing and Communication

Before delving into the distributed information exchange, we establish a foundational assumption concerning nodes that lack direct observations of the system state at a given time instant.

Assumption 5.1. *If the system states are not directly observed by the agent $i \in \mathcal{V}$ at the time k , then $R_i(k)^{-1} = 0$, and the measurement $y_i(k)$ is considered arbitrary.*

After computing its prior estimate $\hat{x}_i(k|k-1)$, each sensor node i gathers its local measurement $y_i(k)$ and prepares its information for transmission to neighboring nodes. This information encapsulates both the prior estimate and the measurement update information and is packed into a standardized format.

The core elements of the prior estimation information are packed as follows:

$$\begin{aligned} \Xi_i(k) &= \hat{\mathbf{P}}_i(k|k-1)^{-1}, \\ \xi_i(k) &= \hat{\mathbf{P}}_i(k|k-1)^{-1} \hat{x}_i(k|k-1). \end{aligned} \quad (100)$$

The above variables serve as building blocks for the fusion algorithm. To handle the nonlinearities in the local measurement function $h_i(\cdot)$, we utilize the unscented measurement

transformation approach from [165]. This allows us to represent the measurement model in a form that is compatible with information fusion:

$$\begin{aligned}\mathcal{Y}_i(k) &= \mathcal{H}_i(k)^T \mathbf{R}_i(k)^{-1} \mathcal{H}_i(k), \\ z_i(k) &= \mathcal{H}_i(k)^T \mathbf{R}_i(k)^{-1} (y_i(k) - \hat{y}_i(k|k-1) + \mathcal{H}_i(k) \hat{x}_i(k|k-1)),\end{aligned}\tag{101}$$

where $\mathcal{H}_i(k)$ denotes the pseudo-measurement matrix defined by:

$$\mathcal{H}_i(k) \triangleq (\hat{\mathbf{P}}_i^{xy}(k))^T \hat{\mathbf{P}}_i(k|k-1)^{-1},\tag{102}$$

and $\hat{\mathbf{P}}_i^{xy}(k)$ denotes the cross-covariance between the prior state estimate and the prior output estimate that is computed according to:

$$\begin{aligned}\hat{\mathbf{P}}_i^{xy}(k) &= \sum_{r=0}^{2n} W_{i,r}^c (\mathcal{X}_{i,r}(k|k-1) - \hat{x}_i(k|k-1)) \\ &\quad \times (h_i(\mathcal{X}_{i,r}(k|k-1)) - \hat{y}_i(k|k-1))^T.\end{aligned}\tag{103}$$

The prior output estimate $\hat{y}_i(k|k-1)$ is calculated using the mean of the transformed sigma points, namely

$$\hat{y}_i(k|k-1) = \sum_{r=0}^{2n} W_{i,r}^m h_i(\mathcal{X}_{i,r}(k|k-1)).\tag{104}$$

Each node then constructs the full communication packet containing $\mathcal{Y}_i(k)$, $z_i(k)$, $\Xi_i(k)$, $\xi_i(k)$, the current local estimate $\hat{x}_i(k)$, and the set of suspected compromised links $\mathcal{A}_i(k)$, which will be discussed in the following subsections. These data packets are sent to all out-neighbors $j \in N_{i,\text{out}}(k)$, and likewise, node i receives corresponding packets from its in-neighbors $j \in N_{i,\text{in}}(k)$.

It is crucial to account for the possibility that the communication links themselves may be under FDI attacks. To capture this vulnerability, the received data at node j from node i is modeled as follows:

$$\mathbf{Y}_{ij}^A(k) = \mathbf{Y}_i(k) + D_{ij}^A A^{\mathbf{Y}_{ij}}(k),\tag{105}$$

where $\mathbf{Y}_i(k)$ denotes the true transmitted information, $A^{\mathbf{Y}_{ij}}(k)$ is the additive malicious signal introduced by the attacker, and D_{ij}^A characterizes the structure of the attack. The

adversary has full freedom in designing $A^{\mathbf{Y}_{ij}}(k)$, which poses a significant threat to integrity of the collaborative state estimation process.

5.2.4 Cyber-Attack Detection and Isolation

After each sensing node i receives data from its neighboring nodes $j \in N_{i,\text{in}}(k)$, it must assess integrity of the received information to identify any potential FDI attacks that may have occurred during transmission over the communication links. This step is essential for maintaining the robustness and reliability of the distributed estimation process, especially in adversarial environments.

To accomplish this, each sensing node utilizes a detection function to evaluate the trustworthiness of every received message. For a given neighboring node $j \in N_{i,\text{in}}(k)$, the detection function is computed by measuring the discrepancy between the local posterior estimate $\hat{x}_i(k)$ and the estimate $\hat{x}_{ji}^A(k)$ that is extracted from the received signal $\mathbf{Y}_{ij}^A(k)$, which may have been altered by an attacker:

$$\forall j \in N_{i,\text{in}}(k) : \eta_{ji}^A(k) = (\hat{x}_i(k) - \hat{x}_{ji}^A(k))^T (\hat{x}_i(k) - \hat{x}_{ji}^A(k)) \quad (106)$$

Here, $\hat{x}_{ji}^A(k)$ is derived from the potentially compromised signal and represents node i 's interpretation of node j 's transmitted estimate. The function $\eta_{ji}^A(k)$ serves as a quantitative indicator of inconsistency between local and received information. In absence of attacks, this discrepancy should remain within a tolerable range determined by system noise, modeling error, and communication imperfections. However, significant deviations suggest the possibility of an FDI attack.

Due to presence of system noise, nonlinearities, and the sophisticated behavior of intelligent cyber adversaries, simple threshold-based detection methods are often unreliable or inadequate. To address these challenges—and to minimize delays in the subsequent recovery process—we leverage the DRL framework introduced in Algorithms 4 and 5, which was originally designed for a different CSQ-based architecture. In this context, we adapt the DRL-based decision maker to perform cyber-attack detection within the sensor communication network. Specifically, building upon the sensor fault detection strategy discussed in Subsection 5.2.1, we train two deep Q-networks using the detection functions defined in equations (95) and (106). With these trained models, the DRL decision maker is capable of detecting and isolating both cyber-attacks on the communication network and faults in local sensors. Given the similarity to the previously presented algorithms and to avoid redundancy, the adapted versions are not explicitly restated here.

Each node independently executes the trained DRL model to classify each incoming signal as benign or malicious based on the observed discrepancy. Because $\eta_{ji}^A(k)$ only reflects discrepancies linked to sender j , each link can be evaluated in isolation. This

localized nature of detection allows node i to pinpoint which specific communication links are compromised, ensuring precise isolation of the malicious data and enhancing the resilience of the distributed estimation algorithm.

Tracking Malicious Communication

To further reinforce integrity of the communication network, each node maintains a dynamically updated list of compromised communication links. This information is also embedded into the outgoing messages and propagated to neighboring nodes. Such collaborative sharing improves global situational awareness and can support collective mitigation strategies.

Formally, let $\mathcal{A}_i(k)$ denote the set of communication links that the node i identifies as compromised at the time step k , based on the output of the DRL-based detection module. Specifically, a link ji is included in $\mathcal{A}_i(k)$ if the trained DRL agent detects an anomaly in the signal received from node j :

$$\mathcal{A}_i(k) = \{ji \mid \text{An attack is detected on link } ji \text{ at time } k\}. \quad (107)$$

By disseminating $\mathcal{A}_i(k)$ through regular transmissions, nodes enable early detection and cooperative isolation of adversarial links throughout the network, as elaborated in the following step.

5.2.5 Update and System Recovery

Following the reception of information from neighboring nodes and the execution of cyber-attack detection and isolation procedures, each sensing node proceeds to update its local state estimate. This step is critical to ensuring that the collaborative estimation process remains both accurate and resilient in the face of cyber threats. However, when a cyber-attack is detected on any of the incoming communication links, the corresponding corrupted signal must be excluded from the update to prevent the contamination and propagation of erroneous or malicious data throughout the network.

To address the absence of reliable information caused by these exclusions, a graph-switching mechanism is introduced. This mechanism allows the network topology to reconfigure itself dynamically by redirecting communication through alternative and uncompromised links. As a result, the system can maintain continuity in the estimation process even under adversarial conditions.

Let $J_i(k)$ denote the set of nodes from which the node i receives information at the time step k , that is defined as:

$$J_i(k) \triangleq N_{i,\text{in}}(k) \cup \{i\},$$

where $N_{i,\text{in}}(k)$ includes the current set of inbound neighbors, and node i includes itself in this set only if it has direct sensing capabilities of the system state.

Once an attack is detected on a communication link ji , the transmitting node j is identified as a potentially compromised source and added to a dedicated set of unreliable nodes:

$$J_i^A(k) \triangleq \{j \in J_i(k) \mid \text{An attack is detected on link } ji \text{ at time } k\}. \quad (108)$$

To preserve integrity and consistency of the distributed state estimation, the update equations are modified to exclude contributions from nodes in $J_i^A(k)$. The revised update rule is given by:

$$\begin{aligned} \hat{\mathbf{P}}_i(k) &= \left(\sum_{j \in J_i(k) \setminus J_i^A(k)} \mathcal{Y}_j(k) + \sum_{j \in J_i(k) \setminus J_i^A(k)} d_{ij}(k) \Xi_j(k) \right)^{-1}, \\ \hat{x}_i(k) &= \hat{\mathbf{P}}_i(k) \left(\sum_{j \in J_i(k) \setminus J_i^A(k)} z_j(k) + \sum_{j \in J_i(k) \setminus J_i^A(k)} d_{ij}(k) \xi_j(k) \right) \end{aligned} \quad (109)$$

The weights $d_{ij}(k)$ are determined locally at each node and do not require global knowledge of the network topology [98]. These weights satisfy the constraints $\sum_{j \in J_i(k)} d_{ij}(k) = 1$, and are strictly positive only for nodes in the uncompromised set, i.e., $d_{ij}(k) > 0$ if $j \in J_i(k) \setminus J_i^A(k)$, and $d_{ij}(k) = 0$, otherwise.

Graph Switching for Dynamic Recovery

To mitigate the adverse impact of compromised communication links on the estimation process, the network employs a dynamic graph-switching strategy. This strategy facilitates the reconfiguration of the network by replacing compromised communication paths with alternative healthy links in a distributed and autonomous manner.

The mechanism operates according to the following procedure:

- Each node maintains a predefined set of backup nodes, denoted by $\tilde{N}_{j,\text{out}}(k) \subseteq N_{\text{global}}(k)$, which are not part of its primary communication set.
- At each time step, every node receives from its neighbors the set of currently identified compromised links, $\mathcal{A}_i(k)$, via the shared message $\mathbf{Y}_i(k)$. If a node j learns that its outgoing link $j \rightarrow i$ has been compromised, it does not attempt to re-establish communication with i on its own.
- Instead, a predetermined backup node $j^* \in \tilde{N}_{j,\text{out}}(k)$ —selected based on topological criteria and its proximity to node i to preserve strong connectivity of the graph—autonomously initiates a new communication link $j^* \rightarrow i$.

- Consequently, the updated set of active neighbors for the node i is redefined as:

$$J_i^{\text{new}}(k) = (J_i(k) \setminus J_i^A(k)) \cup \{j^*\}. \quad (110)$$

- Once the new link is established, node j^* transmits its data to node i , ensuring that the newly received and trustworthy information is seamlessly integrated into the update process in place of the compromised data.

This dynamic switching mechanism ensures that the distributed state estimation framework remains resilient and adaptable in presence of cyber-attacks. Importantly, the entire process is executed in a decentralized fashion without relying on any centralized controller or global network coordinator, thereby enhancing scalability and robustness.

5.3 Stability Analysis

In this section, we present a rigorous analysis of the stochastic stability of the proposed distributed estimation strategy introduced in the previous section. To facilitate clarity and focus on the key aspects of the stability arguments, we restrict our attention to the case where the local sensing models are linear. Although this assumption simplifies the exposition, it does not limit the generality of the results. In fact, the analysis can be extended to more general nonlinear sensing models by leveraging the methodology proposed for Theorem 3.1, wherein a Taylor series expansion is utilized in the analysis of the Unscented Kalman Filter (UKF). This approach permits the derivation of an approximate linear relationship between the output estimation error and the underlying state estimation error, thereby enabling a tractable stability analysis even in the nonlinear regime. Rather than employing the general nonlinear sensing model introduced earlier in (94), we adopt the following linear measurement model for the node $i \in \mathcal{V}$:

$$y_i(k) = H_i(k)x(k) + v_i(k), \quad (111)$$

where $H_i(k) \in \mathbb{R}^{m_i \times n}$ denotes the measurement matrix associated with node i and $v_i(k) \in \mathbb{R}^{m_i}$ represents the additive measurement noise.

Under this linear sensing assumption, the packing steps for measurement pairs are modified as follows:

$$\mathcal{Y}_i(k) = H_i^T(k)R_i^{-1}(k)H_i(k), \quad (112)$$

$$z_i(k) = H_i^T(k)R_i^{-1}(k)y_i(k), \quad (113)$$

Before presenting the main result, we introduce key derivations and notation that will be used in the subsequent theorems. The posterior estimation error of the node i at the time k is defined as $\tilde{x}_i(k) \triangleq x(k) - \hat{x}_i(k)$.

To approximate the state transition, we apply a first-order Taylor series expansion around $\hat{x}_i(k)$, yielding:

$$x(k+1) \approx f(\hat{x}_i(k)) + \nabla_{x(k)} f(\hat{x}_i(k)) \tilde{x}_i(k) + w(k).$$

Similarly, each sigma point after the transformation can be approximated by:

$$\begin{aligned} \mathcal{X}_{i,r}(k+1) &\triangleq f(\mathcal{X}_{i,r}(k)) \approx f(\hat{x}_i(k)) \\ &+ \nabla_{x(k)} f(\hat{x}_i(k)) (\mathcal{X}_{i,r}(k) - \hat{x}_i(k)). \end{aligned}$$

Consequently, the predicted state estimate $\hat{x}_i(k+1|k)$ can be expressed as:

$$\begin{aligned} \hat{x}_i(k+1|k) &= \sum_{r=0}^{2n} W_{i,r}^m f(\mathcal{X}_{i,r}(k)) \approx f(\hat{x}_i(k)) \\ &+ \nabla_{x(k)} f(\hat{x}_i(k)) \left(\sum_{r=0}^{2n} W_{i,r}^m \mathcal{X}_{i,r}(k) - \hat{x}_i(k) \right) = f(\hat{x}_i(k)). \end{aligned}$$

The prior estimation error of the node i at the time $k+1$ is defined as: $\tilde{x}_i(k+1|k) \triangleq x(k+1) - \hat{x}_i(k+1|k)$. By expanding $x(k+1)$ using a first-order Taylor series expansion around $\hat{x}_i(k)$, we obtain:

$$\tilde{x}_i(k+1|k) = \alpha_i(k) \mathcal{F}_i(k) \tilde{x}_i(k) + w(k), \quad (114)$$

where $\mathcal{F}_i(k) = \nabla_{x(k)} f(\hat{x}_i(k))$ denotes the Jacobian of the system dynamics, and $\alpha_i(k)$ is an unknown diagonal scaling matrix associated with the node i .

It will be shown that under certain sufficient conditions, the local prior estimation errors at each agent, as a stochastic process, remain bounded in the mean square sense.

Theorem 5.1. *Let $\mathcal{F}_i(k)$ and $\alpha_i(k)$ be defined as in (114). Suppose that the communication graph $\mathcal{G}(k)$ is strongly connected and remains fixed over time. Then, in absence of cyber-attacks, the prior estimation error $\tilde{x}_i(k+1|k)$ is bounded in the mean square for all $i \in V$, provided that the following conditions hold for each $i \in V$, that is, there exist positive constants $p_{min}, p_{max}, f_{min}, f_{max}, \hat{q}_{min}, r_{min}$, and h_{max} such that for all $k \in \mathbb{Z}^+$:*

$$p_{min}I \leq \hat{\mathbf{P}}_i(k+1|k) \leq p_{max}I, \quad (115)$$

$$f_{min}I \leq \mathcal{F}_i(k) \mathcal{F}_i(k)^\top \leq f_{max}I, \quad (116)$$

$$\hat{Q}_i(k) \geq \hat{q}_{min}I, \quad (117)$$

$$R_i(k) \geq r_{min}I, \quad (118)$$

$$H_i(k)H_i(k)^\top \leq h_{max}I. \quad (119)$$

where $\hat{\mathbf{P}}_i(k+1|k)$ represents the covariance matrix of the prior estimation error $\tilde{x}_i(k+1|k)$, and $\hat{Q}_i(k)$ denotes the extended process noise covariance.

Proof: Let $\rho_i(k)$ denote the i -th entry of the vector $\rho(k) \in \mathbb{R}^n$, where $\rho(k)$ is the left eigenvector associated with the largest eigenvalue (i.e., 1) of the matrix $\mathbf{D}(k)$. Since the graph $\mathcal{G}(k)$ is strongly connected, it follows that $\rho_i(k) > 0$ for all $i \in \mathcal{V}$ [145].

Let us define the global prior estimation error vector and the corresponding block diagonal covariance matrix as follows:

$$\tilde{x}(k+1|k) \triangleq (\tilde{x}_i(k+1|k))_{i \in \mathcal{V}},$$

$$\hat{\mathbf{P}}(k+1|k) \triangleq \text{blkdiag}(\hat{\mathbf{P}}_i(k+1|k)/\rho_i(k))_{i \in \mathcal{V}}.$$

Now, consider the Lyapunov function candidate according to:

$$V^{(k+1)}(\tilde{x}(k+1|k)) \triangleq (\tilde{x}(k+1|k))^\top (\hat{\mathbf{P}}(k+1|k))^{-1} (\tilde{x}(k+1|k)).$$

For each node i , define the local Lyapunov function component according to:

$$V^{(i,k+1)}(\tilde{x}_i(k+1|k)) \triangleq (\tilde{x}_i(k+1|k))^\top (\hat{\mathbf{P}}_i(k+1|k))^{-1} (\tilde{x}_i(k+1|k))$$

By weighting these local components with the eigenvector elements, the global Lyapunov function can be rewritten as:

$$V^{(k+1)}(\tilde{x}(k+1|k)) \triangleq \sum_{i \in \mathcal{V}} \rho_i(k+1) V^{(i,k+1)}.$$

By using condition (115) and results from [166] on the properties of stochastic processes, we obtain the following bounds:

$$(p'_{\max})^{-1} \|\tilde{x}(k+1|k)\|^2 \leq V^{(k+1)} \leq (p'_{\min})^{-1} \|\tilde{x}(k+1|k)\|^2,$$

where $p'_{\max} \triangleq p_{\max} \max_{i \in \mathcal{V}} \{\rho_i\}$ and $p'_{\min} \triangleq p_{\min} \min_{i \in \mathcal{V}} \{\rho_i\}$.

Following a similar approach as in [165], which analyzed a distributed nonlinear state estimation without considering cyber-attacks and switching topologies, one can establish that

$$\mathbb{E}[V^{(k+1)}] - V^{(k)} \leq \mu - \lambda V^{(k)}, \quad (120)$$

for some constants $\mu > 0$ and $0 < \lambda \leq 1$.

