LAKEHEAD UNIVERSITY

Detection, Identification, and Mitigation of False Data Injection Attacks and Faults in Vehicle Platooning

by

Najeebuddin Ahmed

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the
Faculty of Engineering
Lakehead University

September 2023

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

Supervisor (1):	Dr. Amir Ameli Assistant Professor, Department of Electrical & Computer Engineering Lakehead University
Supervisor (2):	Dr. Hassan Naser Associate Professor, Department of Software Engineering Lakehead University
Committee Member (1):	Dr. Thangarajah Akilan Assistant Professor, Department of Software Engineering Lakehead University
Committee Member (2):	Dr. Waleed Ejaz Associate Professor, Department of Electrical & Computer Engineering Lakehead University

Declaration of Authorship

I, Najeebuddin Ahmed, declare that this thesis titled, 'Detection, Identification, and Mitigation of False Data Injection Attacks, and Faults in Vehicle Platooning' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Name: Najeebuddin Ahmed

Date: 8/15/2023

"God does not burden any soul with more than it can bear..."

- (Al-Quran 2:286)

Abstract

Smart vehicles are designed leveraging advanced hardware, including sensors, and cutting-edge technologies, such as artificial intelligence, Vehicle-to-Vehicle (V2V) communication, and Vehicle-to-Infrastructure (V2I) communication. These components are seamlessly integrated through software systems, empowering vehicle to make intelligent decisions and navigate safely in diverse environments.

V2V communication plays a vital role in facilitating information exchange among vehicles, encompassing crucial parameters, such as speed, acceleration, location, and vehicle size. One of the key applications of V2V communication is vehicle platooning, where a group of vehicles travels closely together, forming a cohesive convoy. Platooning has garnered significant attention due to its potential to revolutionize road safety, fuel efficiency, and traffic flow. By reducing the distance between vehicles, platooning minimizes aerodynamic drag, leading to improved fuel efficiency and reduced emissions. Moreover, the tight coordination and communication between vehicles enable enhanced safety through faster reaction times and response capabilities. Additionally, platooning optimizes road capacity and traffic flow, potentially alleviating congestion and enhancing overall transportation efficiency.

However, the effectiveness of platooning heavily relies on the robustness of interconnected technologies and communication systems, emphasizing the critical importance of robust cybersecurity measures. In response to this challenge, this dissertation proposes an innovative attack detection and identification technique specifically designed to secure vehicle platoons against cyber-attacks, with a particular focus on False Data Injection Attacks (FDIAs). The dissertation commences by developing a comprehensive state-space model tailored to capture the dynamics of a platoon of vehicles. This model is adaptable and flexible, accommodating a varying number of vehicles and adaptable to different information flow topologies. Leveraging the Unknown Input Observer (UIO) methodology, the dissertation employs state estimation techniques to accurately estimate the internal states of each vehicle within the platoon, including position, velocity, and acceleration. This estimation process becomes the cornerstone for attack detection, as any deviations between the received and estimated internal states during FDIAs trigger an increase in the Residual Function (RF) of the UIO.

Expanding its contributions further, the dissertation introduces multiple attack identification UIOs, allowing for the identification of compromised vehicles within the platoon and estimation of the associated attack inputs. These novel techniques pave the way for effective FDIA mitigation strategies, ensuring the restoration of the platoon's integrity and reliability. Furthermore, the dissertation recognizes that the intricate combination

of hardware and software components in the vehicles introduces potential risks of faults and issues. In line with the UIOs to tackle attacks, the dissertation further extends its focus to develop UIOs for fault detection and identification. These UIOs are designed to monitor crucial parameters, such as position, velocity, and acceleration, within each vehicle of the platoon. By promptly identifying abnormalities in these parameter values, the fault detection and identification UIOs enable effective fault mitigation strategies, thereby bolstering the overall robustness and reliability of the platoon.

To validate the effectiveness of the proposed methodology, the dissertation extensively employs MATLAB simulations, examining diverse scenarios and evaluating the performance of the attack detection and identification techniques, as well as the fault detection and identification mechanisms. Through these simulations, the dissertation effectively demonstrates the method's efficacy in securing and maintaining the optimal operation of vehicle platoons, even in the presence of cyber-attack threats and fault conditions.

In summary, this dissertation makes significant contributions to the advancement of vehicular technologies by proposing an innovative attack detection and identification technique, specifically tailored to secure vehicle platoons against cyber-attacks, notably FDIAs. Moreover, it addresses the crucial aspect of fault detection, further enhancing the reliability and resilience of platooning systems. Through comprehensive MATLAB simulations, the dissertation effectively showcases the method's effectiveness, providing a solid foundation for ensuring the safety, security, and efficiency of future vehicle platooning systems in real-world scenarios. The findings of this research significantly contribute to the field of cybersecurity and fault detection and identification, shaping the future of automotive transportation.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to the Almighty God for granting me the strength, knowledge, and perseverance to complete this thesis. Without His blessings and guidance, this achievement would not have been possible.

I extend my heartfelt appreciation to my supervisors, Dr. Amir Ameli and Dr. Hassan Naser, for their unwavering support and valuable guidance throughout my research. Their expertise, encouragement, and constructive feedback have been instrumental in shaping the direction of this thesis and enhancing the quality of my work. I am truly grateful for the time and effort they dedicated to helping me navigate through the challenges and complexities of this study. I am also deeply thankful for their availability and willingness to assist me no matter how early or late in the day it was. Their constant presence and belief in my abilities have instilled in me a sense of confidence and determination, enabling me to overcome obstacles and strive for excellence. To both my supervisors, I owe a debt of gratitude for believing in the potential of this work and guiding me towards its successful completion. Your mentorship has been invaluable, and I am honored to have had the opportunity to learn from you.

I would also like to thank the committee members Dr. Thangarajah Akilan and Dr. Waleed Ejaz, whose dedication to academic excellence has provided me with an enriching learning environment. Their feedback to my education and research have been invaluable, and I am sincerely appreciative of their efforts.

Furthermore, I wish to acknowledge my fellow students and friends for their camaraderie and support, which made my academic journey more enjoyable and memorable.

Last but not least, I am filled with immense gratitude for my family, who have been my pillars of support and inspiration. I want to begin by thanking my parents, whose unconditional love, sacrifices, encouragement, and unwavering belief in me have shaped my academic journey. Their guidance and understanding have been instrumental in my achievements, and I am truly blessed to have them by my side.

To my dear brothers, Imad and Safi, your presence in my life has been a constant source of strength and motivation. Your unwavering support and belief in me have propelled me forward, even in the face of challenges. I hope that my accomplishments serve as a driving force for each of you to pursue your dreams passionately and achieve greatness in your own endeavors.

Contents

List of Figures

List of Tables

Abbreviations

BF	**B**idirectional **F**ollowing
BSM	**B**asic **S**afety **M**essage
DoS	**D**enial **o**f **S**ervice
DSRC	**D**edicated **S**hort **R**ange **C**ommunication
DSRC MS	**D**edicated **S**hort **R**ange **C**ommunication **M**essage **S**et
EKF	**E**xtended **K**alman **F**ilter
FDIA	**F**alse **D**ata **I**njection **A**ttack
FLOPS	**F**loating **P**oint **O**perations **P**er **S**econd
GPS	**G**lobal **P**ositioning **S**ystem
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IFT	**I**nformation **F**low **T**opology
IMU	**I**nertial **M**easurement **U**nit
LBF	**L**eader **B**idirectional **F**ollowing
LiDAR	**Li**ght **D**etection **A**nd **R**anging
LPF	**L**eader **P**redecessor **F**ollowing
MHE	**M**oving **H**orizon **E**stimation
OBU	**O**n-**B**oard **U**nit

PF	**P**redecessor **F**ollowing
RADAR	**RA**dio **D**etection **A**nd **R**anging
RF	**R**esidual **F**unction
RSU	**R**oad **S**ide **U**nit
SAE	**S**ociety of **A**utomotive **E**ngineers
UIO	**U**nknown **I**nput **O**bserver
UKF	**U**ncented **K**alman **F**ilter
V2X	**V**ehicle-**to**-**Everything**
V2V	**V**ehicle-**to**-**V**ehicle
V2I	**V**ehicle-**to**-**I**nfrastructure

Symbols

n	Number of follower vehicles in the platoon
$i = 0, 1, 2, \ldots, n$	Vehicle number where $i = 0$ is the Lead Vehicle
x_i	Position of vehicle i
v_i	Velocity of vehicle i
a_i	Acceleration of vehicle i
Δx_i	Difference in Positions of vehicles i and 0
Δv_i	Difference in Velocities of vehicles i and 0
Δa_i	Difference in Accelerations of vehicles i and 0
τ_i	Engine time constant of vehicle i
β_i	Auxiliary input signal of vehicle i
K_i	Position Control Gain of vehicle i
B_i	Velocity Control Gain of vehicle i
H_i	Acceleration Control Gain of vehicle i
L	Vehicle Length
d_i^{i+1}	Distance between consecutive vehicles
d_{ij}	Distance between vehicles i and j
I_i	Set of vehicles sending information to vehicle i
C_i	Cardinality of set I_i
Θ	Attack input matrix
μ	Attack input vector
F	Fault input matrix
f	Fault input vector
α	State Estimation Delay
λ	Unknown input matrix
Λ	Unknown input vector

r	Residual Function
δ	Detection threshold
$\ddagger$	Pseudo-inverse Operator

To my Mom, Dad, Imad and Safi

Chapter 1

Introduction

1.1 Smart Vehicles

Smart vehicles rely on advanced hardware and technology for safe and efficient operation. They have revolutionized the automotive industry by providing alternatives to traditional transportation methods and enhancing overall road safety.

Equipped with a range of sensors, including GPS, encoders, Inertial Measurement Units (IMUs), LiDAR, RADAR, and cameras, these vehicles gather crucial data to navigate their surroundings. The GPS sensor provides precise location information, while rotary encoders and IMUs collect data on heading, speed, and acceleration. LiDAR, RADAR, and cameras accurately measure the distance between objects and the vehicle, effectively capturing the surrounding environment [1]. By continuously analyzing the environment, these vehicles can make informed decisions and take appropriate actions to ensure the safety of passengers and other road users. This includes detecting and avoiding potential obstacles, responding to changes in traffic conditions, and predicting and preventing potential collisions.

Smart vehicles are also equipped with advanced driver assistance systems that provide additional layers of safety and convenience. These systems, such as adaptive cruise control, lane-keeping assistance, automatic emergency braking, and parking assistance, assist drivers in various tasks, making driving more comfortable and reducing the risk of accidents.

Furthermore, these vehicles optimize routes and employ intelligent algorithms to minimize traffic congestion, leading to smoother traffic flow and reduced travel times. The widespread adoption of such vehicles can contribute to a more efficient and sustainable transportation system, benefiting both individuals and the environment.

In addition to their individual capabilities, the effectiveness of smart vehicles is further enhanced through seamless information exchange and collaboration among vehicles, made possible by Vehicle-to-Everything (V2X) communication technology.

1.2 Vehicle-to-Everything communication

V2X communication technology is a crucial component in these vehicles, encompassing Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. V2V communication enables seamless information exchange among vehicles through the utilization of Dedicated Short Range Communication (DSRC) technology. Operating at a frequency of 5.9 GHz, DSRC adheres to standards, such as IEEE 802.11 [2], 1609.x [3], SAE J2735 [4], and SAE J2945 [5], ensuring real-time interactions with low latency and high reliability. By facilitating the sharing of vital data like position, speed, and acceleration, V2V communication promotes cooperative driving, collision avoidance, and situational awareness.

DSRC's dedicated frequency band ensures uninterrupted communication, establishing a secure and private channel for vehicles and infrastructure. Utilizing a broadcast communication approach, DSRC disseminates messages containing valuable data essential for informed decision-making and optimized traffic management. With a range of up to 300 meters, DSRC enables close-proximity communication among vehicles, making it particularly suitable for applications, such as cooperative collision warning, intersection safety, and platooning. To ensure standardized communication, the Society of Automotive Engineers (SAE) has established the DSRC Message Set (DSRC MS), which defines a set of standardized message formats. One essential message format is the Basic Safety Message (BSM), which is always shared and includes, but is not limited to, the following BSMcoreData:

1. Latitude
2. Longitude
3. Speed
4. Acceleration
5. Heading
6. Vehicle Size

Complementing V2V communication, V2I communication establishes connections between vehicles and infrastructure elements like traffic lights and Road Side Units (RSUs). This connectivity enhances situational awareness and decision-making capabilities by providing vehicles with valuable information sourced from the infrastructure. V2I communication plays a vital role in optimizing traffic flow and enabling more intelligent transportation systems.

1.3 Vehicle Platooning

The synergy between V2V and V2I communication systems significantly enhances road safety and efficiency. Through real-time information sharing and collaboration among vehicles, proactive responses to hazards, improved maneuverability, and coordinated movements become possible. This collaborative environment unlocks transformative applications, such as vehicle platooning, where groups of vehicles travel closely together (Fig. 1.1), resulting in reduced aerodynamic drag and enhanced fuel efficiency. Coordinated movements within platoons enable synchronized and efficient maneuvers, leading to improved safety and optimized road capacity.

In addition to fuel efficiency and safety, vehicle platooning advancements have wide-ranging implications. They facilitate collaborative decision-making, adaptive navigation systems, and intelligent intersection management, which contribute to reduced travel time, minimized collisions, and enhanced overall traffic efficiency. Ongoing research and development in vehicle platooning and V2X-enabled solutions are reshaping transportation by offering improved road safety, enhanced fuel efficiency, optimized traffic flow, and the development of a sustainable mobility ecosystem. These technologies hold immense promise for transformative applications and positive societal impact as they continue to evolve, revolutionizing roads and cities.

For V2V communication, the specific sharing and acceptance of information within a platoon depend on the adopted Information Flow Topology (IFT). Different IFTs are depicted in Fig. 1.1, where the arrows represent the transmission of information from sending to receiving vehicles [6].

One commonly studied IFT is the Leader-Predecessor Following (LPF) IFT, as shown in Fig. 1.1a. In this configuration, each vehicle receives information from both the leader and its predecessor, facilitating coordinated communication and data exchange.

Another IFT is the Predecessor Following (PF) IFT, depicted in Fig. 1.1b. Here, each vehicle receives information solely from its predecessor, allowing for a sequential flow of information within the platoon.

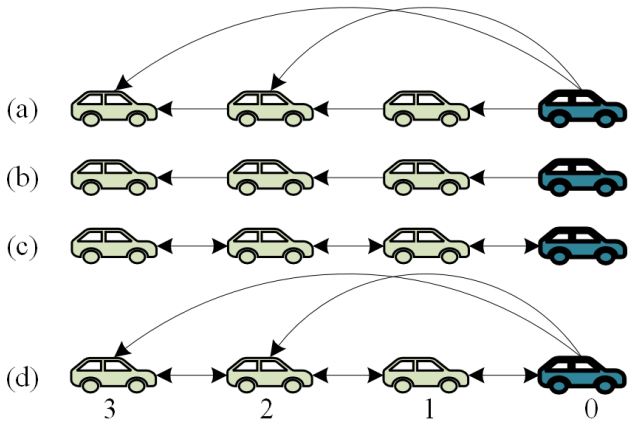


FIGURE 1.1: Vehicle Platooning IFTs: (a) leader-predecessor following, (b) predecessor following, (c) bidirectional following, and (d) leader bidirectional following.

The Bidirectional Following (BF) IFT, shown in Fig. 1.1c, involves each vehicle receiving information from both its predecessor and its successor. This bidirectional communication enables enhanced situational awareness and coordination among vehicles.

Lastly, the Leader-Bidirectional Following (LBF) IFT, illustrated in Fig. 1.1d, extends the communication network by including information from the leader, predecessor, and successor vehicles. This IFT promotes comprehensive data sharing and collaboration throughout the platoon.

The effectiveness and reliability of vehicle platooning heavily rely on the integrity and security of the exchanged information. Unfortunately, malicious attacks in the form of False Data Injection Attacks (FDIAs) pose a significant threat to the trustworthiness of the V2V communication channel.

1.4 FDIAs

FDIAs represent a severe and concerning type of attack where malicious intruders gain unauthorized access to a legitimate system, introducing false information into it. Unfortunately, the wireless nature of V2V technology creates vulnerabilities that attackers can exploit to compromise the system. By intercepting and cleverly manipulating messages while eavesdropping on the communication, attackers can manipulate and relay altered information to the intended vehicles. This manipulation poses a significant threat to the integrity, security, and trustworthiness of the communication.

Moreover, the critical role of Road Side Units (RSUs) in vehicles, providing vital environmental information through V2I technology, also introduces vulnerabilities that

attackers can exploit. Unauthorized access to RSUs allows attackers to eavesdrop on legitimate information exchanges or even inject malicious data into the vehicle's systems. By manipulating this information, attackers undermine the safety and reliability of vehicles, potentially leading to dangerous consequences.

It is important to recognize that these attackers can be skilled adversaries who possess the necessary expertise and tools to execute sophisticated attacks. They can exploit weaknesses in the cryptographic protocols currently in use, bypassing the security measures designed to safeguard V2V and V2I communication channels. The injection of incorrect or malicious data has the potential to mislead and misguide vehicles, leading them off course and resulting in severe and potentially catastrophic outcomes.

