5-2017

A Resilient Control Approach to Secure Cyber Physical Systems (CPS) with an Application on Connected Vehicles

Zoleikha Abdollahi Biron
Clemson University, zabdoll@g.clemson.edu

A RESILIENT CONTROL APPROACH TO SECURE CYBER PHYSICAL SYSTEMS (CPS) WITH AN APPLICATION ON CONNECTED VEHICLES

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Automotive Engineering

---

by
Zoleikha Abdollahi Biron
May 2017

Accepted by:
Dr. Pierluigi Pisu, Committee Chair
Dr. Richard Brooks, Co-chair
Dr. Beshah Ayalew
Dr. Yongqiang Wang

ABSTRACT

The objective of this dissertation is to develop a resilient control approach to secure Cyber Physical Systems (CPS) against cyber-attacks, network failures and potential physical faults. Despite being potentially beneficial in several aspects, the connectivity in CPSs poses a set of specific challenges from safety and reliability standpoint. The first challenge arises from unreliable communication network which affects the control/management of overall system. Second, faulty sensors and actuators can degrade the performance of CPS and send wrong information to the controller or other subsystems of the CPS. Finally, CPSs are vulnerable to cyber-attacks which can potentially lead to dangerous scenarios by affecting the information transmitted among various components of CPSs. Hence, a resilient control approach is proposed to address these challenges. The control approach consists of three main parts:(1) *Physical fault diagnostics*: This part makes sure the CPS works normally while there is no cyber-attacks/ network failure in the communication network; (2) *Cyber-attack/failure resilient strategy*: This part consists of a resilient strategy for specific cyber-attacks to compensate for their malicious effects ; (3) *Decision making algorithm*: The decision making block identifies the specific existing cyber-attacks/ network failure in the system and deploys corresponding control strategy to minimize the effect of abnormality in the system performance. In this dissertation, we consider a platoon of connected vehicle system under Co-operative Adaptive Cruise Control (CACC) strategy as a CPS and develop a resilient control approach to address the aforementioned challenges.

The first part of this dissertation investigates fault diagnostics of connected vehicles assuming ideal communication network. Very few works address the real-time diagnostics problem in connected vehicles. This study models the effect of different faults in sensors and actuators, and also develops fault diagnosis scheme for detectable and identifiable faults. The proposed diagnostics scheme is based on sliding model observers to detect, isolate and estimate faults in the sensors and actuators. One of the main advantages of sliding model approach lies in applicability to nonlinear systems. Therefore, the proposed method can be extended for other nonlinear cyber physical systems as well.

The second part of the proposed research deals with developing strategies to maintain performance of cyber-physical systems close to the normal, in the presence of common cyber-attacks and network failures. Specifically, the behavior of Dedicated Short-Range Communication (DSRC) network is analyzed under cyber-attacks and failures including packet dropping, Denial of Service (DOS) attack and false data injection attack. To start with, packet dropping in network communication is modeled by Bernoulli random variable. Then an observer based modifying algorithm is proposed to modify the existing CACC strategy against the effect of packet dropping phenomena. In contrast to the existing works on state estimation over imperfect communication network in CPS which mainly use either holding previous received data or Kalman filter with intermittent observation, a combination of these two approaches is used to construct the missing data over packet dropping phenomena. Furthermore, an observer based fault diagnostics based on sliding mode approach is proposed to detect, isolate and estimate sensor faults in connected vehicles platoon.

Next, Denial of Service (DoS) attack is considered on the communication network. The effect of DoS attack is modeled as an unknown stochastic delay in data delivery in the communication network. Then an observer based approach is proposed to estimate the real data from the delayed measured data over the network. A novel approach based on LMI theory is presented to design observer and estimate the states of the system via delayed measurements. Next, we explore and alternative approach by modeling DoS with unknown constant time delay and propose an adaptive observer to estimate the delay. Furthermore, we study the effects of system uncertainties on the DoS algorithm. In the third algorithm, we considered a general CPS with a saturated DoS attack modeled with constant unknown delay. In this part, we modeled the DoS via a PDE and developed a PDE based observer to estimate the delay as well as states of the system while the only available measurements are delayed.

Furthermore, as the last cyber-attack of the second part of the dissertation, we consider false data injection attack as the fake vehicle identity in the platoon of vehicles. In this part, we develop a novel PDE-based modeling strategy for the platoon of vehicles equipped with CACC. Moreover, we propose a PDE based observer to detect and isolate the location of the false data injection attack injected into the platoon as fake identity.

Finally, the third part of the dissertation deals with the ongoing works on an optimum decision making strategy formulated via Model Predictive Control (MPC). The decision making block is developed to choose the optimum strategy among available strategies designed in the second part of the dissertation.

DEDICATION

This dissertation is dedicated to my parents whose value to me only grows with age.

ACKNOWLEDGMENTS

First, I would like to extend my gratitude towards my advisor Prof. Pierluigi Pisu whose valuable guidance has been instrumental throughout my Ph.D. program. His excellent teaching and mentorship helped me understand big picture in context to a particular research domain as well as the depth of the technical details. These aspects were particularly helpful when crafting my research proposal in terms of scope and specific algorithms. His knowledge of systems theory, insightful suggestions and critical feedback have been very helpful during my research. I have learnt a lot about technical writing under his mentorship. His teaching on fault diagnosis of dynamic systems and sliding mode theory have been extremely helpful during my research. I am also thankful to him for the long hours he spent with me discussing several minute aspects of "convergence proofs". Next, my appreciation extends to Prof. Richard Brooks for being my committee member. His teaching and knowledge on network security extremely helpful during my research. I am thankful to him for the hours he spent with me discussing regarding to the selected control- oriented approaches from network security perspectives. Those discussions have been really helpful in solidifying my technical concepts on systems, controls and network security. Lastly, his continuous support during the program is sincerely appreciated. I would also thank Prof. Beshah Ayalew for his support during my Ph.D. program. Dr. Ayalew was so dedicated to spend his valuable time to proofread my conference and journal papers along with his critical feedbacks. I have worked with Dr. Ayalew as his teaching assistant which has provided me with a large set of teaching skills. I also want to thank him for the many letters of recommendation he wrote for me for various scholarships

and awards. Next, I would like to thank my committee member Prof. Yongqiang Wang for their insightful questions and critical feedback that helped making this dissertation a better one.

Next, I would like to express my gratitude to my beloved siblings for their supports in my whole life. I would like to thank my dearest sister Roghieh for her endless kindness and caring. She is the most awesome, supportive and inspiring sister in the world. I would like to thank Maryam for all her pure love, Soraya for her motivating words encouraging me to face challenges with confidence. I would like to thank my amazing sister, my best friend and best part of me, Laila for all her sacrificing and devotions. I am thankful of my brother Abdollah for all his enthusiastic perspectives he spreads into the family and Reza and Darab for all they have done for me.

At last but not least, I would like to acknowledge my dear friends Dr. Satadru Dey and Dr. Sara Mohon. Satadru's guidance and technical discussions along with detailed explanations made several concepts clearer for me; and Sara's excellent pieces of advice eased PhD life's challenges for me.

TABLE OF CONTENTS

Page

Page

Page

LIST OF FIGURES

Figure Page

Page

Page

LIST OF TABLES

PUBLICATIONS

Journals:

- Z. Abdollahi, and P. Pisu, "Sensor and Actuator Fault Detection of Connected Vehicles under imperfect Communication Network", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10.6 (2016): 968-974.
- S. Dey, Z. A. Biron, S. Tatipamula, N. Das, S. Mohon, P. Pisu, and B. Ayalew, "Model-based Real-time Thermal Fault Diagnosis of Lithium-ion Batteries" , Journal of Control Engineering Practice, 56 (2016): 37-48.
- Z. Abdollahi, and P. Pisu, "Observer Design for State Estimation in Cyber Physical Systems with Unknown Delay in Measurements" under review in International Journal of Control.
- Z. Abdollahi, and P. Pisu, "Real-time False Data Injection Attack Detection in Connected Vehicle Systems with PDE modelling", submitted to IEEE Transaction on Control System Technology.
- Z. Abdollahi, S. Dey, and P. Pisu, "Real-time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems", submitted to IEEE Transaction on Intelligent Transportation System.
- L.Qiu, Z. Abdollahi, L. Qian, Z. Du, P. Pisu, "Engine map based predictive fuel efficient control strategies for a group of connected vehicles", submitted to IET Intelligent Transport system.

- L. Qiu, P. Chen, L. Qian, Z. Abdollahi, P. Pisu “Predictive Fuel Efficient Control Strategies for a Group of Connected Vehicles Considering Vertical Vibration”, under review in Science China Technological Sciences

Conference Proceedings:

- Z. Abdollahi, B. HomChaudhuri and P. Pisu, "Observer Design Based Cyber Security for Cyber Physical Systems", Cyber and Information Security Research Conference, 2015.
- Z. Abdollahi, and P. Pisu, “Distributed Fault Detection and Estimation for Cooperative Adaptive Cruise Control System in a Platoon,” PHM conference, 2015.
- Z. Abdollahi, S.Dey, and P. Pisu,” Sensor Fault Diagnosis of Connected Vehicles under imperfect Communication Network“, DSCC 2016.
- Z. Abdollahi, and P. Pisu,” Sensor and Actuator Fault Detection of Connected Vehicles under imperfect Communication Network“, Accepted in 18th International Conference on Intelligent Transportation Systems, 2016.
- Z. Abdollahi, S.Dey, and P. Pisu, “On Resilient Connected Vehicles under Denial of Service “, American Control Conference 2016.
- Z. Abdollahi, and P. Pisu, “Observer-Based Diagnostic Scheme for Lithium-Ion Batteries,” In Proceedings of the ASME 2015 Dynamic Systems Control Conference (DSCC), October 28-30, 2015, Columbus, Ohio, USA, 2015.
- S. Dey, Z. A. Biron, S. Tatipamula, N. Das, S. Mohon, P. Pisu, and B. Ayalew, “On-board Thermal Fault Diagnosis of Lithium-ion Batteries for Hybrid Electric Vehicle

Application," In Proceedings of the IFAC Workshop on Engine and Powertrain Control, Simulation and Modeling 2015, Columbus, OH, Aug 2015.

CHAPTER ONE

INTRODUCTION

1.1. Research Objectives

Cyber Physical Systems (CPS) represent a diverse class of systems with various applications in critical industrial systems as well as infrastructures such as power grids [1], water distribution systems [2]-[3], Intelligent Transportation System (ITS)[4]-[5], building automation and many other systems vital for human well-being [5]. In general, CPS denoted to a certain category of systems containing three main parts: (i) Physical plants, (ii) Controller and (iii) Communication network (see Fig. 1). Connectivity among different subsystems and the controller via communication network makes CPS faster, more efficient and cost effective. Indeed, communication network eases data transfer process between sensors to controller and controller to actuators. Furthermore, shared communication network is less expensive comparing to wired network of private communication network for each subsystem. However, due to the control center and multi-purpose communication network, critical cyber physical systems are vulnerable to cyber-attacks and network failures as well as physical faults [6].

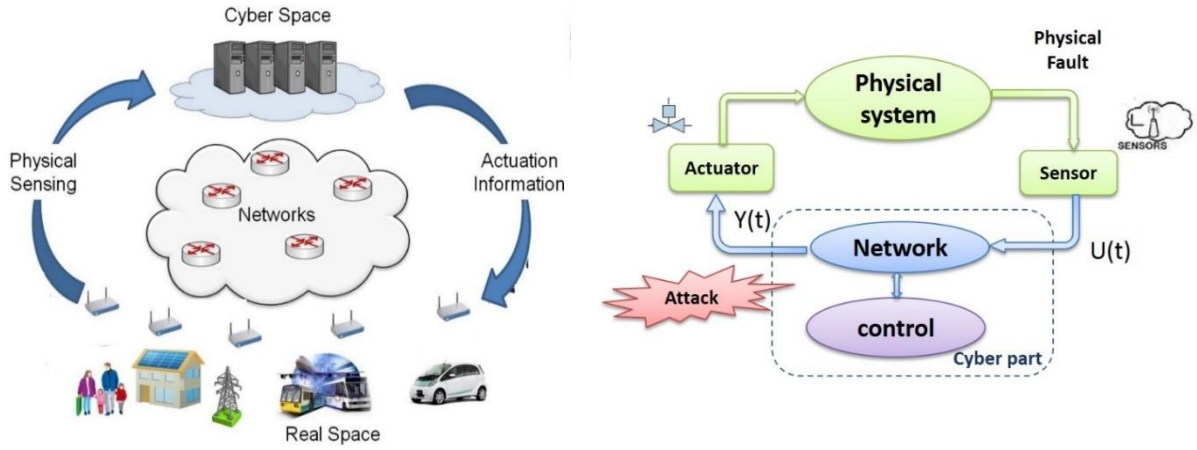

Figure 1: Cyber physical systems and schematic representation of it.

Cyber-attacks, network failures and physical faults (in the physical parts of the CPS) are potential causes that degrade the performance of the cyber physical systems. Physical fault diagnostics of CPS is possible by utilizing the following approaches: 1) model-based approaches, 2) Signal processing based approaches, and 3) Knowledge-based approaches. In contrast, from the system control perspective, security and resiliency of cyber physical systems against cyber-attacks and network failures is more challenging due to the unexpected inherent of cyber-attacks. Some of the common network failures and possible cyber-attacks in CPS referring to the existing literatures are packet drop out [7]-[8], Denial of Service (DoS) attack [9]-[10], replay attack [11] and false data injection [12].

Resiliency of cyber physical systems is indeed a 3S-oriented design, that is, stability, security, and systematicness: Stability means the CPS can achieve a stable sensing-actuation close-loop control even though the inputs (sensing data) have noise or attacks; Security means that the system can overcome the cyber–physical interaction attacks; and Systematicness means that the system has a seamless integration of sensors and actuators.

There two main approaches to tackle the security problem of cyber physical systems: (i) computer science methods (ii) Control oriented methods.

Some of the most common cyber-attacks modeled in CPS in control oriented frame works are depicted in Fig. 3. In majority of the modeling approaches, the CPS is is considered as a linear time invariant (LTI) system or descriptor system.

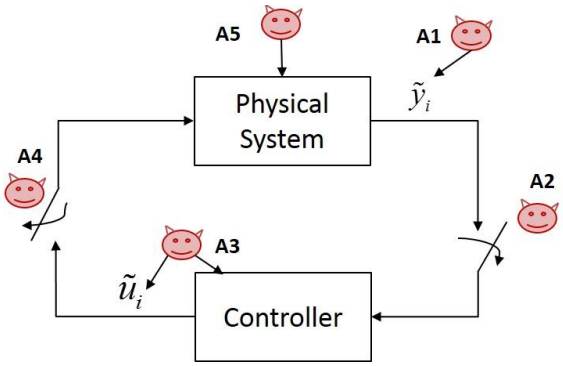

Figure 2: Potential cyber-attacks for a subsystem of CPS

Referring to the control oriented attack analysis in CPS, the false information can include: an incorrect measurement, an incorrect time when the measurement was observed, or an incorrect sender id. The adversary can launch these attacks by obtaining the secret key or by compromising some sensors (A1) or controllers (A3). A2 and A4 represent ***denial of service*** (DoS) attacks where the adversary prevents the controller from receiving sensor measurements or sending an input update. To launch a DoS the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, etc. A5 represents a ***direct attack (false data injection)*** against the actuators or an external physical attack on the plant. Along with cyber-attacks and network failures (such as packet dropping), CPSs subject to physical failures and faults. To secure cyber physical systems against cyber-attacks, we need to make sure that anomaly in CPS

performance is not caused by physical faults of the system. Hence, as a pre-requisite for securing the CPS, a fault diagnostics algorithm is designed to detect potential faults in the system [9].

In light of the above discussion, the objective of this proposed research is to develop a general approach that improves the performance of cyber physical systems making them more resilient to cyber-attacks/ network failures as well as physical failures. Hence, for each possible cyber-attacks/network failure, an algorithm to modify the controller of system and maintain the performance of whole CPS close to normal is presented. Also, along with modified controllers, a fault diagnosis scheme is presented to detect, isolate and estimate physical faults in CPS. Furthermore, as the last part of thesis, we develop a decision making strategy to switch among available control signals to choose the optimum control strategy which guarantees the smoothness of the performance as well as safety. As a case study of this approach, a platoon of connected vehicles communicating through Dedicated Short-Range Communication (DSRC) network is considered.

1.2. Research Motivation

In recent years, we have noticed a rise of ***smart vehicles*** with capabilities like wireless communication, gateways and driving assistance systems. Such smart vehicular advancements have led to several emerging vehicular technologies. One of such technologies as a particular focus of this research is ***connected vehicles*** which is classified as a distributed cyber physical system. Indeed the concept of the connectivity in vehicular network can potentially results in improvements, e.g. minimizing the risk of accident and

increasing traffic throughput. However, this connectivity also introduces new challenges from security point of view.

In modern transportation systems, smart vehicles are not isolated mechanical devices with merely mobility purposes anymore. Nowadays, smart vehicles are equipped with wireless gateways, Bluetooth and Wi-Fi connection enabling them to connect and communicate with external world [13]-[14]. Hence, by developing the communication capabilities to peer to peer, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, the new promising technology as connected vehicles will emerge which, essentially, can improve the safety, efficiency, and effectiveness of the overall transportation system. However, similar to other CPSs, this technology suffers from several challenges, mainly from safety and reliability point of view and is vulnerable to the aforementioned cyber-attacks and network failures [15]-[16].

Hacking the smart vehicles is not an impossible mission and several existing literature explore the vulnerabilities of the smart car regarding to cyber-attack and hacking issues. In [13]-[14], and [17] vulnerabilities of car regarding to the Control Area Network (CAN) bus are explored. Although for the aforementioned vulnerabilities having physical access to the car and more specifically to the On-Board Diagnostics, attacker do not limit themselves to having physical access to the car. Indeed, comprehensive studies in University of California San Diego, University of Washingtonand University of South Carolina reveal that, car hacking without physical access is possible [20]-[18]. In [20], authors present a privacy and security evaluation of wireless Tire Pressure Monitoring Systems (TPMS) using both laboratory experiments with isolated tire pressure sensor modules and experiments

with a complete vehicle system. Fig. 3 shows existing vulnerabilities of a smart car to potential cyber-attacks.

Since each individual smart car is already vulnerable to cyber-attacks, the threat is more critical when a group of vehicles share their information through communication network together as connected vehicles. Fig. 4 explains the potential threat through the internet and telematics units to compromise data in connected vehicles. More specifically, connected vehicular networks are vulnerable to packet dropping [21], communication induced delay [22], scheduling issues and malicious cyber-attacks [23]. Hence, the vehicular control systems must be capable of handling and surviving such adverse situations. The outcome of these researches support importance of the treat of cyber-attacks in connected vehicles that can be injected to the communication network via a hacked car or with a malicious car generating fake identity. A crucial need for designing the in-vehicle control/management systems that takes such issues into consideration and maintains the safety and reliability of the overall system does exist in automotive industries.