Since the above inequality ensures that $V^{(k)}$ is stochastically bounded, it follows that $\tilde{x}(k+1|k)$ is bounded in the mean square senses. This completes the proof of theorem. ■

5.3.1 Stability Under Switching Topologies

In static communication settings, where the underlying graph remains fixed, the distributed state estimation algorithm guarantees boundedness of the estimation error due to the contraction properties of the fusion process, as shown in Theorem 5.1. However, in practical scenarios, particularly in CPS with mobile nodes or dynamic environments, the communication topology is subject to change over time. These changes may result from agent mobility, network constraints, or adversarial conditions. Such variations in the communication graph can significantly impact the convergence behavior of the estimation process.

To maintain stability in presence of these dynamic changes, we introduce the concept of *dwell time*, which quantifies the minimum duration of time each graph topology must persist before a switch occurs. This notion is extended through the *average dwell time* which regulates the frequency of switching events by ensuring that, over a long period of time, the system spends sufficient time in each stable configuration.

When switching occurs too frequently, the estimation process may fail to leverage the contraction induced by strongly connected topologies, leading to possible divergence or unbounded growth of the estimation error. The analysis below establishes a sufficient condition on the average dwell time that is denoted by Γ_d to guarantee the mean-square boundedness of the estimation error, even under arbitrary switching sequences.

Theorem 5.2. *Consider the CPS system, containing a nonlinear system (93) and the sensor models (111), employing the proposed distributed data fusion approach. Assume that the conditions of Theorem 5.1 hold and that the time-varying communication graph $\mathcal{G}^{\sigma(k)}$ is strongly connected at each time step k . Then, for any subgraph $\hat{\mathcal{G}}^{\sigma(k)}$, the prior estimation error $\tilde{x}_i(k|k-1)$ for all $i \in \hat{\mathcal{V}}^{\sigma(k)}$ remains ultimately bounded in the mean-square sense, even under graph switching, provided that the average dwell time Γ_d satisfies the following condition:*

$$\Gamma_d > \frac{\log(1/\gamma_{\max})}{\log(1 - \lambda_{\min})}, \quad (121)$$

where $\gamma_{\max}$ represents the maximum transient growth factor among all switching graphs, while $\lambda_{\min}$ denotes the minimum decay rate across all admissible topologies.

Proof: From Theorem 5.1, under a fixed communication graph, the global Lyapunov function $V^{(k)}$, defined in terms of the expected mean-square error, satisfies the following recursive inequality:

$$\mathbb{E}[V^{(k+1)}] - V^{(k)} \leq \mu - \lambda V^{(k)}, \quad (122)$$

for some positive constants μ and λ , which characterize the contraction behavior of the estimation error dynamics. Assuming that the stochastic process exhibits mild variability,

one can approximate $\mathbb{E}[V^{(k+1)}] \approx V^{(k+1)}$, yielding:

$$V^{(k+1)} \leq (1 - \lambda)V^{(k)} + \mu, \quad (123)$$

where $\lambda \in (0, 1)$ represents the decay rate associated with a fixed strongly connected topology. This recursive inequality implies decay of the Lyapunov function, and hence of the estimation error, in absence of the switching graph.

Now consider a general switching sequence $\sigma(k)$, where the active topology may vary at each time step. At each instance of switching, the convergence behavior may be temporarily disrupted, particularly when the system transitions from a stable to a less favorable topology. Let $\gamma_{\max} > 1$ denote the maximum transient growth factor introduced due to a switch. Then, immediately after the switch, the Lyapunov function may experience a bounded increase in the form of:

$$V^{(k^+)} \leq \gamma_{\max} V^{(k)}, \quad (124)$$

where k^+ denotes the time instant just after the switch. This factor encapsulates the worst-case instantaneous destabilizing effect due to the switching topology.

To preserve stability despite such disturbances, the system must remain in each topology for a sufficiently long interval. During this average dwell time Γ_d , the contraction dynamics induced by the decay rate must be sufficiently strong to outweigh the growth introduced by the switching. Let $\lambda_{\min} \in (0, 1)$ represent the minimum decay rate across all admissible topologies, ensuring we consider the worst-case convergence scenario. Applying the decay iteratively over Γ_d steps, the Lyapunov function evolves as:

$$V^{(k+\Gamma_d)} \leq (1 - \lambda_{\min})^{\Gamma_d} V^{(k)} + \frac{\mu}{\lambda_{\min}}. \quad (125)$$

The above inequality accounts for both the geometric decay and the accumulated effect of the additive term μ . However, for the purpose of bounding the transient impact of the switching, we focus on the multiplicative term.

To ensure that the overall system continues to exhibit contraction across switching events, we must require that the decay over Γ_d steps strictly compensates for the worst-case instantaneous growth, i.e.,

$$\gamma_{\max}(1 - \lambda_{\min})^{\Gamma_d} < 1. \quad (126)$$

Taking logarithms on both sides yields the explicit lower bound on the minimum dwell time, namely:

$$\Gamma_d > \frac{\log(1/\gamma_{\max})}{\log(1 - \lambda_{\min})}. \quad (127)$$

The above condition guarantees that, in the long run, the contraction properties

dominate over any temporary destabilizing effect introduced by the switching. Hence, under the stated assumptions and with a dwell time satisfying (127), the estimation error remains ultimately bounded in the mean-square sense. This completes the proof of the theorem. ■

Remark 5.1. *Under the conditions of Theorem 5.2, consider the scenario where cyber-attacks compromise certain communication links, which are subsequently removed upon detection. If the resulting communication graph remains strongly connected and the average dwell-time condition (121) continues to hold for the updated topology sequence, then the estimation error $\tilde{x}_i(k)$ remains ultimately bounded in the mean-square sense. Although the removal of compromised links introduces additional topology switches, the stability guarantees of Theorem 5.1 still apply, provided that the switching does not violate the average dwell-time constraint. Therefore, the system maintains resilient estimation despite adversarial disruptions.*

Remark 5.2. *While Theorem 5.2 assumes that the communication graph remains strongly connected at each time step, real-world CPS may experience severe cyber-attacks that compromise critical communication links. In such cases, the resulting subgraphs may temporarily lose strong connectivity. Nevertheless, resilience can still be achieved under certain conditions. In particular, suppose that after a cyber-attack, the resulting subgraph $\hat{\mathcal{G}}^{\sigma(k)}$ is no longer strongly connected but can be decomposed into strongly connected components (SCC), and that within each SCC, the assumptions of Theorem 5.2 hold. If the estimation nodes in each SCC continues to exchange information internally using the proposed data fusion mechanism, and if the switching among SCCs still respect a sufficient average dwell time Γ_d , then each SCC can maintain local mean-square boundedness of its estimation error. Consequently, when persistent full connectivity is infeasible, designing the network to ensure sufficient internal connectivity within SCCs, along with eventual global connectivity and appropriate average dwell-time enforcement, offers a practical and effective mechanism to achieving resilient distributed state estimation.*

5.4 Case Study Simulations

As a case study an unmanned aerial vehicle (UAV) modeled as a nonlinear system moving through a region monitored by multiple sensor nodes, as illustrated in Figure 5.2. Each node has a limited sensing range and communicates with its neighbors. The sensor network collectively aims to estimate the UAV's state. Additionally, cyber-attacks are introduced through the communication links. The objective is to detect and isolate these attacks and maintain robust distributed state estimation by using the proposed methods introduced in previous sections.

The UAV model used here is the same as in Chapter 3. The angular rate dynamics are given by:

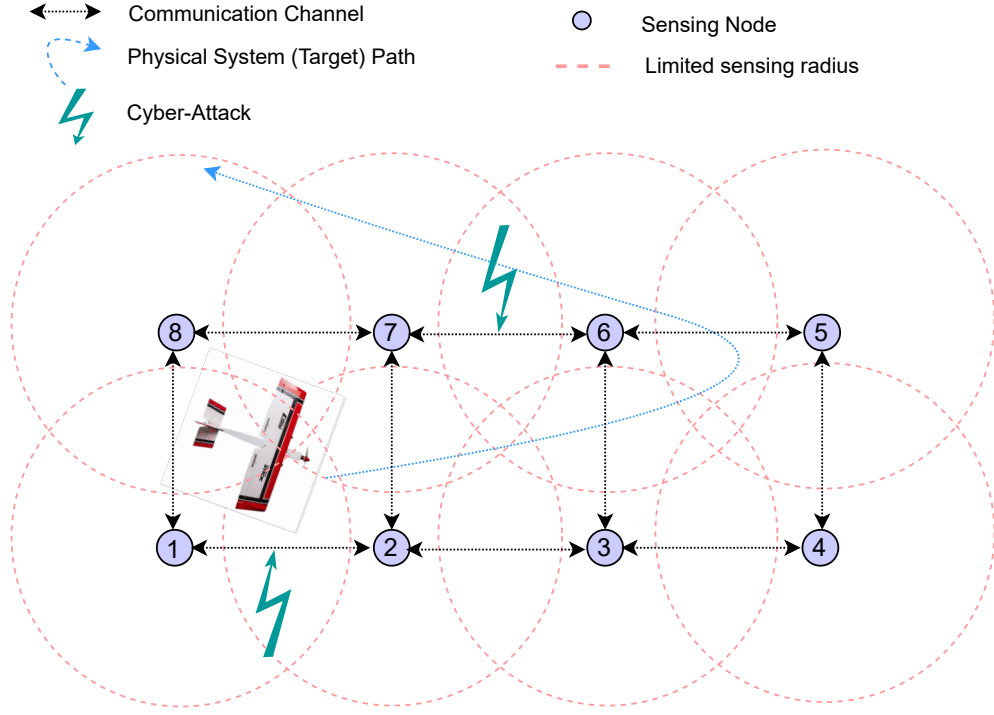


Figure 5.2: UAV integrated with a distributed sensor network.

$$\begin{aligned}
 \dot{p} - \frac{I_{xz}}{I_{xx}} \dot{r} &= \frac{p_d S b}{I_{xx}} c_l - \frac{I_{zz} - I_{yy}}{I_{xx}} q r + \frac{I_{xz}}{I_{xx}} q p \\
 \dot{q} &= \frac{p_d S \bar{c}}{I_{yy}} c_m - \frac{I_{xx} - I_{zz}}{I_{yy}} p r - \frac{I_{xz}}{I_{yy}} (p^2 - r^2) + \frac{I_p}{I_{yy}} w_p r \\
 \dot{r} - \frac{I_{xz}}{I_{zz}} \dot{p} &= \frac{p_d S b}{I_{zz}} c_n - \frac{I_{yy} - I_{xx}}{I_{zz}} p q - \frac{I_{xz}}{I_{zz}} q r - \frac{I_p}{I_{zz}} w_p q
 \end{aligned} \tag{128}$$

In these equations, p , q , and r (rad/s) represent the angular velocities about the body axes, while ϕ , θ , and ψ (rad) are the roll, pitch, and yaw angles, respectively. The kinematics of the rotational motion are described by:

$$\begin{aligned}
 \dot{\phi} &= p + \tan \theta (q \sin \phi + r \cos \phi) \\
 \dot{\theta} &= q \cos \phi - r \sin \phi \\
 \dot{\psi} &= \frac{q \sin \phi + r \cos \phi}{\cos \theta}
 \end{aligned} \tag{129}$$

For a detailed description of the parameters in the above equations, refer to Section 3.6.

In the CPS framework shown in Figure 5.1, the UAV acts as the physical system, while each sensor node can observe the system output $y_i = [\phi, \theta, \psi]$ when the UAV is within its

sensing range. Each node estimates the UAV’s state using the proposed distributed data fusion algorithm and shares its estimate with neighboring nodes over the communication network. In this case study, we consider a network with 8 sensing nodes and investigate the system behavior under this setup.

5.4.1 Scenario 1: Sensor Network under Cyber-Attacks

Initially, the CPS is assumed to operate under healthy conditions, without any cyber threats or sensor fault. Figure 5.3 illustrates the distributed state estimation results for each sensing node compared against the actual UAV output states. These plots confirm that each node in the network can accurately estimate the system states when no adversarial activity is present.

To complement this analysis, Figure 5.4 displays the sensing availability of each local node, indicating the time intervals during which each node has access to direct measurements of the UAV’s state variables. Due to the limited sensing range of each node, coverage is intermittent and varies with the UAV’s trajectory.

Under these favorable conditions, the proposed distributed estimation algorithm performs effectively. Leveraging the fact that the communication graph remains strongly connected throughout this phase, information from directly sensing nodes is efficiently propagated across the entire network. As a result, all estimation nodes—even those lacking direct measurements at certain times—can still compute reliable state estimates by fusing information received from their neighbors.

Following the healthy operation phase, the communication network is assumed to be compromised by two FDI cyber-attacks. The first attack occurs at $t = 20$ s and targets the communication link from node 2 to node 1—referred to as Attack21. The second attack is launched at $t = 45$ s, compromising the communication link from node 6 to node 7, and is denoted as Attack67.

To counter these threats, DRL-based cyber-attack detectors are embedded in nodes 1 and 7. These detectors are designed to monitor the incoming communication links and identify abnormal patterns indicative of cyber intrusions. Upon detecting the respective attacks, the detectors successfully raise alarms and broadcast the compromised link information to the rest of the network. The probability of attack occurrence, as estimated by the DRL models, is depicted in Figure 5.5, demonstrating timely and accurate detection.

Once the attacks are detected, a predefined network recovery strategy is triggered. Specifically, nodes 7 and 3 are designated as backup nodes responsible for initiating topology reconfiguration. In response to Attack21, node 7 establishes a new communication link with node 1, effectively bypassing the compromised path. Following Attack67, node 3 creates a new connection with node 7, reestablishing a strongly connected graph structure. The switched communication topologies resulting from these reconfiguration actions are shown in Figure 5.6. The left-hand graph represents the topology adjustment after the first attack,

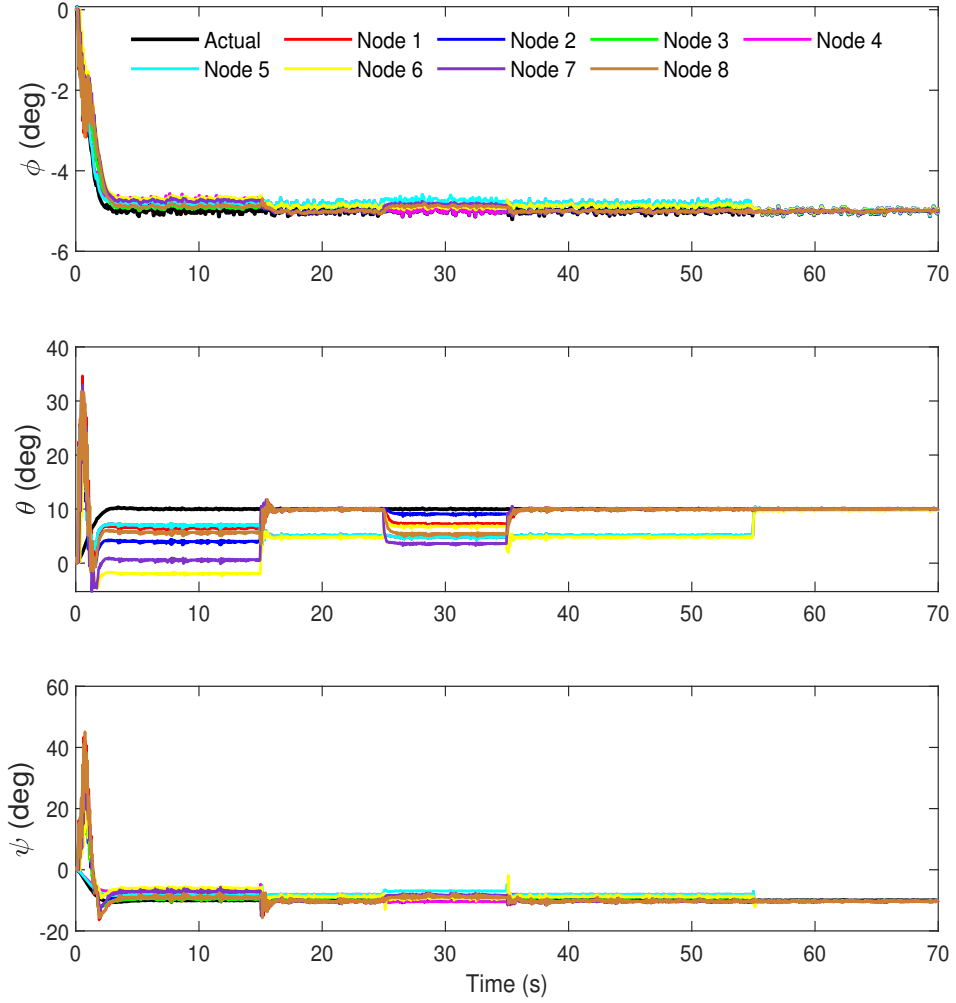


Figure 5.3: Distributed state estimation results for sensor network under healthy conditions.

while the right-hand graph depicts the final configuration after both attacks have been mitigated.

The recovered distributed state estimation results are presented in Figure 5.7. The final subplot in this figure highlights the timing of both cyber-attacks. As demonstrated, the proposed cyber-resilient recovery mechanism effectively maintains estimation performance. Once the compromised links are isolated and removed, the reconfigured communication topology allows the estimation algorithm to resume normal operation. Despite the occurrence of two coordinated cyber-attacks, the distributed estimator exhibits resilience and successfully recovers to maintain bounded and accurate state estimates.

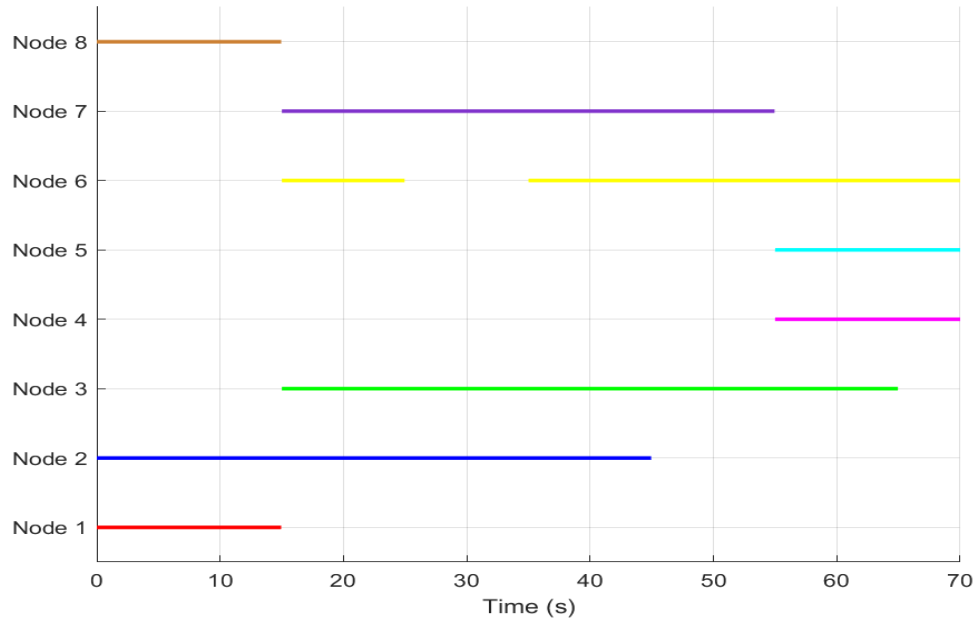


Figure 5.4: Sensing status of each local node over time.