Considerable research efforts have been devoted to protecting vehicle platoons from FDIAs. This dissertation provides a concise literature review of this attack type, emphasizing on two main categories: data-driven [7, 8] and model-based [9–15] techniques.

Data-driven techniques, as the name suggests, rely on analyzing and processing large amounts of data to detect and mitigate FDIAs. These techniques often utilize machine learning and deep learning algorithms to identify patterns and anomalies in the data. By training models on extensive datasets, data-driven approaches aim to detect deviations from normal behavior and identify potential attacks. Articles [7] and [8] utilize deep learning approaches for securing platoons. In [7], Convolutional Neural Networks are employed to detect and localize attacks within platoons. However, this study heavily relies on onboard LiDAR and RADAR sensors of the vehicle for accurate speed and distance measurements. It also assumes that the lead vehicle cannot be attacked, which may not always be the case. In [8], Long Short-Term Memory is used to detect FDIAs based on a vehicle's speed and acceleration. However, the presented approach is limited to the LPF IFT, and it assumes that the vehicle's position cannot be manipulated. Additionally, the majority of approaches in this category, such as [7] and [8], require a large dataset for training and testing.

On the other hand, model-based techniques involve developing mathematical models and algorithms to characterize the behavior of the platoon and detect potential attacks. These techniques often rely on the knowledge of the system dynamics and employ methods, such as state estimation, observer design, and statistical analysis to identify discrepancies caused by FDIAs. Model-based approaches aim to capture the fundamental properties of the platoon and exploit them to detect and mitigate attacks. Studies [9–15] employ model-based approaches to address FDIAs in vehicle platoons. In [9], an Unbiased Finite Impulse Response algorithm focuses on detecting and estimating deception attacks on a vehicle's GPS receiver. Moving on to platoons adhering only to

the PF IFT, article [10] utilizes state-space modeling and observers for FDIA detection but emphasizes identifying attack targets rather than mitigating attacks. Similarly, in [11], a distributed Kalman filter combined with a modified Generalized Likelihood Ratio algorithm is employed for vehicle state estimation and attack detection. For platoons following the PF topology, article [12] proposes a vehicle-specific attack detection system based on state prediction and estimation. Reference [13] introduces an attack-resilient Distributed State Estimation algorithm, utilizing onboard sensors like RADAR and LiDAR for error estimation, but with limited capability in identifying long-duration attacks. Additionally, in [14], FDIAs involving ghost or fake vehicles are detected using a partial differential equation model and observer algorithms, tailored for the LPF IFT and relying on RADAR sensors for detection. A different approach is presented in [15], where transmissibility operators are employed to compare the platoon's behavior under healthy conditions with its actual behavior, enabling the detection, identification, and mitigation of cyber-attacks. However, this method is dependent on onboard perception sensors.

However, each study focuses on specific aspects of the problem, such as GPS specific deception attacks, attack detection in specific IFTs, or attack detection using particular sensors. As a result, there is a research gap in the literature, where a comprehensive and unified approach to address FDIAs in various platoon configurations and across multiple parameters is lacking. Therefore, the identified research gap serves as an objective to accomplish the research goal. In Section 1.8, this research goal will be elaborated upon, and the proposed methodology to address the research gap in securing platoons against FDIAs will be presented.

Recognizing the significant impact of attacks, ensuring the overall resilience and dependability of smart vehicles becomes paramount. To achieve this, it is crucial to address the challenges that arise from their complex systems.

1.5 Faults

The vehicles in the platoon are characterized by their complexity, involving numerous hardware and software components, which inevitably give rise to faults. Various factors can contribute to these faults. For instance, obstructions such as tall buildings can temporarily disrupt GPS functionality, compromising accurate position determination when passing through tunnels [16]. Improper accelerometer readings can occur due to poor connectors, exposure to extreme temperatures, shocks, or electrostatic discharge [17]. Malfunctions in encoders can stem from issues like incorrect wiring, electrical noise, dirt/dust accumulation, moisture, or overheating [18]. Other factors, such as inclement

weather, signal outages, sensor aging, or manufacturing defects can also result in incorrect or missing sensor data. Furthermore, impairments in On-Board Units (OBUs), including electronic noise, intermodulation interference, cable leakage, or unlicensed or incorrect band operations, can impact V2V communication [19].

Utilizing sensor measurements that are inaccurate or unreliable can have significant repercussions, potentially diverting the platoon from its intended path, vehicle safety, and operational efficiency. Therefore, it is crucial to address these faults to ensure the proper functioning and safety of the platoon.

Extensive research has been conducted on faults in vehicle platoons. In [20], a distributed finite-time observer, an Adaptive Optimal Finite Time Parameter Estimation rule, and a fault-tolerant controller are employed, but the work is restricted to platoons with LPF IFT. Reference [21] proposes an active fault diagnosis method for detecting and identifying sensor faults in vehicles operating in a platoon formation. The method introduces a probing signal to actively excite the system, revealing a residual component that can be analyzed for fault identification. However, it is limited to PF IFTs (Fig. 1.1.b) and assumes only one faulty sensor at a time. Reference [22] presents a fault-tolerant control mechanism utilizing event-triggered controllers and Lyapunov theory to ensure stability in platoons. However, it primarily focuses on mitigating faults in position and velocity, without specifically addressing acceleration. Reference [23] has developed an exponential spacing policy, a nonlinear observer, and a distributed adaptive fault-tolerant control scheme for BF IFT (Fig. 1.1.c). Similarly, [24] has utilized a quadratic spacing error policy, adaptive estimation laws, and an adaptive sliding mode control for actuator faults. Finally, in [25], a velocity fault detection and correction algorithm is introduced that uses a distributed function calculation strategy for position and velocity gathering, enabling vehicles to assess their own velocity estimation through interaction with others in the network.

These studies reveal several research gaps in the literature. Firstly, there is limited exploration of various platoon configurations and the consideration of multiple faulty parameters simultaneously. Notably, most studies assume single or two faulty parameters, overlooking the possibility of three concurrent faulty parameters. This identified research gap emerges from the possibility that the OBU, responsible for handling all three parameters (position, velocity, and acceleration), could be faulty, leading to the simultaneous occurrence of multiple or all faulty parameters. Secondly, the lack of focus on acceleration as a critical parameter for fault detection represents a significant gap in current research efforts. Including acceleration in fault detection approaches could substantially enhance their effectiveness in ensuring platoon safety. Lastly, the need for

more unified and comprehensive approaches is evident, addressing diverse platoon configurations and multiple faulty parameters in an integrated manner. Failing to address these research gaps can undermine the trustworthiness of vehicle platooning systems and hinder their widespread adoption. The consequences of such shortcomings may include increased risk of accidents, compromised road safety, reduced fuel efficiency, and diminished overall traffic efficiency.

The research gaps identified in the literature set the objectives for this study. A goal of this dissertation is to develop a comprehensive framework that effectively addresses fault detection, identification, and mitigation in vehicle platoons, taking into account diverse platoon configurations and considering all three parameters (position, velocity, and acceleration) to solve multiple faulty parameters simultaneously.

Therefore, in Section 1.8, the research objectives and proposed framework to address these research gaps and contribute to the field of fault detection and mitigation in vehicle platooning will be presented.

1.6 State-Space Modeling

State-space modeling presents a promising approach to address the research gaps identified in Sections 1.4 and 1.5 regarding vehicle platooning. State-space modeling is a powerful technique used to represent dynamical systems using matrices and vectors. It provides a comprehensive analysis of intricate nonlinear systems, offering a deeper understanding of their behavior over time. Engineers can accurately predict how modifications to specific elements may influence overall performance through state-space modeling, gaining insights into critical points where the output may undergo significant changes.

One of the key advantages of state-space models is their ability to identify critical thresholds or conditions that could substantially impact the system's behavior or performance. This insight empowers engineers to make informed decisions and devise strategies to optimize the system's design and operation. Moreover, state-space modeling facilitates the development of robust control algorithms. By comprehending the dynamics of a given system through state-space representation, engineers can design control algorithms that effectively manipulate the system's variables to achieve desired behaviors. This ensures precise control and facilitates the attainment of specific performance objectives.

There are two primary approaches to state-space modeling: continuous state-space modeling and discrete state-space modeling.

Continuous state-space modeling deals with systems whose state variables change continuously over time, described by a set of continuous differential equations. This approach is ideal for representing systems with continuous and smooth dynamics, such as physical systems governed by differential equations. This method enables a precise understanding of the system's behavior as it evolves smoothly through time. The general continuous state-space model can be represented as follows [26–28] and it is important to note that the style presented below for continuous models will be consistently employed throughout this dissertation:

$$\dot{\mathbb{X}}(t) = \mathbb{A}\mathbb{X}(t) + \mathbb{B}\mathbb{U}(t) \tag{1.1}$$

$$\mathbb{Y}(t) = \mathbb{C}\mathbb{X}(t) + \mathbb{D}\mathbb{U}(t) \tag{1.2}$$

where at time t, $\mathbb{A}$, $\mathbb{X}(t)$, $\mathbb{B}$, $\mathbb{U}(t)$, $\mathbb{C}$, and $\mathbb{D}$, represent the state matrix, state vector, input matrix, input vector, output matrix, and feedthrough matrix, respectively; $\dot{\mathbb{X}}(t)$ is the derivative of $\mathbb{X}$; and $\mathbb{Y}(t)$ is the output vector. Additionally, equation (1.1) captures the dynamics of the system and how it responds to control inputs whereas equation (1.2) describes the relationship between the state variables and the measurable outputs of the system.

On the other hand, discrete state-space modeling is employed for systems with state variables that change in discrete steps or time intervals, represented by difference equations. This approach is well-suited for systems with quantized or discrete behaviors, such as digital control systems or systems with sampling and feedback intervals. The discrete approach offers valuable insights into how the system's state changes at specific time points. Similar to the general continuous state-space model representation, the general discrete state-space model can be represented as follows [27, 28], with this style being utilized for discrete models in this dissertation:

$$X[k+1] = AX[k] + BU[k] \tag{1.3}$$

$$Y[k] = CX[k] + DU[k] \tag{1.4}$$

where at time step k, A, $X[k]$, B, $U[k]$, C, and D, represent the state matrix, state vector, input matrix, input vector, output matrix, and feedthrough matrix, respectively; $X[k]$ is the state vector at time step k+1; and $Y[k]$ is the output vector. Similar to equations (1.1) and (1.2), equation (1.3) captures the dynamics of the system and how it responds to control inputs whereas equation (1.4) describes the relationship between the state variables and the measurable outputs of the system.

In the context of vehicle platooning, state-space modeling plays a vital role in estimating the true states of the vehicles by integrating sensor data and accounting for vehicle dynamics. In Chapter 2, a deeper exploration of the principles and applications of both continuous and discrete state-space modeling will be conducted, examining their efficacy in addressing the identified research gaps and contributing to the development of robust FDIA and fault detection and identification strategies. By intelligently selecting the appropriate state-space modeling approach, effective modeling and understanding of the complex dynamics of vehicle platooning systems can be achieved

1.7 State Estimation Techniques

Upon establishing the state-space models of the vehicle platoon, an essential tool is incorporated known as, State estimation techniques. These are utilized in dynamic systems to estimate the system states that cannot be directly measured. These techniques leverage the available measurement information to accurately estimate the states. Ensuring the accuracy, reliability, and convergence of state estimation techniques requires satisfying one or more of the following conditions:

- **Stability**: The estimated states must converge and remain within a reasonable range, even in the presence of uncertainties such as noise, to prevent divergence and erratic estimation. A given state-space model $X[k+1] = A \cdot X[k]$ is stable if starting from $X[0]$;

$$\lim_{k \to \infty} X[k] = 0 \tag{1.5}$$

  and the magnitude is less than 1 for all the eigenvalues of A [28, 29]. This ensures that the state estimation process remains stable.

- **Observability**: It is essential to establish that the states of the system can be determined given the available measurements. Observability is a critical aspect of state estimation techniques to ensure that the estimation process can uniquely determine the states from the available sensor data. A continuous system with input equation (1.1) and output equation (1.2) or a discrete system with input equation (1.3) and output equation (1.4) is considered to be stable if and only if;

$$\text{rank} \left(\begin{bmatrix} \mathbf{C} \\ \mathbf{CA} \\ \mathbf{CA}^2 \\ \vdots \\ \mathbf{CA}^{n-1} \end{bmatrix} \right) = n \tag{1.6}$$

where n is the number of state variables [29, 30].

This condition ensures that the states are uniquely observable, and the state estimation process can reliably estimate the unmeasured states based on the available observable states and input data.

- **Invertibility**: The estimated states should be able to approximate the actual states of the system. Invertibility ensures that the state estimation process can accurately approximate the true states of the system based on the available measurements. A reliable and invertible state estimation technique provides valuable insights into the system's behavior and allows for precise control and analysis of the dynamic system [28].

Prominent state estimation techniques include:

- **Kalman Filter**: A powerful recursive algorithm used for state estimation in linear dynamic systems. By considering uncertainties, such as noise in measurement values, it efficiently estimates the system's state. One of its key strengths lies in providing an optimal estimate in terms of mean squared error, especially when both the dynamic system and measurement noise follow Gaussian distributions [29, 31]. This makes the Kalman Filter an essential tool for linear systems where its assumptions are met, allowing for accurate and reliable state estimation.

- **Extended Kalman Filter (EKF)**: An extension of the Kalman Filter that is specifically designed to handle non-linear dynamic systems. While the original Kalman Filter is effective for linear systems, the EKF linearizes the non-linear system using local linear approximations to perform state estimation [31, 32].

- **Unscented Kalman Filter (UKF)**: Another extension of the Kalman Filter designed explicitly for non-linear systems, eliminating the necessity for linearization. Linearizing a non-linear system can often lead to inaccurate dynamics representation at a single sample point. To overcome this limitation, the UKF employs a unique approach known as the unscented transformation. The unscented transformation is a pivotal step in the UKF that involves selecting a set of sigma points to approximate the system's state distribution. These sigma points are deterministically chosen to capture the underlying distribution's characteristics accurately. The UKF passes these sigma points through the non-linear process model. The transformed sigma points then provide estimates for the predicted mean and covariance of the system's state distribution. By utilizing the unscented transformation, the UKF enables a more accurate representation of the non-linear system's dynamics [29, 32].

- **Moving Horizon Estimation (MHE)**: An optimization-based technique used for state estimation in dynamic systems. It leverages the available noisy measurements of the system over a fixed time window to estimate the states. Unlike traditional recursive approaches, MHE considers a limited time horizon, typically denoted as N, and performs an optimization to find the most probable values of the state trajectory within that window [32]. By focusing on a finite time window, MHE takes into account the most recent and relevant measurements, making it well-suited for systems with nonlinear models or constraints on the estimates. This approach allows MHE to provide accurate state estimates even in the presence of uncertainties and disturbances in the system. The use of optimization in MHE ensures that the state estimates are obtained by solving an optimization problem, which offers flexibility in handling complex system dynamics and measurement noise.

- **Particle Filtering**: A non-linear state estimation technique that represents the system's probability density function using a set of particles, where each particle carries a state hypothesis with associated weight. The Particle Filter propagates these particles through the system's non-linear dynamics, and the weights are updated based on the likelihood of the measurements. By resampling particles according to their weights, the Particle Filter adapts to changes in the system's behavior and provides accurate state estimates even in highly non-linear scenarios [33, 34].

- **Luenberger Observer**: A state estimation technique specifically designed for linear systems. It operates in a sequential or recursive manner, continuously refining its estimate of the internal state of a real system over time. This technique utilizes input and output measurements obtained from the real system to iteratively update its estimations [35, 36]. The sequential or recursive nature of the Luenberger Observer involves an iterative process where each new estimation incorporates the latest available measurements and previous estimates. This approach enables the observer to adapt and respond to changes in the system's behavior over time, making it valuable for real-time monitoring and control of linear systems. By combining input and output measurements with its iterative process, the Luenberger Observer provides insights into the otherwise unobservable aspects of linear systems, contributing to improved system understanding and control.

- **Unknown Input Observers (UIOs)**: An advanced state estimation technique utilized in dynamic systems to accurately estimate the system states in the presence of unknown inputs [37]. These elusive inputs, which cannot be directly measured or observed, could be external disturbances, attacks, or faults, and they

significantly impact the system's behavior. The primary objective of UIOs is to reconstruct these unknown inputs while concurrently estimating the system states based on available measurements. By effectively handling these unknown inputs, UIOs enhance the overall resilience and reliability of the dynamic system, making them particularly valuable for attack or fault detection, identification, and control applications.

In this dissertation, the UIO state estimation technique is employed. Within the context of vehicle platooning, these unknown inputs refer to attacks and faults that can impact the behavior of the vehicles but cannot be directly measured or known. These elusive inputs play a significant role in compromising the platoon's performance and safety, making their estimation essential for effective attack and fault detection and identification. In Chapter 3, a deeper exploration into the principles and applications of Unknown Input Observers within the context of vehicle platooning will be conducted. This exploration sheds light on how UIOs enable addressing the challenges posed by unknown inputs, ultimately enhancing the platoon's overall resilience and reliability.