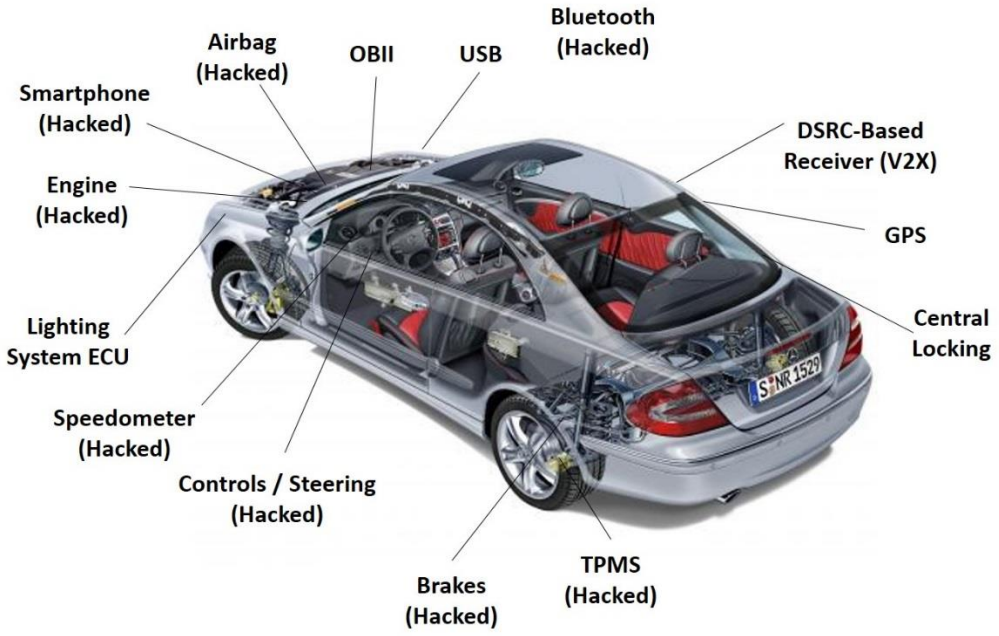

Figure 3: Vulnerabilities in a smart car

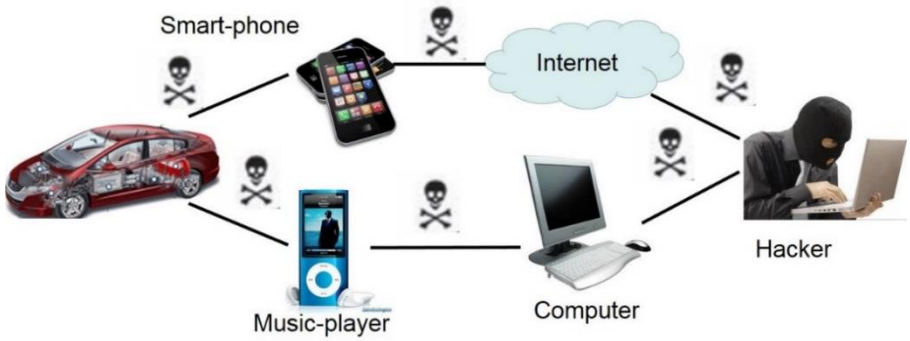

Figure 4: Flow of hacking a car via smart phone

1.3. Research Contributions

The main contribution is the development of control oriented algorithm to provide resiliency in cyber physical systems toward physical faults, network failures and cyber-attacks. This algorithm is an observer based methodology consisting different strategy for different attack scenarios. The best strategy is selected via optimum decision making block

to apply the best available control strategy to the system to maintain the performance under failure or attack. To fulfill this objective, the following contributions are obtained:

- The development of Ordinary Differential Equation (ODE) based and Partial Differential Equation (PDE) based models of connected vehicles for behavior analysis under various cyber-attacks and network failures.
- The development of a fault diagnosis algorithm that detects, isolates and estimates specific sensor faults (relative distance and velocity sensors) and actuator failures (acceleration pedal) in connected vehicles.
- The development of estimation algorithm that estimates the lost pack in the packet dropping phenomena to provide the correct information to the controller. So, the control action maintains resiliency against packet drop incident.
- The development resilient algorithms against DoS attack in the communication network. These algorithms consist of three methodologies for different modeling of DoS attack.
- The development of novel method to model false data injection attack in cyber physical systems as fake node (ghost node).
- The development of PDE based diagnostics algorithm to detect and isolate the false injection attack into the system.

- The development of optimum decision making methodology to select the best in the fault/ cyber-attack occurrence in the system to maintain the performance of the system close to the normal condition.

1.4. Dissertation Organization

The rest of the proposal is organized as follows. Chapter2 includes a brief overview of connected vehicles modeling and working principals. Chapter 3 discusses the security problems in cyber physical systems along with state of the art literature review, gap analysis and a brief review on fault diagnostics and observer design tools. In Chapter 4 provides the proposed algorithm for physical fault diagnostics including faults detection, isolation and estimation. Then, Chapter 5 discusses the proposed algorithm on packet dropping phenomena as network failure. Chapter 5 includes three algorithms on DoS attack detection and estimation along with resiliency to the attack. In Chapter 6, a PDE model of connected vehicles along with novel approach for false data injection attack detection is provided. Chapter 7 explain the decision making strategy for the aforementioned algorithms. Finally, Chapter 9 concludes the dissertation along with the discussion of the future extensions.

CHAPTER TWO

WORKING PRINCIPLE AND MODELING OF CONNECTED VEHICLES

2.1. Working Principle

Some principal simplifying assumptions which will hold for the duration of all our analysis in this proposed research are as the following:

1- A single lane highway only is considered; multi-lane scenarios with lane changing effects are not considered.

2- We assume that the characteristics of all vehicles and drivers are the same. This assumption simplifies calculations but is probably not necessary for our analysis to work.

3- DSRC communication network is a shared broadcasting network. Therefore, each vehicle in the platoon is required to listen to the safety messages communicated in the specific time slot dedicated to safety messages.

2.2. Modeling

The car-following methodology for the simulation and analysis of highway traffic models vehicles as discrete entities moving in continuous space. Referring to the existing works, two common car-following methodologies are Gipps's model and Adaptive Cruise Control (ACC). Gipp's model contains a number of parameters which purport to model different behavioral features of driver, and is thus rather more complicated than the reductionist models which can be found in the mathematical literatures. However, Gipps's

model which is explained in detail in [24]-[25], still too mathematical for control purposes. In contrast to Gipps's model a simplified control oriented car-modeling used in several existing literatures is ACC [26]-[28]. In the current existing Adaptive Cruise Control (ACC) system, the range (i.e., relative distance) and range rate to the preceding vehicle are measured with a radar or LIDAR sensor [26]. While, Cooperative Cruise Control (CCC) [15]-[16] and Cooperative Adaptive Cruise Control (CACC) [29]-[33][33]are essentially a vehicle-following control methodology that automatically accelerates and decelerates so as to keep a desired distance to the preceding vehicle. To do this, in addition to onboard sensors like radars, vehicles should be equipped with wireless communication devices, such as Dedicated Short-Range Communication (DSRC), to receive extra information of the preceding vehicle(s).

The use of CACC control strategy, especially in heavy duty vehicles, can cause lower traffic flow in roads. To achieve this task, onboard sensors such as radar are employed that measures relative distance and velocity between vehicles. Further, additional information of preceding vehicle(s), such as the desired acceleration is received through the wireless communication network. In a cooperative setting, a vehicle should adjust its speed/ acceleration using the information from multiple vehicles ahead and behind. To address this objective several control strategies are considered to be implemented in the vehicle to use the receiving information for vehicle in front and behind, combine them with current states of the car and generate corresponding control input for vehicle. Some of the most important control approaches in cooperative adaptive cruise control are model predictive [33], and

PID [30]-[31] controller. Among these controller, the PID is the most common and more effective and less computationally burden.

Following similar notation of [30], a homogenous platoon of m vehicle equipped with CACC strategy is considered as the case study of this proposed research (see Fig. 5).

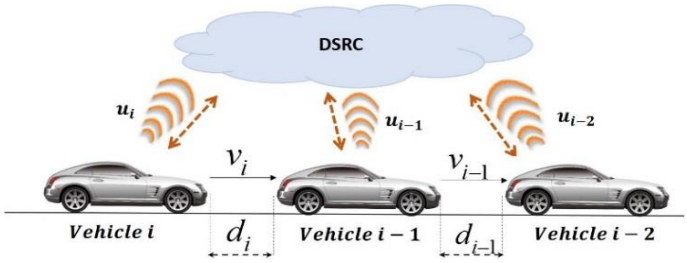

Figure 5: Platoon of vehicles equipped with CACC.

Each vehicle in the platoon can be modeled as a linear system with (1).

$$\begin{bmatrix} \dot{d}_i \\ \dot{v}_i \\ \dot{a}_i \end{bmatrix} = \begin{bmatrix} v_{i-1} - v_i \\ a_i \\ -\frac{1}{\tau} a_i + \frac{1}{\tau} u_i \end{bmatrix} \qquad ,i = S_m \setminus \{1\} \tag{1}$$

where S_m stands for set of all vehicles in the platoon of length of m. $d_i = q_{i-1} - q_i - L_i$ is the distance between vehicle i and $i-1$, where q_i and q_{i-1} are the rear bumper position of vehicle i and $i-1$, respectively, and L_i is the length of vehicle i; v_i is the velocity and a_i is the acceleration of vehicle i. Moreover, u_i is the vehicle input, to be interpreted as desired acceleration, and τ is the time constant representing the driveline dynamics. Also, the following control policy for the inter-vehicle spacing is adopted:

$$d_{r,i}(t) = h v_i(t), \qquad i \in S_m \setminus \{1\} \tag{2}$$

where $d_{r,i}$ is the desired distance between vehicle i and $i-1$, h is the time headway. The main objective is to regulate the d_i to $d_{r,i(t)}$, i.e.,

$$e_i(t) = d_i(t) - d_{r,i}(t) \to 0 \ as \ t \to \infty \tag{3}$$

without losing the generality, we consider $L_i = 0$ for simplicity. Substituting the equation $d_i = q_{i-1} - q_i - L_i$ in (3), the regulating error can be re-written as:

$$e_i(t) = q_{i-1}(t) - q_i(t) - hv_i(t) \tag{4}$$

The following dynamic controller is considered to achieve the zero regulation error:

$$\dot{u}_i = -\frac{1}{h}u_i + \frac{1}{h}(k_p e_i + k_d e_i) + \frac{1}{h}u_{i-1} \tag{5}$$

where u_{i-1} is the desired acceleration for the preceding vehicle. This information is communicated through the DSRC network, hence, it is subject to packet drop failure in the network. k_p and k_d are the controller coefficients. Furthermore, it is shown that for a bounded u_{i-1} and subject to following constraints on the controller gains: $k_p, k_p > 0$, the inter-vehicle distance d_i is regulated to $d_{i,r}$ as defined by spacing policy (2)[31].

The block diagram of the closed- loop system for vehicle *i*, subject to the controller is shown in Fig.6

with

$$G(s) = \frac{q_i(s)}{u_i(s)} = \frac{1}{s^2(\tau s + 1)}$$
$$H(s) = hs + 1$$
$$K(s) = k_p + k_d s$$
$$D(s) = \frac{1}{s} \quad (6)$$

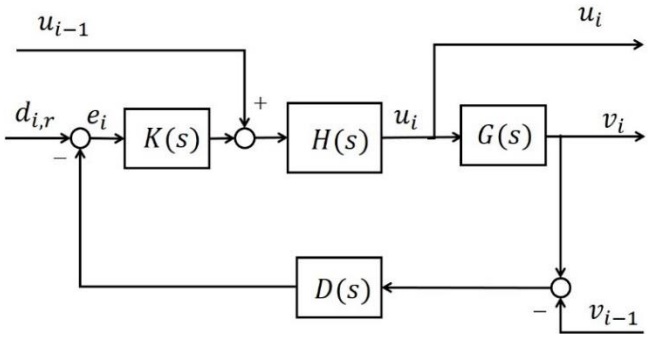

Figure 6: Block scheme of the CACC system

TABLE I: Vehicle platooning model nomenclature

Symbol	Definition and Unit	Symbol	Definition and Unit
$d_{r,i}$	reference relative distance	T_s	network sampling time
h	time headway.	$\chi(k)$	a variable that represents the packet drop out phenomenon at time instant *k*
$e_i(t)$	error	u_i	control input of vehicle *i*
u_{i-1}	the desired acceleration for the preceding vehicle (vehicle $i-1$)	τ	time constant
k_p	controller coefficients	θ_d	equivalent output error injection
k_d	controller coefficients	θ_v	equivalent output error injection
d_i	inter-vehicle distance		
Superscript			
$\pm$	positive/negative electrode		

CHAPTER THREE

SECURITY PROBLEMS IN CYBER PHYSICAL SYSTEMS

As it mentioned in the introduction section, cyber physical systems are subject to physical faults, network failures and cyber-attack. To secure a CPS against these potential sources of performance degradation, a control oriented algorithm is proposed. The algorithm contains three main parts: (1) Physical fault diagnostics; (2) Cyber-attacks/failure resilient strategies; (3) Decision making.

1) Physical Faults Diagnostics: This part includes an observer based fault diagnostics scheme to address issues regarding to the potential physical faults and failures in hardware components in the CPS.
2) Cyber-attacks/network failure resilient strategies: This component acts as a state machine system with several strategies designed for specific cyber-attacks or network failure. Each strategy is designed by utilizing different control theory tools e.g. observer design, adaptive control, and sliding mode theory. These methodologies are used to design resilient strategies for CPS to maintain the functionality of CPS and keep its performance close to the normal when cyber-attacks occur. Hence, by applying corresponding strategy, the CPS will be resilient to that specific attack or network failure.
3) Decision maker: Since all strategies in the Cyber resilient component are independent from each other, to apply the best strategy for the existing cyber-attack or network failure, a decision needs to be made. To obtain this objective a decision making block based on Model Predictive Control (MPC) is designed. At each

sample time, the decision maker block chooses best available control action designed in the previous part while guaranteeing smooth behavior of CPS.

The overview of this research is depicted in Fig.7. In the following each of this component with their design approach will be discussed in details.

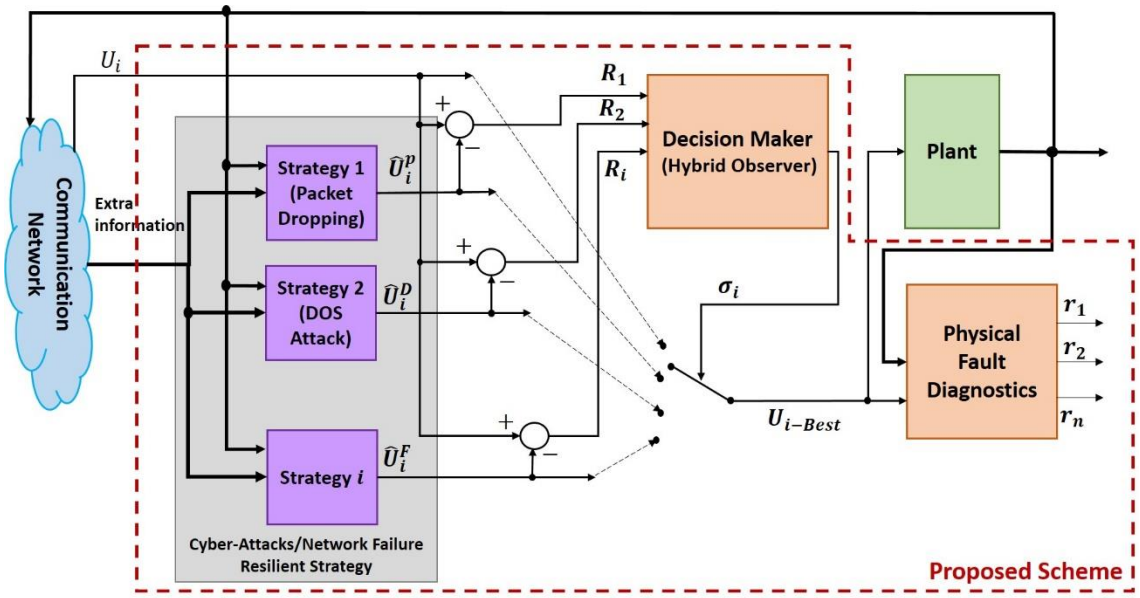

Figure 7: Overview of proposed scheme to secure a CPS

Next, we have a literature review for each component in more detail to provide the existing research gaps.

3.1. Physical Fault Diagnostics Problem

3.1.1. Problem Formulation and Challenges

Similar to any physical systems, cyber physical systems are subjected to physical faults in their components including sensors and actuators and hardware. To secure the CPS against cyber-attacks, normal operation of CPS in no cyber-attacks condition should be guaranteed. This is important due to the connectivity of different parts of a CPS which can

causes to propagate the error of one part to other components of CPS. In more detailed explanation, small error in a sensor readings which is transmitted and propagated to several controller of supplants of a CPS can compromise performance of those sub-plants and interpreted as cyber-attacks while in reality there is no cyber-threat in the system. Similarly, in our case study of connected vehicles, wrong velocity sensor or acceleration information can be transmitted to follower vehicles and degrade their control strategy and provide an error in regulating the desire distance. Consequently, the error propagation inside the string of the platoon can treat the stability of sting by either breaking the platoon or causing accident in the platoon. Hence, reliability of CPS is a critical issue that need to be addressed. Different failure mechanisms can occur in a CPS during operation, but, the most important and significant ones relate to sensor and actuator faults. Some of these faults, if not detected or isolated, may lead to catastrophic failures. At a higher level, diagnostic problem in a CPS can be classified into three types based on the component where the failure occurs: sensor fault, process/system fault, actuation fault.

In a broad classification, existing approaches can be divided into three groups: 1) Model-based approaches, 2) Signal processing based approaches, and 3) Knowledge-based approaches. Model-based approaches utilize a dynamic model of the system in their diagnostic algorithm. Signal processing based approaches use different kinds of spectral analysis, time series analysis and statistical methods such as pattern recognition, feature extraction etc. In knowledge based approaches, a priori knowledge of the system is used along with some reasoning algorithms. In this discussion, we will concentrate on model-

based diagnostic approaches due to the availability of the dynamic model of most of the CPSs.

3.1.2. Literature Review

In this research, we focus on model-based fault diagnostics approach to detect, isolate faults and failures in CPS. In the model-based diagnostics a dynamic model of the system is used to predict the output which is compared to the measured signals from the physical system. The difference between the measured data and predicted data is used to generate a residual signal which has the idealized property of being zero in case of no faults and nonzero in presence of faults. This residual signal is then processed further to achieve isolation of the detected faults. Model-based designs of fault diagnosis scheme follow the sequential steps: system and fault modeling, fault detectability analysis, residual generation, fault isolation and decision making. Surveys of different model-based schemes can be found in [34]-[35]. Faults generally occur in sensors, actuators or in the process. Actuator and sensor faults are generally modeled as additive deviations from the nominal model whereas process faults are generally modeled as multiplicative faults which reflect as changes in parameters. In our case study as CPS, the potential faults and failures can occur in vehicles actuators and sensor measurements which are transmitted to other vehicles in the platooning network via DSRC.

Vehicle diagnostics are widely explored and is one of the utmost interest for automotive industries and OEMS. Hence, several researches for improving the functionality of On-Board Diagnostics (OBD_II) are going on. However, unlike fault diagnostics on engine operation which is explored widely, kinematic characteristics of the vehicle such

velocity sensor, radar sensor faults as well as acceleration pedal failure are not considered in the on-board diagnostics [36]-[37].In the intelligent transportation where a vehicle shares its information among other vehicles in the vehicular network, wrong information not only treat the safety of individual car, but also, it can threaten other vehicles performance. Faulty sensors can affect the individual vehicle's safe operation and in turn will create a potentially unsafe node in the vehicular network. Nevertheless, there are very few literatures address this issue of connected vehicles. [38], presents an approach to address some of the challenges in connected vehicle system fault diagnostics, such as the diagnostics of unexpected faults, and infrequent or intermittent faults. However, the existing literatures do not consider potential faults in the sensor measurements which can be transmitted through the DSRC communication network to other vehicles in the vehicular network. In this research, we address the sensor and actuator fault detection and analyze the identifiability of these faults and failures in connected vehicles.

3.1.2. Gaps in Existing Literature

- There is no complete research on connected vehicles fault diagnostics with specific focus on sensor and actuator fault detection which their data is transmitted through communication network.
- No fault estimation approach to compensate the effect of existing faults in the system and design fault tolerant control.
- Most of the existing model-based fault detection approaches have one or more of the following issues: 1) utilize a linearized model, 2) are computationally expensive, and 3) lack theoretical guarantees of the convergence of the estimator.

3.2. Cyber Attacks/Network Failures Problem

3.2.1. Problem Formulation and Challenges

The performance of CPS highly relies on the reliability of its communication network specifically if there is no physical malfunctioning in the system. Hence, providing good maintenance on the hardware of the CPS and health monitoring via fault diagnostics approaches, guarantees the physical performance of a CPS. However, cyber-attacks, malicious adversaries and network failure are still some of the crucial sources of performance degradation in cyber physical systems which are not possible to detect via physical fault diagnostics methods.