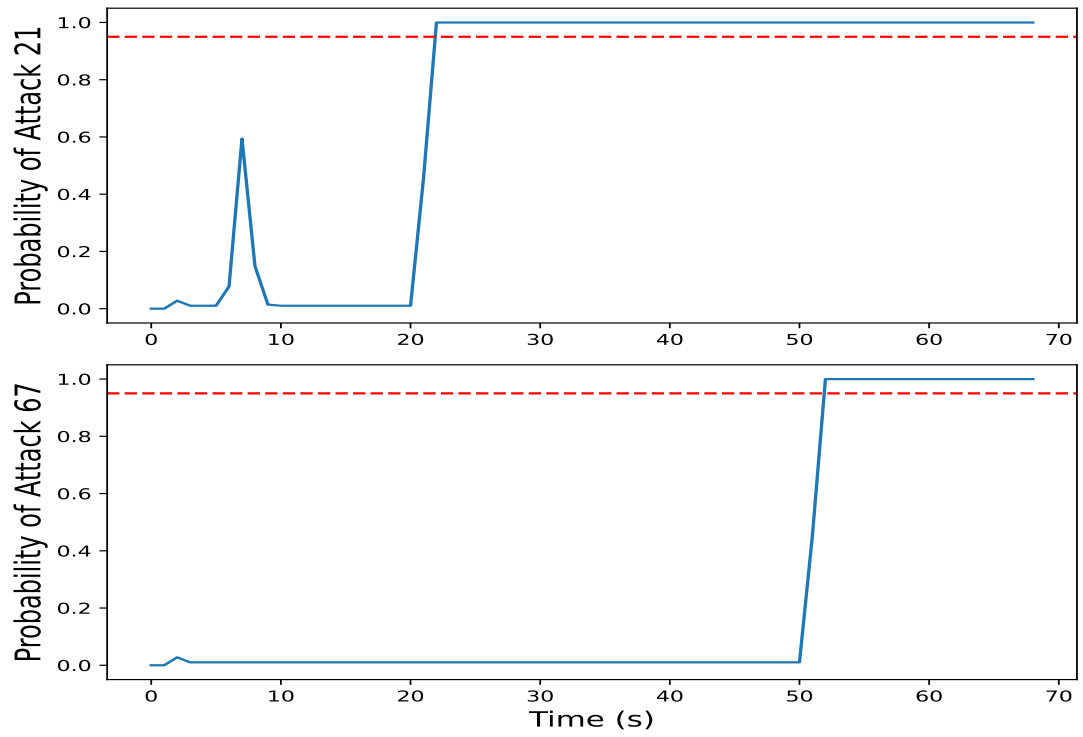


Figure 5.5: Detection results of the DRL-based cyber-attack detector for Attack21 and Attack67.

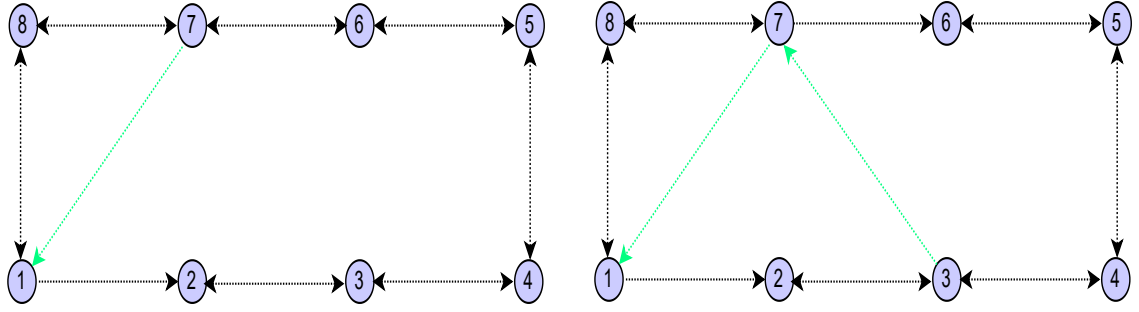


Figure 5.6: Switched graphs resulting from the recovery system under cyber-attacks: Attack21 (left) and both Attack21 and Attack67 (right).

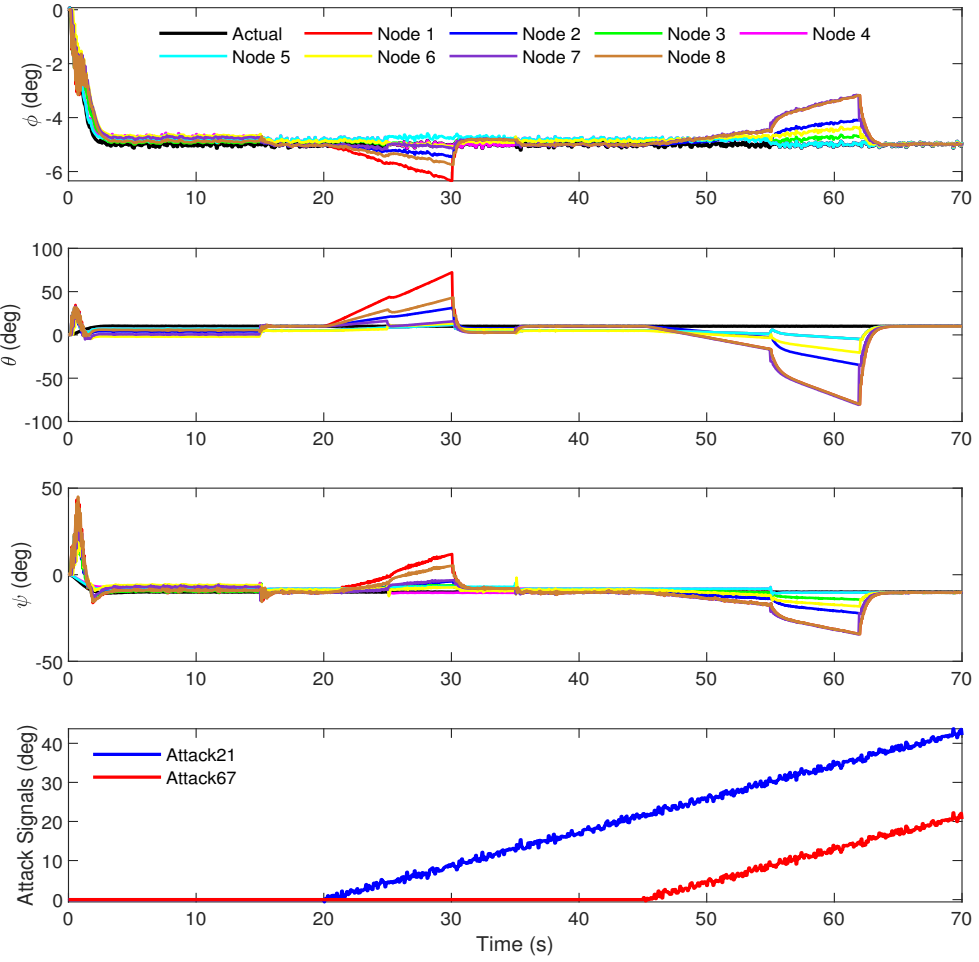


Figure 5.7: Recovered distributed state estimation results under cyber-attacks on links 21 and 67.

5.4.2 Scenario 2: Simultaneous Sensor Fault and Cyber-Attacks

In the second simulation scenario, the sensor network is exposed to more complex disturbances, including a sensor fault and two cyber-attacks. Specifically, two new FDI attacks—referred to as Attack12 and Attack45—target the communication links from node 1 to node 2 and node 4 to node 5, respectively. A fault is injected into sensing node 1 at $t = 15$ s, rendering its measurements unreliable. Subsequently, Attack12 is launched at $t = 30$ s, followed by Attack45 at $t = 55$ s. Figure 5.8 illustrates the sensor fault at node 1 alongside its state estimation generated using the AUKF. The second subplot depicts the temporal occurrence of the cyber-attacks on the communication links.

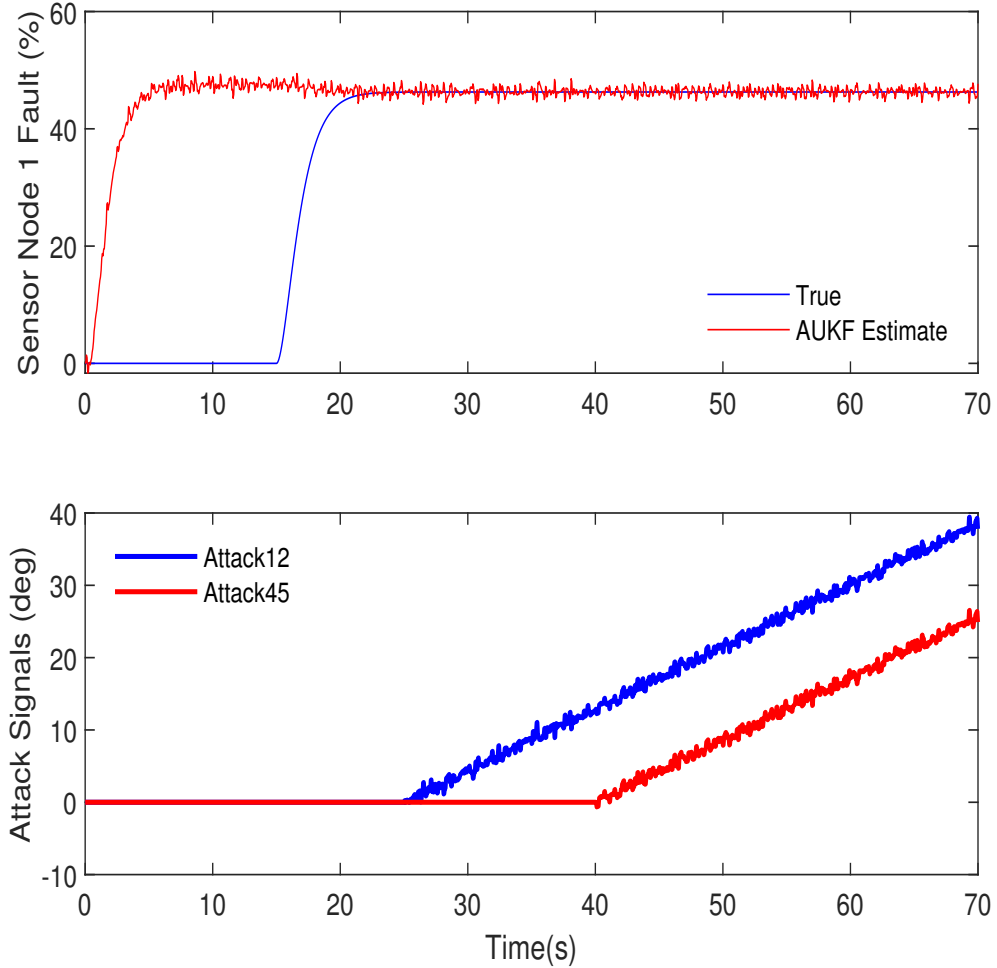


Figure 5.8: Sensor fault at node 1 and cyber-attacks on links 12 and 45. The first subplot shows the faulty measurement and its estimation using AUKF. The second subplot highlights the attack signals initiated at $t = 30$ s and $t = 55$ s.

To evaluate detection performance, Figure 5.9 compares the results of the DRL-based detection algorithm with those of the traditional χ^2 detector. As illustrated, the DRL detector consistently outperforms the χ^2 test in both fault and cyber-attack scenarios, providing earlier detection. This highlights the benefit of employing learning-based techniques for real-time anomaly detection.

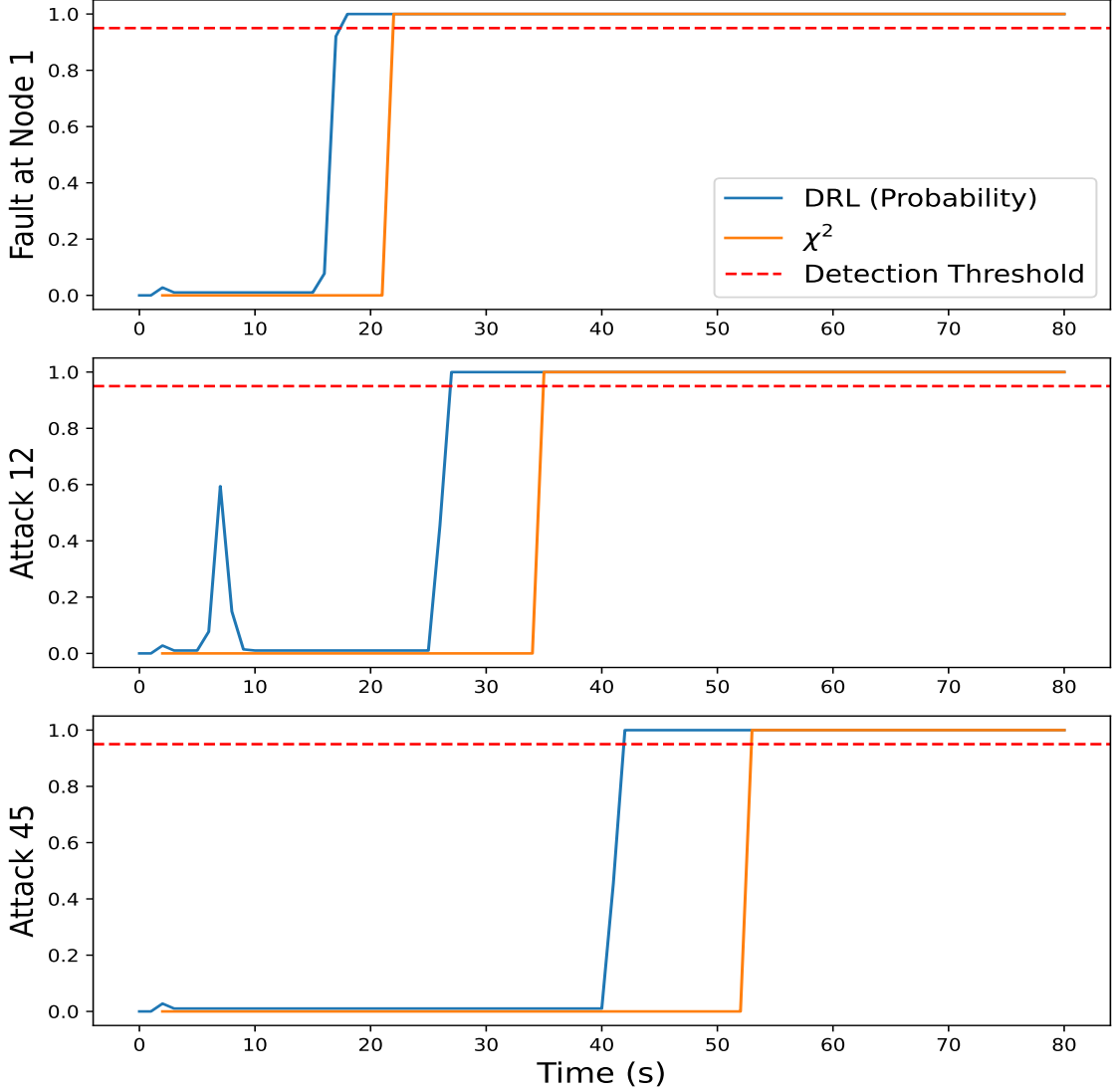


Figure 5.9: Comparison of detection and isolation results using DRL-based and χ^2 -based detectors under sensor fault and cyber-attacks.

Upon successful detection of the compromised links and the faulty sensor, the predefined system recovery and fault-tolerant protocol is activated. Specifically, sensing node 1 is identified as faulty, and its measurements are excluded from the distributed estimation process to prevent propagation of erroneous data. Meanwhile, the DRL-based detectors embedded in nodes 2 and 5 issue attack alerts to the network, prompting a

dynamic reconfiguration of the communication topology. Based on the predefined backup connectivity list, node 8 establishes a new communication link with node 2, and node 3 forms a connection with node 5.

The updated communication topologies are presented in Figure 5.10. The left graph corresponds to the reconfiguration following Attack12, while the right graph represents the final network structure after both attacks and sensor isolation.

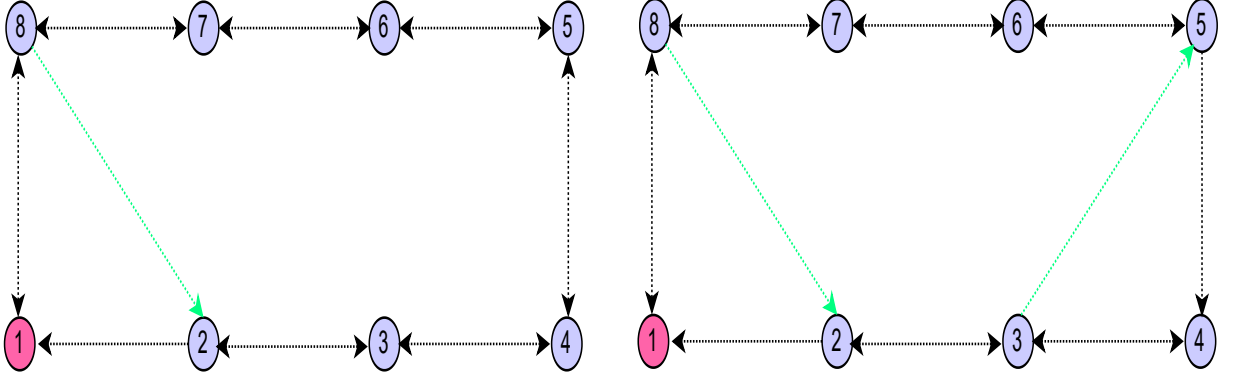


Figure 5.10: Reconfigured communication topologies under the joint effects of sensor fault and cyber-attacks. The left graph shows the updated topology following Attack12; the right graph shows the configuration after Attack45. Node 1 is marked as faulty, and its measurements are excluded from estimation.

The resulting distributed state estimation performance is shown in Figure 5.11. Despite the concurrent challenges introduced by sensor degradation and two cyber-attacks, the proposed resilient framework enables accurate and bounded estimation results. Once the affected links are isolated and the faulty node is excluded, the reconfigured communication network allows the distributed estimator to resume its normal operation.

To further evaluate the robustness of the detection mechanisms, the intensity of the noise associated with the cyber-attacks is increased. Figure 5.12 presents a comparative analysis of the DRL and χ^2 detectors under these more adverse conditions. The DRL-based detector continues to deliver reliable detection performance, highlighting its resilience and suitability for cyber-physical systems. In contrast, the increased noise levels lead to noticeable detection delays in the χ^2 detector.