1.8 Research Goals

The goals of the dissertation are to tackle FDIAs and faults in vehicle platooning. To address the consequences of FDIAs and faults and overcome the identified research limitations (Sections 1.4 and 1.5), robust and comprehensive frameworks are developed for tackling these issues in vehicle platooning by combining state-space modeling (Section 1.6) with UIOs (Section 1.7). Therefore, the following objectives need to be met to achieve the goals:

- Present a state-space model for vehicle platoons that is adaptable to any number of vehicles and independent of a specific IFT.
- Develop UIOs specifically tailored for attack detection, identification, and mitigation, enabling the detection of FDIAs, identification of the attacked parameters, and the implementation of effective mitigation strategies.
- Design and implement UIOs dedicated to fault detection, identification, and mitigation, enabling the detection of faults within the platoon, identification of the faulty parameters, and the execution of appropriate mitigation measures.

Figure 1.2 visually represents an overview of the objectives, providing a graphical depiction of the path undertaken throughout the dissertation.

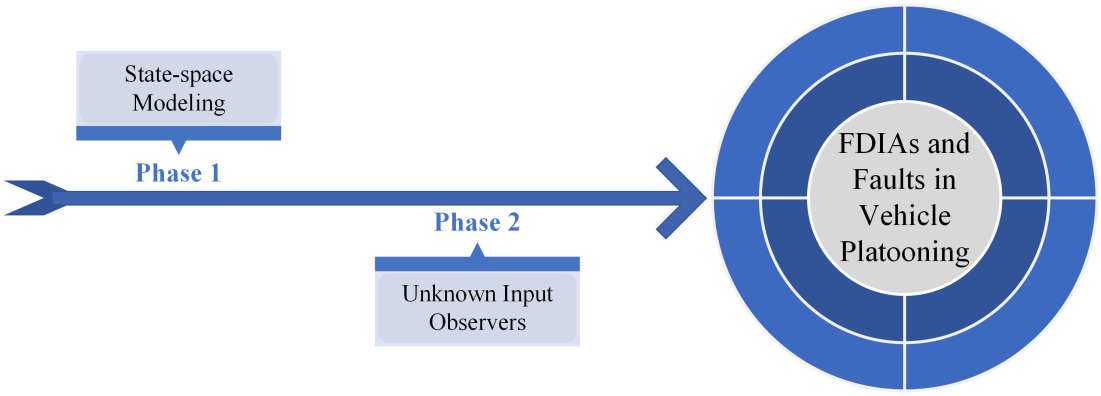


FIGURE 1.2: Research Objectives

1.9 Dissertation Outline

The subsequent chapters delve into specific facets of this research through an in-depth exploration of various topics,

Chapter 2 focuses on vehicle platoon modeling, specifically addressing the dynamic behavior of vehicles within a platoon. Furthermore, the state-space modeling technique is applied to capture the dynamics of a vehicle platoon under various conditions, including anomaly-free scenarios, attacks, and faults. The models developed in this chapter provide a comprehensive understanding of the behavior and interactions of vehicles within a platoon, allowing for analysis and investigation of different operational scenarios.

Chapter 3 specifically highlights Unknown Input Observers (UIOs) as a robust method for state estimation within the vehicle platoon. UIOs enable accurate estimation of the state variables for each vehicle, even in the presence of unknown inputs, such as attacks and faults. By effectively accounting for these unknown inputs, the UIOs provide a reliable framework for maintaining accurate and up-to-date state information throughout the platoon. Furthermore, the chapter lays the foundation for safeguarding the vehicle platoon against potential attacks and faults, ensuring the reliability and robustness of the overall system. The capabilities of the UIOs are leveraged to develop comprehensive frameworks for the detection, identification, and mitigation of attacks and faults within the vehicle platoon. Building upon the state estimation provided by the UIOs, these frameworks enable effective detection of attacks and faults, precise identification of the parameters involved, and the implementation

Chapter 4 thoroughly assesses the effectiveness of the attack and fault detection, identification and mitigations techniques under diverse circumstances. By subjecting the system to rigorous testing and analysis, it provides valuable insights into the system's capabilities, and overall performance. This evaluation serves as a crucial step towards ensuring the reliability and efficiency of the proposed solution, validating its effectiveness in real-world scenarios.

Chapter 5 serves as the concluding chapter of the dissertation, summarizing the key findings, contributions, and implications of the research conducted. This chapter provides a comprehensive overview of the entire dissertation, highlighting the main accomplishments and outcomes achieved throughout the study. It discusses the significance of the research in addressing the identified problem statement and its potential impact on the field.

Chapter 2

Vehicle Platoon Modelling

In this chapter, the exploration commences with examining the fundamental equations governing the motion of individual vehicles within the platoon. This initial investigation lays the foundation for a deeper understanding of the underlying principles of vehicle dynamics. Subsequently, the insights are extended to encompass the behavior of the entire platoon as a unified system. The first major milestone in the investigation involves creating a state-space model representing an attack and fault-free platoon. This model serves as the reference point for the state-space models incorporating attacks and faults. Next, a step further is taken by designing a state-space model that incorporates FDIAs. By doing so, valuable insights are gained into the impact of such attacks on the platoon's stability and safety. To ensure a comprehensive analysis, the presence of faults within the platoon is also addressed. Developing a state-space model that accounts for faults allows studying their influence on the overall system performance.

2.1 Dynamic Behaviour of Vehicles in a Platoon

In this section, the fundamental equations that govern the motion of individual vehicles within the platoon are established. The leader of a platoon of vehicles is denoted as vehicle 0, while the following vehicles are numbered from 1 to n (Fig. 2.1). Each vehicle is characterized by its position, velocity, and acceleration, represented by x_i, v_i, and a_i, respectively. Furthermore, L_i refers to the length of vehicle i and d_i^{i+1} represents the distance between vehicle i and the successor vehicle $i+1$ (as illustrated in Fig. 2.1).

According to the literature, such as the works presented in [38, 39], the dynamics of any vehicle in a longitudinal platoon can be described as follows:

$$\dot{x}_i(t) = v_i(t) \tag{2.1}$$

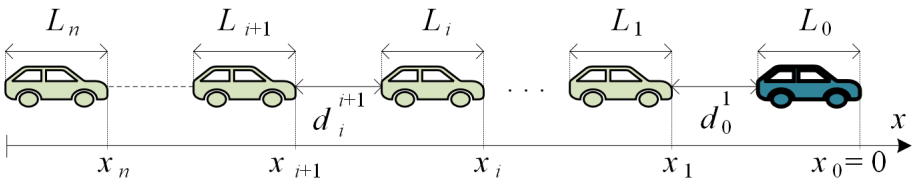


FIGURE 2.1: Longitudinal platoon system.

$$\dot{v}_i(t) = a_i(t) \tag{2.2}$$

$$\dot{a}_i(t) = -\frac{1}{\tau_i} a_i(t) + \frac{1}{\tau_i} \beta_i(t) \tag{2.3}$$

where the dot notation represents the derivative with respect to time, τ_i is the engine time constant of vehicle i, and β_i is the auxiliary input signal for vehicle i. By taking the parameters of the leader as reference, and given that the acceleration of the leader is zero and velocity is constant [7, 14, 38, 40, 41], equations (2.1)-(2.3) can be rewritten in the following form:

$$\Delta\dot{x}_i(t) = \Delta v_i(t) \tag{2.4}$$

$$\Delta\dot{v}_i(t) = \Delta a_i(t) \tag{2.5}$$

$$\Delta\dot{a}_i(t) = -\frac{1}{\tau_i} \Delta a_i(t) + \frac{1}{\tau_i} \beta_i(t) \tag{2.6}$$

where Δx_i represents the difference between the position of vehicle i and the position of the leader ($\Delta x_i = x_i - x_0$), Δv_i represents the difference in velocity of vehicle i and the leader ($\Delta v_i = v_i - v_0$), and Δa_i represents the difference in acceleration of vehicle i and the leader ($\Delta a_i = a_i - a_0$). According to the literature, the auxiliary input signal $\beta_i(t)$ in (2.3) and (2.6) for any follower vehicle i can be obtained using the following equation [38]:

$$\beta_i(t) = -\sum_{j \in I_i} K_i \left[\Delta x_i(t) - \Delta x_j(t) - d_{ij}(t)\right] + B_i \left[\Delta v_i(t) - \Delta v_j(t)\right] + H_i \left[\Delta a_i(t) - \Delta a_j(t)\right] \tag{2.7}$$

where K_i, B_i and H_i are the control gains of the position, velocity and acceleration of vehicle i, respectively. Furthermore, d_{ij} denotes the desired distance between any two vehicles i and j in the platoon, which can be derived using:

$$d_{ij} = -\text{sgn}(i-j) \sum_{k=\min(i,j)}^{\max(i,j)-1} (L_k + d_k^{k+1}) \tag{2.8}$$

Here sgn(.) denotes the sign function [38]. Moreover, in the context of the adopted IFT, set I_i in (2.7) denotes the vehicles in the platoon that send information to vehicle i. For instance, if vehicle 1 receives information from the leader (i.e. vehicle 0), vehicle 2, and

vehicle 3, then $I_1 = \{0, 2, 3\}$.

By placing (2.7) for $\beta_i(t)$ in (2.6) and simplifying the resultant equation the following expression is obtained:

$$\Delta\dot{a}_i(t) = -\frac{C_i K_i}{\tau_i}\Delta x_i(t) - \frac{C_i B_i}{\tau_i}\Delta v_i(t) - \frac{1 + C_i H_i}{\tau_i}\Delta a_i(t) +$$

$$\frac{K_i}{\tau_i}\sum_{j\in I_i}\Delta x_j(t) + \frac{B_i}{\tau_i}\sum_{j\in I_i}\Delta v_j(t) + \frac{H_i}{\tau_i}\sum_{j\in I_i}\Delta a_j(t) + \frac{K_i}{\tau_i}\sum_{j\in I_i} d_{ij}(t) \tag{2.9}$$

where C_i represents the cardinality of set I_i.

These equations lay the foundation for subsequent analysis, enabling the extension of insights to encompass the behavior of the entire platoon as a unified system.

2.2 State-Space Modeling of an Attack and Fault Free Platoon

In this section, the development of the state-space model for a platoon operating without attacks or faults is undertaken. This model represents a significant milestone in the investigation, providing the foundation for the subsequent state-space models incorporating attacks and faults.

The state-space model for an attack-free platoon is obtained by expressing (2.4), (2.5), and (2.9) for all the vehicles in the platoon in a matrix form:

$$\dot{\mathbb{X}}(t) = \underbrace{\begin{bmatrix} Z_{n\times n} & I_{n\times n} & Z_{n\times n} \\ Z_{n\times n} & Z_{n\times n} & I_{n\times n} \\ \Xi & \Omega & \Lambda \end{bmatrix}}_{\mathbb{A}} \mathbb{X}(t) + \underbrace{\begin{bmatrix} Z_{n\times n} \\ Z_{n\times n} \\ I_{n\times n} \end{bmatrix}}_{\mathbb{B}} \mathbb{U}(t) \tag{2.10}$$

In this model, the state vector $\mathbb{X}(t)$ represents the states of follower vehicles 1 to n within the platoon and is defined as follows:

$$\mathbb{X}(t) = [\Delta x_n,\ \Delta x_{n-1},\ \cdots,\ \Delta x_1,\ \Delta v_n,\ \Delta v_{n-1},\ \cdots,\ \Delta v_1,$$

$$\Delta a_n,\ \Delta a_{n-1},\ \cdots,\ \Delta a_1]^T \tag{2.11}$$

Additionally, $\mathbb{U}(t)$ is the input vector, which is defined as:

$$\mathbb{U}(t) = \left[\frac{K_n}{\tau_n} \sum_{j \in I_n} d_{nj},\ \frac{K_{n-1}}{\tau_{n-1}} \sum_{j \in I_{n-1}} d_{(n-1)j}\ \cdots\ \frac{K_1}{\tau_1} \sum_{j \in I_1} d_{1j} \right]^T \tag{2.12}$$

The sub-matrices Z and I in the state matrix $\mathbb{A}$ and input matrix $\mathbb{B}$ are the zero matrix (consisting of all zeros) and the identity matrix of dimensions of $n \times n$, respectively. The remaining sub-matrices of $\mathbb{A}$, namely Ξ, Ω, and Λ, are constructed using a binary function S_j^n. This function takes the value of one if vehicle j is in the set I_n, and zero otherwise:

$$S_j^n = \begin{cases} 1, & \text{if } j \in I_n \\ 0, & \text{otherwise} \end{cases} \tag{2.13}$$

With this definition, the sub-matrices Ξ, Ω, and Λ can be characterized as follows:

$$\Xi = \begin{bmatrix} -\frac{C_n K_n}{\tau_n} & \frac{K_n}{\tau_n} S_{n-1}^n & \cdots & \frac{K_n}{\tau_n} S_1^n \\ \frac{K_{n-1}}{\tau_{n-1}} S_n^{n-1} & -\frac{C_{n-1} K_{n-1}}{\tau_{n-1}} & \cdots & \frac{K_{n-1}}{\tau_{n-1}} S_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{K_1}{\tau_1} S_n^1 & \frac{K_1}{\tau_1} S_{n-1}^1 & \cdots & -\frac{C_1 K_1}{\tau_1} \end{bmatrix} \tag{2.14}$$

$$\Omega = \begin{bmatrix} -\frac{C_n B_n}{\tau_n} & \frac{B_n}{\tau_n} S_{n-1}^n & \cdots & \frac{B_n}{\tau_n} S_1^n \\ \frac{B_{n-1}}{\tau_{n-1}} S_n^{n-1} & -\frac{C_{n-1} B_{n-1}}{\tau_{n-1}} & \cdots & \frac{B_{n-1}}{\tau_{n-1}} S_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{B_1}{\tau_1} S_n^1 & \frac{B_1}{\tau_1} S_{n-1}^1 & \cdots & -\frac{C_1 B_1}{\tau_1} \end{bmatrix} \tag{2.15}$$

$$\Lambda = \begin{bmatrix} -\frac{1+C_n H_n}{\tau_n} & \frac{H_n}{\tau_n} S_{n-1}^n & \cdots & \frac{H_n}{\tau_n} S_1^n \\ \frac{H_{n-1}}{\tau_{n-1}} S_n^{n-1} & -\frac{1+C_{n-1} H_{n-1}}{\tau_{n-1}} & \cdots & \frac{H_{n-1}}{\tau_{n-1}} S_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{H_1}{\tau_1} S_n^1 & \frac{H_1}{\tau_1} S_{n-1}^1 & \cdots & -\frac{1+C_1 H_1}{\tau_1} \end{bmatrix} \tag{2.16}$$

To fully represent the state-space model of the platoon, it is important to define output equations alongside the state equations. These output equations determine the parameters that serve as the outputs of the state-space model. When selecting outputs, certain criteria should be considered: 1) they must be physically measurable, 2) they should be readily available, and 3) they can be mathematically described as linear functions of the states and inputs. In this context, all system states are selected as outputs since they are shared among the vehicles through the communication system. As a result, the output equation of the state-space model can be expressed as:

$$\mathbb{Y}(t) = C\mathbb{X}(t) \tag{2.17}$$

Here, $\mathbb{Y}(t)$ represents the output vector, and C is the output matrix, which is an identity matrix of dimensions $3n \times 3n$.

The continuous-time state-space model represented by (2.10) and (2.17) requires discretization for numerical analysis. To achieve this, the state matrix $\mathbb{A}$ and input matrix $\mathbb{B}$ must be discretized using the following equations:

$$A = e^{\mathbb{A} \times t_d} \tag{2.18}$$

$$B = \int_{x=0}^{t_d} e^{(A \times x)} \, \mathbb{B} \, dx \tag{2.19}$$

where t_d represents the discretization time-step [42] and the integral in equation (2.19) accumulates the effects of the matrix A over the entire discretization time step t_d, allowing for the discretization of matrix B. Consequently, the discrete-time state-space model of the platoon can be characterized as:

$$\begin{cases} X[k+1] = AX[k] + BU[k] \\ Y[k] = CX[k] \end{cases} \tag{2.20}$$

Here, $X[k] \in \mathbb{R}^{3n}$, $U[k] \in \mathbb{R}^{n}$, and $Y[k] \in \mathbb{R}^{3n}$ represent the state, input, and output vectors at time step k, respectively.