One of the most common failure in the communication network is packet dropping phenomena. Wireless links are known to be prone to errors and failures. Packet dropping occurs due to a number of factors including occasional hardware failures, degradation in link quality, and channel congestion *etc*. Although many network protocols have re-transmission mechanisms embedded, for real-time feedback control data, it may be advantageous to discard the failed packets on their first transmission because re-transmitted packets may have too large latency to be useful [39]. Re-transmission may also delay the transmission of new packets. In a typical CPS, due to limited computing power of the communication modules, error correction techniques are not common on the lower network levels. However, cyber-attacks are not considered as network failures and in fact they have designed smartly by attacker. Hence, modeling the cyber-attacks from control perspective is more challenging than network failures and requires detailed analyses over network and attacker capabilities. The most common cyber-attacks on CPS referring to the existing

literature consists of Denial of Service (DoS) attack, False Data Injection attack (or deception attack), Replay attack and Stealthy attack.

Denial of service (DoS) attacks are perhaps the most detrimental attack to CPSs that affects the packet delivery because they have been proven capable of shutting an organization off from the Internet or dramatically slowing down network links [40]. Definition of DoS attack may vary in different studies on DoS attack, however, all these studies describe the effect of DoS attack as the same. The violation of availability of sensor and control data is known as denial-of-service (DoS). DoS attacks can be classified into several different types, in which the packet flooding attack and data jamming or compromising by a malicious adversary are prevalent [41]-[42]. Attackers may flood a network with a large volume of data to deliberately consume the limited resources, such as CPU cycles, memory, network bandwidth, and packet buffers. Consequently, time delay and packet loss of transmitted information in CPS become worse under such attacks, which in turn may significantly impair the system performance. False data injection attack is a well-studied attack in cyber physical systems particularly in recent years. In false data injection attack scenario, the attacker has the capability to corrupt the original message by injecting additional false data into the actual value. The message either is transmitted form sensors to the controller or from the controller to actuators [43]. The attacker in the replay attack intercepts data of the system and re-transmits it while corrupting the performance of the system [44] . Another cyber-attack studied in the cyber physical systems is stealthy attack. In the stealthy attack, the attacker wishes to induce perturbation in the

control loop by compromising a subset of the sensors and injecting an exogenous control input, without incurring detection from an anomaly detector [45].

With every day new emerging technologies, new cyber-attacks are developed and it is not possible to keep track of all existing cyber-attacks in one research. However, the effect of the majority of these attacks can be modeled with one or several of these existing dominant attacks.

3.2.2. Literature Review

The main challenges regarding to securing a CPS toward cyber-attacks contains of modeling the cyber-attacks, detecting and developing resilient strategy to maintain the functionality of the CPS in the presence of cyber-attacks. In this section, we provide literature review over all these three challenges on cyber-attacks in cyber physical systems.

Modeling cyber-attacks is essential for understanding and analyzing their impacts on Cyber-physical Systems (CPSs). There are two main methods for modeling cyber-attacks: *graph-based* approaches, and *mathematical (Control-oriented)* modeling approaches.

Both static and dynamic graph-based techniques such as attack trees and Bayesian networks are well-known for attack modeling as they have the advantage of combining user friendly, visual features with algorithms that allow analysis of the behavior of the attack in the network [46]-[49]. For example, Petri net modeling approaches [49] have been used as a more flexible method for modeling the cyber-attacks in large cyber physical infrastructures such as smart grids. For such a complex CPS, hierarchical methods for

constructing large petri nets from smaller size petri nets have also been proposed [49]. Although graph-based approaches have their advantages for engineering applications that involve the design of attack detection methods, security analysis and security design in large scale CPSs, in industrial applications these models are too complex to be used. Instead of graph-based models, mathematical approaches for modeling the attack in SCADA (Supervisory Control and Data Acquisition) have been used for CPSs such as power networks and smart grids. In [50] In mathematical approaches, cyber-physical systems are typically modeled as time-varying or, the authors considered the large scale CPS as linear discrete-time decentralized system, which can be modeled by state space equations and the cyber-attacks are modeled as additional exogenous inputs that comprise behavior of system's components [51]-[53]. However, it is not possible to model all cyber-attacks and network failures just as an exogenous inputs in the system as they affect the whole CPS dynamics in different manners. Several investigation are done on modeling the cyber-attacks in control frameworks with particular focus on specific attack.

A wide range of works exists on that explored the data loss problem and physical fault diagnosis problem in general networked control systems. Packet dropping phenomena provides unreliability and uncertainty into the communication which makes the modeling of the network and analysis of data more challenging task [27]-[28], [37]. In general, there are two methods to model the packet drop out phenomenon in communication networks: (1) Bernoulli model [54],[15] [58]- [64]and (2) Markov Model [7]-[8], [55]-[56]. Bernoulli random variable is a simple memory less random variable while, modeling the packet

dropping with Markov Model is a more complex and sophisticated methodology which captures most of the characteristics of the packet dropping phenomena.

Cyber-attacks are explored and modeled in various cyber physical systems. DoS attack is explore in power system [66] [68], smart grids [69], SCADA [70], and networked control systems [66]-[67]. [69] discusses Malicious attacks targeting availability of gird network as denial-of-service (DoS) attacks, which attempt to delay, block or even corrupt information transmission in order to make network resources unavailable to communicating nodes that need information exchange in the smart grid. In the existing literature on DoS modeling, there are two main methodologies to model Denial of Service attack in a CPS with control frame work; 1) time delay 2) packet loss [40]-[41]. Indeed, based on the network communication protocol and attacker capabilities, DoS attacker can flood too much data on the network to make packet congestion on the network and consequently packet will loss. However, if the attacker does not make the attack too obvious on the network, it may flood the packets randomly on the network and try to increase the service time on the communication network [42].

False Data Injection attack is widely explored in cyber physical systems e.g. power grid [75]-[76] electricity marker [71], water distribution and control systems [72]-[73]. The false data injection attack in CPS refers to a class of cyber-attacks in which the attacker wishes to alter the integrity of system by compromising a subset of sensors and sending inaccurate readings to controller or actuators data from controller. To operate the attack, the attacker needs to carefully design his input to fool the controller since abnormal sensor measurements will generally trigger an alarm [72]. In the majority of

existing literature on modeling false data injection attack in control oriented framework, the attack is modeled as an additive sensor/actuator fault on the original data. Hence, existing fault detection algorithms, including Kalman filter [71]-[72] observer design [75], are capable of detecting the false data injection attack in the system. However, developing new skills to inject the cyber-attacks in the cyber physical system, attackers can induce more intelligent attacks which are not diagnosable with fault detection methodologies.

The second challenge in securing the CPS toward cyber-attacks is to provide the CPS with an attack detection algorithm. There exist several investigations on modeling and detection of cyber-attacks from computer science perspective. The current state of the art methods used for cyber-attack detections are utilization of Intrusion Detection Systems (IDS) and Honeypots. Intrusion detection systems continuously monitor the computer system or network and generate alarms to inform the system administrator of suspicious events. IDSs are now considered a necessary addition to the security infrastructure of an organization [77]-[78]. The objective of intrusion detection is to detect malicious activities, and accurately differentiate them from benign activities. Honeypots are needed to supplement IDSs in the proposed security scheme because they complement most other security technologies by taking a proactive stance. A honeypot is a closely monitored computing resource used as a trap to ensnare attackers. As defined by Spitzner, "A honeypot is a security resource whose value lies in being probed, attacked, or compromised [79]." The principal objectives of honeypots are to divert attackers away from the critical resources and study attacker exploits to create signatures for intrusion detection. The attraction of

attackers to honeypots mitigates the threat of malicious attacks and thus helps secure valuable information and important services located on the real targets.

As the last but very crucial challenge of cyber security in CPS, attack resiliency is utmost importance to maintain the functional of the CPS in the presence of cyber-attacks. However, very few works explore resiliency of systems under attacks and network failures. Several groups have looked at control systems with packet loss in their communication network, an area that has been recently surveyed in the context of packet-switched networks by Hespanha [57]. In particular, there has been considerable effort in analyzing the effect of packet loss [58]-[60]. Also, several approaches have been used to compensate the impact of packet drop out in networked control systems. For instance [61], uses a predictor to modify the controller in the presence of packet drop out. Generally speaking referring to the existing literature, to modify the controller in most of the networked control systems and cyber physical systems, a good state estimation is required. State estimation over packet dropping networks is explored in the existing literature with different methodologies such as discrete Kalman filter with intermittent observation [54], [64], optimal estimation [59],[61], and using multiple description coding [62]. Although these general results exist for networked control systems, very few attempts have been made towards the similar issues in connected vehicle applications [64]. In [10],[113] DoS is considered as a class of attack strategies primarily intended to affect the timeliness of information exchange. The fundamental challenge in DoS attack compensation is to develop a resilient controller to keep the performance of the CPS close to the normal while measured sensor information

are corrupted by attacker. In [5],[113][112], authors comprehensively survey the concept and strategies for building a resilient and integrated cyber–physical system (CPS).

Furthermore, the DoS attack in the DSRC network degrades the quality of packet transmission and induce delay in network service time and consequently in transmission. Therefore, to develop a countermeasure on DoS attack in the connected vehicles system, an estimation of states over delay induced by the attack on communication network is required. The state estimation and fault detection problems over random measurement delays are studied for cyber physical systems and the networked control systems in several existing literatures [114]-[118]. Different approaches including sliding mode observer design [118], robust estimation [119], Continuous Time Hidden Markov Model (CTHMM) [120] and discrete time approaches based on state feedback theory and Kalman filter observer design [115] are developed and proposed in literatures to estimate the states of the CPS under delayed measurements. However, in majority of the existing literatures, the delay induced in the measurements due to the communication network is considered to be known. While, under the DoS attack this assumption no longer is valid. Consequently, a new approach to estimate the state of the CPS under DoS attach which degrade the service time of the communication network is required.

3.2.3. Gaps in Existing Literature

- Majority of existing literature address the effect of packet dropping in CPS system by holding the previous value of lost data which is not necessarily applicable for connected vehicles system with changing driving profile.

- Several studies try to estimate the lost information using Kalman filter with intermittent observation, while this approach is limited for discrete time systems.
- **Very few** study on fault estimation over imperfect communication network and in all these works the dynamics of fault are known and it changes very slow which is a big assumption.
- Real time fault diagnostics under communication failure was not explored for connected vehicles
- Very few literature exists on actuator fault detection in connected vehicles
- State estimation under unknown delay are not explored for CPS and connected vehicles.
- Very few researches on probabilistic delay with known distribution, however, there is no estimation on delay in observer.
- Lack of theoretical proof of estimation error convergence
- In the majority of existing literature, the false data injection attack is modeled very similar to additive fault/failure in the control oriented frameworks Considering general topology (configuration) for cyber physical systems, it is very likely to detect the injected attack using different methodologies available for model-based diagnosis e.g. Kalman filter [28]. However, with all technology enhancements, cyber-attacks are become smarter and smarter which make them impossible to be detected via traditional fault diagnosis methods.
- The effects of fake identity (fake node) in cyber physical systems is explored very rarely.

- There is no work on detection and isolating the fake identity in cyber physical system as well as connected vehicles.

3.3. Brief Review of Existing Fault Diagnosis and Observer Design Approaches

In this section, a brief review of the existing fault diagnosis approaches for general systems has been provided. In a broad classification, existing approaches can be divided into three groups: 1) Model-based approaches, 2) Signal processing based approaches, and 3) Knowledge-based approaches [34]. Model-based approaches utilize a dynamic model of the system in their diagnostic algorithm. Signal processing based approaches use different kinds of spectral analysis, time series analysis and statistical methods such as pattern recognition, feature extraction etc. In knowledge based approaches, a priori knowledge of the system is used along with some reasoning algorithms. In model-based approaches, dynamic system model is used to predict the output which is compared to the measured signals from the physical system. The difference between the measured data and predicted data is used to generate a residual signal which has the idealized property of being zero in case of no faults and nonzero in presence of faults. This residual signal is then processed further to achieve isolation of the detected faults.

Model-based designs of fault diagnosis scheme follow the sequential steps: system and fault modeling, fault detectability analysis, residual generation, fault isolation and decision making. Surveys of different model-based schemes can be found in [35], [83]. Faults generally occur in sensors, actuators or in the process. Actuator and sensor faults are

generally modeled as additive deviations from the nominal model whereas process faults are generally modeled as multiplicative faults which reflect as changes in parameters. Coming to the residual generation, there are various existing approaches some of which are given below:

Parity relation approach: In parity space approach [86], the fundamental idea of diagnosing a fault is by checking consistency of the mathematical relationships of the system using available measurements [35].

Observer based method: In this method, an observer is used to estimate the states of the system using available measurements. Then the estimated states along with the measurements are used to generate the residual signals. There are several variations of the observer based methods. For example, in unknown input observers [84], the state estimation error is decoupled from the unknown input disturbance and noise. In Kalman filter based method [85], the innovation sequence is used as residual signals.

Parameter estimation approach: This approach is based on the hypothesis that faults in the system change the system parameters **Error! Reference source not found.**. Therefore, ny deviation from the nominal parameter value will be an indication of fault.

Decision making is another important aspect of the fault diagnosis scheme. After the residual is generated, it needs to be evaluated. This is critical because in general the residuals do not have the ideal property of being zero in non-faulty condition due to model uncertainties, disturbances, noise etc.

CHAPTER FOUR

PHYSICAL FAULT DIAGNOSTICS ALGORITHM

Fault detection, isolation and estimation play important roles in assuring normal performance of the CPS. Health monitoring of the CPS including the fault diagnostics improves the reliability of the system and prohibits physical malfunctions to degrade the whole functionality of the CPS. Indeed, fault detection and estimation provide necessary information for the system to make the controller fault tolerant. In this chapter, a model based diagnostics scheme based on sliding mode approach is proposed to detect and isolate sensors faults and actuator failures in the platoon of vehicles as an example of CPSs.

In this part, we consider a platoon of connected vehicles equipped with CACC as our case study. Furthermore, two nonlinear observer designs have been presented based-on a linear model of each vehicle in the platoon. Both observers are based on sliding mode approach based on the measurement on relative distance and velocity of each vehicle. Using this algorithm, apart from detecting and isolating faults in relative distance and velocity and failure in actuator, it is possible to estimate the fault in both sensors. The convergence of error dynamics is proved using Lyapunov theorem. The developed scheme is a new contribution to connected vehicles diagnostics research area with the following characteristics: 1) Considers essential faults and failures in the system, 2) Theoretical verification of the convergence of the state estimation error, 3) Theoretical verification of fault estimation, and 4) Simple design and computationally efficient.

4.1. State Space Modeling

Each vehicle in the platooning can be modeled as a linear time invariant system as it is discussed in Chapter 2. This linear model is written in the form of state space representation as following

$$\begin{bmatrix} \dot{d}_i \\ \dot{v}_i \\ \dot{a}_i \end{bmatrix} = \begin{bmatrix} v_{i-1} - v_i \\ a_i \\ -\frac{1}{\tau} a_i + \frac{1}{\tau} u_i \end{bmatrix}, \qquad i = S_m \backslash \{1\} \tag{7}$$

where the control input dynamics changes with state feedback and external inputs coming from the vehicle in front through the DSRC network.

$$\dot{u}_i = -\frac{1}{h} u_i + \frac{1}{h}(k_p e_i + k_d \dot{e}_i) + \frac{1}{h} u_{i-1} \tag{8}$$

and

$$e_i(t) = d_i(t) - h v_i(t) \tag{9}$$

Remark 1: We consider a homogenous platoon of vehicles. Therefore, all vehicles in the platoon the same parameters. Also, each vehicle in the platoon, measures relative distance with respect to preceding vehicle d_i and its velocity.

Remark 2: The estimates of the sensor faults are fed back to the control policy to compensate for the effect of these faults. Therefore, the control policy is extended to be reconfigurable under such sensor faults.

Remark 3: Considering measurement on actuator signal of the vehicle, similar approach can be applied for actuator fault to detect and estimate the failure in acceleration pedal position. To avoid redundancy for now we focus on sensor faults.

4.2. Diagnostics Scheme

The objective of the *Sensor Fault Observers* is to detect, isolate and estimate faults in the on-board sensors, namely the range sensor (which measures d_i) and velocity sensor (which measures v_i). It consists of two observers designed based on sliding mode methodology which will be discussed shortly.

In presence of the faults, the measurements from the sensors can be written as:

$$d_{im} = d_i + \Delta d_i \tag{10}$$

$$v_{im} = v_i + \Delta v_i \tag{11}$$

where d_{im} and v_{im} are the measured variables and, Δd_i and Δv_i represent the sensor faults.

Remark 4: Note that, we have modelled the sensor faults as additive variables. These additive variables represent: 1) bias type of faults which could be constant or time-varying, or, 2) sensor gain faults where $d_{im} = Kd_i = d_i + \Delta d_i$ with $\Delta d_i = (K-1)d_i$ where K represents the gain fault.

The observer structure is depicted in Fig. 8 and mathematically expressed as

$$\begin{bmatrix} \dot{\hat{d}}_i \\ \dot{\hat{v}}_i \\ \dot{\hat{a}}_i \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix} \begin{bmatrix} \hat{d}_i \\ \hat{v}_i \\ \hat{a}_i \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} v_{i-1} + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} u_i + \begin{bmatrix} L_{12} \\ 0 \\ 0 \end{bmatrix} (v_{im} - \hat{v}_i)$$

$$+ \begin{bmatrix} \eta_{11} & 0 \\ 0 & \eta_{22} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \mathrm{sgn}(d_{im} - \hat{d}_i) \\ \mathrm{sgn}(v_{im} - \hat{v}_i) \end{bmatrix}$$

$$i = S_m \backslash \{1, 2\} \tag{12}$$

Furthermore, we define

$$\tilde{d}_i = d_i - \hat{d}_i, \tilde{v}_i = v_i - \hat{v}_i, \tilde{a}_i = a_i - \hat{a}_i \quad (13)$$

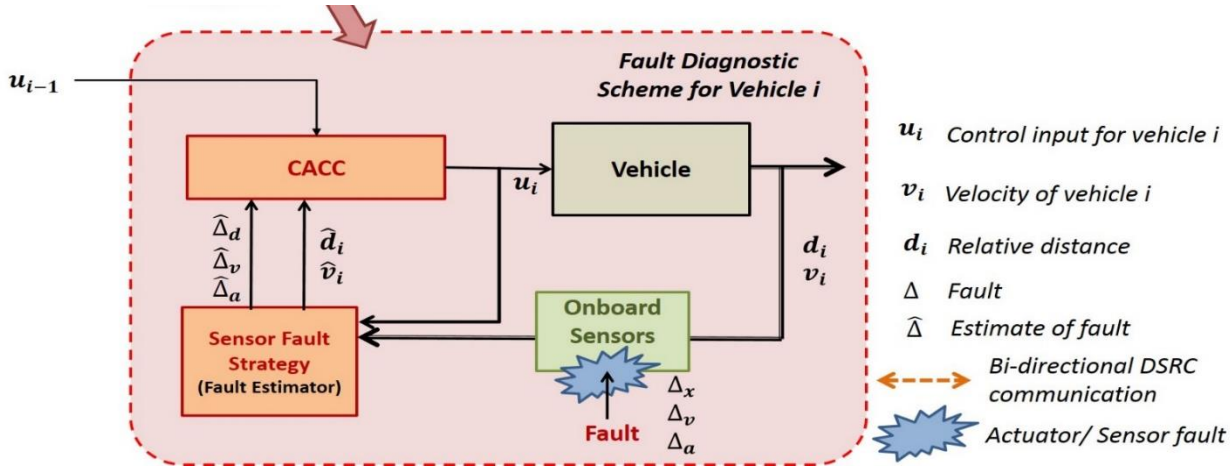

Figure 8: Fault diagnostics scheme for connected vehicles

Remark 5: Note that, u_i is control input of vehicle i which derived by the following dynamics:

$$\dot{u}_i = -\frac{1}{h}u_i + \frac{1}{h}(k_p e_i + k_d \dot{e}_i) + \frac{1}{h}u_{i-1}$$

Next, choosing $L_{12} = -1$, the error dynamics under faults can be written as:

$$\begin{bmatrix} \dot{\tilde{d}}_i \\ \dot{\tilde{v}}_i \\ \dot{\tilde{a}}_i \end{bmatrix} = \begin{bmatrix} \Delta v_i - \eta_{11}\mathrm{sgn}(\tilde{d}_i + \Delta d_i) \\ \tilde{a}_i - \eta_{22}\mathrm{sgn}(\tilde{v}_i + \Delta v_i) \\ -\frac{1}{\tau}\tilde{a}_i \end{bmatrix} \quad (14)$$

Note that, under asymptotic condition, $\tilde{a}_i \to 0$ as $t \to \infty$ due to its first order stable dynamics represented by the time constant τ. Under the condition $\tilde{a}_i \to 0$, we analyze the observer error under two different fault cases.