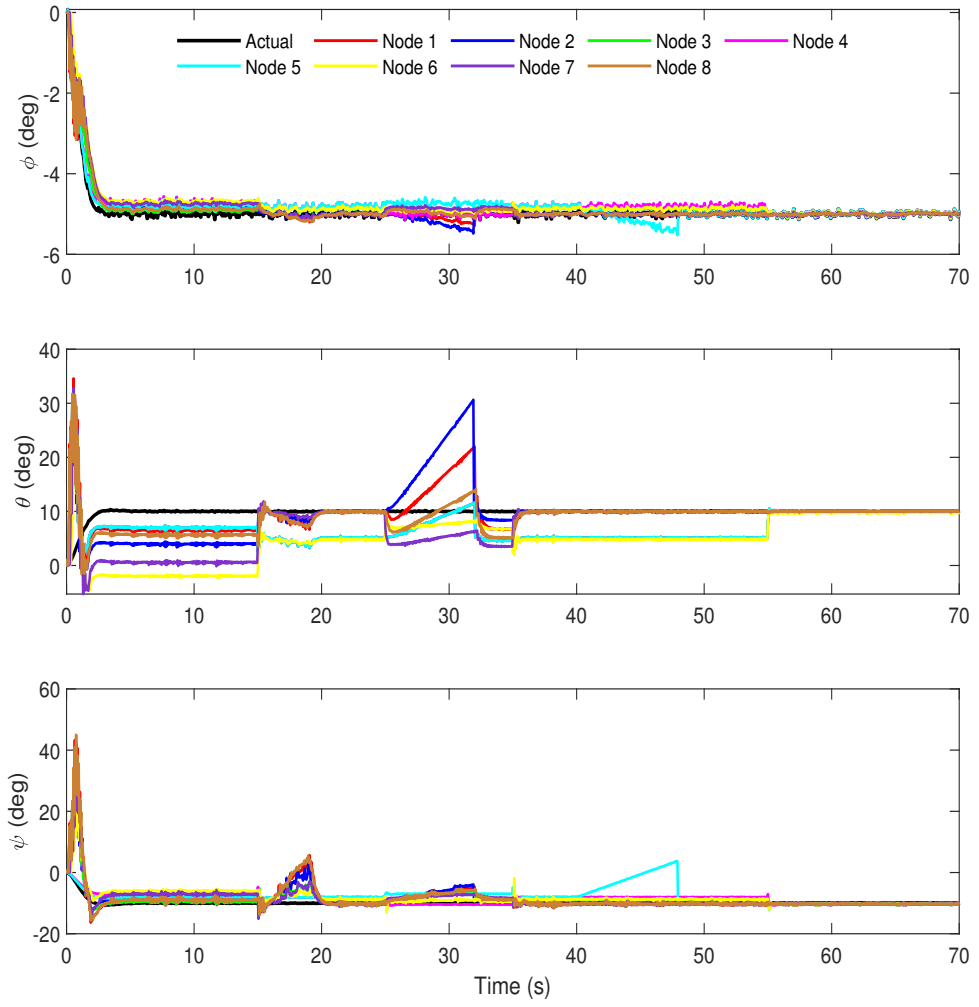


Figure 5.11: Recovered distributed state estimation results under a sensor fault and cyber-attacks on links 12 and 45.

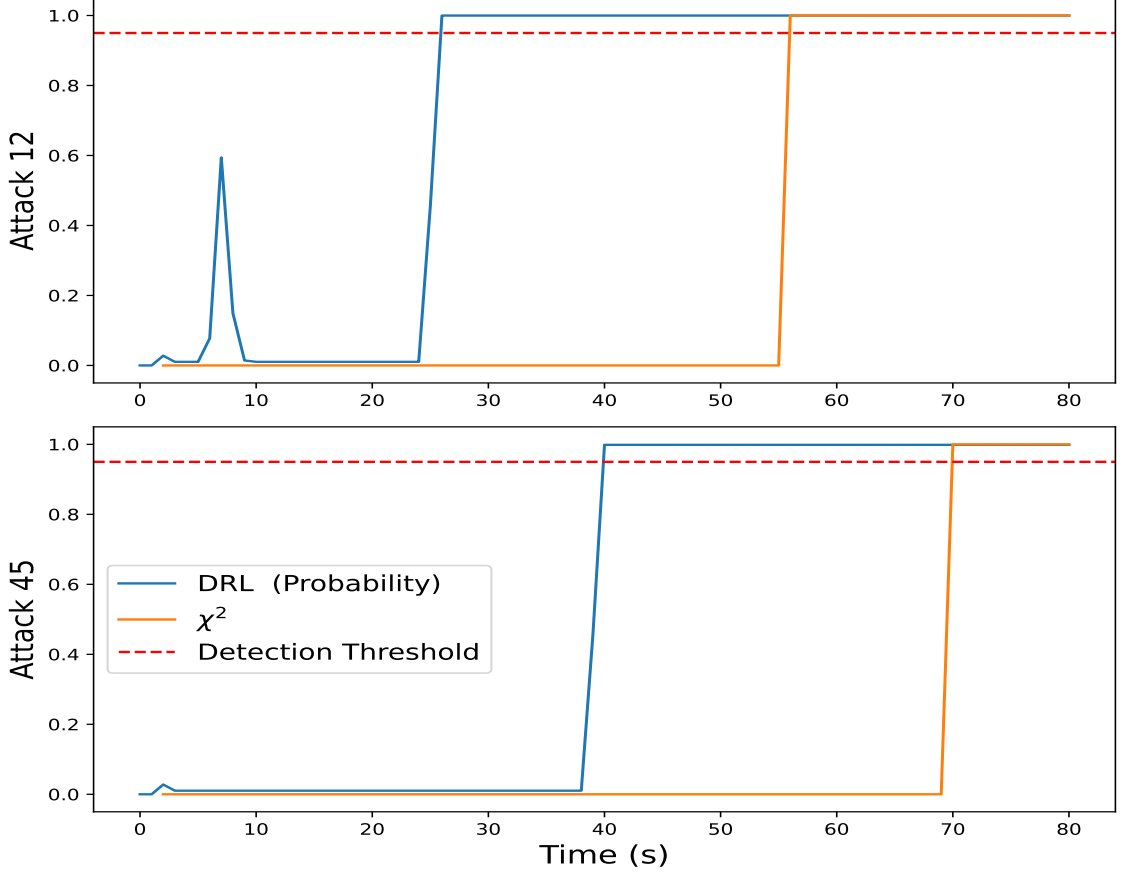


Figure 5.12: Detection and isolation results based on DRL and χ^2 detectors under increased cyber-attack noise.

5.4.3 Scenario 3: UAV Path Following with Cyber-Attack Detection and Recovery

In the third simulation scenario, we examine a realistic flight mission in which the UAV traverses through a distributed sensor network composed of eight sensing nodes. The UAV enters, passes through, and eventually exits the sensing region. Figure 5.13 illustrates the sensing status of each node over time, showing which nodes are directly observing the UAV as it moves.

Initially, the system operates under healthy conditions. Figure 5.14 presents the distributed state estimation results. As evident from the figure, each sensing node successfully tracks the UAV's attitude despite changes in its orientation. After a brief transient phase, the estimations converge and maintain high accuracy across the network.

The UAV's translational motion is modeled in a right-handed inertial (world) frame, where its position at time step k is represented by the vector $(x(k), y(k), z(k))$. The UAV moves forward with a known constant velocity v_{fwd} in its body frame. Assuming

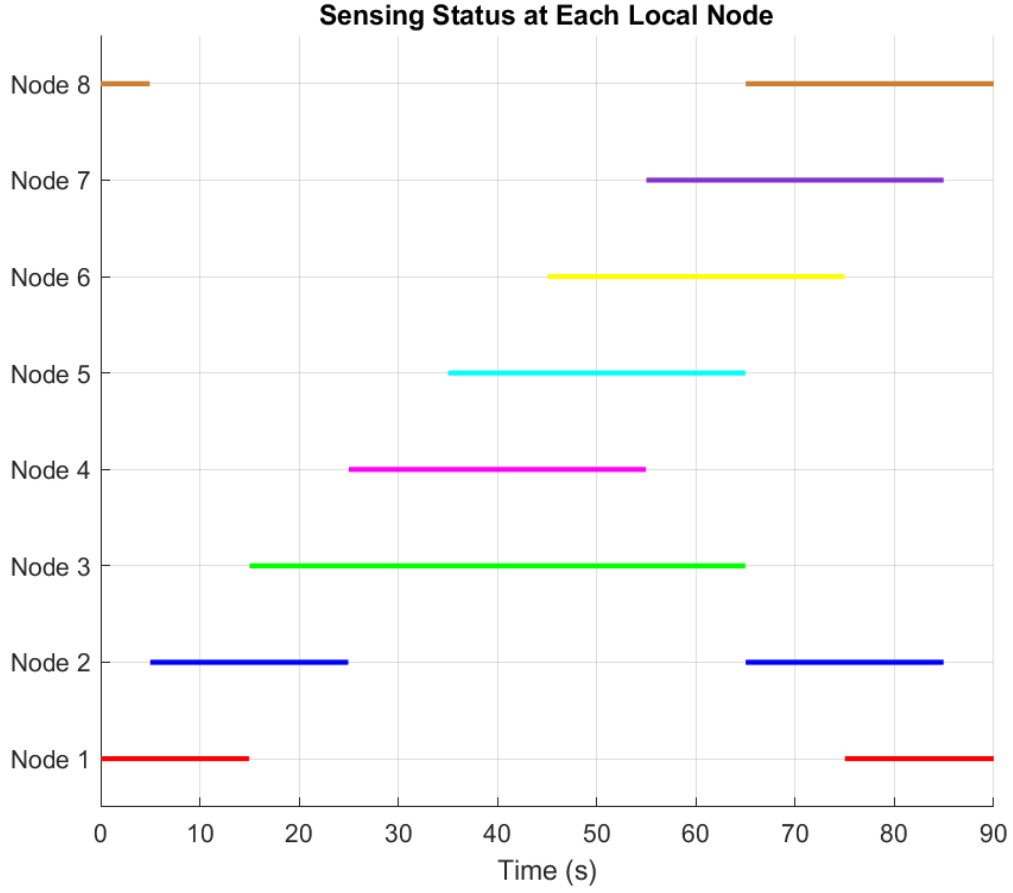


Figure 5.13: Sensing status of each local node over time.

coordinated flight with negligible side-slip, the body-frame velocity vector aligns with the UAV's longitudinal axis. Only the pitch $\theta(k)$ and yaw $\psi(k)$ angles influence the translational dynamics, while the roll $\phi(k)$ is omitted in this simplified kinematic model.

The position update equations, derived under the above assumptions, are given by [167]:

$$\begin{aligned}
 x(k+1) &= x(k) + v_{\text{fwd}} \cos(\theta(k)) \cos(\psi(k)) \\
 y(k+1) &= y(k) + v_{\text{fwd}} \cos(\theta(k)) \sin(\psi(k)) \\
 z(k+1) &= z(k) - v_{\text{fwd}} \sin(\theta(k))
 \end{aligned} \tag{130}$$

The UAV's actual positions and their corresponding estimates provided by each node under healthy conditions are shown in Figure 5.15. Additionally, Figure 5.16 illustrates the UAV's 3D trajectory along with the distributed state estimates from the local nodes at four different time snapshots. As observed, the estimates remain accurate and stable throughout the UAV's flight path.

To assess the network's resilience against malicious disturbances, we simulate the effects

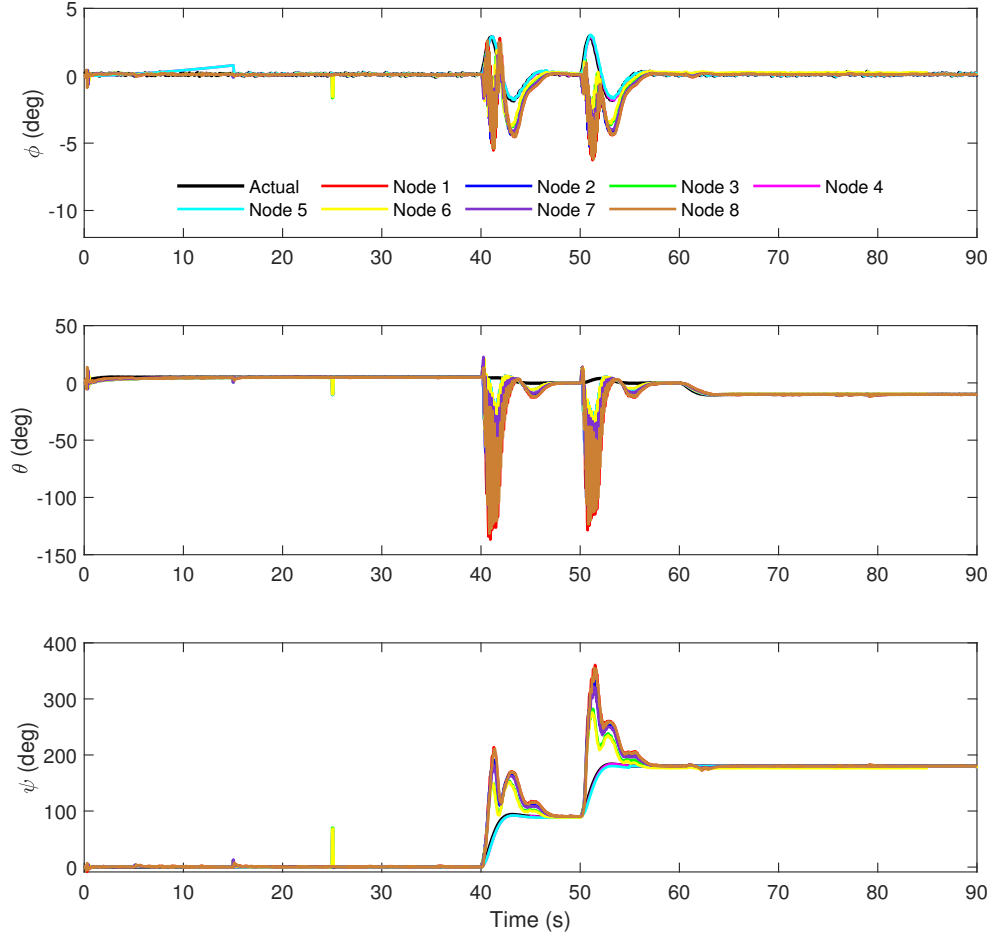


Figure 5.14: State estimation results under healthy conditions.

of targeted cyber-attacks on the communication infrastructure of the sensor network. Specifically, two FDI attacks—referred to as Attack12 and Attack67—are introduced. These attacks are launched at $t = 20$ s and $t = 45$ s, respectively, and aim to corrupt the communication links between nodes 1–2 and 6–7. These compromised links carry falsified data designed to mislead the state estimation process. The injected malicious signals corresponding to these attacks are illustrated in Figure 5.17. These signals emulate the effect of a coordinated cyber threat that seeks to degrade the performance and integrity of the distributed estimator by injecting persistently biased information into the network.

Figure 5.18 illustrates the UAV’s 3D trajectory under the influence of Attack12 and Attack67, in absence of any recovery or mitigation mechanisms. As the UAV follows its designated path, corrupted data from the compromised links is incorporated into the estimation process, significantly degrading the estimator’s accuracy. The small

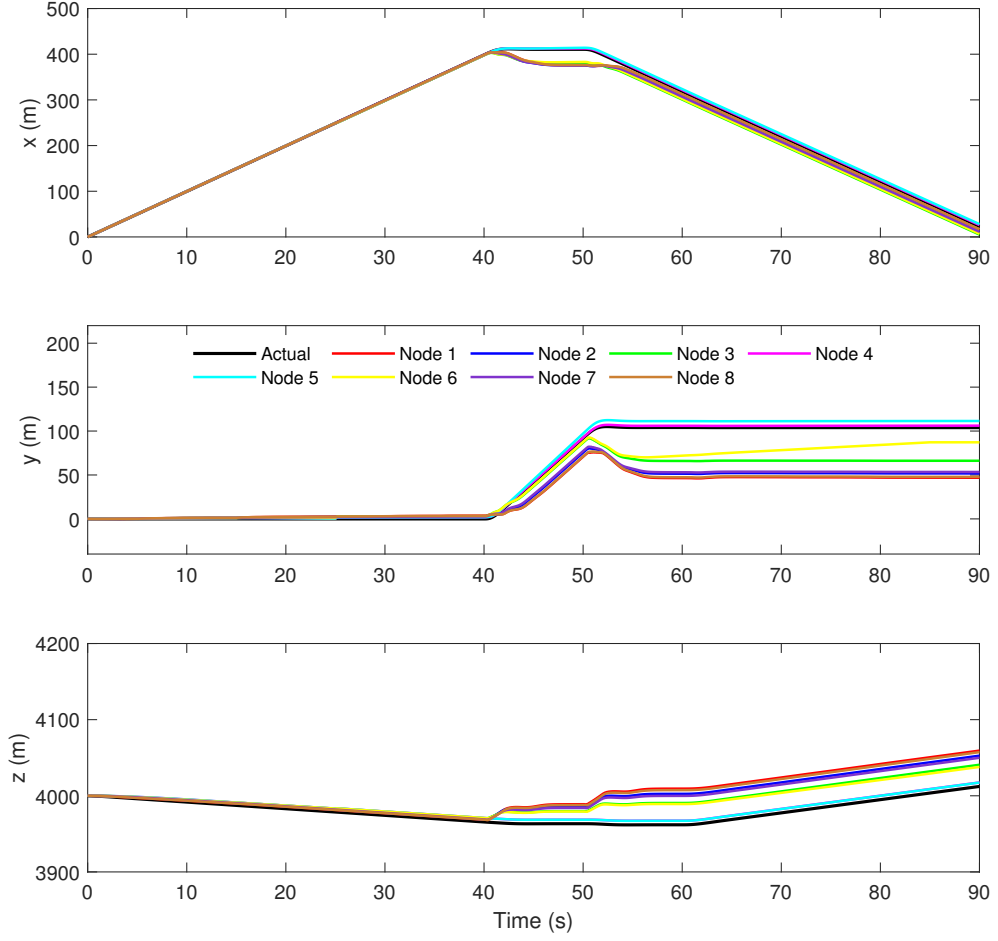


Figure 5.15: UAV positions under healthy conditions.

circles represent the nodes' estimation results, which, due to the cyber-attacks, deviate substantially from the actual positions marked by diamonds, shown for four selected sample times. As depicted in Figure 5.19, this disruption causes a pronounced deviation from the expected trajectory, highlighting the adverse effects of the FDI attack. The deterioration in estimation quality becomes increasingly severe as the system continues to operate, ultimately destabilizing the distributed state estimation framework. This scenario clearly demonstrates the sensor network's vulnerability to cyber threats in the absence of a defensive strategy.