2.3 State-Space Modeling of a Platoon under Attacks

This section presents the state-space equation of a platoon of vehicles during FDIAs. The model is developed from the perspective of vehicle i, assuming that its own information obtained from local sensors is secure and unattacked. However, information received from other vehicles, including the leader, is vulnerable to attacks. To capture FDIAs, attack inputs $\mu_{x,k}$, $\mu_{v,k}$, and $\mu_{a,k}$ are introduced for each vehicle k in the platoon, except for vehicle i. These attack inputs represent changes in the position, velocity, and acceleration of the attacked vehicle k caused by FDIAs. Since the leader has zero acceleration, it is not susceptible to acceleration attacks (i.e., $\mu_{a,0} = 0$). By incorporating these attack inputs into equations (2.4), (2.5), and (2.9), the equations for vehicle i are modified as follows:

$$\Delta \dot{x}_i(t) = v_i(t) - (v_0(t) + \mu_{v,0}) = \Delta v_i(t) - \mu_{v,0} \tag{2.21}$$

$$\Delta \dot{v}_i(t) = a_i(t) - (a_0(t) + \mu_{a,0}) = \Delta a_i(t) \tag{2.22}$$

$$\Delta \dot{a}_i(t) = \frac{C_i K_i}{\tau_i} \Delta x_i(t) \quad \frac{C_i B_i}{\tau_i} \Delta v_i(t) \quad \frac{1 + C_i H_i}{\tau_i} \Delta a_i(t) +$$

$$\frac{K_i}{\tau_i}\sum_{j\in I_i}\Delta x_j(t)+\frac{B_i}{\tau_i}\sum_{j\in I_i}\Delta v_j(t)+\frac{H_i}{\tau_i}\sum_{j\in I_i}\Delta a_j(t)+\frac{K_i}{\tau_i}\sum_{j\in I_i}\mu_{x,j}+$$
$$\frac{B_i}{\tau_i}\sum_{j\in I_i}\mu_{v,j}+\frac{H_i}{\tau_i}\sum_{j\in I_i}\mu_{a,j}+\frac{K_i}{\tau_i}\sum_{j\in I_i}d_{ij}(t) \tag{2.23}$$

The state equations for vehicle $k \neq i$ during FDIAs are also formulated in a similar manner. These equations account for the impact of attack inputs $\mu_{x,k}$, $\mu_{v,k}$, and $\mu_{a,k}$ on the position, velocity, and acceleration of vehicle k:

$$\Delta\dot{x}_k(t) = (v_k+\mu_{v,k})-(v_0+\mu_{v,0}) = \Delta v_k(t)+\mu_{v,k}-\mu_{v,0} \tag{2.24}$$

$$\Delta\dot{v}_k(t) = (a_k+\mu_{a,k})-a_0 = \Delta a_k(t)+\mu_{a,k} \tag{2.25}$$

$$\Delta\dot{a}_k(t) = \frac{C_kK_k}{\tau_k}\Delta x_k(t)\quad\frac{C_kB_k}{\tau_k}\Delta v_k(t)\quad\frac{1+C_kH_k}{\tau_k}\Delta a_k(t)+$$
$$\frac{K_k}{\tau_k}\sum_{j\in I_k}\Delta x_j(t)+\frac{B_k}{\tau_k}\sum_{j\in I_k}\Delta v_j(t)+\frac{H_k}{\tau_k}\sum_{j\in I_k}\Delta a_j(t)\quad\frac{C_kK_k}{\tau_k}\mu_{x,k}$$
$$\frac{C_kB_k}{\tau_k}\mu_{v,k}\quad\frac{1+C_kH_k}{\tau_k}\mu_{a,k}+\frac{K_k}{\tau_k}\sum_{j\in I_k}\mu_{x,j}+\frac{B_k}{\tau_k}\sum_{j\in I_k}\mu_{v,j}+$$
$$\frac{H_k}{\tau_k}\sum_{j\in I_k}\mu_{a,j}+\frac{K_k}{\tau_k}\sum_{j\in I_k}d_{kj}(t) \tag{2.26}$$

Writing the state equations (2.21)-(2.26) in a matrix form yields the following state-space model for a platoon of vehicles under FDIAs:

$$\dot{\mathbb{X}}(t) = \mathbb{A}\mathbb{X}(t)+\mathbb{B}\mathbb{U}(t)+\underbrace{\begin{bmatrix} Z_{n\times n} & \rho & Z_{n\times(n-1)} \\ Z_{n\times n} & Z_{n\times n} & \psi \\ \phi & \varphi & \Phi \end{bmatrix}}_{\theta}\mu(t) \tag{2.27}$$

The first two terms on the right-hand side of (2.27) remain unchanged from the attack-free state-space model given by equation (2.10). The third term introduces the impact of FDIAs on the states, and it is expressed as the product of the attack vector $\mu(t)$ and the attack matrix θ. The sub-matrices of θ are defined in equations (2.28) to (2.32).

$$\rho = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & -1 \end{bmatrix}_{n\times n} \tag{2.28}$$

$$\psi = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{bmatrix}_{n \times n-1} \tag{2.29}$$

$$\phi = \begin{bmatrix} -\frac{C_n K_n}{\tau_n} & \frac{K_n}{\tau_n} S_{n-1}^n & \dots & \frac{K_n}{\tau_n} S_{i+1}^n & \frac{K_n}{\tau_n} S_{i-1}^n & \dots & \frac{K_n}{\tau_n} S_1^n & \frac{K_n}{\tau_n} S_0^n \\ \frac{K_{n\ 1}}{\tau_{n\ 1}} S_n^{n-1} & -\frac{C_{n\ 1} K_{n\ 1}}{\tau_{n\ 1}} & \dots & \frac{K_{n\ 1}}{\tau_{n\ 1}} S_{i+1}^{n-1} & \frac{K_{n\ 1}}{\tau_{n\ 1}} S_{i-1}^{n-1} & \dots & \frac{K_{n\ 1}}{\tau_{n\ 1}} S_1^{n-1} & \frac{K_{n\ 1}}{\tau_{n\ 1}} S_0^{n-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{K_{i+1}}{\tau_{i+1}} S_n^{i+1} & \frac{K_{i+1}}{\tau_{i+1}} S_{n-1}^{i+1} & \dots & -\frac{C_{i+1} K_{i+1}}{\tau_{i+1}} & \frac{K_{i+1}}{\tau_{i+1}} S_{i-1}^{i+1} & \dots & \frac{K_{i+1}}{\tau_{i+1}} S_1^{i+1} & \frac{K_{i+1}}{\tau_{i+1}} S_0^{i+1} \\ \frac{K_i}{\tau_i} S_n^i & \frac{K_i}{\tau_i} S_{n-1}^i & \dots & \frac{K_i}{\tau_i} S_{i+1}^i & \frac{K_i}{\tau_i} S_{i-1}^i & \dots & \frac{K_i}{\tau_i} S_1^i & \frac{K_i}{\tau_i} S_0^i \\ \frac{K_{i\ 1}}{\tau_{i\ 1}} S_n^{i-1} & \frac{K_{i\ 1}}{\tau_{i\ 1}} S_{n-1}^{i-1} & \dots & \frac{K_{i\ 1}}{\tau_{i\ 1}} S_{i+1}^{i-1} & -\frac{C_{i\ 1} K_{i\ 1}}{\tau_{i\ 1}} & \dots & \frac{K_{i\ 1}}{\tau_{i\ 1}} S_1^{i-1} & \frac{K_{i\ 1}}{\tau_{i\ 1}} S_0^{i-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{K_1}{\tau_1} S_n^1 & \frac{K_1}{\tau_1} S_{n-1}^1 & \dots & \frac{K_1}{\tau_1} S_{i+1}^1 & \frac{K_1}{\tau_1} S_{i-1}^1 & \dots & -\frac{C_1 K_1}{\tau_1} & \frac{K_1}{\tau_1} S_0^1 \end{bmatrix}_{n \times n} \tag{2.30}$$

$$\varphi = \begin{bmatrix} -\frac{C_n B_n}{\tau_n} & \frac{B_n}{\tau_n} S_{n-1}^n & \dots & \frac{B_n}{\tau_n} S_{i+1}^n & \frac{B_n}{\tau_n} S_{i-1}^n & \dots & \frac{B_n}{\tau_n} S_1^n & \frac{B_n}{\tau_n} S_0^n \\ \frac{B_{n\ 1}}{\tau_{n\ 1}} S_n^{n-1} & -\frac{C_{n\ 1} B_{n\ 1}}{\tau_{n\ 1}} & \dots & \frac{B_{n\ 1}}{\tau_{n\ 1}} S_{i+1}^{n-1} & \frac{B_{n\ 1}}{\tau_{n\ 1}} S_{i-1}^{n-1} & \dots & \frac{B_{n\ 1}}{\tau_{n\ 1}} S_1^{n-1} & \frac{B_{n\ 1}}{\tau_{n\ 1}} S_0^{n-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{B_{i+1}}{\tau_{i+1}} S_n^{i+1} & \frac{B_{i+1}}{\tau_{i+1}} S_{n-1}^{i+1} & \dots & -\frac{C_{i+1} B_{i+1}}{\tau_{i+1}} & \frac{B_{i+1}}{\tau_{i+1}} S_{i-1}^{i+1} & \dots & \frac{B_{i+1}}{\tau_{i+1}} S_1^{i+1} & \frac{B_{i+1}}{\tau_{i+1}} S_0^{i+1} \\ \frac{B_i}{\tau_i} S_n^i & \frac{B_i}{\tau_i} S_{n-1}^i & \dots & \frac{B_i}{\tau_i} S_{i+1}^i & \frac{B_i}{\tau_i} S_{i-1}^i & \dots & \frac{B_i}{\tau_i} S_1^i & \frac{B_i}{\tau_i} S_0^i \\ \frac{B_{i\ 1}}{\tau_{i\ 1}} S_n^{i-1} & \frac{B_{i\ 1}}{\tau_{i\ 1}} S_{n-1}^{i-1} & \dots & \frac{B_{i\ 1}}{\tau_{i\ 1}} S_{i+1}^{i-1} & -\frac{C_{i\ 1} B_{i\ 1}}{\tau_{i\ 1}} & \dots & \frac{B_{i\ 1}}{\tau_{i\ 1}} S_1^{i-1} & \frac{B_{i\ 1}}{\tau_{i\ 1}} S_0^{i-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{B_1}{\tau_1} S_n^1 & \frac{B_1}{\tau_1} S_{n-1}^1 & \dots & \frac{B_1}{\tau_1} S_{i+1}^1 & \frac{B_1}{\tau_1} S_{i-1}^1 & \dots & -\frac{C_1 B_1}{\tau_1} & \frac{B_1}{\tau_1} S_0^1 \end{bmatrix}_{n \times n} \tag{2.31}$$

$$\Phi = \begin{bmatrix} -\frac{1+C_n H_n}{\tau_n} & \frac{H_n}{\tau_n} S_{n-1}^n & \dots & \frac{H_n}{\tau_n} S_{i+1}^n & \frac{H_n}{\tau_n} S_{i-1}^n & \dots & \frac{H_n}{\tau_n} S_1^n \\ \frac{H_{n\ 1}}{\tau_{n\ 1}} S_n^{n-1} & -\frac{1+C_{n\ 1} H_{n\ 1}}{\tau_{n\ 1}} & \dots & \frac{H_{n\ 1}}{\tau_{n\ 1}} S_{i+1}^{n-1} & \frac{H_{n\ 1}}{\tau_{n\ 1}} S_{i-1}^{n-1} & \dots & \frac{H_{n\ 1}}{\tau_{n\ 1}} S_1^{n-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{H_{i+1}}{\tau_{i+1}} S_n^{i+1} & \frac{H_{i+1}}{\tau_{i+1}} S_{n-1}^{i+1} & \dots & -\frac{1+C_{i+1} H_{i+1}}{\tau_{i+1}} & \frac{H_{i+1}}{\tau_{i+1}} S_{i-1}^{i+1} & \dots & \frac{H_{i+1}}{\tau_{i+1}} S_1^{i+1} \\ \frac{H_i}{\tau_i} S_n^i & \frac{H_i}{\tau_i} S_{n-1}^i & \dots & \frac{H_i}{\tau_i} S_{i+1}^i & \frac{H_i}{\tau_i} S_{i-1}^i & \dots & \frac{H_i}{\tau_i} S_1^i \\ \frac{H_{i\ 1}}{\tau_{i\ 1}} S_n^{i-1} & \frac{H_{i\ 1}}{\tau_{i\ 1}} S_{n-1}^{i-1} & \dots & \frac{H_{i\ 1}}{\tau_{i\ 1}} S_{i+1}^{i-1} & -\frac{1+C_{i\ 1} H_{i\ 1}}{\tau_{i\ 1}} & \dots & \frac{H_{i\ 1}}{\tau_{i\ 1}} S_1^{i-1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{H_1}{\tau_1} S_n^1 & \frac{H_1}{\tau_1} S_{n-1}^1 & \dots & \frac{H_1}{\tau_1} S_{i+1}^1 & \frac{H_1}{\tau_1} S_{i-1}^1 & \dots & -\frac{1+C_1 H_1}{\tau_1} \end{bmatrix}_{n \times n-1} \tag{2.32}$$

Additionally, the attack vector $\mu(t)$ in (2.27) is defined as follows

$$\mu(t) = \begin{bmatrix} \mu_x & \mu_v & \mu_a \end{bmatrix}^T \tag{2.33}$$

where

$$\mu_x = \begin{bmatrix} \mu_{x,n} & \dots & \mu_{x,i+1} & \mu_{x,i-1} & \dots & \mu_{x,0} \end{bmatrix}^T \tag{2.34}$$

$$\mu_v = \begin{bmatrix} \mu_{v,n} & \dots & \mu_{v,i+1} & \mu_{v,i-1} & \dots & \mu_{v,0} \end{bmatrix}^T \tag{2.35}$$

$$\mu_a = \begin{bmatrix} \mu_{a,n} & \dots & \mu_{a,i+1} & \mu_{a,i-1} & \dots & \mu_{a,1} \end{bmatrix}^T \tag{2.36}$$

Given that FDIAs do not alter the output equation of the platoon, (2.17) can be utilized as the output equation for under-attack platoons as well.

In the final step, to perform numerical analysis, the obtained state-space representation shown in (2.27) and (2.17) needs to be discretized. For the discretization of matrices $\mathbb{A}$ and $\mathbb{B}$, equations (2.18) and (2.19) can be employed, respectively. Additionally, the matrix θ should be discretized with a time-step of t_d using the following equation:

$$\Theta = \int_{x=0}^{t_d} e^{(A \times x)} \; \theta \, dx \tag{2.37}$$

By following these steps, the discrete-time state-space model of the platoon with FDIA can be described as follows:

$$\begin{cases} X[k+1] = AX[k] + BU[k] + \Theta M[k] \\ Y[k] = CX[k] \end{cases} \tag{2.38}$$

where $M[k] \in R^{3n-1}$ is the discretized attack vector.

2.4 State-Space Modeling of a Platoon under Faults

The numerous hardware and software components of smart vehicles may inevitably lead to faults or errors in the measurement of the vehicle's position, velocity, and/or acceleration. As this information is exchanged within the platoon, any inaccuracies in the actual vehicle's position, velocity, and/or acceleration could potentially cause catastrophic failures in the platooning system. In this section, a model is developed to represent faults in the position, velocity, and acceleration of a perspective vehicle, denoted as $f_{x,i}$, $f_{v,i}$, and $f_{a,i}$, respectively. By incorporating these fault inputs into the state equation (2.10), the resulting state-space model for the platoon under a fault can

be represented as follows:

$$\dot{\mathbb{X}}(t) = \mathbb{A}\mathbb{X}(t) + \mathbb{B}\mathbb{U}(t) + \mathbb{F}\underbrace{\begin{bmatrix} f_{x,i} & f_{v,i} & f_{a,i} \end{bmatrix}^T}_{\mathbb{f}(t)} \tag{2.39}$$

Here $\mathbb{f}(t) \in \mathbb{R}^3$ is the fault vector; and $\mathbb{F}$ is a $3n \times 3$ matrix that includes only the columns of matrix $\mathbb{A}$ associated with the position, velocity, and acceleration of vehicle i. The output equation of the state-space model remains unchanged from the fault-free model, as expressed in (2.17).

Following a similar approach as in the fault-free model, the discrete-time state-space model of the platoon under faults can be represented as:

$$\begin{cases} X[k+1] = AX[k] + Bu[k] + Ff[k] \\ Y[k] = CX[k] \end{cases} \tag{2.40}$$

in which, $f[k] \in R^3$ is the fault vector at time step k, and F is a discrete-time version of the fault matrix $\mathbb{F}$.

Chapter 3

State Estimation for Vehicle Platoons using Unknown Input Observers

State estimation using UIOs is a technique employed to estimate the internal states of a dynamic system, such as the positions, velocities, or other relevant variables, when some inputs or disturbances are not directly measurable or known. The UIO is designed as an observer that takes the system's measurable outputs and control inputs as inputs and generates estimates of the unmeasured internal states as outputs.

Hence, this chapter presents the development of a UIO to estimate the states of the platoon in the presence of FDIAs and faults, which are not known beforehand. To ensure the UIO's adaptability within both the attack and fault frameworks, the unknown input matrix λ serves as a representation encompassing both the attack input matrix Θ in equation (2.38) and the fault input matrix F in equation (2.40). Similarly, the unknown input vector Λ represents both the attack input vector M in equation (2.38) and the fault input vector f in equation (2.40). The symbols λ and Λ allow for a unified representation of attack and fault inputs, facilitating a consistent approach in upcoming equations in this chapter. This UIO will play a critical role in mitigating the effects of FDIAs and faults on the platoon's operation, safeguarding its security and reliability. By providing reliable state estimates even in the presence of unknown inputs, the UIO enhances the platoon's ability to maintain safe inter-vehicle distances and execute coordinated maneuvers effectively.