The sliding surfaces (which are defined by the terms inside 'sign') are $S_d = \tilde{d}_i + \Delta d_i$ and $S_v = \tilde{v}_i + \Delta v_i$. The convergence to the first sliding surface can be analyzed using

the Lyapunov function candidate $V_d = 0.5S_d^2$. The derivative of the Lyapunov function candidate can be written as:

$$\dot{V}_d = S_d \dot{S}_d = S_d \left(\dot{\tilde{d}}_i + \Delta \dot{d}_i \right)$$

$$\dot{V}_d = S_d \left(\Delta v_i - \eta_{11} \text{sgn}(S_d) + \Delta \dot{d}_i \right)$$

$$\Rightarrow \dot{V}_d \leq |S_d| \left(|\Delta v_i + \Delta \dot{d}_i| - \eta_{11} \right) \quad (15)$$

Therefore, under the assumption of bounded Δv_i and $\Delta \dot{d}_i$, and a choice of sufficiently high positive gain η_{11}, we have $\dot{V}_d < 0$ and, hence the sliding surface $S_d = 0$ can be reached. Now, on the sliding surface, we have $S_d = \dot{S}_d = 0$ [88]. Therefore, based on the error dynamics equation (14) and the aforementioned conditions $S_d = \dot{S}_d = 0$, we can write that:

$$-\Delta \dot{d}_i = \Delta v_i - \theta_d$$

$$\Rightarrow \Delta \dot{d}_i + \Delta v_i = \theta_d \quad (16)$$

where θ_d is the equivalent output error injection which is the filtered version of the switching term $\eta_{11} \text{sgn}(S_d)$. For implementation, we can extract θ_d by passing $\eta_{11} \text{sgn}(S_d)$ through a low-pass filter of unity gain [88].

Similarly, the convergence to the second sliding surface can be analyzed using $V_v = 0.5S_v^2$. The derivative can be written as:

$$\dot{V}_v = S_v \dot{S}_v = S_v \left(\dot{\tilde{v}}_i + \Delta \dot{v}_i \right)$$

$$\Rightarrow \dot{V}_v = S_v (-\eta_{22} \text{sgn}(S_v) + \Delta \dot{v}_i)$$

$$\Rightarrow \dot{V}_v \leq |S_v|(|\Delta\dot{v}_i| - \eta_{22}) \quad (17)$$

Therefore, under the assumption of bounded $\Delta\dot{v}_i$ and a choice of sufficiently high positive gain η_{22}, we have $\dot{V}_v < 0$ and, hence the sliding surface $S_v = 0$ can be reached. Now, on the sliding surface, we have $S_v = \dot{S}_v = 0$ [88]. Therefore, based on the error dynamics equation (14) and the aforementioned conditions, we can write that:

$$\Delta\dot{v}_i = \theta_v \quad (18)$$

where θ_v is the equivalent output error injection which is the filtered version of the switching term $\eta_{22}\text{sgn}(S_v)$[74]. For implementation, we can extract θ_v by passing $\eta_{22}\text{sgn}(S_v)$ through a low-pass filter of unity gain [88].

Assumption 1: we consider only one fault can occur at the same time (either Δv_i or Δd_i) as single fault scenario.

Next, we analyze these two fault cases separately:

Case 1 ($\Delta v_i = 0, \Delta d_i \neq 0$): We have $\Delta\dot{d}_i = \theta_d$, $\theta_v = 0$. Therefore, we can construct the following filter to estimate the fault:

$$\dot{R}_{1i} = \theta_d \quad (19)$$

where R_{1i} is the residual signal (output of the filter (30)) which serves as an estimate of the fault Δd_i; and the input signal θ_d to the filter (19) is extracted from the switching term $\eta_{11}\text{sgn}(S_d)$ as mentioned before.

Case 2 ($\Delta v_i \neq 0, \Delta d_i = 0$): We have $\Delta v_i = \theta_d, \Delta\dot{v}_i = \theta_v$. Therefore, we can construct the following filter to estimate the fault:

$$\dot{R}_{2i} = \theta_v \quad (20)$$

where R_{1i} is the residual signal (output of the filter (20)) which serves as an estimate of the fault Δv_i; and the input signal θ_v to the filter (20) is extracted from the switching term $\eta_{22}\text{sgn}(S_v)$ as mentioned before.

Based on the above analysis, the following fault signature table (Table 3) can be constructed. Note that, in case of Δd_i fault, we have $\theta_d \neq 0, \theta_v = 0$ and hence $R_{1i} \neq 0, R_{2i} = 0$. In case of Δv_i fault, we have $\theta_d \neq 0, \theta_v \neq 0$ and hence $R_{1i} \neq 0, R_{2i} \neq 0$. This signature can be used to detect and isolate the faults. Further, the estimates of the faults Δd_i and Δv_i will be R_{1i} and R_{2i} respectively.

Table 2. Fault signature table

Residual	Velocity sensor fault	Range sensor fault
R_{1i}	1	1
R_{2i}	1	0

4.3. Simulation studies

This subsection shows the results regarding the performance of *Sensor Fault Observers*. Note that, the estimated value of the fault under fault occurrence is fed back to the CACC controller to compensate for the fault effect. To evaluate the performance of the proposed diagnostic scheme, two scenarios are considered:

Scenario 1: A bias fault of 3 m/s is injected in the velocity sensor of vehicle 3 at $t = 450\ s$. Fig. 9 illustrates the performance of the diagnostic scheme (*Sensor Fault Observers*) under two cases: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme. The first subplot of Fig.9 shows the injected velocity sensor fault and the estimated value of this fault by the *Sensor Fault Observer*. In the second subplot of Fig. 9, the relative distance between vehicle 3 and vehicle 2 is shown. It can be seen from Fig. 9 that at least four crashes happen in this specific driving cycle under typical CACC. However, applying the CACC with the proposed diagnostic scheme, these crashes are avoided. Therefore, it can be concluded that the proposed diagnostic scheme is able to improve the performance of the connected vehicle system.

Scenario 2: Similar to the velocity sensor's fault scenario, a bias fault with amplitude of $1.5\ m$ is injected on range sensor at $t = 350\ s$. Fig.10 illustrates the performance of the diagnostic scheme (*Sensor Fault Observers*) under two cases: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme. The first subplot of Fig.10 shows the injected range sensor fault and the estimated value of this fault by the *Sensor Fault Observer*. In the second subplot of Fig. 10, the relative distance between vehicle 3 and vehicle 2 is shown. It can be seen from Fig. 10 that six crashes happen in this specific driving cycle under typical CACC. However, applying the CACC with the proposed diagnostic scheme, these crashes are avoided. Therefore, it can be concluded that the proposed diagnostic scheme is able to improve the performance of the connected vehicle system.

Simulation Scenario: A homogenous platoon of five vehicles equipped with CACC control strategy is considered. The leader of the platoon follows the scaled and modified US06 driving cycle. Vehicle parameters are taken from [30] and [31]. The results are illustrated as the follows.

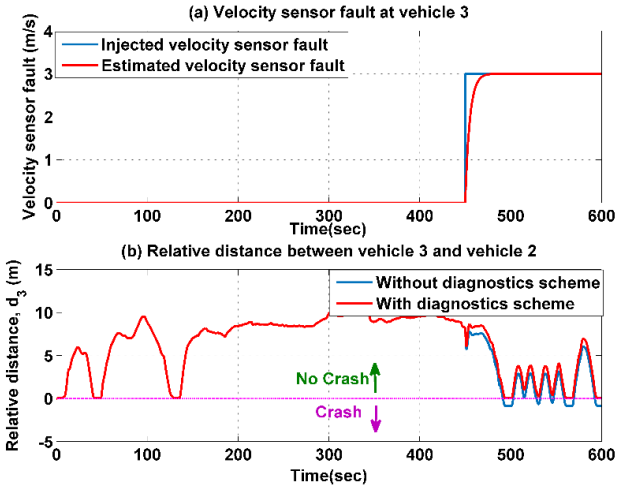

Figure 9: (a) Injected and estimated velocity sensor bias fault. Fault amplitude 3 m/s and injection time t=450 s. (b) Relative distance between vehicle 2 and vehicle 3 (d_3) under the velocity sensor fault. Two cases are considered: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme.

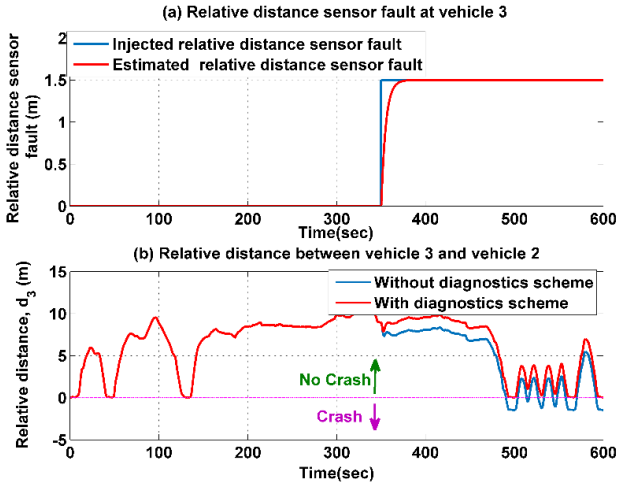

Figure 10: (a) Injected and estimated range sensor bias fault. Fault amplitude 1.5 m and injection time t=350 s. (b) Relative distance between vehicle 2 and vehicle 3 (d_3) under the range sensor fault. Two cases are considered: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme.

Remark 6: In case of having measurement on acceleration of the system, we can isolate and estimate the actuator fault in the similar way.

Table 3. Fault signature table II

Residual	*Velocity sensor fault*	*Range sensor fault*	*Actuator fault*
R_{1i}	1	1	0
R_{2i}	1	0	1

Fig.11 shows the results of having fault in relative distance sensor, velocity sensor and acceleration pedal sensor. In order to distinguish and estimate failure in actuator we need measurement on acceleration pedal position. However, with lack information we still can detect this failure too.

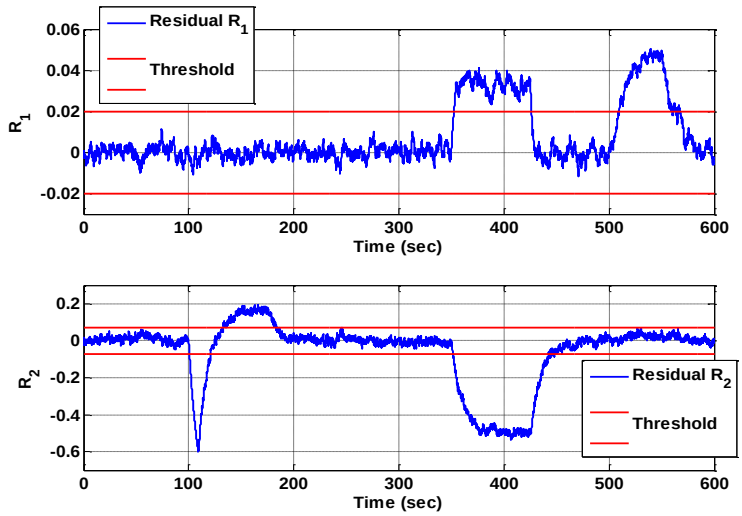

Figure 11: Physical faults and failures signatures

CHAPTER FIVE

RESILIENT STRATEGY TOWARD PACKET DROP OUT

In this section, we explore the problem of network failure simultaneously with on-board sensor faults for a connected vehicle system. A homogeneous platoon of vehicles under Cooperative Adaptive Cruise Control (CACC) strategy is considered as a case study of connected vehicles. The aim of this section of the proposed research is to modify the existing control strategy by adding a new modifying observer based strategy to estimate the lost information due to the packet dropping of the communication network. This will make the CACC controller robust to the packet drop out in the network. The proposed scheme consists of two components: 1) a Kalman filter to reconstruct the data received via unreliable communication network and by adding the fault diagnostics in previous section we can have, 2) sensor fault observers based on sliding mode methodology to detect, isolate and estimate the sensor faults under packet dropping phenomena.

5.1. Packet Dropping Modeling

Analyzing DSRC communication network [23],[110]-[111] with particular attention of sending safety messages, we concluded that Bernoulli approach is a proper methodology to model the packet dropping in DSRC network [15], [23]. Consider T_s as the network sampling time. The time instant k is defined as $k \times T_s \leq t < (k+1) \times T_s$. Between each sample time instant, the value of information received through the communication network will be held.

In occurrence of packet drop out in the communication network, the control dynamics (5) can be rewritten as the following:

$$\dot{u}_i = -\frac{1}{h}u_i + \frac{1}{h}(k_p e_i + k_d \dot{e}_i) + \frac{1}{h} \times \chi(k) \times u_{i-1} \quad (21)$$

where $\chi(k)$ a variable that represents the packet drop out phenomenon at time instant k. The variable χ is modeled as a Bernoulli random variable. If the packet is delivered correctly, we have $\chi(k) = 1$; otherwise, if packet is lost in the network, we have $\chi(k) = 0$.

Therefore, we can model packet drop out in the communication network as below:

$$\chi(k) \in \{0,1\} \quad (22)$$

where the probability of packet loss is $p(\chi(k) = 0) = \lambda$ and the probability of successful arrival of packet is $p(\chi(k) = 1) = 1 - \lambda$.

Remark 7: With the probability of λ, the packet in the network will be lost and the vehicle receives no information on the preceding vehicle's desired acceleration. With the probability of $1 - \lambda$, the vehicle will receive correct data from the network

Assumption 2: Each vehicle in the platoon receives the desired acceleration data of the preceding vehicle through DSRC network.

5.2. Proposed Strategy

The control policy of CACC strategy for vehicle i, shown in (5), depends on two crucial sets of information: 1) desired acceleration of the preceding vehicle (u_{i-1}) which is received via communication network (***Assumption 2***) and, 2) velocity of vehicle i (v_i) and the relative distance between vehicle i and vehicle $i - 1$ (d_i), both of which are measured by on-board sensors (***Assumption 1***). Therefore, data loss due to packet drop out in the communication network, and faults in these on-board sensors, will affect the individual

vehicle's behavior and create potentially unsafe situations in the connected vehicle system. In this section of proposed research, we propose a diagnostic scheme that improves the performance of CACC in presence of these issues. The scheme is shown in Fig. 14. As it can be inferred from the schematic, the diagnostic scheme has two components: Filter to compensate the packet dropping and fault diagnostics which discussed in the previous section

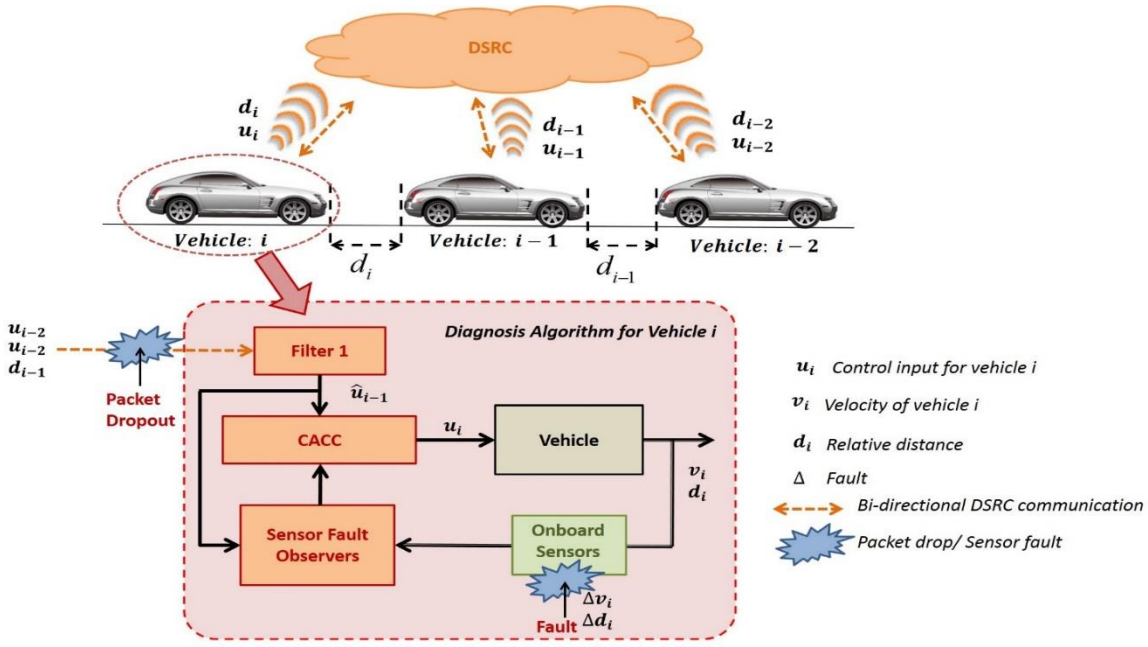

Figure 12: Packet dropping strategy for connected vehicles combined with physical fault diagnostics

Filter 1*:* The objective of the *Filter 1* is to receive the data from communication network (DSRC) which is possibly subjected to packet drop and reconstruct the actual data (u_{i-1}) with certain accuracy. *Filter 1* is essentially a Kalman filter which will be detailed shortly.

We take the following assumptions which facilitate the filter design.

Assumption 3: Vehicle i receives the following information through the DSRC.

d_{i-1}: The relative distance of vehicle $i-1$.

u_{i-1}: The desire acceleration of vehicle $i-1$.

d_{i-2}: The relative distance of vehicle $i-2$.

u_{i-2}: The desire acceleration of vehicle $i-2$.

Assumption 4: Vehicle i measures v_{i-1} using its own velocity information and on board relative velocity sensor data.

As mentioned before, the goal of *Filter 1* is to reconstruct u_{i-1} which is subjected to packet drop out.

Considering the control policy (8) for vehicle $i-1$, the dynamics of u_{i-1} can be written as

$$\dot{u}_{i-1} = -\frac{1}{h}u_{i-1} + \frac{1}{h}(k_p e_{i-1} + k_d \dot{e}_{i-1}) + \frac{1}{h}u_{i-2} \tag{23}$$

where

$$e_{i-1}(t) = d_{i-1}(t) - hv_{i-1}(t) \tag{24}$$

The structure of Filter 1, which is implemented in vehicle i, is chosen as:

$$\dot{\hat{u}}_{i-1} = -\frac{1}{h}\hat{u}_{i-1} + \frac{1}{h}\left(k_p \hat{e}_{i-1} + k_d \dot{\hat{e}}_{i-1}\right) + \frac{1}{h}\hat{u}_{i-2}$$

$$+L_K(u_{i-1} - \hat{u}_{i-1}) \tag{25}$$

where L_K is the Kalman gain and , $\hat{d}_{i-1}$ and $\hat{u}_{i-2}$ are defined as follows:

$$\hat{d}_{i-1}(t) = \begin{cases} d_{i-1}\big((k-1)T_s\big) & if\ \chi(k) = 0 \\ d_{i-1}(kT_s) & if\ \chi(k) = 1 \end{cases} \quad for\ kT_s \le t < (k+1)T_s \tag{26}$$

$$\hat{u}_{i-2}(t) = \begin{cases} u_{i-2}\big((k-1)T_s\big) & if\ \chi(k) = 0 \\ u_{i-2}(kT_s) & if\ \chi(k) = 1 \end{cases} \quad for\ kT_s \le t < (k+1)T_s \tag{27}$$

Note that, the variables $\hat{d}_{i-1}$ and $\hat{u}_{i-2}$ are the modified from the data d_{i-1} and u_{i-2}, received by vehicle i. Using the holding strategy, explained in (26)-(27), the error (24) in presence of packet dropping will be:

$$\hat{e}_{i-1}(t) = \hat{d}_{i-1}(t) - hv_{i-1}(t) \tag{28}$$

Assumption 5: The probability of having packet drop outs on consecutive time instants $t = kT_s$ and $t = (k-1)T_s$ is assumed to be negligible.