To counteract the degradation caused by these attacks, the proposed DRL-based detection and dynamic network recovery mechanism is deployed. As shown in Figure 5.20, the embedded DRL detectors within nodes 2 and 7 successfully detect Attack12 and Attack67, respectively. Once the cyber-attacks are detected, the system autonomously

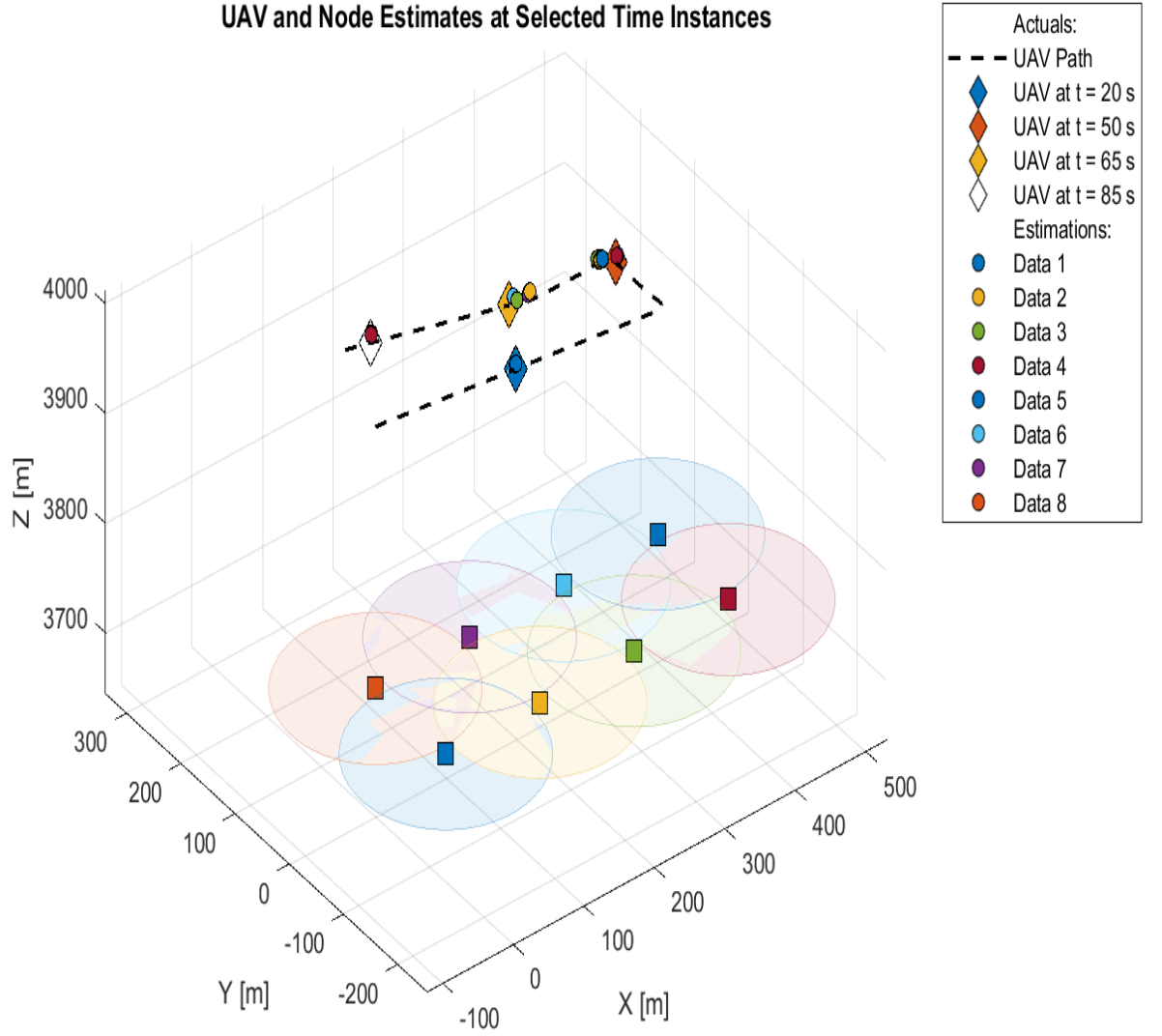


Figure 5.16: 3D UAV actual positions and distributed state estimates from local nodes at four different time snapshots under healthy conditions.

activates the proposed recovery strategy, as detailed in Subsection 5.2.5, where node 6 establishes a new communication link with node 2, while node 3 initiates a connection with node 7. Guided by predefined backup nodes, these alternative paths are designed to maintain estimation integrity in presence of the compromised links.

The resulting network topologies after each recovery step are depicted in Figure 5.21. The left panel corresponds to the reconfigured network after mitigating Attack12, while

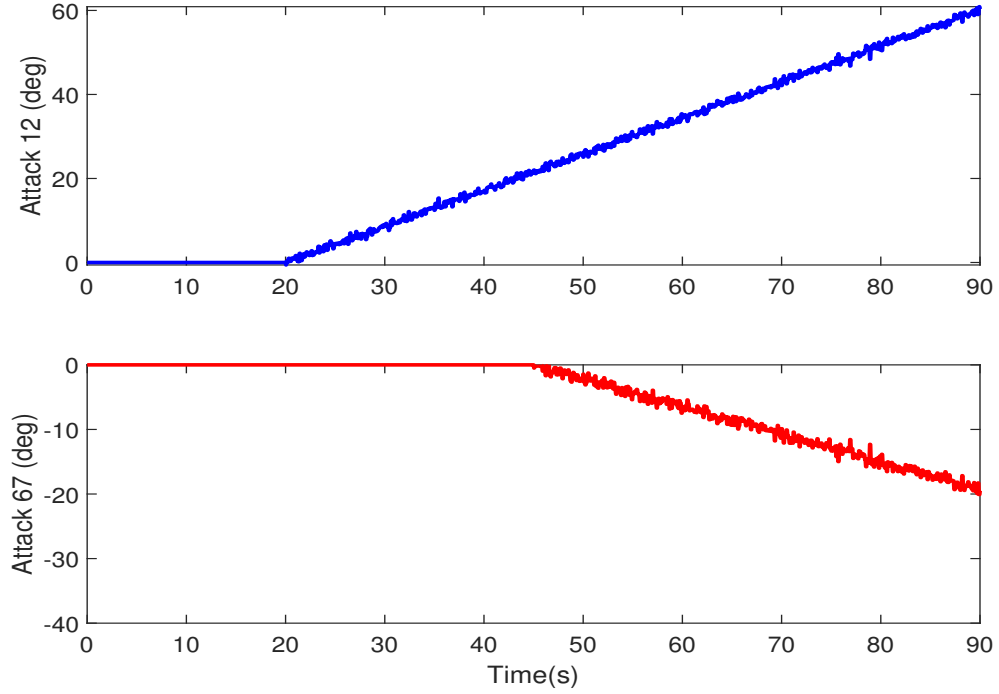


Figure 5.17: Attack signals injected into communication links x_{12} and x_{67} .

the right panel illustrates the final communication structure following both recovery actions. These dynamically switched topologies are critical for ensuring continued estimator performance, as they prevent the propagation of malicious information throughout the network.

Figure 5.22 presents the distributed state estimation results after the attack detection and subsequent recovery mechanisms have been executed. Despite the disruptions introduced by Attack12 and Attack67, the system exhibits a strong ability to restore estimation accuracy and maintain bounded error behavior across the network. This enables the estimator to resume proper data fusion without relying on the corrupted information. The figure clearly shows that after the initial transient response caused by the cyber-attacks, the estimation errors rapidly converge back to acceptable bounds, indicating both stability and resilience. These results validate the robustness of the proposed architecture in mitigating the impact of cyber-attacks and ensuring continued estimation performance under adversarial conditions.

Figures 5.24 and 5.25 further reinforce the effectiveness of the proposed resilience framework by illustrating the UAV's position estimates and the reconstructed 3D trajectories post-recovery. In Figure 5.24, the UAV's x , y , and z position components are estimated with bounded error, even in the aftermath of two consecutive cyber-attacks. Figure 5.25 complements this observation by visualizing the full 3D trajectory from the

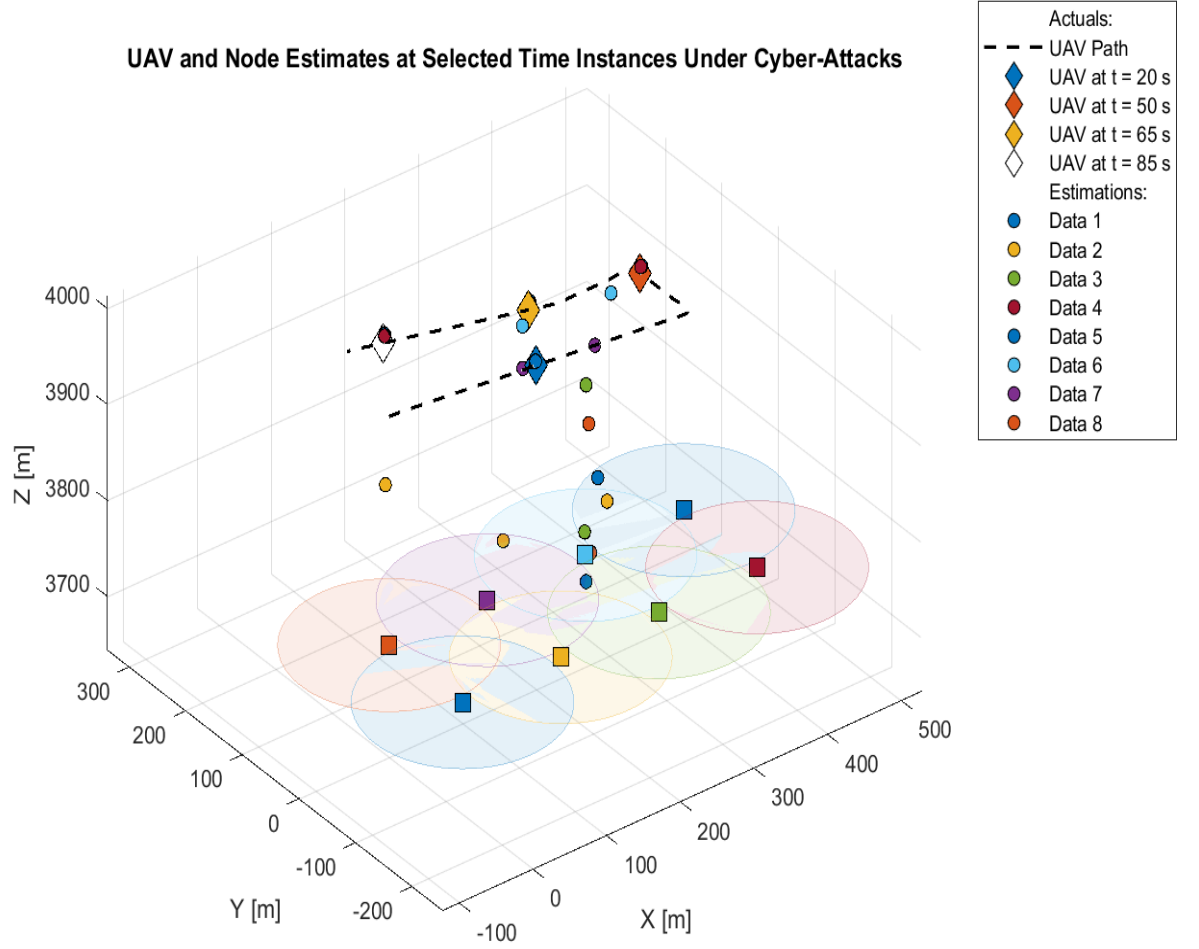


Figure 5.18: 3D UAV actual positions and estimation results under cyber-attacks affecting links 12 and 67.

perspective of each node's local estimation. The paths reconstructed by the distributed estimator align closely with the actual UAV trajectory, suggesting that the network-wide estimation process has been effectively restored.

To provide a comprehensive quantitative assessment of estimation performance under different operating conditions, Figure 5.23 illustrates the mean estimation errors of the UAV's x , y , and z position components across three distinct phases: healthy operation, during cyber-attacks, and after system recovery. Moreover, Table 5.1 provides the mean absolute estimation errors for each sensing node over the full 90-second simulation scenario.

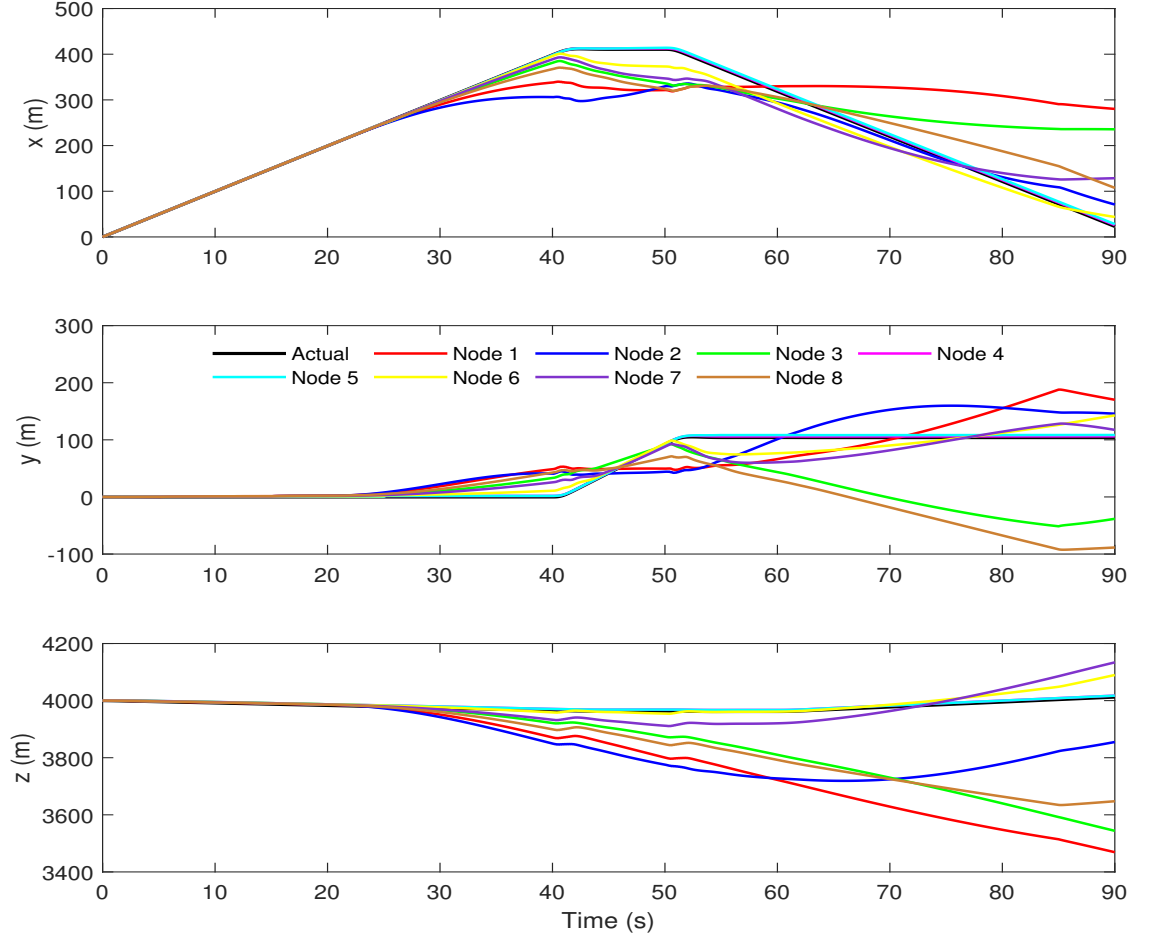


Figure 5.19: UAV positions under cyber-attacks affecting links 12 and 67, initiated at $t = 20$ s and $t = 45$ s, respectively.

These results are presented for the same three phases and include both rotational angle errors ($\phi(k)$, $\theta(k)$, $\psi(k)$, in degrees) and positional coordinate errors ($x(k)$, $y(k)$, $z(k)$, in meters).

The comparison of average values (shown in the last row of the table) highlights a substantial degradation in both angular and positional accuracy during the attack phase subject to FDI attacks. Following the activation of the proposed recovery mechanism, estimation errors were significantly reduced, with mean errors approaching to those values observed under healthy conditions. This indicates the effectiveness of the resilience framework in mitigating the effects of cyber-attacks and restoring distributed state estimation performance—yielding over 90% improvement in accuracy as compared to the compromised phase.

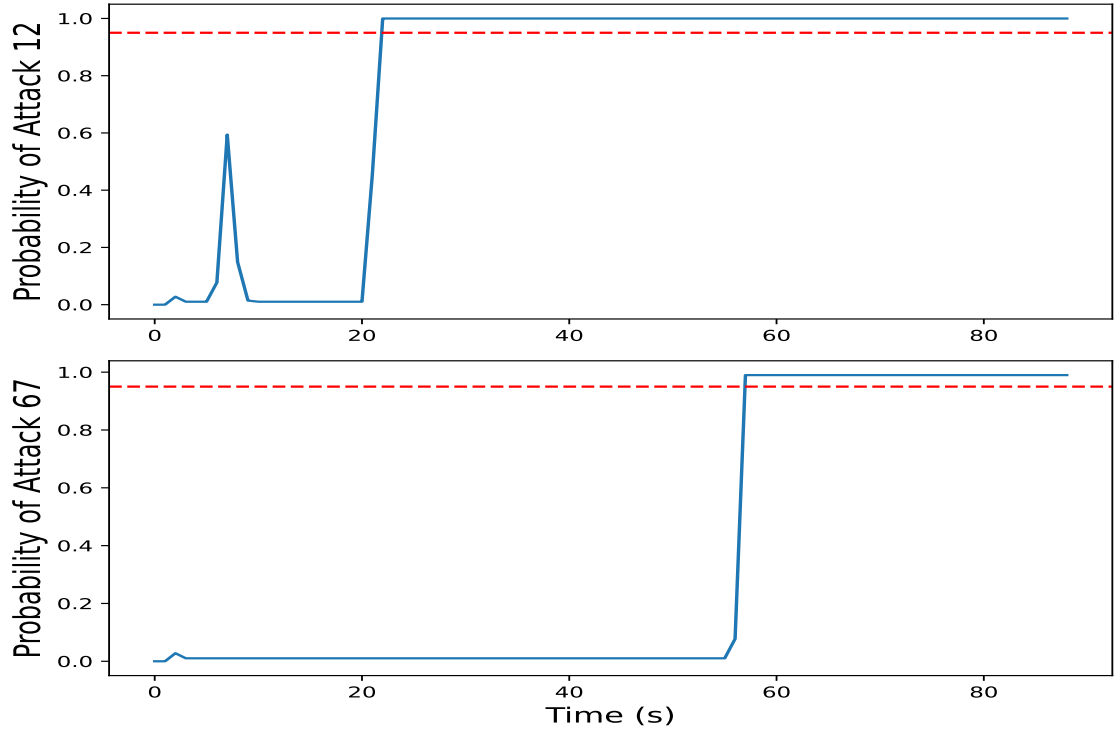


Figure 5.20: DRL-based attack detection results for Attack12 and Attack67.

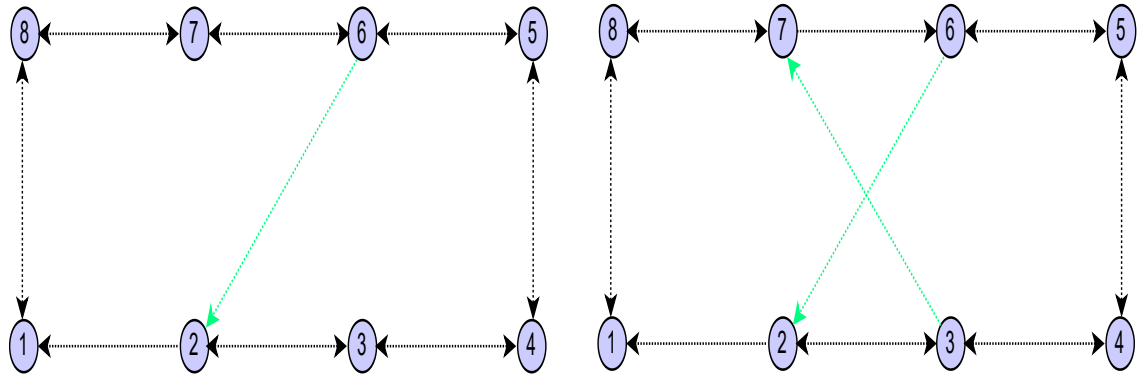


Figure 5.21: Network reconfiguration in response to the Attack12 (left) and both Attack12 and Attack67 (right).