The UIO utilizes a fixed window of $\alpha+1$ time steps to estimate the states of the platoon at time step k, incorporating the system's outputs from time steps k to $k+\alpha$, denoted

as $Y[k], Y[k+1], ..., Y[k+\alpha]$ [43]. Consequently, the UIO estimates the system's states with a delay of α time steps. The specific value of α depends on the system's parameters, which will be further explained later. By incorporating this fixed delay, the UIO's error tends to approach zero even in the presence of unknown inputs, such as attacks and faults.

In the first step, the outputs of the system from time steps k to $k+\alpha$ are recursively formulated using the state-space equations (2.38) and (2.40):

$$\begin{aligned}
Y[k] &= CX[k] \\
Y[k+1] &= CX[k+1] = C(AX[k] + Bu[k] + \lambda\Lambda[k]) = CAX[k] + CBu[k] + C\lambda\Lambda[k] \\
Y[k+2] &= CX[k+2] = C(A(AX[k] + Bu[k] + \lambda\Lambda[k]) + Bu[k+1] + \lambda\Lambda[k+1]) \\
&= CA^2X[k] + CABu[k] + CA\lambda\Lambda[k] + CBu[k+1] + C\lambda\Lambda[k+1] \\
&\vdots \\
Y[k+\alpha] &= CX[k+\alpha] = CA^{\alpha}X[k] + CB\sum_{j=0}^{\alpha-1} A^{\alpha-1-j}u[k+j] + C\lambda\sum_{j=0}^{\alpha-1} A^{\alpha-1-j}\Lambda[k+j]
\end{aligned} \tag{3.1}$$

This recursive formulation allows for the representation of the output vector as follows:

$$Y[k:k+\alpha] = O_\alpha X[k] + J'_\alpha U[k:k+\alpha] + J_\alpha \Lambda[k:k+\alpha] \tag{3.2}$$

where

$$Y[k:k+\alpha] = \begin{bmatrix} Y[k]^T, & Y[k+1]^T, & \cdots, & Y[k+\alpha]^T \end{bmatrix}^T \tag{3.3}$$

$$J'_\alpha = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ CB & 0 & 0 & \cdots & 0 \\ CAB & CB & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ CA^{\alpha-1}B & CA^{\alpha-2}B & \cdots & \cdots & 0 \end{bmatrix} \tag{3.4}$$

$$J_\alpha = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ C\lambda & 0 & 0 & \cdots & 0 \\ CA\lambda & C\lambda & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ CA^{\alpha-1}\lambda & CA^{\alpha-2}\lambda & \cdots & \cdots & 0 \end{bmatrix} \tag{3.5}$$

$$O_\alpha = \begin{bmatrix} C^T & (CA)^T & (CA^2)^T & \ldots & (CA^{\alpha})^T \end{bmatrix}^T \tag{3.6}$$

$$U[k:k+\alpha] = \begin{bmatrix} U[k]^T, & U[k+1]^T, & \ldots, & U[k+\alpha]^T \end{bmatrix}^T \tag{3.7}$$

$$\Lambda[k:k+\alpha] = \begin{bmatrix} \Lambda[k]^T, & \Lambda[k+1]^T \ldots & \Lambda[k+\alpha]^T \end{bmatrix}^T \tag{3.8}$$

Therefore, by combining the contributions of internal states, control inputs, and unknown inputs over a time window, the system's output vector is computed.

As shown in [44], a UIO can estimate the system's states at time step $k+1$ using the following equation:

$$\hat{X}[k+1] = A\hat{X}[k] + Bu[k] + F\Big[Y[k:k+\alpha] - O_\alpha \hat{X}[k] - J'_\alpha u[k:k+\alpha]\Big] \tag{3.9}$$

where $\hat{X}[k]$ is the estimate of $X[k]$ and F is the UIO's gain. To ensure accurate estimation, the UIO's gain F should be designed in a way that the UIO's error ($e[k+1] = \hat{X}[k+1] - X[k+1]$) approaches zero as k approaches infinity. This mechanism illustrates how the UIO projects the system's states to the subsequent time step ($[k+1]$) based on the available information at the current time step ($[k]$), facilitating robust state estimation. Additionally, F should ensure the stability of the UIO. To design F, the UIO's error $e[k+1]$ should be formulated using equations (2.38), (3.2), and (3.9). This results in the following expression for the error:

$$e[k+1] = \underbrace{(A - FO_\alpha)}_{A'} e[k] + FJ_\alpha \Lambda[k:k+\alpha] - \lambda\Lambda[k] \tag{3.10}$$

In order for the error $e[k+1]$ to approach zero in the presence of attacks and faults as $k \to \infty$, the sum of the last two terms on the right-hand side of equation (3.10) must be zero. To meet this condition, F can be designed such that FJ_α satisfies the following relation:

$$FJ_\alpha = \begin{bmatrix} \lambda & Z \end{bmatrix} \tag{3.11}$$

where Z is a zero matrix with dimensions $3n \times \alpha(3n-1)$. By placing the formula just found for FJ_α into (3.10) and after some simplifications, (3.10) can be written as:

$$e[k+1] = A'e[k] + \lambda\Lambda[k] + Z\Lambda[k+1:k+\alpha] - \lambda\Lambda[k] = A'e[k] \tag{3.12}$$

that satisfies the error objective.

As shown in [44], there exists an F that satisfies (3.11) if

$$\operatorname{rank}(J_\alpha) - \operatorname{rank}(J_{\alpha-1}) = 3n - 1 \tag{3.13}$$

where $3n-1$ denotes the size of Λ vector, and $J_{\alpha-1}$ can be found using J_α in (3.5):

$$J_{\alpha-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ C\lambda & 0 & 0 & \cdots & 0 \\ CA\lambda & C\lambda & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ CA^{\alpha-2}\lambda & CA^{\alpha-3}\lambda & \cdots & \cdots & 0 \end{bmatrix} \tag{3.14}$$

Equation (3.13) represents a necessary condition for constructing an accurate UIO for the given system. If this condition is not fulfilled, it becomes impossible to estimate the

system's states without knowledge of its unknown inputs. For a platoon of vehicles, it can be demonstrated that a minimum time delay of $\alpha = 2$ satisfies this condition. The proof involves demonstrating that condition (3.13) holds for the continuous-time model of a general platoon, which encompasses various IFTs. This is achieved by substituting matrices $\mathbb{A}$, $\mathbb{B}$, and C from equations (2.10) and (2.17) into (3.13) and subsequently evaluating the ranks of $J_{\alpha-1}$ and J_α. According to reference [45], it is indicated that the discretized platoon model satisfies condition (3.13) if and only if the continuous platoon model does so.

As presented in [44], an F matrix in the following form can satisfy (3.11):

$$F = \begin{bmatrix} F_1 & F_2 \end{bmatrix} Q \tag{3.15}$$

where sub-matrices F_1 and F_2 have dimensions $3n \times (3n-1)(\alpha-1)$ and $3n \times (3n-1)$, respectively, and Q is a $(3n-1)\alpha \times 3n(\alpha+1)$ matrix, which can be designed to satisfy the following equation:

$$QJ_\alpha = \begin{bmatrix} Z_{11} & Z_{12} \\ I_{21} & Z_{22} \end{bmatrix} \tag{3.16}$$

where Z_{11}, Z_{12}, and Z_{22} are zero matrices with dimensions $(\alpha-1)(3n-1) \times (3n-1)$, $(\alpha-1)(3n-1) \times \alpha(3n-1)$, and $3(n-1) \times \alpha(3n-1)$, respectively. Additionally, I_{21} is an identity matrix with dimensions $3(n-1) \times 3(n-1)$.

By placing the formula for F from (3.15) into (3.11) and substituting QJ_α with the right-hand side of (3.16), the following expression is obtained:

$$F_2 = \lambda \tag{3.17}$$

By choosing a Q that satisfies (3.16) and setting F_2 as λ, the accuracy condition in equation (3.11) is fulfilled. It is noted that while Q and F_2 contribute to meeting the accuracy condition of the UIO, F_1 does not play a role in this aspect. However, F_1 is significant in satisfying another crucial condition—the stability condition of the UIO—which will be discussed next.

The stability of the UIO depends on the location of the eigenvalues of the matrix A' in (3.10) in the complex plane. If all eigenvalues are within the unit circle, the UIO is considered stable [42]. To assess the stability of the UIO, F from (3.15) is inserted into A', and the resulting matrix QO_α is partitioned into two sub-matrices: S_1 and S_2. This yields the transformation of A' as shown below:

$$A' = A - F_1 S_1 - \lambda S_2 \tag{3.18}$$

where

$$\begin{bmatrix} S_1^T & S_2^T \end{bmatrix}^T = QO_\alpha \tag{3.19}$$

Based on [46], the existence of an F_1 that stabilizes the eigenvalues of A' in (3.18) is contingent upon the satisfaction of the following equation for every complex number z with a magnitude greater than or equal to one:

$$\operatorname{rank}\begin{pmatrix} A - zI_{3n} & \lambda \\ C & Z_{3n\times n} \end{pmatrix} = 4n \tag{3.20}$$

Both conditions (3.13) and (3.20) are crucial for the development of a stable and accurate UIO. It can be proven that condition (3.20) is satisfied when all the eigenvalues of A are in unit circle and condition (3.13) is met. As a result, (3.20) is also met for a platoon of vehicles if $\alpha = 2$. Therefore, there exists an F_1 that stabilizes the system poles using a pole-placement method, such as the method presented in [47]. The method incorporates $3n$ desired stable eigenvalues and designs F_1 to align the eigenvalues of matrix A' with the desired ones. During the design process, the method assigns $3n$ linearly independent eigenvectors to the desired eigenvalues while aiming for an eigenvector matrix that is as well-conditioned as possible. Matrix F_1 can be determined using these eigenvalues and eigenvectors. Once F_1 is designed, the UIO can estimate the system's states at time step $k+1$ using (3.9).

3.1 Attack Detection, Identification and Mitigation

In the context of vehicle platoons, ensuring the security and reliability of the communication system is paramount. However, the presence of attacks such as FDIAs, poses significant threats to the integrity of the platoon system. To address these challenges, a comprehensive approach for detecting, identifying, and mitigating attacks is essential by building upon the state-space model developed in Section 2.3.

During an FDIA, certain elements of the attack input vector M become non-zero. Detecting attacked vehicles and identifying the potential attack inputs and their corresponding distribution matrix Θ is critical for safeguarding the platoon's operation. To achieve this, the Detection UIO$_j$ is introduced. The Detection UIO$_j$ utilizes the state-space equation of the attacked system presented in (2.38), with the removal of the attack inputs specific to vehicle j, namely $\mu_{x,j}$, $\mu_{v,j}$, and $\mu_{a,j}$, as well as the associated columns from the Θ matrix. Therefore, the state-space model for designing UIO$_j$ is as follows:

$$\begin{cases} X[k+1] = AX[k] + Bu[k] + \Theta^{(-j)}M^{(-j)}[k] \\ Y[k] = CX[k] \end{cases} \tag{3.21}$$

Here, $M^{(-j)}$ represents the remaining vector M after removing the attack inputs $\mu_{x,j}$, $\mu_{v,j}$, and $\mu_{a,j}$ associated with vehicle j, and $\Theta^{(-j)}$ is a matrix that includes all columns

of Θ except for those associated with the removed attack inputs. The UIO$_j$ designed based on (3.21) is insensitive to attacks on all vehicles in the set I_i, except for vehicle j, as these attacks are treated as unknown inputs. In fact, for UIO$_j$, the error equation in (3.10) becomes

$$e[k+1] = A'e[k] + FJ_{\alpha}^{(-j)}M^{(-j)}[k:k+\alpha] - \Theta^{(-j)}M^{(-j)}[k] \tag{3.22}$$

where $J_{\alpha}^{(-j)}$ is obtained from (3.5) by replacing Θ with $\Theta^{(-j)}$.

By following the procedure outlined in Section 3, the gain matrix F is designed to ensure that the last two terms on the right-hand side of (3.22) are equal, resulting in their cancellation. This design choice allows the error of UIO$_j$ to approach zero when facing attacks included in the $M^{(-j)}$ vector. However, it is important to note that this UIO remains sensitive to attacks specifically targeting vehicle j as the state-space model used for designing UIO$_j$ does not account for attacks against vehicle j. In cases where an attack is directed at vehicle j, an additional term is introduced to the right-hand side of (3.22) as follows:

$$e[k+1] = A'e[k] + FJ_{\alpha}^{(j)}M^{(j)}[k:k+\alpha] \tag{3.23}$$

where $M^{(j)}$ represents the attack vector that includes the attack inputs $\mu_{x,j}$, $\mu_{v,j}$, $\mu_{a,j}$ associated with vehicle j. Similarly, $\Theta^{(j)}$ is a matrix that includes all columns of Θ associated with the attack inputs of $M^{(j)}$. Additionally, $J_{\alpha}^{(j)}$ is a matrix obtained from (3.5) by replacing Θ with $\Theta^{(j)}$. This extra term in the right-hand side of (3.23) results in a deviation of the error of UIO$_j$ from zero. This error leads to a discrepancy between the estimated values by UIO$_j$ and the information received through the communication system. This discrepancy is referred to as the Residual Function (RF) of UIO$_j$ and is defined as follows:

$$r_j[k] = Y[k] - C\hat{X}[k] \tag{3.24}$$

As mentioned earlier, the RF of UIO$_j$ does not increase during attacks on vehicles other than vehicle j, as these attacks are already considered in the state-space model of UIO$_j$ as unknown inputs. Therefore, the information received from vehicle j is considered untrustworthy if the following condition is met:

$$\|r_j[k]\| \leq \delta_j \tag{3.25}$$

Here, $\|r_j[k]\|$ represents the *second norm* of the RF of UIO$_j$, and δ_j denotes the *detection threshold* for UIO$_j$. The detection threshold δ_j is a dimensionless value that takes into account non-attack disturbances, such as measurement noise and errors. To set the threshold δ_j, a practical approach involves measuring $\|r_j[k]\|$ under various conditions (e.g., different numbers of vehicles and/or IFTs) in the absence of attacks. Subsequently, δ_j is determined as the highest measured $\|r_j[k]\|$ value plus a security margin.

After detecting the attacked vehicle(s), it is crucial to identify which parameter(s) have been manipulated to mitigate the effects of the attack and prevent the compromise of the entire vehicle platoon system. To achieve this, an Identification UIO is introduced in this section. The Identification UIO is designed based on the state-space model of the attacked system presented in (2.38), which includes all potential attack inputs. The Identification UIO is capable of estimating the states of the platoon at time steps k and $k+1$ and utilizes them, along with (2.38), to estimate the elements of M using the equation:

$$\hat{M}[k] = \Theta^{\ddagger}\left(\hat{X}[k+1] - A\hat{X}[k] - BU[k]\right) \tag{3.26}$$

Here, the symbol ‡ denotes the pseudo-inverse operator. The vector $\hat{M}$ contains the estimated attack inputs, with non-zero elements indicating the manipulated parameters. In order to mitigate the attack, each estimated non-zero attack input must be subtracted from its associated received information before being used by the platoon controller.

3.2 Fault Detection, Identification and Mitigation

Further securing the platoon, this section presents the fault detection, identification, and mitigation framework designed to address equipment faults in vehicle platoons by building upon the state-space model developed in Section 2.4. To mitigate the effects of equipment faults in vehicle i, it is crucial to identify which parameter(s) (position, velocity, or acceleration) have been measured erroneously. For this purpose, vehicle i utilizes three fault detection and identification UIOs: $\text{UIO}_{x,i}$, $\text{UIO}_{v,i}$, and $\text{UIO}_{a,i}$. These UIOs are designed to detect and identify specific elements of the fault input vector F ($f_{x,i}$, $f_{v,i}$, and $f_{a,i}$) that may become nonzero due to equipment malfunction. The design of these UIOs follows a similar pattern, and the generic name $\text{UIO}_{p,i}$ is used, where p can be substituted with x, v, or a to correspond to position, velocity, or acceleration, respectively.

The $\text{UIO}_{p,i}$ is designed by removing the fault input $f_{p,i}$ from vector f and its associated columns from matrix F introduced in Section 2.4. The state-space model of $\text{UIO}_{p,i}$ is given below:

$$\begin{cases} X[k+1] = AX[k] + Bu[k] + F^{-(p,i)}f^{-(p,i)}[k] \\ Y[k] = CX[k] \end{cases} \tag{3.27}$$

Here, $f^{-(p,i)}$ represents the remaining vector f after removing $f_{p,i}$, and $F^{-(p,i)}$ is a matrix that includes all columns of F except those associated with the removed faulty input. Based on this design, $\text{UIO}_{p,i}$ is only sensitive to the specific fault ($f_{p,i}$) that it targets

but not to others. In fact, for $\text{UIO}_{p,i}$, the error formulation (3.10) becomes:

$$e[k+1] = A'e[k] + GJ_{\alpha}^{-(p,i)} f^{-(p,i)}[k:k+\alpha] - F^{-(p,i)} f^{-(p,i)}[k] \tag{3.28}$$

Here, $J_{\alpha}^{-(p,i)}$ is obtained from (3.5) by replacing F with $F^{-(p,i)}$.