Subtracting (14) from (12), the filter estimation error dynamic can be written as:

$$\dot{\tilde{u}}_{i-1} = -\frac{1}{h}\tilde{u}_{i-1} - L_K\tilde{u}_{i-1} + \Delta u_{PD} \tag{29}$$

$$\tilde{u}_{i-1} = u_{i-1} - \hat{u}_{i-1} \tag{30}$$

where $\tilde{u}_{i-1}$ is the estimation error, Δu_{PD} represents lumped effect of the uncertainties due to packet drop outs, holding strategy (26)-(27) and measurement noise. The Kalman gain L_K is designed following the process detailed in [89]. In the design, the uncertain term Δu_{PD} is considered as a bounded Gaussian process noise which can potentially be suppressed by tuning the error covariance matrices.

5.3. Simulation Studies

In this section, we present the simulation studies to verify the effectiveness of the scheme.

Simulation Scenario: A homogenous platoon of five vehicles equipped with CACC control strategy is considered. The leader of the platoon follows the scaled and modified US06 driving cycle (Fig. 13). Performance of Filter 1 (Data reconstruction under packet drop out). This subsection shows the results regarding the performance of *Filter 1*. It verifies the effectiveness of the *Filter 1* in reconstructing the actual data which is subjected to packet drop outs. Furthermore, it also shows how CACC performance is improved by the addition of *Filter 1*.

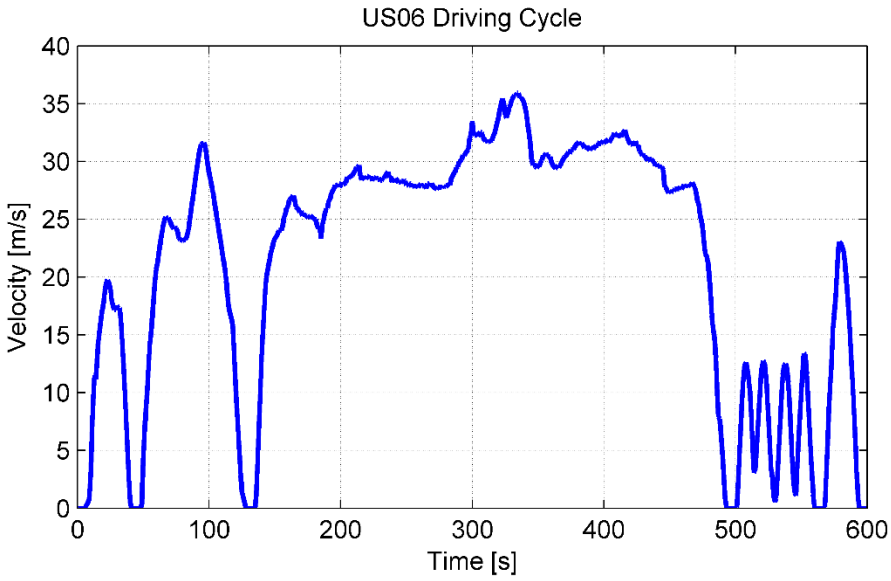

Figure 13. Velocity profile of US06 Driving cycle

The performance of the vehicle i in the platoon can be evaluated by considering its relative distance d_i with respect to the preceding vehicle. The CACC strategy attempts to

keep the relative distance very small to enhance the traffic throughput. However, failure in the communication network may cause degraded performance in CACC and consequently, lead to crashes. The relative distance d_i should be greater than zero to avoid crashes between two consecutive vehicles.

In this simulation study, the relative distance between vehicle 3 and vehicle 2 is used to illustrate the scheme. Fig. 14 shows the relative distance in the presence of packet drop outs with different probabilities. Note that, the vehicles are not equipped with the proposed scheme and only have typical CACC. It can be seen from Fig. 14 that under higher packet drop out probabilities, the relative distance between vehicle 2 and 3 becomes negative indicating crashes.

Next, we evaluate the proposed scheme where the vehicles are equipped with diagnostic scheme (*Filter 1*). A network with probability of packet drop out $\lambda = 0.2$ is considered. Fig.15 shows the relative distance of vehicle 2 and vehicle 3 under two cases: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme. It can be seen from Fig. 15 that at least four crashes happen in this specific driving cycle under typical CACC. However, applying the CACC with the proposed diagnostic scheme, these crashes are avoided. Therefore, it can be concluded that the proposed diagnostic scheme is able to improve the performance of the connected vehicle system.

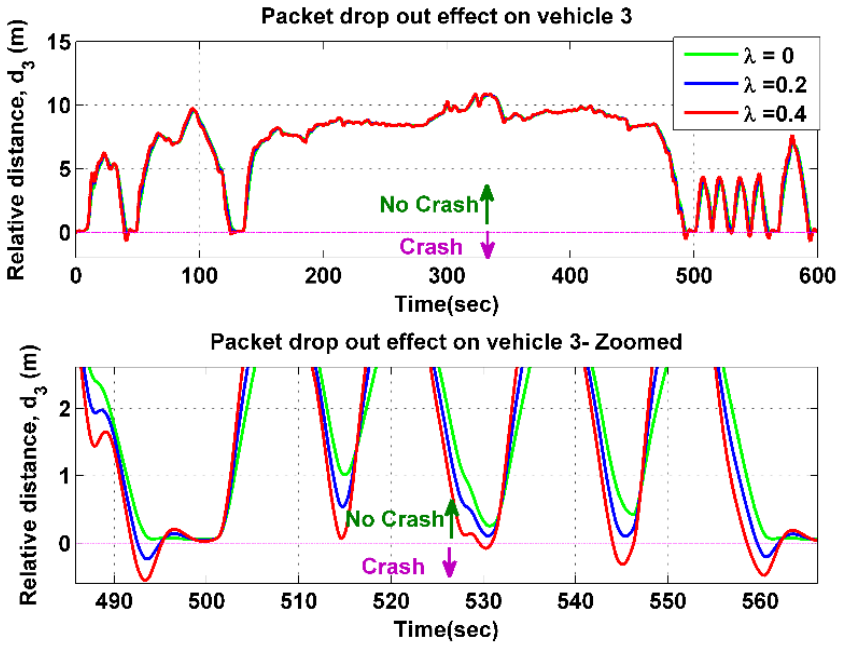

Figure 14: Relative distance between vehicle 2 and vehicle 3 (d_3), with different probabilities of packet drop out in the communication network.

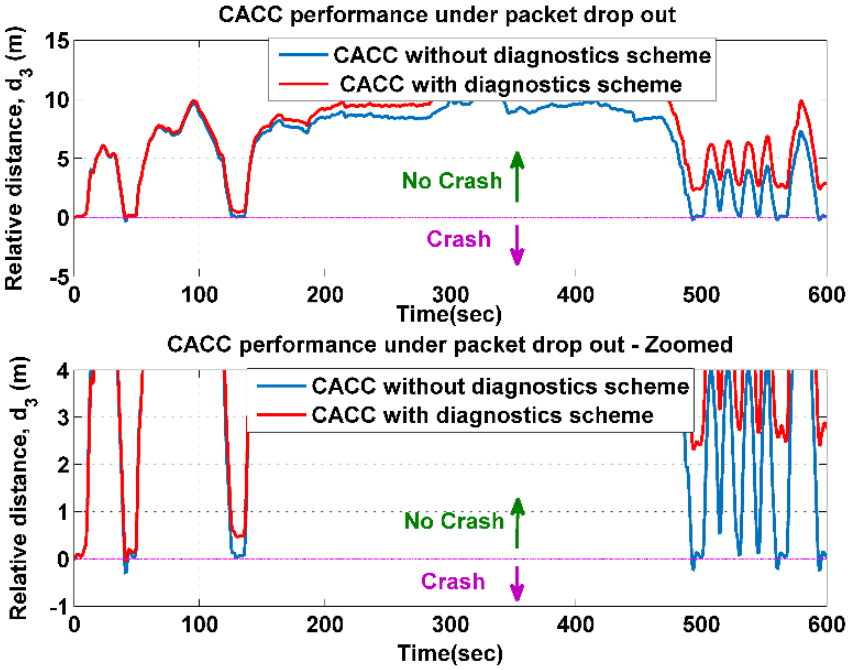

Figure 15: Relative distance between vehicle 2 and vehicle 3 (d_3) with the probability of packet drop out $\lambda = 0.2$, under two cases: 1) typical CACC without the diagnostic scheme, 2) CACC with the proposed diagnostic scheme.

CHAPTER SIX

RESILIENT STRATEGIES TOWARD DENIAL OF SERVICE ATTACK

In cyber physical systems such as connected vehicles, DoS attack changes the average service time of the communication network by imposing illegitimate requests. Indeed, the DoS attack induces an additional service time which in turn corresponds to additional delay in the transmission network [42]. In the majority of the existing control frameworks, the effect of DoS attack has been modelled in two ways: (i) stochastic time delay which can be represented by random variables e.g. Bernoulli [41] or probabilistic approaches with memory e.g Markov Model [90] ; (ii) constant time delay [42]. In this chapter, our main case study is connected vehicle system with Co-operative Adaptive Cruise Control (CACC). We develop three different strategies to detect and estimate the effect of DoS attack as time-delay. In the first algorithm, we model the DoS attack with stochastic time delay in DSRC network. We propose a strategy to estimate the mean value of the delay as well as estimating correct value of signal subjected to the delay to modify the CACC algorithm correspondingly to maintain the functionality of the platoon. In the second strategy, we model DoS attack in DSRC with as constant unknown delay and proposed an adaptive observer to estimate the delay. Also, we studied the effects of system uncertainties on the DoS estimation algorithm. Finally, in the third algorithm, we considered a general CPS system with a saturated DoS attack modeled with constant unknown delay. In this part we modeled DoS via a PDE and developed a PDE based observer and an adaptive observer to estimate the delay as well as states of the system while the only available measurements are delayed.

6.1. Strategy Number One

In this section we consider DoS attack in DSRC which degrades the quality of packet delivery of the communication network. To countermeasure the DoS attack in the platoon system, the conventional CACC algorithm is modified by adding an estimation algorithm consisting of two Luenberger observers and a delay estimator. The effectiveness of the overall online algorithm scheme is verified via simulation studies. The developed scheme is a new contribution to connected vehicles security research area with the following characteristics: 1) Considers stochastic delay to model the effect of DoS attack in connected vehicles as an example of CPS, 2) Theoretical verification of the convergence of the state estimation error, 3) Theoretical verification of delay estimation, and 4) Simple design and computationally efficient.

6.1.1 DoS Attack Modeling

In this section we simplified the model of the platoon by considering the following dynamic controller is considered to achieve the zero regulation error:

$$\dot{a}_i = -\frac{1}{h}a_i + \frac{1}{h}(k_p e_i + k_d \dot{e}_i) + \frac{1}{h}a_{i-1} \tag{31}$$

$$\dot{a}_i = \frac{k_p}{h}d_i - (k_p + \frac{k_d}{h})v_i - (k_p + \frac{1}{h})a_i + \frac{k_d}{h}v_{i-1} + \frac{1}{h}a_{i-1} \tag{32}$$

where a_{i-1} and v_{i-1} are the desired acceleration and velocity of the preceding vehicle received through DSRC network. The parameters $K_p, K_d > 0$ are controller gains designed such that (i) the inter-vehicle distance is maintained to $d_{r,i}$ and (ii) the a_i is bounded and changes smoothly. As it can be inferred from (32), control signal of vehicle i derived from

CACC algorithm, a_i, depends on states of vehicle i and information received from preceding vehicle $i-1$.

Considering (1) and (6), a new augmented state space representation for vehicle i is shown in (33), where, a_{i-1} and v_{i-1} are two external inputs of the system related to the preceding vehicle $i-1$.

$$\begin{bmatrix} \dot{d}_i \\ \dot{v}_i \\ \dot{a}_i \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ \frac{k_p}{h} & -(k_p + \frac{k_d}{h}) & -(k_p + \frac{1}{h}) \end{bmatrix} \begin{bmatrix} d_i \\ v_i \\ a_i \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ \frac{k_d}{h} \end{bmatrix} v_{i-1} + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{h} \end{bmatrix} a_{i-1} \tag{33}$$

Remark 8: Vehicle i receives the absolute velocity, v_{i-1} and acceleration information of preceding vehicle, a_{i-1}, through DSRC network. Hence, these signals are subjected to network failures and cyber-attacks.

We can write (33) in the form of general state space representation as (8) considering that all states of the system are measured via on-board sensors.

$$\begin{aligned} \dot{x}_i(t) &= Ax_i(t) + Bu_{i-1}(t) \\ y_i(t) &= Cx_i(t) \end{aligned} \tag{34}$$

where $x_i = [d_i,\ v_i, a_i]^T \in R^3$, represents the states of vehicle i. $u_{i-1} = [v_{i-1}, a_{i-1}]^T \in R^2$ are external inputs of the system coming from vehicle $i-1$, and $y_i = [d_i,\ v_i, a_i]^T \in R^3$ stands for measureable outputs of the system.

Denial of Service (DoS) Attack

Denial of service attack is a cyber-attack that affects the timeliness of information exchange. In this section of proposed research, DoS attack is modeled as a stochastic delay on data transmission time in the network. We consider each vehicle updates its data for transmission periodically [15]-[16]. Fig.16 shows the packet transmission in ideal network and network under DoS attack.

If there is no attack in the communication network, the packet is delivered with no delay. However, in presence of DoS, the attacker increases the service time of the network and keeps the network busy. Consequently, vehicle i will not receive the new information of vehicle $i-1$, to update its own information. Therefore, vehicle i holds the previous data of vehicle $i-1$ [15]-[16],[10] .

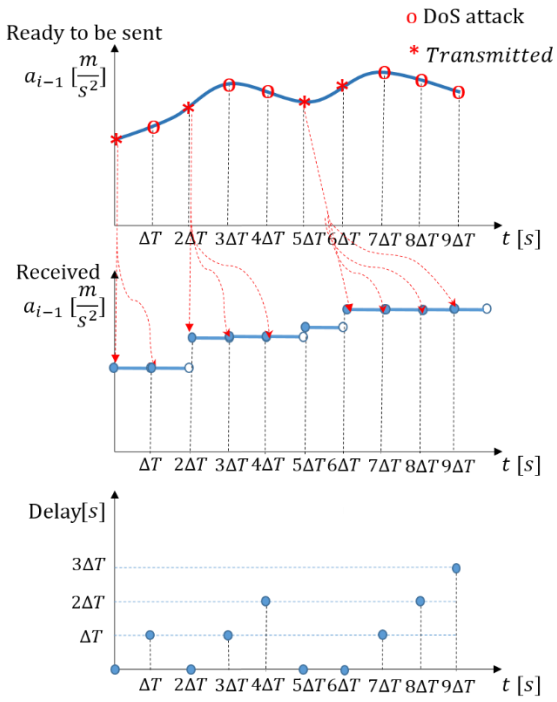

Figure 16: Modeling of Denial of Service attack on signal a_{i-1}

Consider p as the probability of network being idle to transmit a packet and $q = (1-p)$ as the probability of network being busy. The impact of DoS attack can be modeled as a stochastic delay as the following:

$$\tau = l\Delta T < d = l_{max}\Delta T,\ l \in \{1,2,\dots,l_{max}\} \tag{35}$$

where ΔT is the sample time of updating safety messages in vehicles. Therefore, the probability distribution of delay τ can be defined using Bernoulli random variable

$$\begin{aligned} P(\tau = 0) &= p \\ P(\tau = \Delta T) &= p \times (1-p) \\ P(\tau = i \times \Delta T) &= p \times (1-p)^i \end{aligned} \tag{36}$$

The p depends on the DoS attacker capability to keep network busy. Since the DoS attack increases the service time [42] and consequently$q$, in presence of the attack, the probability of finding network idle will be reduced.

In presence of attack the dynamic of the vehicle i will change as (37)

$$\begin{aligned} \dot{x}_i(t) &= Ax_i(t) + Bu_{i-1}(t-\tau) \\ y_i(t) &= Cx_i(t) \end{aligned} \tag{37}$$

where τ is stochastic delay.

Assumption 6: The attacker has a limited access to increase the service time of the network [42]. Hence, the injected delay in data transmission is bounded with an upper limit of τ_{max}

6.1.2. Diagnostics Algorithm

Transmitted data u_{i-1}, is subjected to DoS attack and hence affected by the stochastic delay in the network. The stochastic delay in the receiving data can diminish the performance of platoon and cause collisions. Hence, to avoid collisions and enhance the performance of platoon, a precise estimation of actual u_{i-1} is required. The estimated u_{i-1} can be used in CACC strategy instead of actual u_{i-1}under DoS attack. This strategy can be called modified CACC. To achieve this goal, an estimation algorithm containing three components is proposed: (1) Observer I estimates the states of the preceding car in normal condition. The output error of the observer I is used as a residual signal to detect the attack. (2) Observer II estimates the states of the preceding car with certain accuracy in presence DoS attack. These estimates are used in the modified CACC strategy. (3) Delay estimator estimates the stochastic delay induced by DoS. The schematic of the online estimation scheme is shown in Fig. 17.

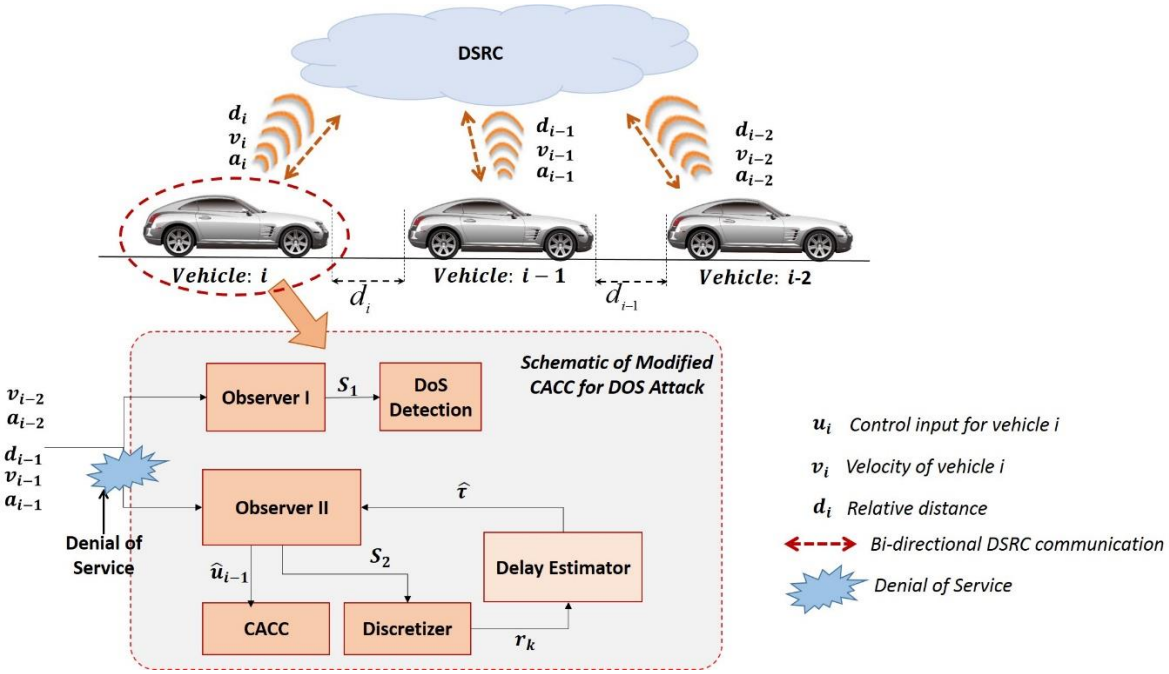

Figure 17: DoS strategy schematic for connected vehicles to modify CACC

In brief, observer I estimates the states of preceding vehicle in ideal case when there is no delay in communication network. In occurrence of DoS, the residual of this observer will be non-zero, detects the DoS attack. Therefore, system switches to observer II and delay estimator to estimate the states of preceding vehicle accurately even in presence of DoS.