This performance can be attributed to the synergy between the proposed cyber-attack detection and recovery approach and the DHIF strategy. The DRL detectors provide timely and accurate identification of anomalies, while the DHIF mechanism enables flexible, topology-aware data fusion that adapts to sudden structural changes in the network. Importantly, the recovery is not just reactive but also proactive—ensuring that malicious data is contained before it can significantly propagate through the system. The

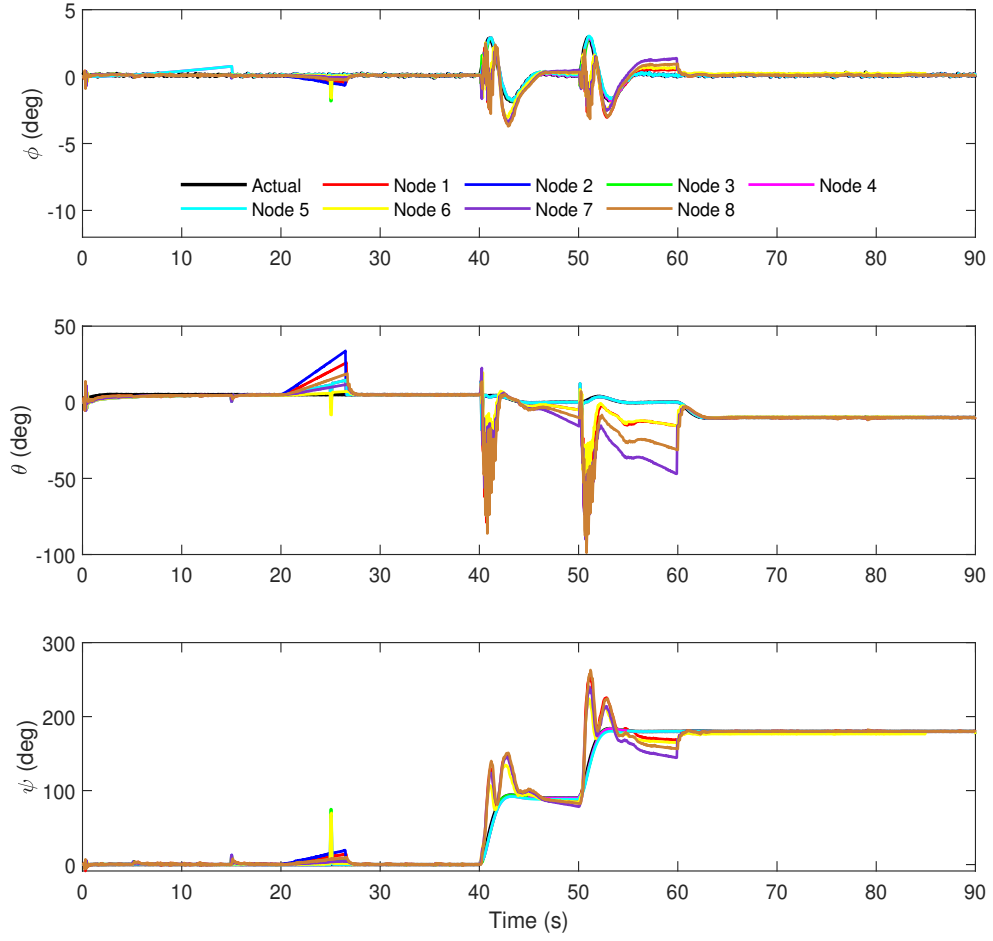


Figure 5.22: State estimation results following recovery from Attack12 and Attack67. The attacks were initiated at $t = 20$ s and $t = 45$ s, detected at $t = 26$ s and $t = 58$ s, and recovered at $t = 28$ s and $t = 60$ s, respectively.

estimator's ability to maintain both accuracy and stability throughout the mission, despite encountering sequential attacks, underscores the real-world viability of the approach. This is especially critical in CPS systems, where delayed or incorrect estimations can compromise safety and mission objectives. Overall, the results confirm that the proposed method not only withstands cyber-attacks but also recovers gracefully with minimal performance degradation, making it a robust solution for resilient distributed state estimation in safety-critical CPS systems.

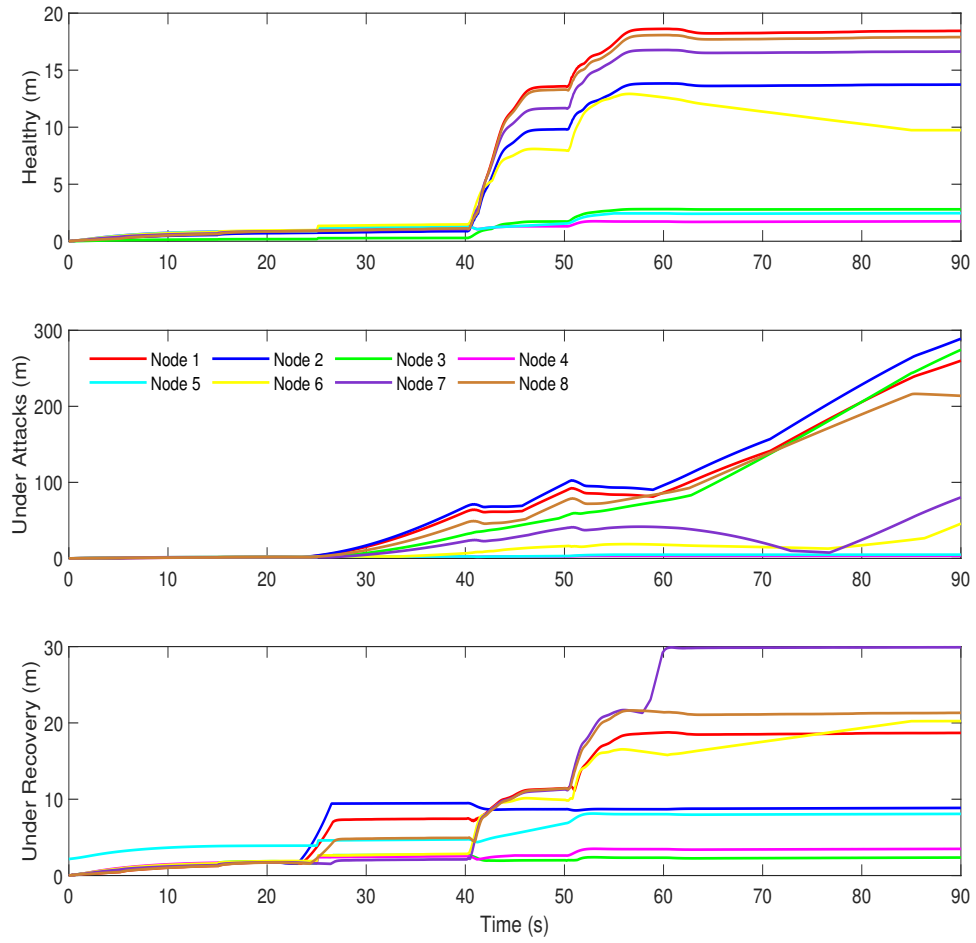


Figure 5.23: Mean estimation errors of the UAV's x , y , and z positions across three phases: healthy operation, under cyber-attacks, and after system recovery.

Table 5.1: Mean absolute estimation errors of rotational angles (Ang.) and position coordinates (Pos.) per node across different operational phases

Node	Healthy		Under Attack		With Recovery	
	Ang. (°)	Pos. (m)	Ang. (°)	Pos. (m)	Ang. (°)	Pos. (m)
1	2.36	9.44	42.71	88.35	3.01	10.66
2	0.94	6.84	67.81	59.48	1.83	9.79
3	0.31	1.26	25.04	71.34	0.51	2.07
4	0.17	1.29	3.56	25.16	0.35	2.59
5	0.22	1.60	4.96	32.06	0.43	3.76
6	1.43	6.10	14.07	20.01	2.52	9.62
7	1.81	8.50	16.97	25.61	3.87	13.91
8	2.25	9.18	20.54	71.40	3.61	11.34
Mean	1.44	5.78	24.46	49.43	2.02	8.22

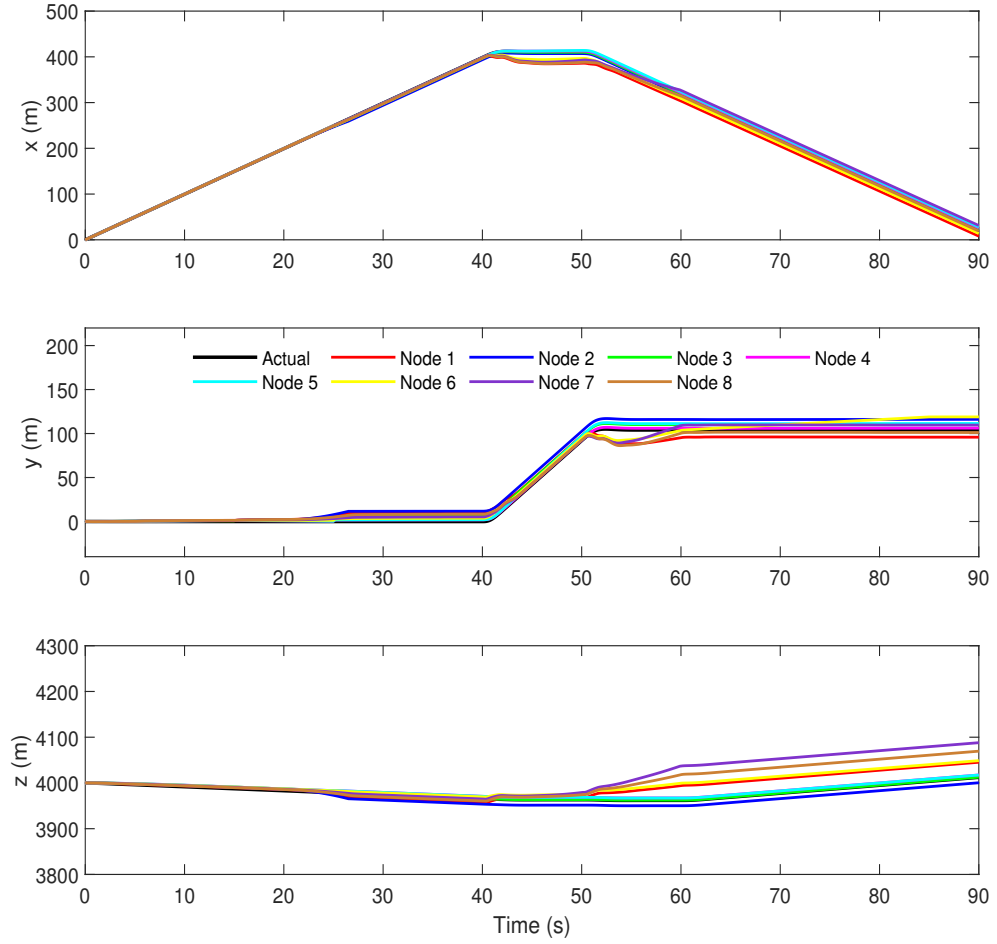


Figure 5.24: UAV positions under the recovery mechanism. The attacks were initiated at $t = 20$ s and $t = 45$ s, detected at $t = 26$ s and $t = 58$ s, and recovered at $t = 28$ s and $t = 60$ s, respectively.

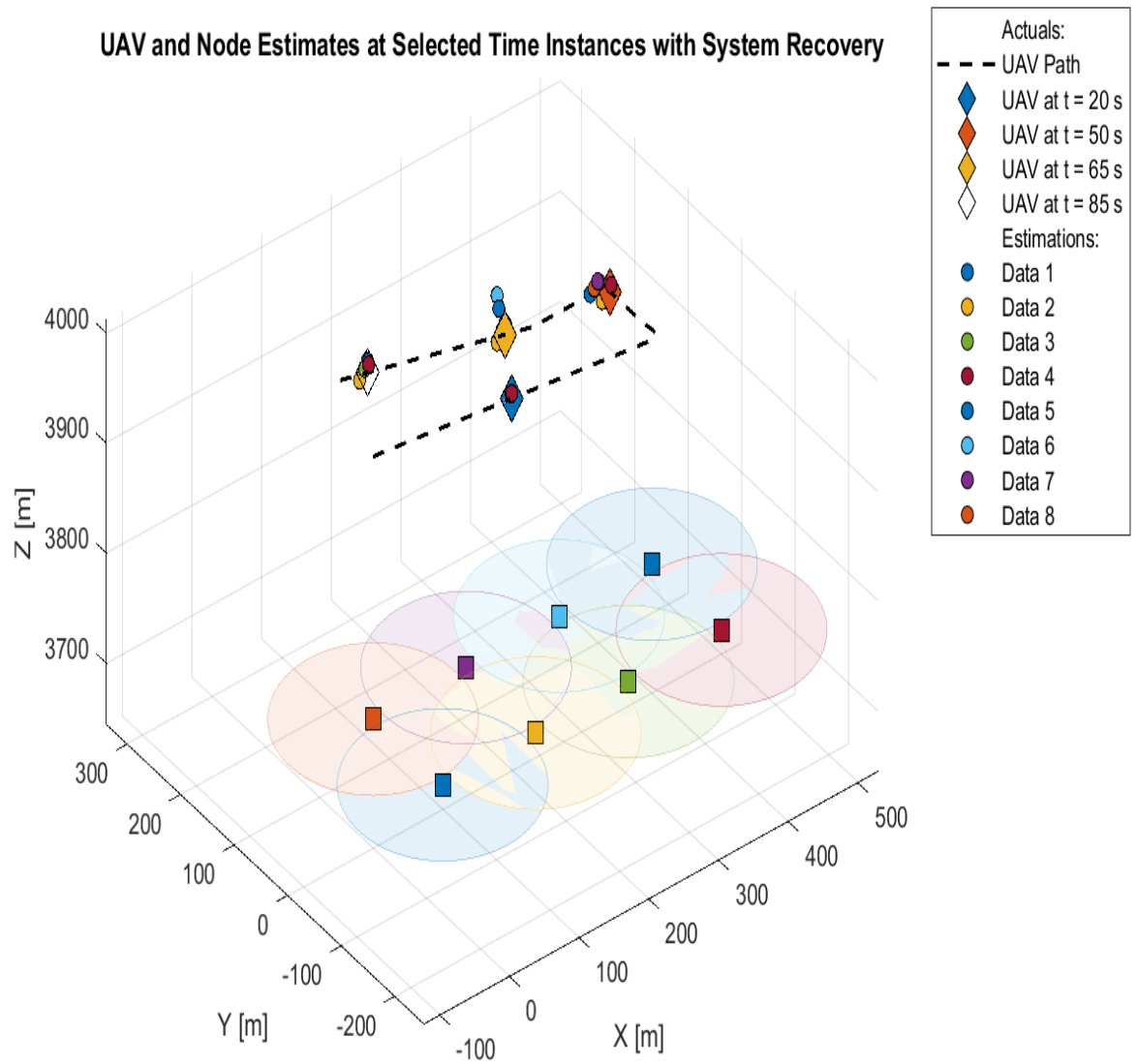


Figure 5.25: 3D UAV actual positions and estimation results after applying the recovery mechanism.

5.5 Conclusion

This chapter developed a resilient distributed state estimation framework for nonlinear cyber-physical systems under sensor faults and cyber-attacks. The approach combines the Distributed Hybrid Information Fusion (DHIF) algorithm with a graph-based reconfiguration strategy that dynamically adjusts the communication topology in response to detected anomalies. Upon identifying faulty sensors or compromised communication links, the system triggers a topology reconfiguration strategy that enables healthy nodes to re-establish communication paths and maintain distributed estimation. This decentralized recovery mechanism ensures that the estimation process remains robust and accurate, even in presence of multiple, coordinated False Data Injection (FDI) attacks. Additionally, the stability of the distributed estimator under switching topologies was rigorously analyzed and formally shown, by guaranteeing bounded estimation error and convergence throughout the network reconfiguration.

The effectiveness of the proposed recovery scheme was demonstrated through UAV simulations involving complex attack scenarios. After reconfiguration, the distributed state estimation remained stable and accurate, as shown by the trajectory tracking and estimation responses. These results highlight the robustness of the reconfiguration-based recovery mechanism and its potential for real-world deployment in resilient CPS applications. Future research could extend this framework to broader classes of attacks and further explore its scalability in large-scale networks.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This thesis has presented a comprehensive study on enhancing the security, resilience, and situational awareness of nonlinear cyber-physical systems (CPS) under adversarial threats and system faults. The proposed frameworks address key challenges in cyber-attack and fault detection, isolation, and recovery, providing robust solutions grounded in both model-based estimation and learning-based optimization. The contributions can be summarized across three major themes.

First, we developed an Augmented Unscented Kalman Filter (AUKF) capable of simultaneously estimating system states and faults, with stability guaranteed under appropriate conditions. To enhance its robustness, the AUKF was further integrated with carefully designed auxiliary residual filters, forming a comprehensive detection mechanism for both sensor and actuator cyber-attacks. This combined approach enabled effective differentiation between unintentional system faults and malicious anomalies. Theoretical guarantees and detailed simulation studies involving an inverted pandemonium and a high-fidelity UAV model confirmed the feasibility and accuracy of the proposed method. These simulations demonstrated that the detection scheme consistently maintains robust estimation performance under both nominal operating conditions and in the presence of sophisticated cyber-attacks.

Second, we introduced Reinforcement Learning (RL) and Deep Reinforcement Learning (DRL)-based frameworks for real-time anomaly detection. By formulating the detection problem as a Partially Observable Markov Decision Process (POMDP), we enabled intelligent agents to learn optimal detection policies that prioritize early identification and minimize response delays through continuous interaction with system dynamics. Initially, a tabular State-action-reward-state-action (SARSA) approach was employed, wherein a lookup table was iteratively updated based on observed system behavior and reward signals to establish a baseline detection mechanism. To overcome scalability limitations

inherent to tabular methods, a DRL-based framework was developed, integrating Deep Q -Network (DQN) with model-based insights derived from the AUKF and auxiliary residual filters. This hybrid approach effectively combines the adaptability of data-driven learning with the robustness and interpretability of physical modeling. Notably, under challenging conditions—such as increased measurement uncertainty and the presence of sophisticated cyber-attack noise—the DRL-based detector exhibited marked improvements in detection accuracy, faster response times, and reduced false alarm rates compared to classical techniques, including χ^2 -based detectors, Euclidean residual checks, and the tabular RL approach.