This error leads to a discrepancy between the estimated value by $\text{UIO}_{p,i}$ and the corresponding measured value obtained by the faulty vehicle sensor. This discrepancy is referred to as the Residual Function (RF) of $\text{UIO}_{p,i}$ and is defined as follows:

$$r_{p,i}[k] = Y[k] - C\hat{X}[k] \tag{3.29}$$

The RF of $\text{UIO}_{p,i}$ does not increase during faults on the other two parameters since they are already accounted for as unknown inputs in the state-space model of this particular UIO. Hence, the measured parameter of vehicle i is considered untrustworthy if the following condition is met:

$$\|r_{p,i}[k]\| \leq \delta_{p,i} \tag{3.30}$$

Here, $\|r_{p,i}[k]\|$ represents the second norm of the RF of $\text{UIO}_{p,i}$, and $\delta_{p,i}$ denotes the detection threshold for the UIO. The detection threshold $\delta_{p,i}$ is a dimensionless value that accounts disturbances other than faults such as noise. To establish $\delta_{p,i}$, a practical approach involves measuring $\|r_{p,i}[k]\|$ in various scenarios where no faults are present. The threshold $\delta_{p,i}$ is then set as the maximum measured $\|r_{p,i}[k]\|$ value, augmented by a security margin.

In order to identify and mitigate the fault, the states of the platoon at time steps k and $k+1$ are estimated using the state-space model (2.38) with all potential fault inputs. The estimated states are then utilized along with (2.38) to estimate the elements of f using the equation:

$$\hat{f}[k] = F^{\ddagger}\left(\hat{X}[k+1] - A\hat{X}[k] - BU[k]\right) \tag{3.31}$$

Here, the symbol ‡ denotes the pseudo-inverse operator. The vector $\hat{f}$ contains the estimated faulty inputs, with non-zero elements indicating the faulty parameters. In order to mitigate the fault, each estimated non-zero faulty input must be subtracted from its associated measured information before being used by the platoon controller.

Chapter 4

Performance Analysis

This chapter presents the simulation results analyzing the performance of the proposed attack detection, identification, and mitigation frameworks, as well as the fault detection, identification and identification framework. To evaluate the system under various conditions, six simulation scenarios are considered for attack detection, identification, and mitigation, along with three scenarios for fault detection and identification. Each scenario involves a different IFT, as depicted in Fig. 1.1.

To maintain consistency and avoid unnecessary complexities, the control gains and engine time constant are assumed to be the same for all vehicles: $K = 3$, $B = 5$, $H = 1$, and $\tau = 0.5$ [38]. The parameters of the lead and following vehicles are listed in Table 4.1, with specific values selected from the table based on the corresponding scenario being described. These settings allow for a comprehensive evaluation of the proposed frameworks' effectiveness in different platoon configurations and scenarios.

TABLE 4.1: Specifications of platoon vehicles.

Vehicle (i)	Leader (0)	1	2	3	4	5	6
L_i (m)	4	4.4	3.8	5.2	4.4	3.8	4.0
Initial x_i (m)	0	-8	-20	-40	-80	-100	-120
Initial v_i (m/s)	25	27.8	22.2	19.4	27.8	22.2	27.8
Initial a_i (m/s^2)	0	2.0	3.0	2.0	2.0	3.0	3.0
d_i^{i+1} (m)	-	3.0	4.0	4.0	3.0	4.0	3.0

By conducting these simulations, the aim is to gain insights into the robustness and reliability of the proposed frameworks in the face of attacks and faults. The results will not only validate the effectiveness of the detection, identification, and mitigation techniques but also highlight their potential for enhancing the overall security and performance of vehicle platoons. Additionally, the simulations will provide a basis for comparative analyses and discussions, ultimately contributing to a comprehensive understanding of the proposed frameworks' capabilities and limitations.

4.1 Attack Cases

In this section, six diverse scenarios are presented to rigorously test and evaluate the performance of the attack detection, identification, and mitigation frameworks. Each scenario involves a different number of vehicles in the platoon and adopts specific IFTs, creating challenging conditions for the simulations. These simulation scenarios are carefully crafted to examine the robustness and effectiveness of the proposed frameworks in detecting, identifying, and mitigating attacks under varying platoon configurations. By subjecting the system to different attack scenarios, thorough assessment of the methodologies can be conducted to ensure the integrity and safety of the platoon.

The scenarios serve as pivotal test cases, validating the performance of the detection, identification, and mitigation techniques. The outcomes will provide empirical evidence of the frameworks' capabilities and insights into their potential to enhance the security and performance of vehicle platoons in real-world scenarios. Each scenario is uniquely tailored to assess specific aspects of the proposed frameworks, facilitating discussions and analyses that highlight their strengths and limitations.

4.1.1 Attack Scenario 1: No attack

The analysis of the proposed frameworks begins with a basic scenario involving a platoon of three vehicles (indexed 1, 2, and 3) following a lead vehicle (indexed 0) using the Bidirectional Following (BF) IFT. In this scenario, the focus is on vehicle 2. The Detection UIO_0, UIO_1, and UIO_3 developed for this vehicle are responsible for detecting attacks on vehicles 0, 1, and 3, respectively, while the Identification UIO of vehicle 2 is responsible for identifying and mitigating attacks on the specific parameters of the attacked vehicle(s). An increase in the RF of a Detection UIO indicates that the corresponding vehicle is under attack (Table 4.2).

TABLE 4.2: Expected behaviour of identifying UIOs for the platoon of Scenario 1.

Attacked vehicle(s)	Increase in the RF of Detection UIOs		
	UIO_0	UIO_1	UIO_3
No attack	-	-	-
Leader	✓	-	-
Leader and 1	✓	✓	-
Leader and 3	✓	-	✓
1	-	✓	-
1 and 3	-	✓	✓
3	-	-	✓
All	✓	✓	✓
other events	✓	✓	✓
Excluded attack inputs	$\mu_{x,0}$, $\mu_{v,0}$	$\mu_{x,1}$, $\mu_{v,1}$, $\mu_{a,1}$	$\mu_{x,3}$, $\mu_{v,3}$, $\mu_{a,3}$

The simulation is conducted from $t = 0$ to 30 seconds, utilizing the parameter values listed in Table 4.1. The results depicted in Fig. 4.1 demonstrate that the RF of the Detection UIOs does not increase in this scenario, indicating the absence of any FDIA. Moreover, the Identification UIO estimates nearly zero for all attack inputs, signifying that none of the parameters are targeted by an FDIA.

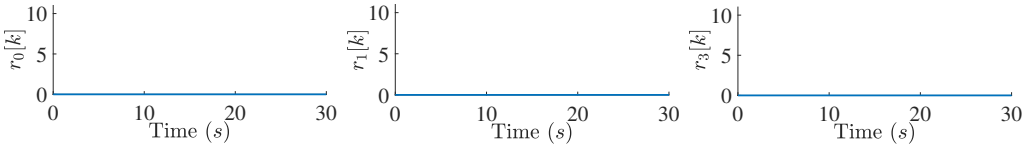


FIGURE 4.1: RF of Detection UIOs in Scenario 1: a) UIO_0, b) UIO_1, and c) UIO_3.

4.1.2 Attack Scenario 2: Attack on lead vehicle

In Scenario 2, an FDIA is initiated on the lead vehicle of a platoon consisting of five follower vehicles (indexed 1 to 5), with specifications selected from Table 4.1. A Predecessor Following (PF) IFT is employed, where the last vehicle in the platoon, vehicle 5, is chosen as the subject vehicle to demonstrate that even a vehicle far from the leader with no direct IFT can detect a compromised leader. The platoon operates normally until the leader is attacked at time $t = 10$ for a duration of 20 seconds, with its velocity randomly manipulated between 0-10 m/s. Fig. 4.2 illustrates the RF of the Detection UIOs associated with the leader and follower vehicles 1, 2, and 4 (the output of UIO_3 is omitted due to space constraints). As observed in the figure, only the RF of UIO_0 has increased, indicating that only the lead vehicle is experiencing an FDIA. Furthermore, Fig. 4.3(a) displays the estimated $\mu_{v,0}$ by the Identification UIO, demonstrating that the estimated and actual attack inputs align perfectly, indicating the high accuracy of the Identification UIO in estimating the attack parameters. Lastly, Fig. 4.3(b) illustrates the actual v_0 before manipulation by the FDIA and the estimated v_0 after mitigating the attack. It can be observed that the actual and estimated v_0 perfectly overlap, indicating the effectiveness of the attack mitigation technique in mitigating the impact of the attack.

4.1.3 Attack Scenario 3: Simultaneous vehicle merge and attack

In this scenario, five vehicles (indexed 1-4 and 6) follow a lead vehicle using LPF IFT. The vehicle specifications are obtained from Table 4.1. Initially, vehicle 5 is absent from the platoon, making vehicles 4 and 6 neighbors with a distance of $d_4^6 = 8$ m. Vehicle 6 is

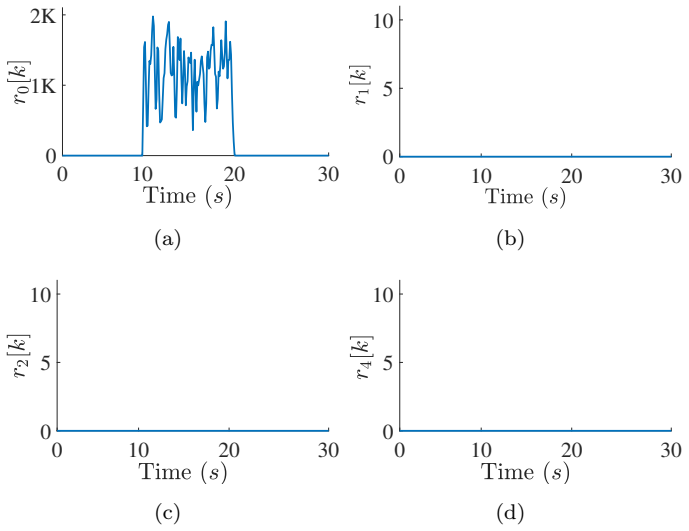


FIGURE 4.2: RF of Detection UIOs in Scenario 2: a) UIO_0, b) UIO_1, c) UIO_2, and d) UIO_4.

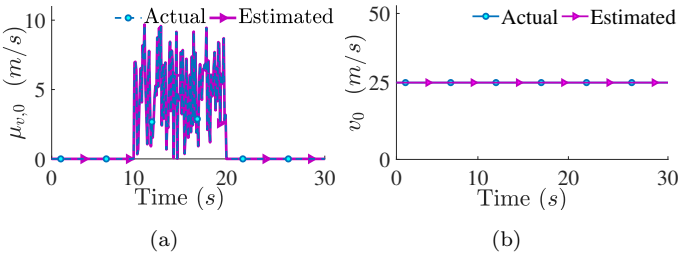


FIGURE 4.3: a) Actual and estimated attack input, and b) actual and estimated velocity for the lead vehicle in Scenario 2.

selected for analysis. The platoon is in a steady state when vehicle 5 (with parameters from Table 4.1) merges into the platoon between vehicles 4 and 6 at $t = 10$ seconds. At $t = 12$ seconds, vehicle 3 is attacked, with an offset of 0.5 m/s^2 added to its acceleration. The attacker manipulates the velocity and position of vehicle 3 as well to maintain stealth.

Immediately after the merge of vehicle 5, vehicle 6 updates the state-space model of the platoon and redevelops the Detection and Identification UIOs. In Fig. 4.4(a), the Residual Function (RF) of Detection UIO_3 initially starts at zero but exhibits a fast-decaying overshoot at $t = 10$ seconds when vehicle 5 joins the platoon. This overshoot occurs due to the initialization of the updated UIO for vehicle 3. As the attack on vehicle 3 initiates at $t = 12$ seconds, the RF of UIO_3 gradually increases, indicating that vehicle 3 is under an FDIA, with the attacker progressively increasing the magnitudes of $\mu_{v,3}$ and $\mu_{x,3}$. However, the RFs of other vehicles in the platoon remain at zero.

Furthermore, Figs. 4.5(a)-4.5(c) demonstrate the successful estimation of vehicle 3's attack inputs, including acceleration, velocity, and position, by the Identification UIO.

Leveraging these estimated attack inputs, the mitigation framework accurately estimates the true position, velocity, and acceleration of vehicle 3, as depicted in Fig. 4.5. These estimated values are then utilized to effectively mitigate the impacts of the attack, replacing the received ones.

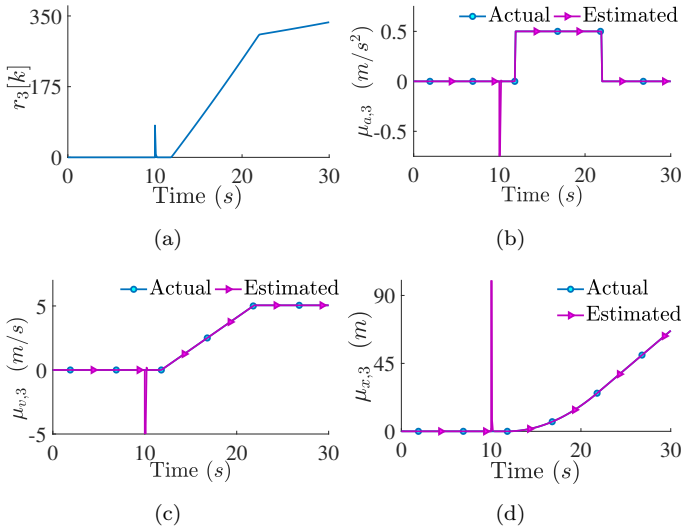


FIGURE 4.4: Results of Scenario 3: a) RF of UIO_3, as well as the actual and estimated attack inputs for the b) acceleration, b) velocity, and c) position of vehicle 3.

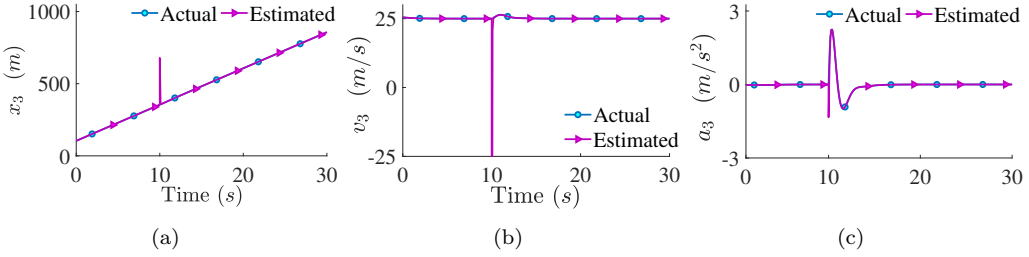


FIGURE 4.5: Actual and estimated a) position, b) velocity, and c) acceleration for vehicle 3 in Scenario 3.

4.1.4 Attack Scenario 4: Multi-vehicle attack

The multi-vehicle attack scenario involves a platoon of six vehicles following a lead vehicle using Leader-Bidirectional Following (LBF) IFT, with vehicle specifications taken from Table 4.1. The objective is to evaluate the effectiveness of the proposed frameworks in detecting and mitigating coordinated attacks on multiple vehicles within the platoon. In this scenario, vehicle 6 is selected as the subject vehicle, while vehicles 1 and 3 are simultaneously targeted.

Vehicle 1's velocity is manipulated in three phases: it is increased linearly with a slope of 0.5 m/s^2 from $t = 10$ to 15 seconds, then decreased linearly with a slope of -0.5 m/s^2 from $t = 16$ to 25 seconds, and finally increased again with a slope of 0.5 m/s^2 from $t = 26$ to 30 seconds. Similarly, vehicle 3's velocity is manipulated in three phases: it is accelerated by 1 m/s^2 from $t = 15$ to 20 seconds, decelerated by 1 m/s^2 from $t = 21$ to 30 seconds, and accelerated again between $t = 31$ and 35 seconds by 1 m/s^2. To maintain stealth, other parameters of both vehicles are adjusted in accordance with the changes in their acceleration throughout the scenario.

Fig. 4.6 displays the RFs of vehicles 1 and 3, showing an immediate increase once their respective FDIAs are initiated, indicating successful detection of the attacks by the proposed framework. Additionally, Fig. 4.7 presents the estimated attack inputs for vehicles 1 and 3, with all six attack inputs accurately estimated by the Identification UIO. Consequently, the attacks can be effectively mitigated by subtracting the estimated inputs from the corresponding information received through the communication system.

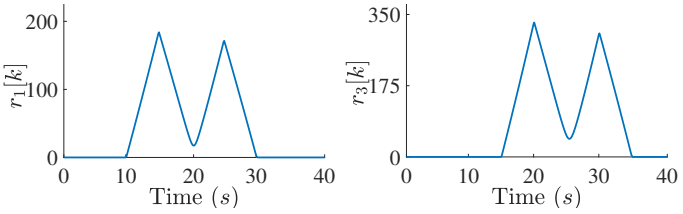


FIGURE 4.6: Attack Scenario 4: a) RF of vehicle 1, and b) RF of vehicle vehicle 3.