Real time measurements from vehicle $i-1$ are $d_{i-1}, v_{i-1}, a_{i-1}$ and inputs for both observers are states of vehicle $i-2$ v_{i-2}, a_{i-2} which are received through DSRC under stochastic delay.

Observer I

Assumption 7: There is no sensor faults in the on-board sensors.

Similar to (34), dynamics of vehicle $i-1$ can be written as:

$$\dot{x}(t) = Ax(t) + Bu(t)$$
$$y(t) = Cx(t) \tag{38}$$

where $x = [d_{i-1},\ v_{i-1}, a_{i-1}]^T \in R^3$, represents the states of vehicle $i-1$. $u = [v_{i-2}, a_{i-2}\ ]^T \in R^2$ are inputs of the system and $y = [d_{i-1},\ v_{i-1}, a_{i-1}]^T \in R^3$stands for measureable outputs of the system.

A Luenberger observer can be designed as (39) and implemented in vehicle i:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L_1\left(y_m(t) - \hat{y}(t)\right) \tag{39}$$

where $y_m(t)$ is the transmitted measurements of vehicle $i-1$ including relative distance, velocity and acceleration. In ideal network with no DoS attack,

$$y_m(t) = Cx(t) \tag{40}$$

Therefore, error dynamics is derived as:

$$\dot{\tilde{x}}(t) = A\tilde{x}(t) - L_1 C\tilde{x}(t) \tag{41}$$

The observer gain, L_1, is selected such that the estimation error $\tilde{x}(t)$, with dynamics of (41), converges to zero exponentially. To do this, $A - L_1 C$ should be negative definite matrix. The residual S_1 is defined as

$$S_1(t) = y_m(t) - \hat{y}\,(t) = C(x_m(t) - \hat{x}\,(t)) \tag{42}$$

In occurrence of DoS attack, since the estimated value is not equal with the measurement due to the delay, the residual will be non-zero. This residual is used as an indicator of DoS attack in the network.

Observer II

Assumption 8: DSRC is a shared communicating network. Therefore, in presence of attack in the network, all exchanging data experience the same delay on the same time, $\tau(t) \in \{\tau \mid p(\tau) < 1\ ,\ 0 \leq \tau \leq\ d\}$.

Assumption 9: The derivative of vehicle acceleration is bounded.

In presence of DoS attack, since vehicle i receives the measurement of vehicle $i-1$ through the DSRC network, (38) can be re-written as (43)

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t-\tau) \\ y(t) &= Cx(t) \end{aligned} \tag{43}$$

Considering the mentioned assumptions, the observer dynamics is given as:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t-\tau) + L\left(y_m(t) - \hat{y}(t-\hat{\tau})\right) \tag{44}$$

where $\hat{\tau}$ is the mean value of estimated delay derived from delay estimator explained in the next section. $y_m(t)$ is the transmitted measurements of vehicle $i-1$ .These information are transferred from vehicle $i-1$ through the DSRC network which is subjected to delay τ. Therefore, the received measurements of vehicle $i-1$ in the vehicle i have delay of τ seconds as it is described in (45).

$$y_m(t) = y(t-\tau) \tag{45}$$

Consequently, the error dynamics can be written as (46)

$$\dot{\tilde{x}}(t) = A\tilde{x}(t) - LC\left(x(t-\tau) - \hat{x}(t-\hat{\tau})\right) \tag{46}$$

$$\dot{\tilde{x}}(t) = A\tilde{x}(t) - LC\left(\tilde{x}(t-\tau)\right) + M(t) \tag{47}$$

With initial condition

$$\tilde{x}(t_0) = \tilde{x}_0 \tag{48}$$

where $M(t)$ represents the lumped noise and uncertainties caused by error in estimating the delay. It is assumed that $M(t)$is bounded as:

$$\left|M_{[t_0,t_\infty]}\right|_\infty < K.\Delta \tag{49}$$

The upper bound of the uncertainty can be derived from the driving cycle, maximum delay and maximum permitted acceleration.

***Remark 9*:** The error dynamics (47) is stable and converges to a bounded region exponentially, if there exists *L* matrix such that the following Lyapunov-Krasovskii function satisfies Proposition 1 [99].

$$\begin{aligned} V(t,\tilde{x},\dot{\tilde{x}}) = {} & \tilde{x}^T(t)P\tilde{x}(t) + \int_{t-\mathrm{d}}^{t} e^{a(s-t)}\tilde{x}^T(s)S\tilde{x}(s)ds \\ & + \mathrm{d}\int_{-\mathrm{d}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{x}}^T(s)R\dot{\tilde{x}}(s)ds\,d\theta \end{aligned} \tag{50}$$

Proposition 1: If there exist $a > 0, b > 0\ and\ 3\times 3 - matrices\ P > 0, S > 0, and\ R > 0$ such that along trajectories of (47) the Lyapunov-Krasovskii function (50) satisfies the condition (51)

$$W \triangleq aV - b|M|^2 + \frac{d}{dt}V < 0 \tag{51}$$

Then the solution of (21) with initial condition of $\tilde{x}(t_0) = \tilde{x}_0$ satisfies the inequality

$$\tilde{x}^T(t)P\tilde{x}(t) < e^{-a(t-t_0)}\tilde{x}_0^T P\tilde{x}_0 + \left[1 - e^{-a(t-t_0)}\right]\frac{b}{a}\left|M_{[t_0,t_\infty]}\right|_\infty^2 \tag{52}$$

Proof: Applying comparison principle [78], we have

$$\tilde{x}^T(t)P\tilde{x}(t) \le V\left(t,\tilde{x}_t,\dot{\tilde{x}}_t\right) < e^{-a(t-t_0)}V\left(t,\tilde{x}_{t0},\dot{\tilde{x}}_{t0}\right) + \int_{t_0}^{t} e^{-a(t-s)}b|M(s)|^2 ds \tag{53}$$

We find

$$\begin{aligned} W \le\ & 2\tilde{x}^T(t)P\dot{\tilde{x}}(t) + a\tilde{x}^T(t)P\tilde{x}(t) - bM^T(t)M(t) \\ & + d^2\dot{\tilde{x}}^T(t)R\dot{\tilde{x}}(t) - de^{-ad}\int_{t-d}^{t}\dot{\tilde{x}}^T(s)R\dot{\tilde{x}}(s)ds + \tilde{x}^T(t)S\tilde{x}(t) \\ & - [\tilde{x}^T(t-h)S(\tilde{x}(t-h)]e^{-ad} \end{aligned} \tag{54}$$

Applying the standard arguments, we obtain that

$$W \le \eta^T(t)\Phi\eta(t) < 0 \qquad \forall\eta(t) \ne 0 \tag{55}$$

where

$\eta(t) = col\left\{\tilde{x}(t), \dot{\tilde{x}}(t), \tilde{x}(t-d), \tilde{x}\left(t-\tau(t)\right), M(t)\right\}$ if the matrix inequality

$$\Phi = \begin{bmatrix} \phi_{11} & \phi_{12} & 0 & P_2^T A_1 + \mathrm{Re}^{-ad} & P_2^T \\ * & \phi_{22} & 0 & P_3^T A_1 & P_3^T \\ * & * & -(S+R)e^{-ad} & Re^{-ad} & 0 \\ * & * & * & -2Re^{-ad} & 0 \\ * & * & * & * & -bI \end{bmatrix} \Phi < 0 \tag{56}$$

is feasible, where

$$A_1 = -LC$$

$$\phi_{11} = A^T P_2 + P_2^T + aP + S - \mathrm{Re}^{-ad} \tag{57}$$

$$\phi_{12} = P - P_2^T + A^T P_3 \tag{58}$$

$$\phi_{22} = -P_3 - P_3^T + d^2 R \tag{59}$$

Thus, the following results will be obtained

Lemma 1. Given $a > 0, b > 0$, $and\ \ d > 0$, let there exist $3 \times 3\ matrices\ P > 0, P_2, P_3,\ S > 0, and\ R > 0$ such that the LMI (56) with notation given in (57)-(59) holds. Then the solution of (47) satisfies (50) for all delays $0 \leq \tau(t) \leq\ d$. Moreover, the ellipsoid

$$\chi_\infty = \left\{\tilde{x} \in R^3 :\ \tilde{x}^T(t) P \tilde{x}(t) < \frac{b}{a} K^2 . \Delta^2\right\} \tag{60}$$

is exponentially attractive with the decay rate a/2 for all $|M(t)|^2 \leq K^2 . \Delta^2$.

Delay Estimator

To estimate states of preceding vehicle, the observer needs estimated average value of delay. We define the following residual

$$S_2(t) = y_m(t) - \hat{y}(t - \hat{\tau}) = y(t - \tau) - \hat{y}(t - \hat{\tau}) \tag{61}$$

By discretizing the residual, (61) can be re-written as

$$r_k = S_2(k.\Delta T) = y(k.\Delta T - \tau) - \hat{y}\left(k.\Delta T - \hat{l}\Delta T\right) \tag{62}$$

$$r_k = y(k - l) - \hat{y}\left(k - \hat{l}\right) \tag{63}$$

Assume that we have observed the data set $r = \{r_1, r_2, \dots, r_k\}$ and we want to estimate the average value of stochastic delay. Since in section III, we have proven that the estimation error converges to a bounded area, we can assume obtained residual is a stationary Gaussian random process [80], with mean μ and variance σ

$$r_k \sim \mathcal{N}(\mu, \sigma_k) \tag{64}$$

Considering (47), we can write:

$$r_{k+1} = Ar_k - LCr_{k-l} + M_k \tag{65}$$

$$E(r_{k+1}) = A.E(r_k) - LC.E(r_{k-l}) + E(M_k) \tag{66}$$

where $E(.)$ is the expectation operator. Since M is assumed to be zero mean white noise, the expected value of r will be

$$E(r_{k+1}) = E(r_k) = \mu = 0 \quad as \quad k \to \infty \tag{67}$$

Furthermore,

$$E(r_{k+1}^2) = A^2E(r_k^2) + L^2C^2E(r_{k-l}^2) + 2ALCE(r_k.r_{k-l}) + E(M_k^2) \tag{68}$$

Based on the definition of the variance of a signal, we have

$$\sigma_{k+1}^2 = E(r_{k+1}^2) - E(r_{k+1})^2 \tag{69}$$

Substituting (40) and (42) in (43), the following equation can be derived:

$$\sigma_{k+1}^2 = A^2\sigma_k^2 + L^2C^2\sigma_{k-1}^2 + 2ALCE(r_k.r_{k-l}) + \sigma_M^2 \tag{70}$$

Considering we have enough observation on r, as $k \to \infty$, we have

$$\sigma_{k+1}^2 = \sigma_k^2 = \sigma_{k-l}^2 = \sigma^2 \tag{71}$$

Therefore, we can write

$$\sigma_k^2 = (A^2 + L^2C^2)\sigma_k^2 + 2ALCR_r(r_k.r_{k-l}) + \sigma_M^2 \tag{72}$$

Since $r = \{r_1, r_2, \dots, r_k\}$ is Gaussian wide sense stationary signal, the correlation is related to delay as

$$R_r(l) = \sigma^2 e^{-|l|/\Delta T} \tag{73}$$

Substituting (45) and (47) in (46), we have:

$$\sigma^2 = (A^2 + L^2C^2)\sigma^2 + 2ALC\sigma^2 e^{-|l|/\Delta T} + \sigma_M^2 \tag{74}$$

$$(I - A^2 - L^2C^2)\sigma^2 - \sigma_M^2 = 2ALC\sigma^2 e^{-\frac{|l|}{\Delta T}} \tag{75}$$

$$\frac{(I-A^2-L^2C^2)\sigma^2-\sigma_M^2}{2ALC\sigma^2} = e^{-\frac{|l|}{\Delta T}} \tag{76}$$

$$\hat{l} = |l| = \Delta T.\, Ln\left(\frac{2ALC\sigma^2}{(I-A^2-L^2C^2)\sigma^2-\sigma_M^2}\right) \tag{77}$$

Using the probability distribution of r and measuring the variance of residual, we can measure the delay l and have an approximation of total delay $\tau = \Delta T.\, l$.

Therefore, we can write

$$\hat{\tau} = \Delta T.\, \hat{l} \tag{78}$$

Every sample time, using the updated τ and updated estimation and new observation, all calculation will be updated. Note that, better estimation of the delay, reduces the uncertainties boundary in (47) and (49).

6.1.3. Results and Discussion

In this section, we simulate a homogenous platoon of 5 vehicles equipped with CACC strategy. Vehicle 1 as the leader of platoon, follows UDDS driving cycle.

Considering $h = 0.3\ s$ and tuning the controller to track the desire relative distance, the nominal system will have the following matrices:

$$A = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 3.33 & -4.33 & -4.33 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 3.33 & 3.33 \end{bmatrix},$$

$$C = I_{3\times 3}$$

We consider vehicle 3 as a case study to demonstrate the results. In vehicle 3, the external input signal is $u_2 = [v_2, a_2]^T$ coming from vehicle 2 through the DSRC. The parameters $L, a > 0, b > 0$ are chosen as

$$L = \begin{bmatrix} 0.15 & 0.15 & 0 \\ 1 & 0.1 & 0.1 \\ 0.1 & -0.15 & 0.1 \end{bmatrix}, a = 1, b = 2$$

These values are selected such that the LMI in (24) is satisfied and matrix Φ is negative definite. Solving the LMI the following positive definite matrixes are obtained.

$$P_1 = \begin{bmatrix} 2.0101 & -1.8057 & -2.2541 \\ -1.8057 & 1.6804 & 2.0358 \\ -2.2541 & 2.0358 & 2.5418 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 2.5974 & -2.1479 & -2.2241 \\ -2.1479 & 2.1467 & 2.0514 \\ -2.2241 & 2.0514 & 2.3303 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 0.7698 & 0.3989 & 0.0589 \\ 0.3989 & 0.3689 & 0.0123 \\ 0.0589 & 0.0123 & 0.0743 \end{bmatrix}$$

$$S = \begin{bmatrix} 1.5109 & -1.3036 & -1.05442 \\ -1.3036 & 1.1607 & 1.3589 \\ -1.05442 & 1.3589 & 1.6182 \end{bmatrix}$$

$$R = \begin{bmatrix} 0.4951 & 0.2406 & 0.0599 \\ 0.2406 & 0.2143 & 0.0618 \\ 0.0599 & 0.0618 & 1.6182 \end{bmatrix}$$

To simulate DoS attack in the platoon, a Bernoulli random variable with probability of success $p = 0.5$ is considered. The corresponding delay in injected as the DoS attack into the communication network at $t = 300\ sec$ and remains in the system. In occurrence of DoS attack, the states of vehicle 2 consisting v_2 and a_2 are estimated by proposed observer II and delay estimator. The modified CACC strategy, uses the estimated $\hat{u}_2 = [\hat{v}_2, \hat{a}_2]$ instead of actual one. Hence, the performance of platoon in presence of DoS enhances. Fig.18 shows the states of vehicle 3, relative distance (d_3) velocity (v_3) and acceleration (a_3) in different scenarios. Solid blue curves represent the states of vehicle 3 in indeal case with no DoS attack in the communication network. Solid red curves show states of vehicle 3 in occurrence of the DoS attack injected at $t = 300\ sec$ when the normal CACC is applied as control strategy. Finally, the green curves represent the states of vehicle 3 in presence of DoS attack when modified CACC control strategy uses the estimated states of vehicle 2.

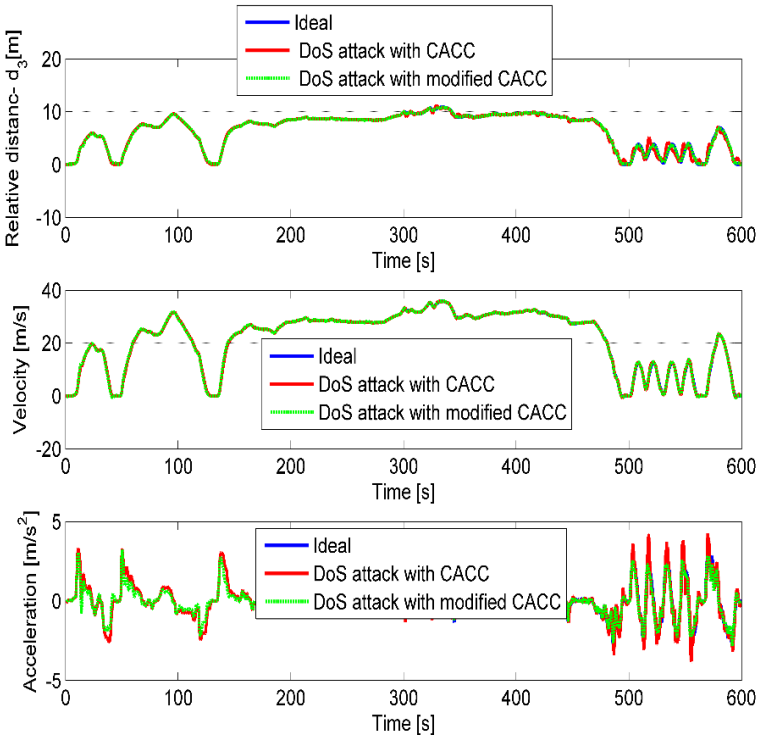

Figure 18: States of vehicle 3, d_3, v_3 and a_3 in ideal network (blue), under attack with normal CACC (red), with modified CACC which uses estimated signals of vehicle 2 $\hat{u}_2 = [\hat{v}_2, \hat{a}_2]$

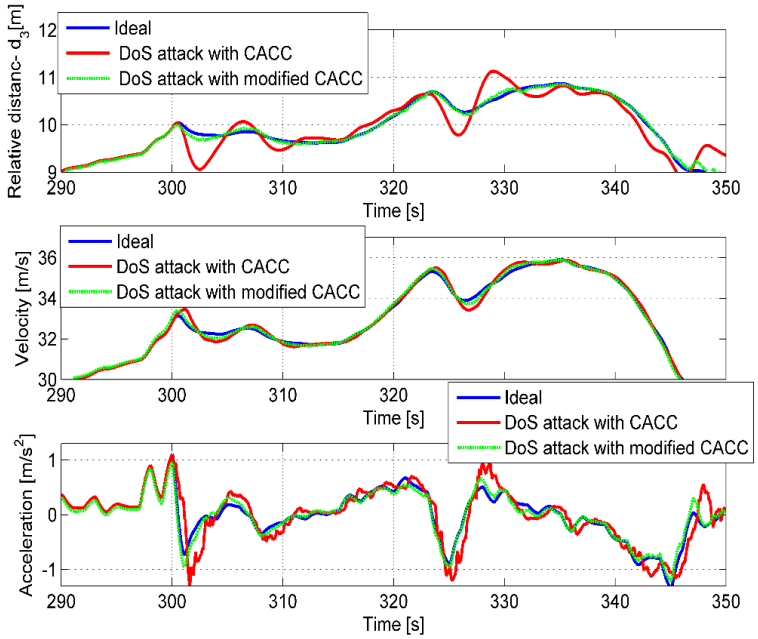

Figure 19: States of vehicle 3, zoomed results for $t = [290\ 350]$, before occurrence of DoS and after that.