Third, we extended the research to the domain of resilient distributed state estimation for CPS operating over sensor networks. We designed a novel architecture that integrates the Distributed Hybrid Information Fusion (DHIF) algorithm with a topology reconfiguration mechanism triggered by cyber-attack and fault detection and isolation. This method enables compromised nodes to be isolated while maintaining global estimation through rerouted communication paths based on backup connectivity plans. A rigorous stability analysis was carried out, demonstrating that the estimation error remains bounded and converges under the resulting switching topology. Simulation results using UAV trajectory tracking further confirmed the robustness of this decentralized recovery scheme, highlighting its potential for large-scale deployment in resilient CPS infrastructures.

Overall, the presented research advances the state-of-the-art in cyber-resilient estimation and anomaly detection. It combines theoretical rigor with practical feasibility, and the simulation-based validation provides strong evidence of real-world applicability. The synergy between model-based filtering, learning-based decision-making, and networked recovery mechanisms forms a versatile and adaptive toolbox for the next generation of secure and intelligent cyber-physical systems.

While the proposed methodologies offer significant advances in the detection, isolation, and recovery of nonlinear CPS under cyber-attacks, certain limitations should be acknowledged. First, the underlying models assume the availability of system dynamics and structured fault representations, which may not fully capture unmodeled nonlinearities or unforeseen attack behaviors in complex CPS. Although in many cases the system dynamics can be identified or reasonably approximated, there may exist scenarios where modeling uncertainties or nonlinear couplings limit the effectiveness of the proposed approaches. Second, the reinforcement learning and deep learning components require integration with the CPS model through residual or detection functions; in cases where the system model is unavailable, suitable observation spaces may be constructed based on measurable system characteristics or statistical features derived through alternative approaches. Furthermore, the distributed estimation framework assumes a connected and cooperative network topology, without accounting for potential communication losses, delays, or asynchronous updates. Addressing these limitations through experimental validation, model uncertainty

handling, and communication-aware algorithms will be essential for transitioning these methods toward practical and reliable real-world deployment.

6.2 Future Directions of Research

This thesis opens several promising avenues for further exploration and development in the field of secure and resilient cyber-physical systems. Potential future directions include:

1. **Data-Driven Detection for Nonlinear Systems:** With the growing availability of operational and sensor data in modern CPS environments, future work could focus on developing purely data-driven cyber-attack detection frameworks. Leveraging techniques such as supervised learning, unsupervised anomaly detection, or generative models (e.g., autoencoders, GANs) for nonlinear systems may provide powerful alternatives or complements to model-based methods.
2. **Detection of Advanced Cyber-Attacks:** The framework can be extended to detect more sophisticated cyber-attacks such as zero-dynamics attacks, or coordinated multi-point intrusions. Developing tailored detection and isolation mechanisms for these stealthy attacks remains a critical challenge in CPS security.
3. **Exploration of Alternative Filtering Techniques:** While the current work uses the Unscented Kalman Filter (UKF), future studies may investigate other nonlinear estimation techniques such as the Ensemble Kalman Filter (EnKF), Particle Filter (PF), or Moving Horizon Estimation (MHE). These filters offer different trade-offs in terms of accuracy, computational complexity, and robustness to non-Gaussian noise and system nonlinearities.
4. **Extension to Multi-Agent Learning:** Future research can integrate multi-agent reinforcement learning (MARL) where multiple agents—such as UAVs, robots, or distributed sensors—collaborate to detect anomalies or coordinate recovery actions. This decentralized learning paradigm may improve scalability, adaptability, and resilience in large-scale networked systems.
5. **Robustness Against Adversarial Learning Attacks:** As DRL-based systems become more prevalent, they may become targets of adversarial learning attacks, including reward manipulation, observation poisoning, or policy spoofing. Future work should explore robust DRL algorithms incorporating adversarial training, certified defenses, or robust exploration to counter these threats.
6. **Modeling of Communication Imperfections:** Real-world CPS often operate under imperfect communication channels with delays, packet drops, or bandwidth constraints. Incorporating communication models into the estimation and detection

framework and designing delay-aware or packet-loss-resilient algorithms is a vital step toward real-world deployment.

7. **Hardware-in-the-Loop (HIL) Implementation:** To assess real-time feasibility and bridge the gap between simulation and deployment, the proposed methodologies could be validated on physical platforms such as UAVs, robotic arms, or autonomous ground vehicles. HIL experiments would offer insights into computation latency, sensor fidelity, and robustness to physical uncertainties.
8. **Integration with Resilient Control:** A natural extension is to couple the anomaly detection and state estimation layers with feedback control systems. This would enable adaptive or resilient control strategies that dynamically reconfigure control laws based on real-time anomaly detection results and state confidence metrics, ensuring both safety and performance in adversarial environments.

These research directions not only address existing limitations but also pave the way toward more intelligent, adaptive, and robust cyber-physical infrastructures. The integration of learning, estimation, control, and network reconfiguration will be key to achieving autonomy and resilience in future CPS ecosystems.

6.3 Accepted and Submitted Journal and Conference Papers

Accepted:

- 1) H. Kazemi and K. Khorasani, Cyber-Attack Detection, and Isolation of Nonlinear Cyber-Physical Systems (UAV case study): An Auxiliary Filter Approach, 63rd IEEE Conference on Decision and Control s, Milan, Italy, 2024.
- 2) H. Kazemi and K. Khorasani, Sensor Cyber-Attack and Fault Detection and Isolation of Nonlinear Cyber-Physical Systems, 7th IEEE Conference on Control Technology and Applications, Barbados, 2023.
- 3) H. Kazemi and K. Khorasani, Particle Filter-based Prognosis and Health Monitoring of Electromechanical Actuators, 9th International Conference on Control, Decision and Information Technologies, Rome, Italy, 2023.

Submitted:

- 1) H. Kazemi and K. Khorasani, Cyberattack and Fault Detection and Isolation of Sensors and Actuators in Nonlinear Cyber-Physical Systems, IEEE/CAA JOURNAL OF AUTOMATICA SINICA, Under Review.
- 2) H. Kazemi and K. Khorasani, Reinforcement Learning-Based Cyberattack and Fault Detection and Isolation of Nonlinear Cyber-Physical Systems, ACM Transactions on Cyber-Physical Systems, Under Review
- 3) H. Kazemi and K. Khorasani, Deep Reinforcement Learning-Based Sensor and Actuator Cyberattack Detection and Isolation of Nonlinear Cyber-Physical Systems, IEEE

Transaction on Control of Network Systems, Under Review.

4) H. Kazemi and K. Khorasani, Secure Distributed State Estimation in Nonlinear Cyber-Physical Systems using Sensor Networks, IEEE Transactions on Cybernetics, Under Review.

5) H. Kazemi and K. Khorasani, Resilient Distributed State Estimation for Nonlinear Cyber-Physical Systems with Sensor Networks under Cyberattacks, 64rd IEEE Conference on Decision and Control, Under Review.

References

- [1] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, “Brief survey on attack detection methods for cyber-physical systems,” *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.
- [2] W. Lucia, G. Franzè, and B. Sinopoli, “A supervisor-based control architecture for constrained cyber-physical systems subject to network attacks,” *IEEE Transactions on Control of Network Systems*, 2022.
- [3] K. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, and P. Chaurasia, “A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions,” *Information*, vol. 14, no. 7, p. 388, 2023.
- [4] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. Ahmed, “Cyber-physical systems security: A systematic review,” *Computers & Industrial Engineering*, vol. 188, p. 109891, 2024.
- [5] M. Kordestani and M. Saif, “Observer-based attack detection and mitigation for cyberphysical systems: A review,” *IEEE Systems, Man, and Cybernetics Magazine*, vol. 7, no. 2, pp. 35–60, 2021.
- [6] P. Zhu, S. Jin, X. Bu, Z. Hou, and C. Yin, “Model-free adaptive control for a class of mimo nonlinear cyberphysical systems under false data injection attacks,” *IEEE Transactions on Control of Network Systems*, vol. 10, no. 1, pp. 467–478, 2022.
- [7] M. Taheri, K. Khorasani, and N. Meskin, “On zero dynamics and controllable cyber-attacks in cyber-physical systems and dynamic coding schemes as their countermeasures,” *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 11, pp. 2191–2203, 2024.
- [8] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, “Bibliographical review on cyber attacks from a control oriented perspective,” *Annual Reviews in Control*, vol. 48, pp. 103–128, 2019.

- [9] W. Xing and J. Shen, “Security control of cyber–physical systems under cyber attacks: A survey,” *Sensors*, vol. 24, no. 12, p. 3815, 2024.
- [10] N. Falliere, L. O. Murchu, and E. Chien, “An in-depth look into stuxnet,” *Symantec Security Response*, vol. 1, no. 1, pp. 1–26, 2012.
- [11] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the ukrainian power grid,” *SANS Industrial Control Systems (ICS)*, vol. 388, pp. 1–26, 2016.
- [12] A. Greenberg, “Cyberattack on florida water treatment facility.” <https://www.wired.com/story/oldsmar-florida-water-hack/>, 2021. Accessed: 2025-05-14.
- [13] C. Tramble, “Colonial pipeline ransomware attack: What we know and what’s next.” <https://www.cisa.gov/news-events/news/colonial-pipeline-ransomware-attack>, 2021. Accessed: 2025-05-14.
- [14] R. M. Lee, M. J. Assante, and T. Conway, “Triton: The first ics cyber attack on safety instrument systems,” *Dragos, Inc.*, 2017. Available at <https://www.dragos.com/blog/industry-news/triton-the-first-ics-cyber-attack-on-safety-instrument-systems/>.
- [15] C.-H. Chiu, C.-H. Lin, C.-M. Wang, and Y.-C. Chen, “Fault detection and diagnosis in industry 4.0: A review on machine learning approaches,” *Sensors*, vol. 25, no. 1, p. 60, 2025.
- [16] L. Liang, R. Su, and H. Xu, “Distributed state and fault estimation for cyber-physical systems under dos attacks,” *IEEE/CAA Journal of Automatica Sinica*, vol. 12, no. 1, pp. 261–263, 2025.
- [17] A. A. Sheydaeian Arani, M. Aliyari Shoorehdeli, A. Moarefianpour, and M. Teshnehlab, “Fault estimation based on ensemble unscented kalman filter for a class of nonlinear systems with multiplicative fault,” *International Journal of Systems Science*, vol. 52, no. 10, pp. 2082–2099, 2021.
- [18] N. Daroogheh, A. Baniamerian, N. Meskin, and K. Khorasani, “Prognosis and health monitoring of nonlinear systems using a hybrid scheme through integration of pfs and neural networks,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 8, pp. 1990–2004, 2016.
- [19] R. M. Asl, Y. S. Hagh, S. Simani, and H. Handroos, “Adaptive square-root unscented kalman filter: An experimental study of hydraulic actuator state estimation,” *Mechanical Systems and Signal Processing*, vol. 132, pp. 670–691, 2019.

- [20] Y. Yu and Y. Yuan, “Event-triggered active disturbance rejection control for nonlinear network control systems subject to dos and physical attacks,” *ISA transactions*, vol. 104, pp. 73–83, 2020.
- [21] Z. Cao, Y. Niu, and J. Song, “Finite-time sliding-mode control of markovian jump cyber-physical systems against randomly occurring injection attacks,” *IEEE Transactions on Automatic Control*, vol. 65, no. 3, pp. 1264–1271, 2019.
- [22] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, “Deep learning algorithms used in intrusion detection systems – a review,” *arXiv preprint arXiv:2402.17020*, 2024.
- [23] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, “Distributed resilient estimator design for positive systems under topological attacks,” *IEEE Transactions on Cybernetics*, vol. 51, no. 7, pp. 3676–3686, 2020.
- [24] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang, “Distributed event-triggered estimation over sensor networks: A survey,” *IEEE transactions on cybernetics*, vol. 50, no. 3, pp. 1306–1320, 2019.
- [25] X. Guo, Y. Wang, H. Zhang, and J. Liu, “Distributed consensus-based estimation for non-linear systems subject to missing measurements and denial of service attacks,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 9, no. 1, pp. 45–56, 2024.
- [26] Z. Cheng, L. Yang, Q. Yuan, Y. Long, and H. Ren, “Distributed consensus estimation for networked multi-sensor systems under hybrid attacks and missing measurements,” *Sensors*, vol. 24, no. 13, p. 4071, 2024.
- [27] Y. Shi, Y. Wang, and J. Tuo, “Distributed secure state estimation of multi-agent systems under homologous sensor attacks,” *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 1, pp. 67–77, 2023.
- [28] J. Hu, X. Yang, and L.-X. Yang, “A framework for detecting false data injection attacks in large-scale wireless sensor networks,” *Sensors*, vol. 24, no. 5, p. 1643, 2024.
- [29] I. Jovanov and M. Pajic, “Relaxing integrity requirements for attack-resilient cyber-physical systems,” *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4843–4858, 2019.
- [30] K. Kaouk, S. Alshammari, R. Alshammari, and M. Alshammari, “Network-based intrusion detection for industrial and robotics systems: A comprehensive survey,” *Electronics*, vol. 13, no. 22, p. 4440, 2024.
- [31] M. Kabir, Y. Zhang, and Y. Zhang, “A survey of network intrusion detection for cyber-physical systems: Machine learning-based solutions and research challenges,” *Future Generation Computer Systems*, vol. 142, pp. 47–67, 2023.

- [32] W. Haider, S. Rehman, *et al.*, “A survey of intrusion detection approaches in the internet of things,” *Journal of Network and Computer Applications*, vol. 159, p. 102597, 2020.
- [33] R. Zhou, G. Shi, and C. Wang, “Trust-based cyber-physical attack detection in distributed control systems,” *IEEE Transactions on Cybernetics*, vol. 52, no. 7, pp. 6772–6783, 2022.
- [34] J. Yang and F. Ahmed, “Anomaly detection techniques for nonlinear cps under adversarial attacks,” *IEEE Transactions on Control Systems Technology*, 2024. Early Access.
- [35] Z. Wang and C. Liu, “Model-based detection of stealthy attacks in nonlinear cyber-physical systems,” *Automatica*, vol. 150, p. 110940, 2023.
- [36] W. Gharibi and D. Tran, “A survey on cyber-physical systems security: Threats, vulnerabilities and defense,” *IEEE Access*, vol. 9, pp. 29666–29691, 2021.
- [37] X. Yin *et al.*, “Cyber-physical security of distributed control systems: A review,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1355–1370, 2022.
- [38] R. Ahmed and A. Ullah, “A review on hybrid intrusion detection systems in cyber-physical systems,” *Journal of Network and Computer Applications*, vol. 215, p. 103547, 2023.
- [39] L. Yuan and J. Zhang, “A hierarchical intrusion detection system for cyber-physical systems based on spatiotemporal correlation analysis,” *Future Generation Computer Systems*, vol. 141, pp. 266–279, 2023.
- [40] Y. Guo and H. Li, “Trust-aware control reconfiguration in networked control systems under deception attacks,” *ISA Transactions*, 2024.
- [41] Z. Cheng and Y. Yang, “Secure control of cps using trust estimation and adaptive fusion,” *IEEE Transactions on Industrial Electronics*, vol. 69, no. 6, pp. 6192–6201, 2022.
- [42] R. Das and D. Roy, “Resilient estimation and fault diagnosis in nonlinear cps with switching topologies and measurement faults,” *ISA Transactions*, 2023.
- [43] X. Li and Q. Wu, “Resilient state estimation for cps under false data injection attacks and measurement noise,” *IEEE Transactions on Cybernetics*, 2023.
- [44] Y. Lin and K. Han, “Survey of security in cyber-physical systems: Issues, challenges, and future directions,” *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 2, pp. 1–27, 2022.

- [45] M. Zhao and L. Xu, “Adaptive thresholding for online anomaly detection in nonlinear cps,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2024.
- [46] L. Hu and F. Sun, “Observer-based resilient estimation for nonlinear cyber-physical systems under false data injection attacks,” *ISA Transactions*, 2024.
- [47] Y. Xue and K. Zhao, “Resilient state estimation for nonlinear multi-agent systems under actuator faults and cyber-attacks,” *IEEE Access*, vol. 12, pp. 28704–28716, 2024.
- [48] X. Chen and J. Liu, “Input-to-state stability of cyber-physical systems under stochastic attacks,” *IEEE Transactions on Automatic Control*, 2023.
- [49] T. K. Tasooji and S. Khodadadi, “Cubature kalman filter as a robust state estimator against model uncertainty and cyber attacks in power systems,” *arXiv preprint arXiv:2503.21070*, 2025.
- [50] S. Liu, G. Wei, Y. Song, and Y. Liu, “Extended kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks,” *Neurocomputing*, vol. 207, pp. 708–716, 2016.
- [51] A. Meng, H. Wang, S. Aziz, J. Peng, and H. Jiang, “Kalman filtering based interval state estimation for attack detection,” *Energy Procedia*, vol. 158, pp. 6589–6594, 2019.
- [52] H. Wang, A. Meng, Y. Liu, X. Fu, and G. Cao, “Unscented kalman filter based interval state estimation of cyber physical energy system for detection of dynamic attack,” *Energy*, vol. 188, p. 116036, 2019.
- [53] J. Lu, W. Wang, and L. Li, “Unscented kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks,” *Asian Journal of Control*, vol. 23, no. 7, pp. 1–10, 2019.
- [54] M. Laila, N. Naveen, and K. Vishakh, “Comparison of estimation capabilities of extended and unscented kalman filter in an rlv,” *Int. J. Adv. Res. Elect. Electron. Instrum. Eng.*, vol. 2, no. 7, pp. 3480–3488, 2013.
- [55] I. Arasaratnam and S. Haykin, “Cubature kalman filters,” *IEEE Transactions on Automatic Control*, vol. 54, no. 6, pp. 1254–1269, 2009.
- [56] M. Gao, J. Zhao, and B. Dong, “Hybrid filtering techniques for resilient state estimation in cps under stealthy attacks,” *Journal of the Franklin Institute*, vol. 359, no. 5, pp. 2405–2427, 2022.
- [57] M. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, “A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking,” *IEEE Transactions on signal processing*, vol. 50, no. 2, pp. 174–188, 2002.

- [58] S. Konatowski, P. Kaniewski, and J. Matuszewski, “Comparison of estimation accuracy of ekf, ukf and pf filters,” *Annual of Navigation*, vol. 23, no. 1, pp. 69–86, 2016.
- [59] M. Mallick, M. Morelande, and L. Mihaylova, “Continuous-discrete filtering using ekf, ukf, and pf,” in *15th International Conference on Information Fusion*, pp. 1087–1094, IEEE, 2012.
- [60] X. Luo, X. Wang, X. Pan, and X. Guan, “Detection and isolation of false data injection attack for smart grids via unknown input observers,” *IET Generation, Transmission & Distribution*, vol. 13, no. 8, pp. 1277–1286, 2019.
- [61] A. A. Abokifa and D. Park, “Adaptive observer design for robust fault detection in nonlinear cps under time-varying disturbances,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 3, pp. 2117–2128, 2023.
- [62] X. Zhou and R. Liu, “Adaptive observer design for cyber-physical systems with unmodeled dynamics,” *ISA Transactions*, vol. 102, pp. 30–40, 2020.
- [63] V. Utkin, J. Guldner, and J. Shi, *Sliding mode control in electro-mechanical systems*. CRC press, 2017.
- [64] W. Yao and Y. He, “Anti-chattering sliding mode observer design for nonlinear uncertain cps under attack,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023. Early Access.
- [65] M. Taheri, K. Khorasani, I. Shames, and N. Meskin, “Cyberattack and machine-induced fault detection and isolation methodologies for cyber-physical systems,” *IEEE Transactions on Control Systems Technology*, 2023.
- [66] G. Ren, H. Liu, Y. Zhang, and Y. Li, “Attack detection based on encoding–decoding approach for cyber–physical systems,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023.
- [67] Q. Zhu, S. Jiang, and F. Pan, “Adaptive event-triggered fault detection for nonlinear networked systems in finite-frequency domain under stochastic cyber-attacks,” *International Journal of Adaptive Control and Signal Processing*, vol. 36, no. 7, pp. 1537–1561, 2022.
- [68] Z. Li, J. Hu, H. Gao, and Z. Dong, “Fault-tolerant control for networked control systems under cyber attacks: An h-infinity approach,” *IEEE Transactions on Industrial Electronics*, vol. 68, no. 12, pp. 12530–12539, 2021.
- [69] X. Li and Q. Wu, “Resilient state estimation for cps under false data injection attacks and measurement noise,” *IEEE Transactions on Cybernetics*, vol. 54, no. 5, pp. 1234–1246, 2024.