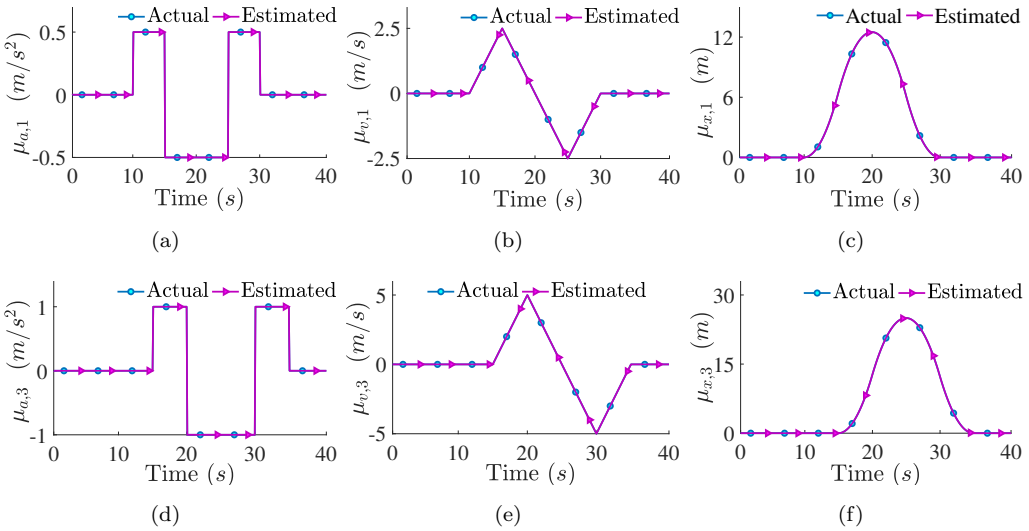


FIGURE 4.7: Attack Scenario 4: Actual and estimated attack inputs a) $\mu_{a,1}$, b) $\mu_{v,1}$, c) $\mu_{x,1}$ d) $\mu_{a,3}$, e) $\mu_{v,3}$, and f) $\mu_{x,3}$.

4.1.5 Attack Scenario 5: Attack on following vehicles

In this scenario, a platoon of five vehicles follows a lead vehicle, incorporating BF IFT. The vehicle specifications are taken from Table 4.1. Vehicle 2 is selected as the subject vehicle, and vehicle 3 is deliberately attacked to demonstrate the system's ability to detect a compromised vehicle sharing IFT with another vehicle from behind. The acceleration of vehicle 3 is increased by 0.5 m/s^2 from $t = 10$ to 20 seconds, and to maintain stealth, the velocity and position of the vehicle are also manipulated accordingly.

As shown in Fig. 4.8(d), the RF of UIO$_3$ gradually increases as the attacker progressively amplifies the magnitudes of $\mu_{v,3}$ and $\mu_{x,3}$. This increase in the RF of UIO$_3$ indicates that vehicle 3 is under an FDIA. However, the RF values for the other vehicles remain at zero. Additionally, Figs. 4.8(a)-4.8(c) demonstrate the successful estimation of the attack inputs for vehicle 3's acceleration, velocity, and position by the Identification UIO. Similar to the previous scenarios, the attack can be mitigated by estimating the actual values of the attacked parameters and utilizing them instead of the manipulated values.

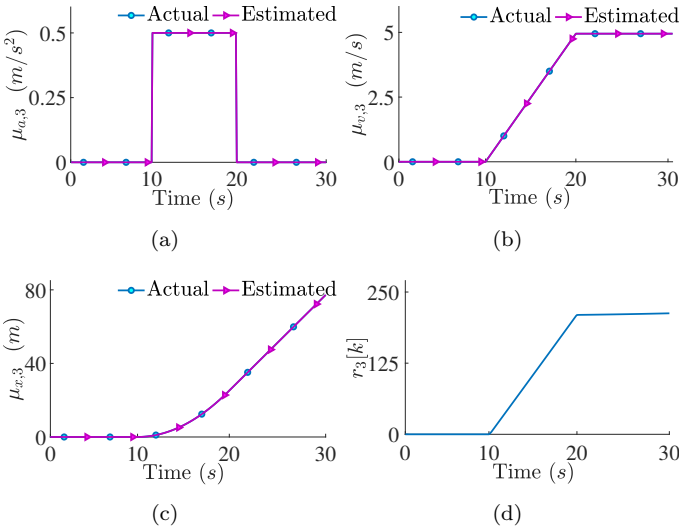


FIGURE 4.8: Attack Scenario 5: Vehicle 3's Actual vs Estimated: a) Acceleration, b) Velocity, and c) Position & d) Vehicle 3 RF.

4.1.6 Attack Scenario 6: Attack on a Vehicle Platoon of Trucks

In this scenario, a platoon of five trucks follows a lead truck, employing the same BF IFT as in Scenario 5. Vehicle platooning comprising solely of trucks is known as truck platooning [48]. The vehicle specifications, derived from Table 4.1, remain consistent across both scenarios, with the exception of two factors: the length of each vehicle and their initial positions. The lengths of the vehicles are inspired by [49], which provides valuable insights into various truck types. The specific lengths and initial positions of the vehicles in this truck platoon are:

TABLE 4.3: Lengths and Initial x_i of the vehicles in the Truck platoon

Vehicle (i)	Leader (0)	1	2	3	4
L_i (m)	27	27.5	24	25	26.5
Initial x_i (m)	0	-35	-69.5	-99.5	-126.5

Vehicle 2 is once again chosen as the subject vehicle, and vehicle 3 is subjected to the same deliberate attack described in Scenario 5. The attack involves an acceleration increase of 0.5 m/s^2 over the time interval $t = 10$ to 20 seconds, with corresponding adjustments made to the vehicle's velocity and position to maintain the attack's stealthiness.

The simulation result depicted in Fig. 4.9 mirrors that of Scenario 5 (Fig. 4.8(d)). Specifically, the RF of UIO_3 shows a gradual increase, conclusively affirming the occurrence of an FDIA on vehicle 3. Similarly, the Identification UIO precisely estimates the attack inputs for vehicle 3's acceleration, velocity, and position. The RF of the other vehicles remains at 0 as they were not attacked. Following the detection and identification of the attack, the framework effectively mitigates its impact by substituting the manipulated values with the actual values, akin to the approaches demonstrated in preceding scenarios.

Through this scenario, the frameworks' capability to effectively address attacks within a platoon of larger vehicles is showcased. The similarity in results between this scenario and Scenario 5 underlines the versatility and reliability of the proposed frameworks across varying vehicle sizes and dynamics, reinforcing their significance in enhancing platoon security

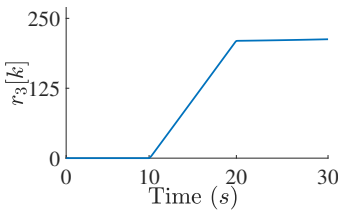


FIGURE 4.9: Attack Scenario 6: Vehicle 3 RF.

4.2 Fault Cases

This section presents three simulations of a platoon comprising of four vehicles, with vehicle 2 being the subject vehicle experiencing measurement errors (faults) in one or more of its position, velocity, and acceleration parameters. The specific parameters for the lead and following vehicles can be found in Table 4.1. Various IFTs are chosen for different simulation scenarios, showcasing the effectiveness of the framework regardless of the selected topology.

By employing the established framework, the aim is to evaluate the platoon's response to different fault parameters for vehicle 2. The expected outcome of simulations in the presence of different fault scenarios is highlighted in Table 4.4. The table illustrates that when a single fault occurs in only one of the vehicle's position (x_2), velocity (v_2), or acceleration (a_2) inputs, the Residual Function (RF) of the corresponding Unknown Input Observer (UIO) increases. In the case of a combination of two or three faulted parameters, the corresponding combination of UIOs experience a non-zero RF.

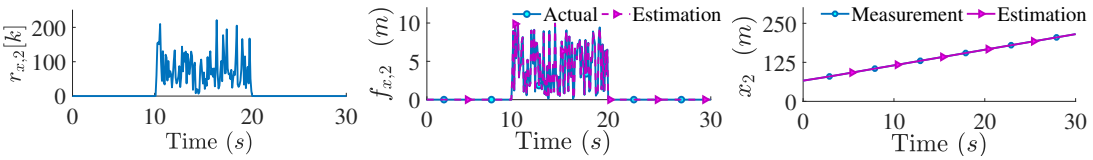
TABLE 4.4: Expected outputs under different fault parameter(s) and other than fault

Anomaly Type	**Residual Function Increase**		
Fault(s)	UIO x_2	UIO v_2	UIO a_2
x_2	✓	-	-
v_2	-	✓	-
a_2	-	-	✓
x_2 and v_2	✓	✓	-
x_2 and a_2	✓	-	✓
v_2 and a_2	-	✓	✓
All	✓	✓	✓
Other than fault	✓	✓	✓
Excluded inputs per UIO	$f_{x,2}$	$f_{v,2}$	$f_{a,2}$

4.2.1 Fault Scenario 1: Position Error

In this scenario, a Predecessor Following (PF) IFT is adopted. Initially, the platoon operates smoothly until vehicle 2 encounters a fault in its position parameter at time $t = 10$ for a duration of 10 seconds. During this period, the position of vehicle 2 randomly varies between 1m to 10m. One possible reason for this position fault could be the erratic GPS signals experienced by vehicle 2 while passing through a tunnel, leading to inaccurate measurements of its position.

Fig. 4.10(a) illustrates the RF of the position UIO ($r_{x,2}[k]$) associated with vehicle 2, indicating a fault in its position measurement. The plots for the RF of the velocity and acceleration UIOs for this vehicle are all zero and omitted in this thesis due to space limitations. Additionally, in Fig. 4.10(b), the estimated fault $f_{x,2}$ obtained by the position UIO is presented. The perfect alignment between the estimated and actual fault inputs demonstrates the high accuracy of this UIO in estimating the fault in the position of vehicle 2. Furthermore, Fig. 4.10(c) showcases a comparison between the measured x_2 in the absence of faults and the estimated x_2 in the presence of the fault, indicating the effectiveness of the fault mitigation technique in accurately estimating and compensating for the fault.



(a) (b) (c)

FIGURE 4.10: Fault Scenario 1: Vehicle 2's Position a) Residual Function, b) Fault Actual and Estimation, and c) Mitigated Measurement and Estimation

4.2.2 Fault Scenario 2: Acceleration Error

A bi-directional following IFT is adopted for this scenario, where the platoon operates smoothly until vehicle 2 encounters a fault in its acceleration parameter at time $t = 10$ for a period of 10 seconds. During this period, the acceleration of vehicle 2 jumps from zero to 1 m/s^2 and stays at that level until it returns to zero at the end of that period. One plausible cause for this fault could be overheating of the rotary encoder and/or IMU sensors of this vehicle.

The plots of the RF of the acceleration UIO ($r_{a,2}[k]$), the estimated fault $f_{a,2}$ obtained by the acceleration UIO, and a comparison between the measured a_2 and the estimated a_2 are shown in Figures 4.11(a), 4.11(b), and 4.11(c), respectively. Similar observations to the previous scenario can be made from the plots in this scenario. Again, there is a perfect alignment between the estimated and actual acceleration fault inputs, demonstrating the high accuracy of the acceleration UIO in estimating the fault in the acceleration of vehicle 2. The effectiveness of the fault mitigation technique in accurately estimating and compensating for the acceleration fault is evident in Figure 4.11(c).

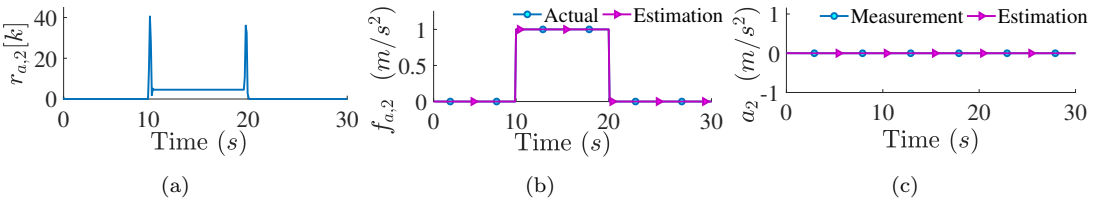
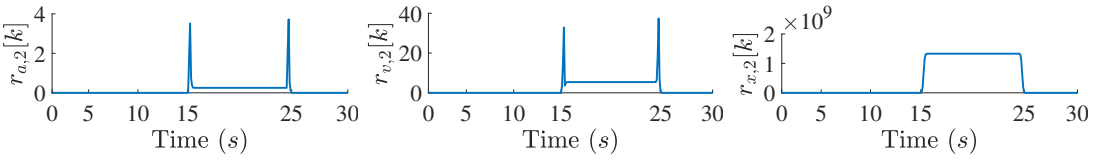


FIGURE 4.11: Fault Scenario 2: Vehicle 2's Acceleration a) Residual Function, b) Fault Actual and Estimation, and c) Mitigated Measurement and Estimation

4.2.3 Fault Scenario 3: Acceleration, Velocity, and Position Error

A leader bi-directional following IFT is adopted for this scenario, where vehicle 2 encounters simultaneous faults in its position, velocity, and acceleration. One plausible cause for these simultaneous faults could be cable leakage, leading to disruptions in the accuracy of acceleration, velocity, and position data transmitted to the On-Board Unit (OBU) by the vehicle's sensors. To simulate this scenario, the acceleration of vehicle 2 jumps from zero to 0.5 m/s^2 during a time interval between 15 and 25 seconds. The velocity and position of this vehicle have also been offset during this period as a result of the change in its acceleration.

Figures 4.12(a) to 4.12(c) illustrate the RF of the acceleration, velocity, and position UIOs associated with vehicle 2, respectively. These figures demonstrate the successful detection of faults in the acceleration, velocity, and position of this vehicle by the respective fault UIOs.



(a) (b) (c)

FIGURE 4.12: Fault Scenario 3: Vehicle 2's Residual Functions: a) Acceleration, b) Velocity, and b) Position.

4.3 Computation Complexity

The computational complexity for on-line implementation can be analyzed using the Big O notation. To this aim, the number of Floating Point Operations (FLOPs) of the proposed method should be calculated at each time-step. To perform the proposed method in real-time, equations (3.9), (3.26), and (3.24) must be run at each time-step for attack detection, identification and mitigation. These equations include basic algebraic operations (i.e., only addition and multiplication) which can be easily implemented by microprocessors. Assuming a total of n vehicles and a delay parameter α, the FLOPS for equation (3.9) can be expressed as $(66n^2 + 12n + 48n^2\alpha + 6n^2\alpha^2 + 6n\alpha)$. Similarly, for equation (3.26), it stands at $(42n^2)$, and for equation (3.24), it totals $(18n^2 + 9n)$. By combining these individual FLOPS, the total FLOPS for the entire computation is given by $(126n^2 + 21n + 48n^2\alpha + 6n^2\alpha^2 + 6n\alpha)$. Finally, as there are n number of UIOs running in parallel for attack detection and identification, the computational complexity is classified as $O(n^3)$.

Similarly, for fault detection, identification and mitigation, real-time computations are performed using equations (3.9), (3.31), and (3.29). FLOPS for equation (3.9) remains as $(66n^2+12n+48n^2\alpha+6n^2\alpha^2+6n\alpha)$, as well as for equation (3.24), it remains $(18n^2+9n)$. As for equation (3.31), the FLOPS are $(30n^2+9n)$. Hence, the total FLOPS is expressed as, $(114n^2 + 30n + 48n^2\alpha + 6n^2\alpha^2 + 6n\alpha)$.For fault detection and identification, three UIOs are run in parallel.

To provide a tangible perspective, consider Scenario 4.1.1 as an illustration, where $n = 3$ and $\alpha = 2$ (as specified in Section 3). In this case, the computations require 1,746 FLOPS for equation (3.9), 378 FLOPS for equation (3.26), and 189 FLOPS for equation (3.24). This accumulates to a total of 2,313 FLOPS for the computational process of one

UIO. With three UIOs working in parallel, it would be a total of 6,939 FLOPS. Using a Intel Core i5-10400 Processor [50], renowned for its capacity to execute 768.0 billion floating-point operations per second, this number of FLOPS would take approximately 9.05 nanoseconds. This estimate does not include the memory access time and it also assumes that the processor is fully dedicated for this task.

Considering scenario 4.2.1, with $n = 3$ and $\alpha = 2$, the FLOPS of equations (3.9), (3.31), and (3.24) are 1,746, 297, and 189, respectively. Then the total FLOPS would be 2,232 for one UIO, resulting in 6,696 FLOPS for all three UIOs running in parallel. Utilizing the same Intel Core i5-10400 Processor, it would take approximately 8.73 nanoseconds to perform the proposed fault detection and identification method in real-time.

Chapter 5

Conclusion

This dissertation presented comprehensive frameworks that address detection, identification, and mitigation of FDIAs and faults in vehicle platoons. These frameworks are designed to be independent of the adopted IFTs (Information Flow Topologies) and the number of vehicles within the platoon, ensuring their applicability in diverse scenarios. By employing state-space modeling and leveraging UIOs, the proposed frameworks effectively detect and identify FDIAs and faults within platoons. Furthermore, the frameworks successfully mitigate attacks and faults by replacing the manipulated or impaired parameters with their actual values, restoring the integrity and functionality of the platoon. This mitigation process further emphasizes the practicality and effectiveness of the proposed frameworks in maintaining the desired operational state of the platoon.