To visualize the results better, Fig. 19 depicts the zoomed area of results for the time interval$t = [\,290, 350]$. As it can be inferred from Fig.18 and Fig.19, in presence of DoS attack, due to the delay in the receiving data, the relative distance in several points is less than critical safety distance. However, using correct estimation, platoon has better performance which is close to ideal case

6.2. Strategy Number Two

The main contribution of the present section is a control-oriented diagnostic framework for connected vehicle systems that is capable of (i) detecting the occurrence of DoS attack and, (ii) providing an estimate of the effect of the attack. Note that, the estimate of the effect of the attack can be extremely useful for designing secure control system for the vehicles. In this section we model the DoS attack by a time delay in information processing by the network. The DoS detection scheme consists of a set of observers designed by combining adaptive estimation and sliding mode theory. Essentially, the goal of the scheme is to track the delay in the information processing by the DSRC. When the delay exceeds a pre-defined threshold, a DoS occurrence is detected. The pre-defined threshold is computed offline considering the modeling, measurement and communication uncertainties. The scheme also estimates the delay providing an estimate of the effect of DoS. This estimated delay can be used for updating (modifying) the safety relative distance to avoid collision.

6.2.1. DoS Attack Modeling

In this section, we assume the DoS attacker focuses on the endpoint (the following vehicle) and flood the communication network with excessive amount of packets; therefore, the authorized user (vehicle i) cannot access to the DSRC network on time and the acceleration data of the leading vehicle $i-1$ will be delivered to the follower with a delay. Since the capability of the attacker is not known, in this section, the delay induced by DoS attack is modeled as unknown constant delay. Considering *Remark 1*, dynamics of vehicle i in (\ref{vehicle}) under DoS attack can be written as

$$\begin{bmatrix} \dot{d}_i(t) \\ \dot{v}_i(t) \\ \dot{a}_i(t) \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ \frac{k_p}{h} & -(k_p + \frac{k_d}{h}) & (k_p + \frac{1}{h}) \end{bmatrix} \begin{bmatrix} d_i(t) \\ v_i(t) \\ a_i(t) \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ \frac{k_d}{h} \end{bmatrix} v_{i-1}(t) + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{h} \end{bmatrix} a_{i-1}(t-\tau) \tag{79}$$

where vehicle i receives the acceleration information of vehicle $i-1$ with unknown delay induced by DoS attack, τ.

Assumption 10: The attacker has a limited capability to keep the network busy. Hence, the effect of DoS attack as the unknown delay has an upper bound corresponding to the maximum capability of the attacker. i.e. $\tau \in [0, \tau_{max}]$.

Assumption 11: We consider a homogeneous platoon of vehicles. Therefore, all vehicles in the platoon have the same parameters e.g. mass, inertia, rolling resistance coefficient.

Assumption 12: Each vehicle in the platoon measures relative distance with respect to preceding vehicle d_i and following vehicle d_{i+1}.

Remark 10: Vehicle i measures the relative velocity via radar and hence can compute the absolute velocity v_{i-1} of vehicle $i-1$. Vehicle i also receives acceleration a_{i-1} information of vehicle $i-1$ via DSRC network which is subjected to network failures and cyber-attacks.

6.2.2. Real-time Detection and Estimation Scheme for DoS Attack

With the formulation discussed in the previous section, the diagnostic problem is to detect when the delay parameter τ is non-zero and if so, estimate the value of τ. The detection and estimation scheme for DoS attack is presented in Fig. 20.

Remark 11: The DoS detection module is implemented in vehicle $i-1$. As mentioned in the previous section, vehicle $i-1$ has access to the following information: (i) $d_i(t)$ and $v_i(t)$ measured by rear radar of vehicle $i-1$ and, (ii) $a_i(t)$ directly measured in vehicle $i-1$. Note that, these measurements are not affected by the occurrence of the DoS attack.

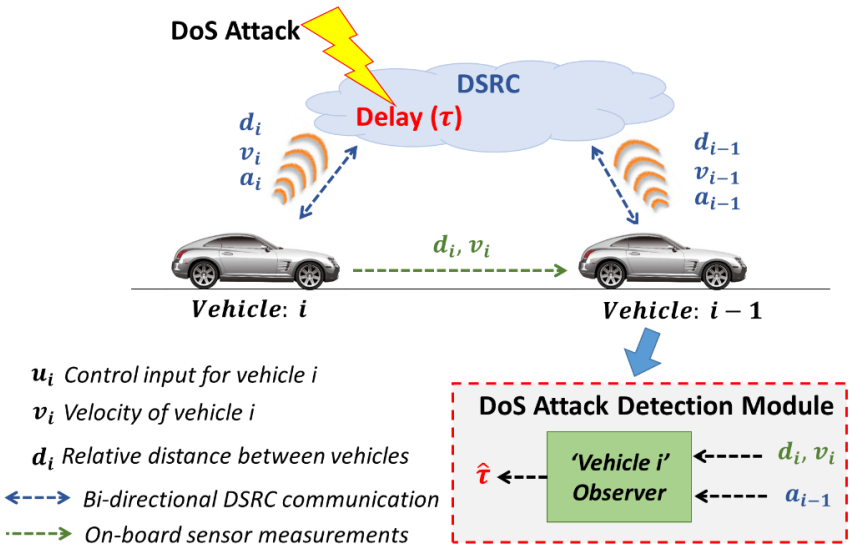

Figure 20. DoS attack detection and estimation scheme.

The proposed scheme consists of a model-based observer, denoted by *Vehicle i Observer*. Based on the available measurements and the model (79), *Vehicle i Observer* detects the occurrence and estimates size of the delayτ. Before detailing the design of the *Vehicle i Observer,* we make the following assumptions.

Assumption 13: The signal $a_{i-1}(t)$ is at least two times differentiable with respect to time. Furthermore, the derivative is bounded by some finite value, i.e. $|\dot{a}_{i-1}(t)| < \bar{a}_d, \forall t > 0$

Assumption 14: Using Taylor's series expansion [91], the delayed signal $a_{i-1}(t-\tau)$can be written as

$$a_{i-1}(t-\tau) = a_{i-1}(t) - \dot{a}_{i-1}(t)\tau + H.O.T \tag{80}$$

where $H.O.T$ represents the higher order terms of the Taylor's series expansion. We assume that \$H.O.T\$ is negligible and hence $a_{i-1}(t-\tau) \approx a_{i-1}(t) - \tau\dot{a}_{i-1}(t)$.

DoS Attack Detection

Applying *Assumption 14*, the system dynamics (79) can be written as:

$$\dot{d}_i(t) = v_{i-1}(t) - v_i(t) \tag{81}$$

$$\dot{v}_i(t) = a_i(t) \tag{82}$$

$$\dot{a}_i(t) = \frac{k_p}{h} d_i(t) - \left(k_p + \frac{k_d}{h}\right) v_i(t) - \left(k_p + \frac{1}{h}\right) a_i(t) + \frac{k_d}{h} v_{i-1}(t) + \frac{1}{h}\left(a_{i-1}(t) - \dot{a}_{i-1}(t)\tau\right), \tag{83}$$

We choose the following structure for *Vehicle i Observer*.

$$\dot{\hat{v}}_i(t) = L_v sgn\left(v_i(t) - \hat{v}_i(t)\right) \tag{84}$$

$$\begin{aligned}\dot{\hat{a}}_i(t) = \frac{k_p}{h} d_i(t) - \left(k_p + \frac{k_d}{h}\right)\hat{v}_i(t) - \left(k_p + \frac{1}{h}\right)\eta(t) + \frac{k_d}{h} v_{i-1}(t) \\ + \frac{1}{h}\left(a_{i-1}(t) - \dot{a}_{i-1}(t)\hat{\tau}\right) + L_a\left(\eta(t) - \hat{a}_i(t)\right),\end{aligned} \tag{85}$$

$$\dot{\hat{\tau}}(t) = -\frac{L_b}{h}\dot{a}_{i-1}(t)\left(\eta(t) - \hat{a}_i(t)\right) \tag{86}$$

where $\hat{v}_i(t)$, and $\hat{a}_i(t)$ are the estimated relative velocity and acceleration, respectively; $\hat{\tau}(t)$ is the estimated delay; L_v, L_a, L_b are the constant observer gains to be designed; $v_{i-1}(t)$ and $a_{i-1}(t)$are measured via on-board sensors in *Vehicle i-1*; $d_i(t)$ and $v_i(t)$are measured by *Vehicle i-1* using radar; η is a filtered version of the signal $L_v sgn(v_i(t) - \hat{v}_i(t)$. Next, we state the main result of the proposed approach.

Main Result: Consider the system model described in (81)-(83), and the observer structure (84)-(86). If the assumptions 13-14 hold true, then the estimated value of DoS attack, $\hat{\tau}(t)$, converges to its true value τ, as $t \to \infty$, given the the observer gains satisfy the following conditions:

$$L_a \ , \ L_b > 0 \tag{87}$$

$$L_v > \left|a_i(t)\right| > 0, \forall t \geq 0 \tag{88}$$

Proof: Subtracting (84)-(85) from (82)-(83), we can write the error dynamics of the observer as:

$$\dot{\tilde{v}}_i(t) = a_i(t) - L_v sgn\left(\tilde{v}_i(t)\right) \tag{89}$$

$$\dot{\tilde{a}}_i(t) = -\left(k_p + \frac{k_d}{h}\right)\tilde{v}_i(t) - \left(k_p + \frac{1}{h}\right)(a_i(t) - \eta(t)) - \frac{1}{h}\dot{a}_{i-1}(t)\tilde{\tau}(t) - L_a\left(\eta(t) - \hat{a}_i(t)\right), \tag{90}$$

where $L_v sgn(v_i(t) - \hat{v}_i(t)$, $\tilde{a}_i(t) = a_i(t) - \hat{a}_i(t)$ and $\tilde{\tau}(t) = \tau(t) - \hat{\tau}(t)$ are the estimation errors. We start with analyzing (89) by choosing the following Lyapunov function candidate$V_v(t) = \frac{1}{2}\tilde{v}_i^2(t)$. The derivative of the Lyapunov function candidate can be written as:

$$\dot{V_v}(t) = \tilde{v}_i(t)\dot{\tilde{v}}_i(t) = \tilde{v}_i(t)a_i(t) - L_v\tilde{v}_i(t)sgn\left(\tilde{v}_i(t)\right) \tag{91}$$

Applying the inequality $AB \leq |A||B|$ on the first term of the right hand side of (91), we can write

$$\dot{V_v}(t) = \left|\tilde{v}_i(t)\right|\left|a_i(t)\right| - L_v\left|\tilde{v}_i(t)\right| = \left|\tilde{v}_i(t)\right|\left(\left|a_i(t)\right| - L_v\right) \tag{92}$$

If the observer gain is such that $L_v > |a_i(t)| > 0, \forall t \geq 0, then\, \dot{V_v}(t) \leq 0$, and hence we can write:

$$\dot{V_v}(t) \leq -\alpha\sqrt{V_v(t)} \tag{93}$$

where $\alpha = \min_{t\geq 0}\sqrt{2}(L_v - |a_i(t)|) \geq 0$. The solution of the differential inequality (\ref{Lyap3}) is given by $V_v(t) \leq \left(-\frac{\alpha}{2}t + \sqrt{V_v(0)}\right)^2$. Therefore, we can conclude that $V_v(t) \to 0$ after some finite time $t_f < \frac{2}{\alpha}\sqrt{V_v(0)}$. After $t > t_f$, we have $V_v(t) = 0, \dot{V_v}(t) = 0$, hence $\tilde{v}_i(t) = 0, \dot{\tilde{v}}_i(t) = 0$ [88]. Therefore, after $t > t_f$ we can re-write (89) as

$$0 = a_i(t) - \eta(t) \Rightarrow \eta(t) = a_i(t) \tag{94}$$

where η is called *equivalent output error injection* to maintain the sliding motion [88]. In practice, η can be extracted by passing the switching signal $L_v sgn(\tilde{v}_i(t))$ through a low-pass filter with unity steady-state gain. Next, we analyze the error dynamics (90) using the Lyapunov function candidate $V_a(t) = \frac{1}{2}\tilde{a}_i^2(t) + \frac{K}{2}\tilde{\tau}^2(t)$ where $K > 0$. The derivative of the Lyapunov function candidate can be written as:

$$\dot{V_a}(t) = \tilde{a}_i(t)\dot{\tilde{a}}_i(t) + K\tilde{\tau}(t)\dot{\tilde{\tau}}(t) \tag{95}$$

After $t > t_f$ we have $\eta(t) = a_i(t)$ and $\tilde{v}_i(t) = 0$. Hence, we can re-write (95) as

$$\dot{V_a}(t) = -\frac{1}{h}\tilde{a}_i(t)\dot{a}_{i-1}(t)\tilde{\tau}(t) - L_a\tilde{a}_i(t)(\tilde{a}_i(t)) + K\tilde{\tau}(t)\dot{\tilde{\tau}}(t) \tag{96}$$

Considering the fact τ is constant and hence $\dot{\tau} = 0$, we can re-write (96) as

$$\dot{V_a}(t) = -\frac{1}{h}\tilde{a}_i(t)\dot{a}_{i-1}(t)\tilde{\tau}(t) - L_a\tilde{a}_i(t)(\tilde{a}_i(t)) - K\tilde{\tau}(t)\dot{\tilde{\tau}}(t) \tag{97}$$

Applying the update law (86) and choosing $K = \frac{1}{L_b}$, (97) becomes

$$\dot{V_a}(t) = -L_a\tilde{a}_i^2(t) \leq 0 \tag{98}$$

This concludes the decaying behavior of $V_a(t)$that is $V_a(t) \leq V(0)$. So, starting from any positive initial value of $V_a(0), V_a(t) \to \gamma < \infty$ is bounded as $t \to \infty$. Hence, by recalling $V_a(t) = \frac{1}{2}\tilde{a}_i^2(t) + \frac{K}{2}\tilde{\tau}^2(t)$, we conclude that $\tilde{a}_i(t)$ and $\tilde{\tau}(t)$are bounded as well.

Convergence of $\tilde{a}_i$: In this part, we prove $\tilde{a}_i(t) \to 0$ as $t \to \infty$. We derive the second derivative of Lyapunov candidate $V_a(t)$ with respect to time as

$$\ddot{V}_a(t) = -2L_a\tilde{a}_i(t)\dot{\tilde{a}}_i(t) \tag{99}$$

After $t > t_f$, replacing $\dot{\tilde{a}}_i(t)$ by

$$\dot{\tilde{a}}_i(t) = -\frac{1}{h}\dot{a}_{i-1}(t)\tilde{\tau} - L_a\tilde{a}_i(t) \tag{100}$$

we have

$$\ddot{V}_a(t) = 2\frac{L_a}{h}\tilde{a}_i(t)\dot{a}_{i-1}(t)\tilde{\tau} + 2L_a^2\tilde{a}_i^2(t) \tag{101}$$

As it mentioned earlier, $\tilde{a}_i(t)$ and $\tilde{\tau}$ are bounded. Furthermore, referring to *Assumption 13*, $\dot{a}_{i-1}$ is bounded. Hence, (101)shows the boundedness of $\ddot{V}_a(t) < \infty$ which equivalently verifies that $\dot{V}_a(t)$ is uniformly continuous. Now, applying Barbalat's lemma [92] on $\dot{V}_a(t)$ combined with the fact that $V_a(t)$ is bounded, we have $\dot{V}_a(t) \to 0$ as $t \to \infty$. Consequently, $\dot{V}_a(t) = -2L_a\tilde{a}_i^2(t) \to 0$. indicates that $\tilde{a}_i(t) \to 0$as $t \to \infty$.

Convergence of $\tilde{\tau}$

In this part, we prove $\tilde{\tau} \to 0$as $t \to \infty$. We know that

$$\int_0^\infty \dot{\tilde{a}}_i(t)dx = \tilde{a}_i(\infty) - \tilde{a}_i(0) = -\tilde{a}_i(0) < \infty \tag{102}$$

Furthermore, $\dot{V}_a(t)$, $\tilde{a}_i(t)$ and $\tilde{\tau}$ are uniformly continuous. Also, referring to *Assumption 13*, second derivative of $a_{i-1}(t)$ exists and is finite which equivalently imply that, $\dot{a}_{i-1}(t)$ is uniformly continuous. Hence, using (100) we conclude $\dot{\tilde{a}}_i(t)$is uniformly continuous. Therefore, by applying Barbalat's lemma [92], and considering the fact that $\dot{\tilde{a}}_i(t)$is bounded, we can conclude $\dot{\tilde{a}}_i(t) \to 0$as $t \to \infty$. Next, considering (78), where $\dot{\tilde{a}}_i(t) \to 0$ and $\tilde{a}_i(t) \to 0$ as $t \to \infty$, it is clear that $\tilde{\tau} \to 0$ as $t \to \infty$.

***Remark 12*:** The estimate of the delay parameter, $\hat{\tau}$, will be used to detect the occurrence of the DoS attack. Ideally, a DoS occurrence will be detected when $\hat{\tau} > 0$. Furthermore, the magnitude of $\hat{\tau}$ will serve as an estimate of the effect of DoS.

The effects of uncertainties have not been considered in the design of the detection observers. However, possible sources of uncertainty that affect the diagnostic scheme are: 1) unmodeled dynamics, 2) Radar measurement noise [93]-[94] 3) inherent communication delay in a practical DSRC network, 4) Driver behavior which affects CACC gains e.g. k_p and k_d [95]. The presence of these uncertainties prohibits $\hat{\tau}$ from having the idealized property of being zero even in the absence of any DoS attack. One of the possible ways to deal with this is to use nonzero threshold set based on a realistic DSRC network behavior. The detection logic will be: DoS attack is detected when $\hat{\tau} > \delta$ and no DoS when $\hat{\tau} \leq \delta$where δ is the threshold. The effect of the uncertainties on $\hat{\tau}$ will be suppressed below this threshold value.

Below are the guidelines for selection of constant threshold values for the evaluation of the residual:

Step 1: Collect $\hat{\tau}$ data under no DoS attack in normal DSRC network conditions from Monte-Carlo simulations or experimental studies.

Step 2: Plot the probability distribution of $\hat{\tau}$. An example probability distribution is shown in Fig. 21.In practice, this probability distribution will depend on uncertainties in the experimental data or of the Monte-Carlo study.

Step 3: Select a maximum allowable probability of false alarms.

Step 4: It can be seen from Fig. 21 that the probability of the false alarms can be computed by the following equation:

$$P_{FA} = \int_{\delta}^{\infty} p_0(x)dx, \tag{103}$$

where P_{FA} is the probability of DoS false alarm, δ is the selected threshold for DoS attack and $p_0(x)$ is the $\hat{\tau}$ probability distribution under no DoS attack in the DSRC network. The goal here is to select δ which will yield an acceptable P_{FA}.

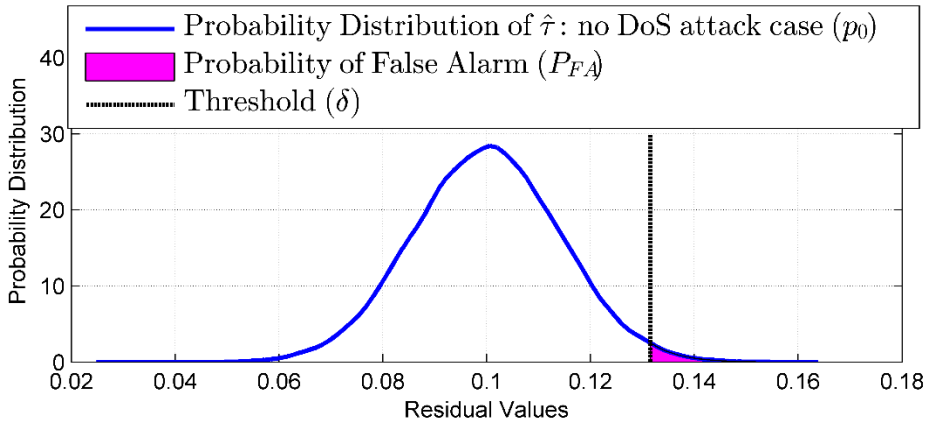

Figure 21. Residual probability distribution under no attack condition

6.2.3. Simulation Studies

In this section, we present simulation studies to evaluate the effectiveness of the proposed scheme. In this simulation setup, we consider a platoon of four identical vehicles equipped with CACC system. The vehicles in the platoon exchange their safety related messages including acceleration information through DSRC network. Furthermore, we assume that the platoon follows a dynamic velocity profile, namely the US06 driving cycle

shown in Fig. 13. In simulation, we repeat this driving cycle 13 times to create velocity trajectory followed by the leader vehicle. Model and control parameters of the platoon and CACC system are chosen as $h = 0.3\ s$, $k_p = 0.7$, and $k_d = 1$ [30]-[31]. To illustrate the results of the proposed algorithm, we particularly focus on the performance of the *Vehicle 3* in the platoon. Since we focus on *Vehicle 3*, the presented algorithm containing two observers implemented in *Vehicle 2*, as noted in *Remark 12*. Next, we present the following case studies.