- [70] Y. Shoukry and P. Tabuada, “Secure state estimation for cyber physical systems under sensor attacks: A satisfiability modulo theory approach,” in *Proceedings of the 2015 IEEE Conference on Decision and Control (CDC)*, pp. 3804–3809, IEEE, 2017.
- [71] H.-D. Le, H.-M. Nguyen, and H. Ishii, “Set-theoretic estimation for nonlinear systems under sensor attacks,” *Automatica*, vol. 130, p. 109702, 2021.
- [72] J. Hou, F. Teng, W. Yin, Y. Song, and Y. Hou, “Locating collaborative attack targets based on physical invariants toward cyber-physical systems,” *International Journal of Information Security*, vol. 23, pp. 999–1017, 2024.
- [73] X. Li and K. W. Hedman, “Enhancing power system cyber-security with systematic two-stage detection strategy,” *arXiv preprint arXiv:1810.05939*, 2018.
- [74] X. Wang, X. Luo, Y. Zhang, and X. Guan, “Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6498–6512, 2019.
- [75] Y. Chen, L. Liu, and H. He, “Detection and localization of cyber-attacks in cps using system dynamics and graph-based methods,” *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1434–1445, 2021.
- [76] Y. Liu, K. Zhao, and J. Wang, “Graph neural network-based attack localization in cps: A data-model fusion framework,” *IEEE Internet of Things Journal*, 2023. Early Access.
- [77] Z. Guan and X. Zhang, “Learning-aided localization of stealthy cyber attacks in distributed nonlinear systems,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6112–6123, 2022.
- [78] N. Mohamed and M. M. A. Salama, “Data mining-based cyber-physical attack detection tool for attack-resilient adaptive protective relays,” *Energies*, vol. 15, no. 12, p. 4328, 2022.
- [79] D. Intriago and Y. Zhang, “Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review,” *arXiv preprint arXiv:2411.14278*, 2023.
- [80] X. Wang *et al.*, “Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review,” *arXiv preprint arXiv:2411.14278*, 2024.
- [81] S. Huda, E. Ahmed, J. Yearwood, M. Alazab, and A. Mahmood, “A hybrid learning approach for network intrusion detection using ensemble of classifiers,” *Journal of Network and Computer Applications*, vol. 66, pp. 198–214, 2016.

- [82] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, “Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765–2777, 2019.
- [83] M. Nasir and Y. Wu, “A gan-based approach for unsupervised intrusion detection in cyber-physical systems,” *IEEE Access*, vol. 9, pp. 122501–122512, 2021.
- [84] N. Baracaldo and A. Bates, “Mitigating false positives in anomaly detection for critical infrastructure using model-agnostic methods,” *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 3, pp. 25:1–25:20, 2022.
- [85] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, “Evaluation of reinforcement learning-based false data injection attack to automatic voltage control,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2018.
- [86] Y. Yu, W. Yang, W. Ding, and J. Zhou, “Reinforcement learning solution for cyber-physical systems security against replay attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4507–4518, 2023.
- [87] S. H. Oh, M. K. Jeong, H. C. Kim, and J. Park, “Applying reinforcement learning for enhanced cybersecurity against adversarial simulation,” *Sensors*, vol. 23, no. 6, p. 3000, 2023.
- [88] M. Najafli and M. Ahmadi, “A novel deep reinforcement learning-based ids for iot-enabled cyber-physical systems,” *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 2104–2115, 2024.
- [89] S. Alam and M. Chowdhury, “Iotwarden: A deep reinforcement learning defense against false data injection in cyber-physical systems,” *Future Generation Computer Systems*, vol. 148, pp. 329–341, 2024.
- [90] J. Wang and H. Liu, “Graph attention-based reinforcement learning for intrusion detection in cyber-physical systems,” *IEEE Transactions on Network and Service Management*, 2023. Early Access.
- [91] J. Cai and H. Zhang, “Stability-guaranteed anomaly detection in nonlinear cps using physics-informed deep learning,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 4891–4902, 2023.
- [92] F. Farivar and X. Zhang, “Artificial intelligence for detection and response in cyber-physical systems: A survey,” *ACM Computing Surveys*, vol. 52, no. 6, pp. 116:1–116:36, 2019.

- [93] H. Liu and M. Zhao, “Transfer learning for cyber-attack detection in cyber-physical systems: A survey,” *Journal of Information Security and Applications*, vol. 66, p. 103155, 2022.
- [94] Y. Xu, Q. Zhang, and R. Zhao, “Self-supervised representation learning for multivariate time series in cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, 2023. Early Access.
- [95] R. Olfati-Saber, “Distributed kalman filter with embedded consensus filters,” in *Proceedings of the 46th IEEE Conference on Decision and Control*, pp. 8179–8184, IEEE, 2007.
- [96] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delay,” *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, 2004.
- [97] G. Battistelli and L. Chisci, “Kullback–leibler average, consensus on probability densities, and distributed state estimation with guaranteed stability,” *Automatica*, vol. 68, pp. 169–178, 2016.
- [98] S. Wang and W. Ren, “On the convergence conditions of distributed dynamic state estimation using sensor networks a unified framework,” *IEEE Transactions on Control Systems Technology*, vol. 26, no. 4, pp. 300–316, 2017.
- [99] A. T. Kamal, J. A. Farrell, and A. K. Roy-Chowdhury, “Information weighted consensus filters and their application in distributed camera networks,” *IEEE Transactions on Automatic Control*, vol. 58, no. 12, pp. 3112–3125, 2013.
- [100] A. Sharifi and W. Ren, “Distributed state estimation for nonlinear cps with unknown inputs using dhif,” *IEEE Transactions on Control of Network Systems*, vol. 9, no. 1, pp. 45–56, 2022.
- [101] Y. Li and J. Zhao, “Robust distributed filtering for cyber-physical sensor networks with data dropout,” *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3780–3794, 2023.
- [102] L. Liu and H. Lin, “Distributed kalman filtering under switching communication topologies and packet loss,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2087–2096, 2021.
- [103] F. S. Cattivelli and A. H. Sayed, “Diffusion strategies for distributed kalman filtering and smoothing,” *IEEE Transactions on automatic control*, vol. 55, no. 9, pp. 2069–2084, 2010.

- [104] D. Valenzuela, M. Mazo Jr, and P. Hovareshti, “Adaptive distributed kalman filter for partially observable systems with communication constraints,” *IEEE Transactions on Control of Network Systems*, vol. 8, no. 2, pp. 679–689, 2021.
- [105] Y. Yuan, H. Yuan, D. W. Ho, and L. Guo, “Resilient control of wireless networked control system under denial-of-service attacks: A cross-layer design approach,” *IEEE transactions on cybernetics*, vol. 50, no. 1, pp. 48–60, 2018.
- [106] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in *First Workshop on Secure Control Systems (SCS)*, (Stockholm, Sweden), 2010.
- [107] D. Ding, H. Liu, H. Dong, and H. Liu, “Resilient filtering of nonlinear complex dynamical networks under randomly occurring faults and hybrid cyber-attacks,” *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2341–2352, 2022.
- [108] H. Wei, K. Zhang, H. Zhang, and Y. Shi, “Resilient and constrained consensus against adversarial attacks: A distributed mpc framework,” *Automatica*, vol. 160, p. 111417, 2024.
- [109] H. M. Saleh, H. Marouane, and A. Fakhfakh, “Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning,” *IEEE Access*, 2024.
- [110] Y. Yang, X. Li, Y. Zhang, S. Liu, and Q. Zhu, “Adaptive anomaly detection threshold using deep reinforcement learning for cyber-physical systems,” *Computers & Security*, vol. 138, p. 103544, 2024.
- [111] L. Zha, Y. Guo, J. Liu, X. Xie, and E. Tian, “Protocol-based distributed security fusion estimation for time-varying uncertain systems over sensor networks: Tackling dos attacks,” *IEEE Transactions on Signal and Information Processing over Networks*, 2024.
- [112] K. Sharma and J. Chen, “Resilient nonlinear distributed estimation under byzantine attacks,” *IEEE Transactions on Automatic Control*, vol. 67, no. 8, pp. 3939–3954, 2022.
- [113] H. Lee and J. Kim, “Federated learning for secure and private distributed cps estimation,” *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 4, pp. 36:1–36:25, 2023.
- [114] J. Li, W. Zhang, and C. Qian, “Reconfigurable distributed observers with topology adaptation for resilient estimation in cps,” *IEEE Transactions on Cybernetics*, 2024. Early Access.

- [115] M. Segovia-Ferreira, J. Rubio-Hernan, A. Cavalli, and J. Garcia-Alfaro, “A survey on cyber-resilience approaches for cyber-physical systems,” *ACM Computing Surveys*, vol. 56, no. 8, pp. 1–37, 2024.
- [116] A. M. Mehrabian, H. Alghassi, and A. Homaifar, “A resilient layered observer for attack-resilient state estimation of cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7182–7191, 2020.
- [117] L. Pan, Y. Zhang, D. Gu, and X. Du, “A survey of microkernel-based secure operating systems,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–36, 2021.
- [118] C. Wu, L. Wu, J. Liu, and Z.-P. Jiang, “Active defense-based resilient sliding mode control under denial-of-service attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 237–249, 2019.
- [119] Y. Guan and X. Ge, “Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, 2017.
- [120] X. Wang and Y. Tan, “Resilient state estimation using deep reinforcement learning in time-varying sensor networks,” *IEEE Transactions on Cybernetics*, 2023. Early Access.
- [121] Y. An, F. Yu, Y. Yang, J. Yang, and Y. Wang, “Trust-aware data aggregation in wireless sensor networks: a survey,” *IEEE Access*, vol. 7, pp. 28216–28237, 2019.
- [122] K. Gatsis, A. Ribeiro, and G. J. Pappas, “Control-aware random access communication: Joint design of control and communication,” in *Proceedings of the IEEE Conference on Decision and Control (CDC)*, pp. 5128–5133, IEEE, 2015.
- [123] H. Rezaee and F. Abdollahi, “Secure consensus control of multiagent cyber-physical systems with uncertain nonlinear models,” *IEEE Systems Journal*, vol. 14, no. 3, pp. 3539–3546, 2019.
- [124] A. Kott, M. J. Weisman, and J. Vandekerckhove, “Mathematical modeling of cyber resilience,” in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*, pp. 849–854, IEEE, 2022.
- [125] D. Clerigues, J. Wubben, *et al.*, “Enabling resilient uav swarms through multi-hop wireless communications,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2024, no. 1, p. 39, 2024.
- [126] C. Zhang, L. Yang, Y. Zhang, and Q. Guo, “A survey on cyber-physical systems security: Requirements, challenges and solutions,” *IEEE Access*, vol. 9, pp. 144008–144036, 2021.

- [127] S. Shahkar and K. Khorasani, “A resilient control against time-delay switch and denial of service cyber attacks on load frequency control of distributed power systems,” in *2020 IEEE Conference on Control Technology and Applications (CCTA)*, pp. 718–725, IEEE, 2020.
- [128] A. Al-Dabbagh, M. Hamdi, and A. Aitouche, “Resilient control of cyber-physical systems against denial-of-service attacks: A survey,” *IEEE Access*, vol. 9, pp. 42282–42306, 2021.
- [129] D. Ye and T.-Y. Zhang, “Summation detector for false data-injection attack in cyber-physical systems,” *IEEE transactions on cybernetics*, vol. 50, no. 6, pp. 2338–2345, 2019.
- [130] R. Huang, W. Chen, W. Zhang, and G. Shi, “Recent advances in resilient state estimation for cyber-physical systems under deception attacks,” *IEEE Transactions on Cybernetics*, vol. 52, no. 7, pp. 6546–6560, 2022.
- [131] M. Ghafouri, E. Nozari, and G. J. Pappas, “Detection and mitigation of replay attacks in networked control systems: A review,” *Annual Reviews in Control*, vol. 51, pp. 157–172, 2021.
- [132] M. Pajic, J. Weimer, O. Sokolsky, and I. Lee, “Attack-resilient state estimation for noisy dynamical systems,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2017.
- [133] K. Tan, J. Dong, and Y. Mo, “Detecting and mitigating false data injection attacks in cps with model-based and learning-based approaches: A review,” *IEEE Transactions on Industrial Informatics*, 2023.
- [134] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “Secure control systems: A quantitative risk management approach,” *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, 2015.
- [135] Z. Li, H. He, and D. Ding, “Undetectable false data injection attacks on nonlinear systems: A unified framework and a data-driven approach,” *IEEE Transactions on Automatic Control*, 2022.
- [136] J. Back, J. Kim, C. Lee, G. Park, and H. Shim, “Enhancement of security against zero dynamics attack via generalized hold,” in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 1350–1355, IEEE, 2017.
- [137] R. S. Smith, “Covert malicious actions in cyber-physical control systems,” *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2927–2941, 2015.

- [138] W. Zhang, G. Shi, and K. H. Johansson, “Covert attacks on cyber-physical systems with dynamic and nonlinear measurement models,” *IEEE Transactions on Automatic Control*, 2022.
- [139] S. Julier, J. Uhlmann, and H. F. Durrant-Whyte, “A new method for the nonlinear transformation of means and covariances in filters and estimators,” *IEEE Transactions on automatic control*, vol. 45, no. 3, pp. 477–482, 2000.
- [140] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, “Online cyber-attack detection in smart grid: A reinforcement learning approach,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5174–5185, 2018.
- [141] W. Jiang, W. Yang, J. Zhou, W. Ding, Y. Luo, and Y. Liu, “Reinforcement learning-based detection for state estimation under false data injection,” *IEEE Access*, vol. 9, pp. 66498–66508, 2021.
- [142] S. Ross, J. Pineau, B. Chaib-draa, and P. Kreitmann, “A bayesian approach for learning and planning in partially observable markov decision processes.,” *Journal of Machine Learning Research*, vol. 12, no. 5, 2011.
- [143] J. Xu, Z. Yang, L. Huang, J. Zhou, and C. Qian, “Reinforcement learning-based adaptive cyberattack detection for cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 6962–6972, 2022.
- [144] Y. Zhou, W. Meng, W. Li, L. Cheng, and Y. Zhang, “Deep reinforcement learning for intelligent intrusion detection systems: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 84–124, 2023.
- [145] N. J. Higham, *Functions of matrices: theory and computation*. SIAM, 2008.
- [146] Q. Li, Z. Wang, J. Hu, and W. Sheng, “Distributed state and fault estimation over sensor networks with probabilistic quantizations: The dynamic event-triggered case,” *Automatica*, vol. 131, p. 109784, 2021.
- [147] J.-W. Zhu and G.-H. Yang, “Robust distributed fault estimation for a network of dynamical systems,” *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 14–22, 2016.
- [148] E. A. Wan and R. Van Der Merwe, “The unscented kalman filter for nonlinear estimation,” in *Proceedings of the IEEE 2000 Adaptive Systems for Signal Processing, Communications, and Control Symposium (Cat. No. 00EX373)*, pp. 153–158, Ieee, 2000.
- [149] K. Xiong, “Nonlinear filter and its application in satellite attitude estimation,” *Doctor Thesis of Beihang University, Beijing, China*, 2006.

- [150] K. Xiong, H. Zhang, and C. Chan, “Performance evaluation of ukf-based nonlinear filtering,” *Automatica*, vol. 42, no. 2, pp. 261–270, 2006.
- [151] T.-J. Tarn and Y. Rasis, “Observers for nonlinear stochastic systems,” *IEEE Transactions on Automatic Control*, vol. 21, no. 4, pp. 441–448, 1976.
- [152] Z. Zhao, Y. Yang, Y. Li, and R. Liu, “Security analysis for cyber-physical systems under undetectable attacks: a geometric approach,” *International Journal of Robust and Nonlinear Control*, vol. 30, no. 11, pp. 4359–4370, 2020.
- [153] Y. C. Paw, *Synthesis and validation of flight control for UAV*. University of Minnesota, 2009.
- [154] M. Lungu and R. Lungu, “Adaptive backstepping flight control for a mini-uav,” *International Journal of Adaptive Control and Signal Processing*, vol. 27, no. 8, pp. 635–650, 2013.
- [155] I. Lakshminarayan, *Model-based fault detection for low-cost UAV actuators*. PhD thesis, University of Minnesota, 2016.
- [156] K. Guo, L. Liu, S. Shi, D. Liu, and X. Peng, “Uav sensor fault detection using a classifier without negative samples: A local density regulated optimization algorithm,” *Sensors*, vol. 19, no. 4, p. 771, 2019.
- [157] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using kalman filter,” *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.
- [158] R. Sutton and A. Barto, “Reinforcement learning: An introduction. mit press; 2018,” *Google Scholar*, pp. 329–331.
- [159] T. Banerjee and V. V. Veeravalli, “Data-efficient quickest change detection in minimax settings,” *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6917–6931, 2013.
- [160] R. S. Sutton and A. G. Barto, “Reinforcement learning: An introduction,” *Robotica*, vol. 17, no. 2, pp. 229–235, 1999.
- [161] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, “Deep reinforcement learning: A brief survey,” *IEEE Signal Processing Magazine*, vol. 34, no. 6, pp. 26–38, 2017.
- [162] T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 8, pp. 3779–3795, 2021.

- [163] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, *et al.*, “Human-level control through deep reinforcement learning,” *nature*, vol. 518, no. 7540, pp. 529–533, 2015.
- [164] C.-Z. Bai, F. Pasqualetti, and V. Gupta, “Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs,” *Automatica*, vol. 82, pp. 251–260, 2017.
- [165] S. Wang, Y. Lyu, and W. Ren, “Unscented-transformation-based distributed nonlinear state estimation: Algorithm, analysis, and experiments,” *IEEE Transactions on Control Systems Technology*, vol. 27, no. 5, pp. 2016–2029, 2018.
- [166] K. Reif, S. Gunther, E. Yaz, and R. Unbehauen, “Stochastic stability of the discrete-time extended kalman filter,” *IEEE Transactions on Automatic control*, vol. 44, no. 4, pp. 714–728, 1999.
- [167] R. W. Beard and T. W. McLain, *Small Unmanned Aircraft: Theory and Practice*. Princeton University Press, 2012.