The frameworks' effectiveness was validated through extensive simulations, which demonstrated their ability to accurately identify and mitigate attacked and faulty parameters while estimating the affected parameters. Specifically, the research gap identified pertained to the absence of a comprehensive and unified approach to addressing FDIAs across diverse platoon configurations and multiple parameters. The set of attack scenarios collectively addresses the identified research gap while also showcasing a series of significant accomplishments in the realm of platoon security. The attack framework demonstrates its potential to revolutionize platoon security and performance by highlighting the following attributes:

- **Robustness against FDIAs:** This attribute is vital to prevent malicious actors from tampering with critical information, such as position, speed, or acceleration, which could otherwise compromise the entire platoon's safety and operation.

- **Adaptation to dynamic changes in platoon composition:** The ability to adapt to dynamic changes, such as vehicles joining the platoon ensures that the attack detection and mitigation mechanisms remain effective regardless of the platoon's size or configuration. This adaptability maintains the platoon's security and performance under evolving circumstances.
- **Effective handling of coordinated attacks:** This ensures that the platoon's defense mechanisms can detect and mitigate complex, synchronized attacks. This capability thwarts attempts to exploit vulnerabilities by combining multiple attack vectors.
- **Versatility and resilience in tackling attacks on different vehicle types and sizes:** Platoon members can vary widely in terms of their type, size, and capabilities in real-world scenarios. The framework's versatility and resilience in addressing attacks ensure that its security measures remain effective across diverse vehicle compositions within the platoon, making it applicable in a wide range of situations.

Through these scenarios, a unified approach emerges for effectively addressing FDIAs in diverse platoon configurations and across multiple parameters. The progression from simple scenarios to intricate attacks serves to emphasize the adaptability and effectiveness of the attack framework in ensuring both platoon security and optimal performance.

As for the research gaps discovered in regards to faults, it's evident that certain themes are reiterated. Notably, most studies tend to overlook the potential occurrence of simultaneous faults across all three parameters, an aspect that gains significance given the possibility of a faulty On-Board Unit (OBU). Additionally, there's a noticeable lack of emphasis on acceleration as a critical parameter when addressing faults. Much like the gap highlighted in the context of FDIAs, there's also a need for a comprehensive and unified approach to address faults in platoons under varying configurations. Together, the fault scenarios collectively contribute to addressing the gaps identified in the existing literature. The seamless transition from individual to complex fault scenarios showcases the flexibility of the fault framework. The scenarios are instrumental in:

- **Addressing the oversight of potential simultaneous faults:** This is beneficial to vehicle platooning because real-world scenarios can often involve multi-faceted faults.
- **Recognizing the significance of acceleration as a vital parameter:** Acceleration is indeed a fundamental parameter that can affect the stability and

performance of platoons, especially during maneuvers or sudden changes in traffic conditions, thus improving the reliability and safety of platoon operations.

- **Showcasing a unified approach for handling faults across diverse platoon setups:** This versatility directly benefits vehicle platooning by offering a single framework that can be applied across different operational contexts, streamlining maintenance and ensuring consistent performance.

In essence, this journey of research and innovation has contributed significantly to the burgeoning field of autonomous and interconnected transportation systems. By addressing security, reliability, and performance within platoon operations, this work contributes to a safer and more efficient future of transportation. The frameworks introduced here promise to be pivotal in shaping the trajectory of vehicular platooning, safeguarding its journey into the future.

As the field of platoon security and autonomy continues to evolve, there is a proactive initiative to further strengthen these frameworks to address emerging challenges and ensure their continued relevance. Future work to strengthen the frameworks includes:

- **Enhancing the Framework to Tackle Denial of Service (DoS) Attacks:** To enhance the resilience of the frameworks against deliberate communication disruptions, it is prudent to incorporate specialized techniques targeting DoS attacks. These attacks aim to overload communication channels or exhaust computing resources, rendering them unavailable to legitimate users. In order to implement this enhancement, the following actions can be undertaken:
  - Explore the implementation of intrusion detection systems that can detect unusual patterns in communication traffic, indicating the presence of DoS attacks
  - Develop adaptive algorithms that can dynamically reconfigure the platoon's communication topology in response to detected disruptions, minimizing the impact of DoS attacks
  - Implement mechanisms, such as backup communication channels or alternate sensing methods, to ensure the platoon's operations even when under attack
- **Exploring Data-Driven Techniques for Improved Detection and Mitigation:** The integration of data-driven techniques can greatly elevate the accuracy and adaptability of the frameworks, fueled by refinement through real-world data. These techniques employ machine learning algorithms and real-world data to enhance detection and response capabilities. To address this technique, the following steps can be taken:

  - Collect and curate a comprehensive dataset that includes various operational scenarios, attack patterns, and environmental conditions
  - Implement machine learning algorithms, such as neural networks or ensemble methods, to learn from the collected data and improve the accuracy of fault and attack detection
  - Investigate the fusion of multiple sensor modalities, such as LiDAR, RADAR, and cameras, to build a holistic picture of the platoon's surroundings and enhance overall robustness
  - Consider reinforcement learning techniques that enable the platoon to autonomously adjust its response strategies based on evolving attack patterns

- **Investigating the Impact of Noise:** A comprehensive understanding of the frameworks capabilities and limitations can be acquired by exploring the influence of noise on their performance. Noise, arising from various sources, can distort sensor data and challenge the accuracy of the detection and mitigation algorithms. Addressing this concern involves the following measures:
  - Develop simulation environments that replicate various noise conditions, including sensor noise, communication noise, and environmental variability
  - Quantify the impact of different noise levels on the accuracy of the frameworks through rigorous simulations or controlled experiments
  - Explore advanced noise filtering and signal processing techniques that can mitigate the adverse effects of noise on fault and attack detection
  - Strive for a balanced approach between noise reduction methods and real-time response requirements, ensuring optimal accuracy without compromising efficiency

Incorporating these improvements would elevate the quality and practicality of the research. They would enable the frameworks to handle a wider range of challenges and uncertainties, making them more robust, accurate, and reliable in real-world platooning scenarios.

Bibliography

[1] Sean Campbell, Niall O'Mahony, Lenka Krpalcova, Daniel Riordan, Joseph Walsh, Aidan Murphy, and Conor Ryan. Sensor technology in autonomous vehicles : A review. In *2018 29th Irish Signals and Systems Conference (ISSC)*, pages 1–4, 2018. doi: 10.1109/ISSC.2018.8585340.

[2] IEEE 802.11. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. Standard, Institute of Electrical and Electronics Engineers.

[3] IEEE 1609.x. Draft standard for wireless access in vehicular environments (wave). Standard, Institute of Electrical and Electronics Engineers.

[4] SAE J2735. V2x communications message set dictionary. Standard, Society of Automotive Engineers International.

[5] SAE J2945. On-board system requirements for v2v safety communications. Standard, Society of Automotive Engineers International.

[6] Jicheng Chen, Hui Zhang, and Guodong Yin. Distributed dynamic event-triggered secure model predictive control of vehicle platoon against dos attacks. *IEEE Transactions on Vehicular Technology*, 72(3):2863–2877, 2023. doi: 10.1109/TVT.2022.3215966.

[7] Eshaan Khanapuri, Tarun Chintalapati, Rajnikant Sharma, and Ryan Gerdes. Learning based longitudinal vehicle platooning threat detection, identification and mitigation. *IEEE Transactions on Intelligent Vehicles*, 8(1):290–300, 2023. doi: 10.1109/TIV.2021.3122144.

[8] Byungjin Ko and Sang Hyuk Son. An approach to detecting malicious information attacks for platoon safety. *IEEE Access*, 9:101289–101299, 2021. doi: 10.1109/ACCESS.2021.3095480.

[9] Zhiyang Ju, Hui Zhang, and Ying Tan. Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified ufir estimator. *IEEE Internet of Things Journal*, 7(5):3693–3705, 2020. doi: 10.1109/JIOT.2020.2966672.

[10] Yu Xuan and Mohammad Naghnaeian. Detection and identification of cps attacks with application in vehicle platooning: a generalized luenberger approach. In *2021 American Control Conference (ACC)*, pages 4013–4020, 2021. doi: 10.23919/ACC50511.2021.9483074.

[11] Zhiyang Ju, Hui Zhang, and Ying Tan. Distributed deception attack detection in platoon-based connected vehicle systems. *IEEE Transactions on Vehicular Technology*, 69(5):4609–4620, 2020. doi: 10.1109/TVT.2020.2980137.

[12] Eman Mousavinejad, Fuwen Yang, Qing-Long Han, Xiaohua Ge, and Ljubo Vlacic. Distributed cyber attacks detection and recovery mechanism for vehicle platooning. *IEEE Transactions on Intelligent Transportation Systems*, 21(9):3821–3834, 2020. doi: 10.1109/TITS.2019.2934481.

[13] Raj Gautam Dutta, Yaodan Hu, Feng Yu, Teng Zhang, and Yier Jin. Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment. *IEEE Transactions on Intelligent Transportation Systems*, 23(4): 3418–3429, 2022. doi: 10.1109/TITS.2020.3036376.

[14] Roghieh A. Biroon, Zoleikha Abdollahi Biron, and Pierluigi Pisu. False data injection attack in a platoon of cacc: Real-time detection and isolation with a pde approach. *IEEE Transactions on Intelligent Transportation Systems*, 23(7):8692–8703, 2022. doi: 10.1109/TITS.2021.3085196.

[15] Abdelrahman Khalil, Mohammad Al Janaideh, Khaled F. Aljanaideh, and Deepa Kundur. Transmissibility-based health monitoring of the future connected autonomous vehicles networks. *IEEE Transactions on Vehicular Technology*, 71(4): 3633–3647, 2022. doi: 10.1109/TVT.2022.3151326.

[16] Franco van Wyk, Yiyang Wang, Anahita Khojandi, and Neda Masoud. Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 21(3):1264–1276, 2020. doi: 10.1109/TITS.2019.2906038.

[17] Wilcoxon Sensing Technologies. Troubleshooting accelerometer installations. 2018.

[18] ACS Industrial Blog. 6 simple tips for encoder repair and troubleshooting. 2017.

[19] 5GAA. V2x functional and performance test procedures – selected assessment of device to device communication aspects. 2018.

[20] Jinheng Han, Junzhi Zhang, Chengkun He, Chen Lv, Xiaohui Hou, and Yuan Ji. Distributed finite-time safety consensus control of vehicle platoon with senor and

actuator failures. *IEEE Transactions on Vehicular Technology*, 72(1):162–175, 2023. doi: 10.1109/TVT.2022.3203056.

[21] António Lopes and Rui Esteves Araújo. Active fault diagnosis method for vehicles in platoon formation. *IEEE Transactions on Vehicular Technology*, 69(4):3590–3603, 2020. doi: 10.1109/TVT.2020.2968961.

[22] Weiping Wang, Baijing Han, Yongzhen Guo, Xiong Luo, and Manman Yuan. Fault-tolerant platoon control of autonomous vehicles based on event-triggered control strategy. *IEEE Access*, 8:25122–25134, 2020. doi: 10.1109/ACCESS.2020.2967830.

[23] Chengwei Pan, Yong Chen, Yuezhi Liu, Ikram Ali, and Wen He. Distributed finite-time fault-tolerant control for heterogeneous vehicular platoon with saturation. *IEEE Transactions on Intelligent Transportation Systems*, 23(11):21259–21273, 2022. doi: 10.1109/TITS.2022.3181460.

[24] Chengwei Pan, Yong Chen, Yuezhi Liu, and Ikram Ali. Adaptive resilient control for interconnected vehicular platoon with fault and saturation. *IEEE Transactions on Intelligent Transportation Systems*, 23(8):10210–10222, 2022. doi: 10.1109/TITS.2021.3087940.

[25] Mohammad Pirani, Ehsan Hashemi, Amir Khajepour, Baris Fidan, Bakhtiar Litkouhi, Shih-Ken Chen, and Shreyas Sundaram. Cooperative vehicle speed fault diagnosis and correction. *IEEE Transactions on Intelligent Transportation Systems*, 20(2):783–789, 2019. doi: 10.1109/TITS.2018.2820044.

[26] Katsuhiko Ogata. *Modern Control Engineering*. Pearson, 5th edition edition, 2010. ISBN 978-0136156734.

[27] Karl J. Åström and Richard M. Murray. *Feedback Systems: An Introduction for Scientists and Engineers*. Princeton University Press, 1st edition edition, 2008. ISBN 978-0691135762.

[28] Shreyas Sundaram. Fault-tolerant and secure control systems. *University of Waterloo, Lecture Notes*, 2012.

[29] Dan Simon. *Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches*. John Wiley & Sons, 2006. ISBN 978-0-471-70858-2.

[30] Robert L. Williams II and Douglas A. Lawrence. *Linear State-Space Control Systems*. John Wiley & Sons, 2007. ISBN 978-0-471-73555-7.

[31] Greg Welch and Gary Bishop. An introduction to the kalman filter. *SIGGRAPH Course Notes*, 1995(8), 1995.

[32] James B. Rawlings, David Q. Mayne, and Moritz M. Diehl. *Model Predictive Control: Theory, Computation, and Design*. Nob Hill Publishing, second edition, 2017.

[33] Graeme Field. Particle filters for state estimation of confined aquifers. Master's thesis, University of North Florida, 2018.

[34] James B. Rawlings and David Q. Mayne. *Model Predictive Control: Theory, Computation, and Design*. Nob Hill Publishing, 2009.

[35] David G. Luenberger. Observing the state of a linear system. *IEEE Transactions on Military Electronics*, 8(2):74–80, 1964. doi: 10.1109/TME.1964.4323124.

[36] Peyman Setoodeh, Saeid Habibi, and Simon Haykin. *Observers*, pages 29–31. 2022. doi: 10.1002/9781119078166.ch3.

[37] Sam Nazari. The unknown input observer and its advantages with examples. *CoRR*, abs/1504.07300, 2015. URL http://arxiv.org/abs/1504.07300.

[38] Amir Zakerimanesh, Tony Qiu, and Mahdi Tavakoli. Heterogeneous vehicular platooning with stable decentralized linear feedback control. In *2021 IEEE International Conference on Autonomous Systems (ICAS)*, pages 1–5, 2021. doi: 10.1109/ICAS49788.2021.9551150.

[39] Hui Liu, Chunpeng Pan, Cheng Lv, Lian Gong, Xunjia Zheng, and Xing Chen. False data injection attack modeling and impact on vehicle platooning. In *2021 China Automation Congress (CAC)*, pages 7757–7761, 2021. doi: 10.1109/CAC53003.2021.9728578.

[40] Dan Zhang, Ye-Ping Shen, Si-Quan Zhou, Xi-Wang Dong, and Li Yu. Distributed secure platoon control of connected vehicles subject to dos attack: Theory and application. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51 (11):7269–7278, 2021. doi: 10.1109/TSMC.2020.2968606.

[41] Yang Zheng, Shengbo Eben Li, Jianqiang Wang, Dongpu Cao, and Keqiang Li. Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies. *IEEE Transactions on Intelligent Transportation Systems*, 17(1):14–26, 2016. doi: 10.1109/TITS.2015.2402153.

[42] Katsuhiko Ogata. *Discrete-time control systems*. Prentice Hall International, 1995.

[43] Ali Saberi, Anton Stoorvogel, and Peddapullaiah Sannuti. Exact, almost and optimal input decoupled (delayed) observers. *International Journal of Control*, 73: 552–581, 05 2000. doi: 10.1080/002071700219425.

[44] Amir Ameli, Ali Hooshyar, Ehab F. El-Saadany, and Amr M. Youssef. Attack detection and identification for automatic generation control systems. *IEEE Transactions on Power Systems*, 33(5):4760–4774, 2018. doi: 10.1109/TPWRS.2018.2810161.

[45] M. Sain and J. Massey. Invertibility of linear time-invariant dynamical systems. *IEEE Transactions on Automatic Control*, 14(2):141–149, 1969. doi: 10.1109/TAC.1969.1099133.

[46] S. Sundaram and C.N. Hadjicostis. On delayed observers for linear systems with unknown inputs. In *Proceedings of the 44th IEEE Conference on Decision and Control*, pages 7210–7215, 2005. doi: 10.1109/CDC.2005.1583324.

[47] Jaroslav Kautsky, Nancy K Nichols, and Paul Van Dooren. Robust pole assignment in linear state feedback. *International Journal of control*, 41(5):1129–1155, 1985.

[48] Brian McAuliffe, Michael Lammert, Xiao-Yun Lu, Steven Shladover, et al. Influences on energy savings of heavy trucks using cooperative adaptive cruise control. *SAE Technical Paper*, (2018-01-1181), 2018. doi: 10.4271/2018-01-1181.

[49] Founder & CEO at Paige Logistics Ltd. Alexander Crane. Ultimate guide to 16 truckload trailer types. https://www.paigelogistics.com/truckload-trailer-types/.

[50] TechPowerUp. Intel core i5-10400, Year. URL https://www.techpowerup.com/cpu-specs/core-i5-10400.c2210. Accessed on September 17, 2023.