Case 1: In this case study, we motivate the need for the DoS attack detection algorithm by illustrating the adverse effects of the attacks on the platoon. In Fig. 22, we show the relative distance (d_3), velocity (v_3) and acceleration (a_3) of *Vehicle 3* in the presence of the DoS attacks. To simulate the the effect of the DoS attacks, different magnitudes of delays are injected to the DSRC network. In the ideal case when there is no delay in DSRC network, i.e.$\tau = 0\ s$, the relative distance of *Vehicle 3* is maintained above the minimum safety distance d_s for all time. However, the performance of *Vehicle 3* degrades when we increase the magnitude of the DoS attacks, i.e. $\tau > 0.2\ s$. In these scenarios, the minimum distance requirement is violated as shown in the top plot in Fig.22. These violations represent crash scenarios in a platoon of self-driving vehicles. From this case study, we can conclude that DoS attack might lead to potentially dangerous situations. Hence, the need for DoS detection is evident for secure control of connected vehicles.

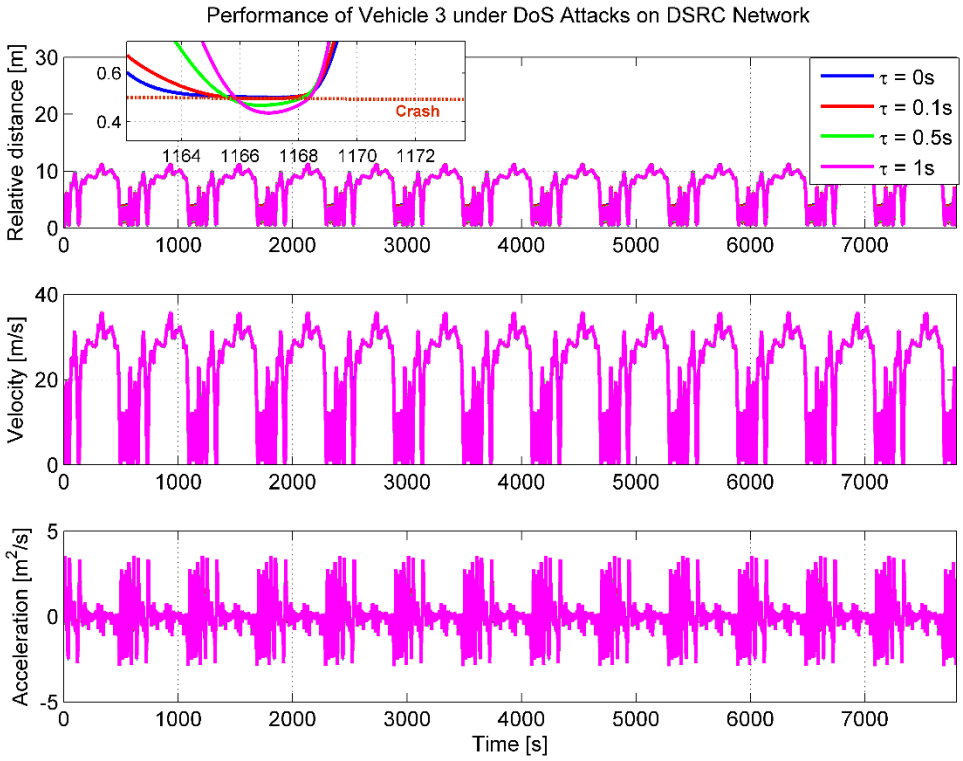

Figure 22: Performance of the Vehicle 3 in the platoon under DoS Attacks in DSRC Network

Case 2: In the second case study, we consider a more realistic scenario in the simulation. Ideal communication does not exist in practical applications, especially for DSRC [23]. Hence, we add a random non-zero mean delay with Gaussian distribution to the communication network. This random delay represents the inherent uncertainties in DSRC communication. The mean value and standard deviation of the network induced delay are chosen as $\mu_N = 0.1\,s$ and $\sigma_N = 0.03\,s$, respectively. Next, we show the performance of the scheme in presence of this inherent communication delay. Note that, there is no DoS attack in this case study. The relative distance (d_3), velocity (v_3) and acceleration (a_3) corresponding to *Vehicle 3* are shown in Fig. 23 under this scenario. We

can see in the top plot of Fig. 23 that the CACC performs reasonably as the inter-vehicle distance between two cars is more than the assigned safety distance, $d_s = 0.5\ m$. Regarding the detection scheme, observers are initialized with incorrect values of $\hat{a}_3(0) = 0$ and $\hat{\tau}(0) = 0$, respectively. The estimated value of acceleration in *Vehicle 3* is shown in the first plot of Fig. 24. As can be seen in Fig. 24, the estimated value ($\hat{a}_3$) converges to its actual value (a_3). The estimation error is given in the bottom plot in Fig. 24. Furthermore, the detection algorithm is able to estimate the mean value of this network-induced delay as shown in the first plot of Fig. 25. We quantify the estimation performance in terms of convergence time. Referring to Fig. 25, the convergence time is within 100 seconds for the delay estimation. Importantly, the estimated delay is within the predefined threshold (δ) indicating no occurrence of DoS.

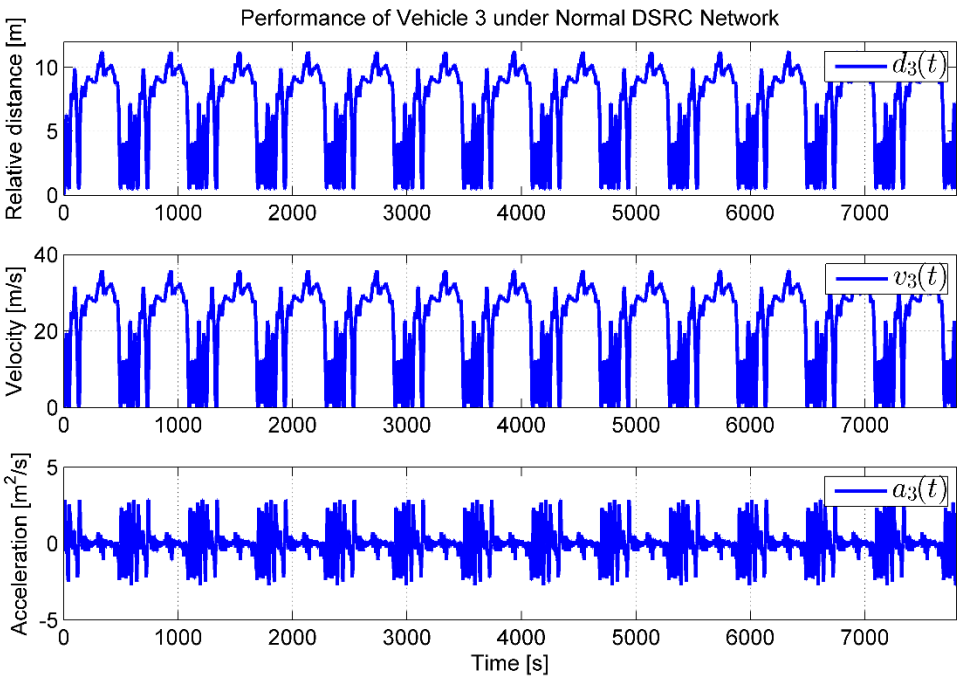

Figure 23: Performance of the *Vehicle 3* in the platoon under normal DSRC Network

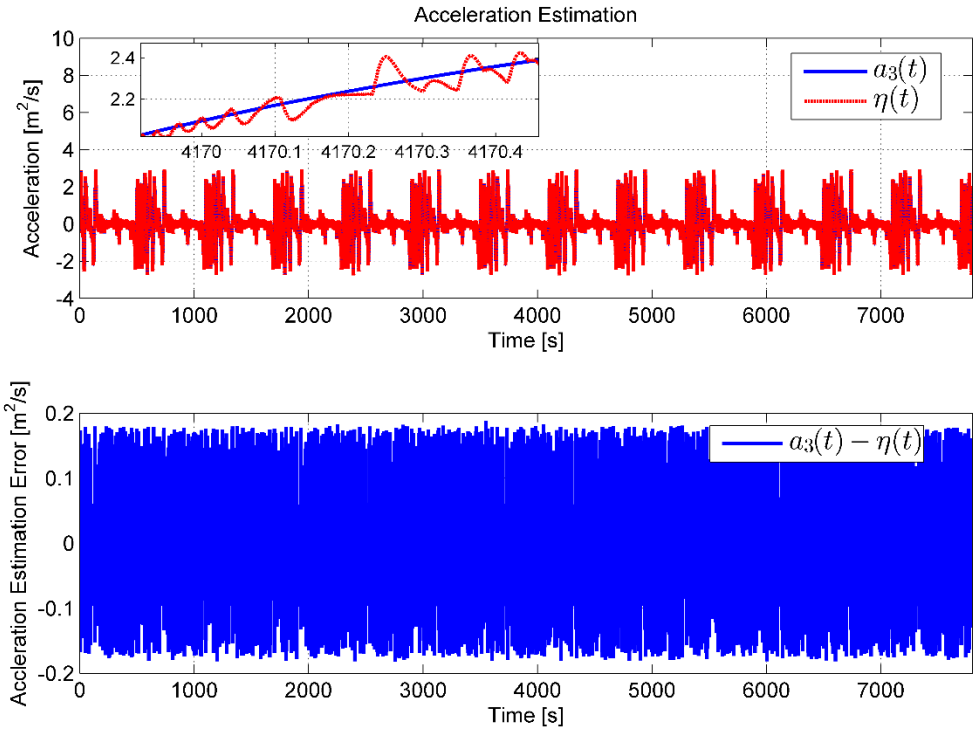

Figure 24: Acceleration estimation in *Vehicle 3*. The variable $a_3$denotes actual value and η denotes estimated value.

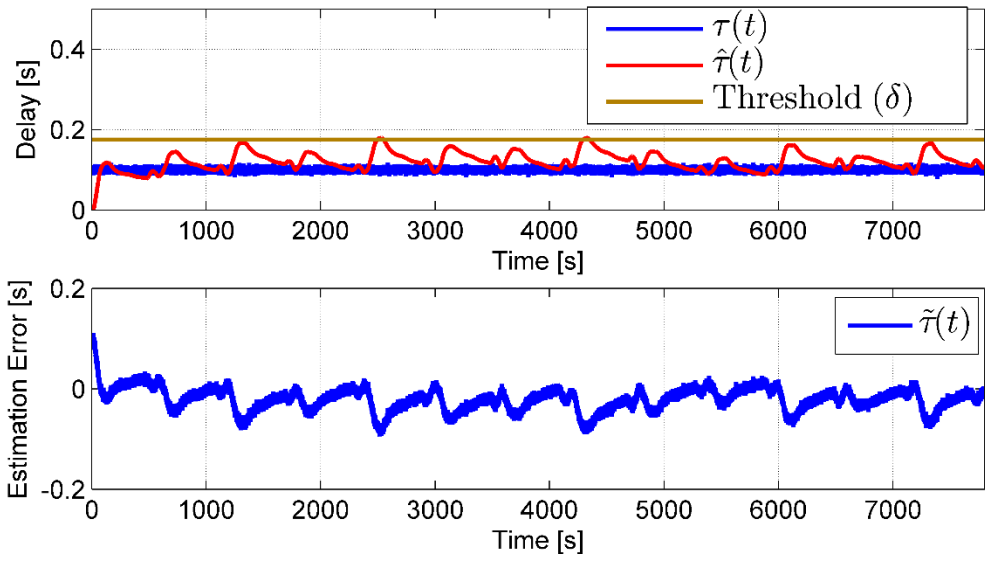

Figure 25: Network induced delay and estimation of the delay in normal DSRC Network

Case 3: In this case, we test the effectiveness of the proposed approach under DoS attack. To emulate the DoS attack, a delay of $\tau = 0.5\ s$ is injected at $t = 3000\ s$ to the communication network apart from the a aforementioned network induced delay. The induced delay takes certain time to reach a constant steady-state value as shown in Fig. 28. This is due to the assumption that it takes certain time for the attacker to jam the network. Fig. 26 shows the relative distance d_3, velocity v_3 and acceleration a_3 of *Vehicle 3* in the presence of this DoS attack. Observers are initialized with incorrect values of $\hat{a}_3(0) = 0$ and $\hat{\tau}(0) = 0$, respectively. The estimated acceleration of vehicle 3, $\hat{a}_3$ is shown in the top plot of Fig. 27 along with the actual value of a_3. The acceleration estimation error given by bottom plot of Fig. 27. These two figures illustrate that the estimated value $\hat{a}_3(t)$ converges to the actual value in finite time. Furthermore, the algorithm is also able to detect and estimate the DoS attack. The top plot in Fig. 28 shows the delay estimation performance. The DoS estimation error is given in the bottom plot of Fig. 28. The attack is detected when the estimated delay ($\hat{\tau}$) crossed the threshold (δ) after the attack occurrence. The estimate $\hat{\tau}$ closely tracks the true delay τ. The steady-state delay estimation error lies within less than 10% of the original value.

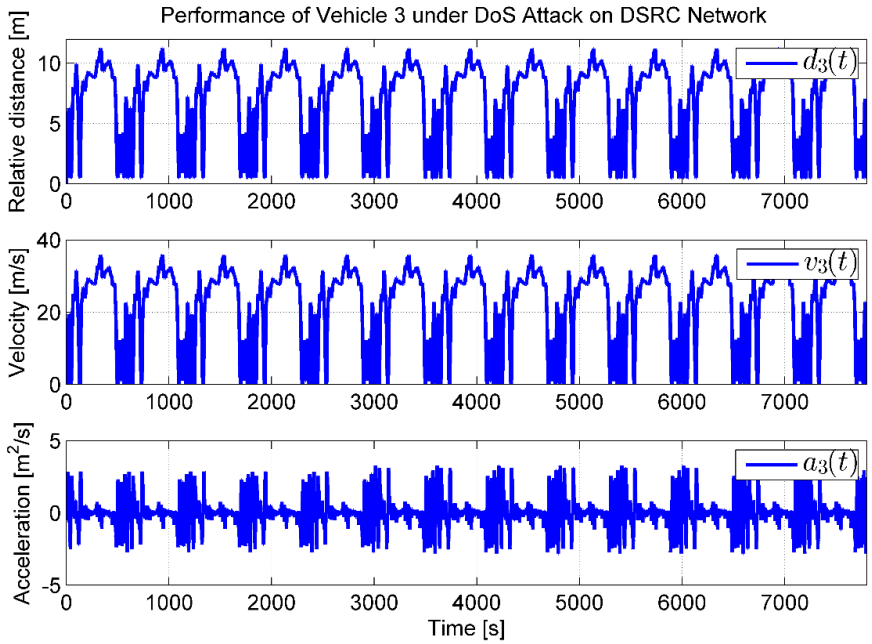

Figure 26: Performance of the *Vehicle 3* in the platoon under DoS attack in DSRC network

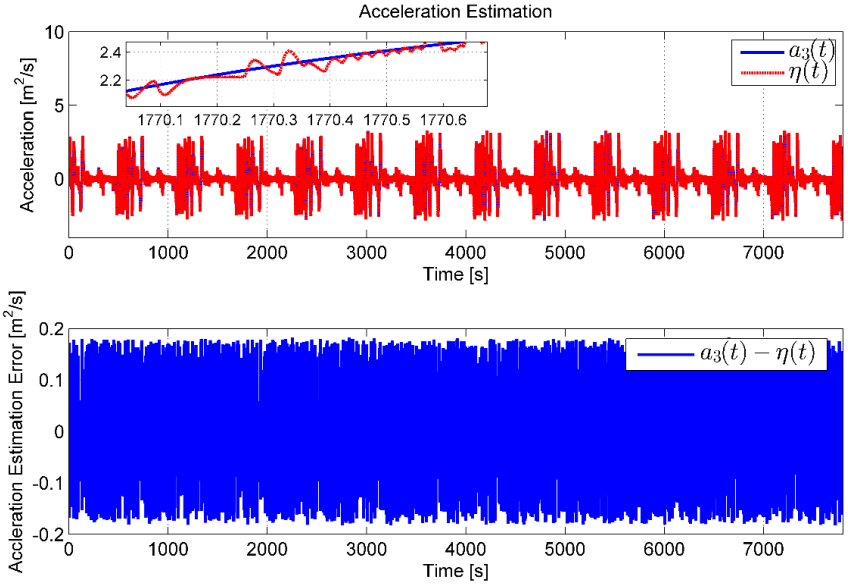

Figure 27: Acceleration estimation in *Vehicle 3*. The variable $a_3$denotes actual value and η denotes estimated value.

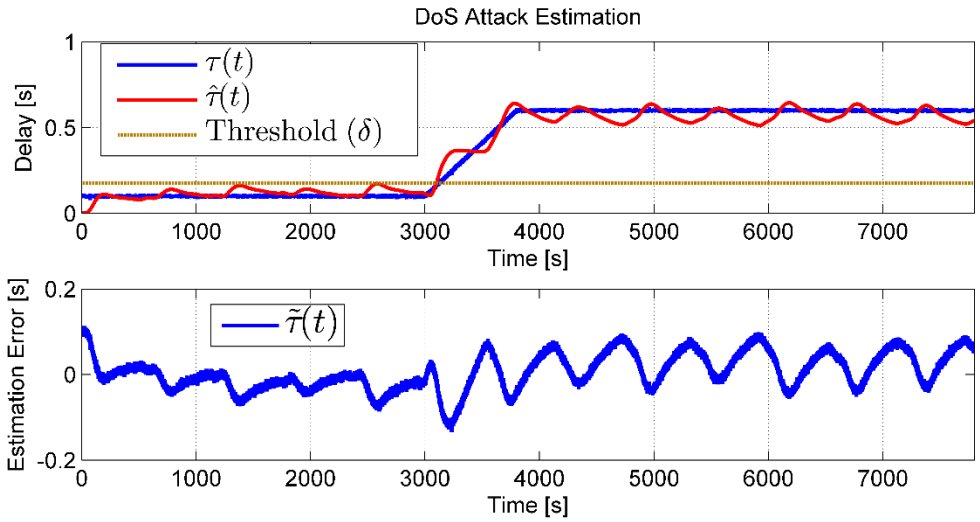

Figure 28: Delay estimation under DoS attack

Next, we illustrate the effectiveness of the proposed approach under several form of uncertainties. In all these following scenarios, a non-zero mean Gaussian delay with the mean value of $\mu_N = 0.1\,s$ and standard deviation of $\sigma_N = 0.03\,s$ is considered as the network induced delay. Furthermore, a constant delay of $\tau = 0.5\,s$ is added to represent the attack at $t = 3000s$.

Case 4: In this case study we demonstrate the robustness of DoS detection algorithm to the uncertainty in the proportional gain k_p. Note that the observers are designed based on the nominal parameter value whereas the actual vehicle parameter is different than the nominal value. The nature of the uncertainty is an additive constant offset added to the nominal value of parameter k_p. We inject 5%, 10%, 15%, and 20% uncertainties to the k_p,

i.e. $k_p = k_{p0} + \Delta k_p$ where k_{p0} is the nominal value and Δk_p is the injected uncertainty. Figure.29 presents the estimated values of the delay under these uncertainties. As can be seen from Fig. 29, the proposed scheme can detect the DoS attack in less than 70 seconds after the attack injection even in the presence of uncertainties. However, delay estimation suffers from these uncertainties leading to 15% or more error.

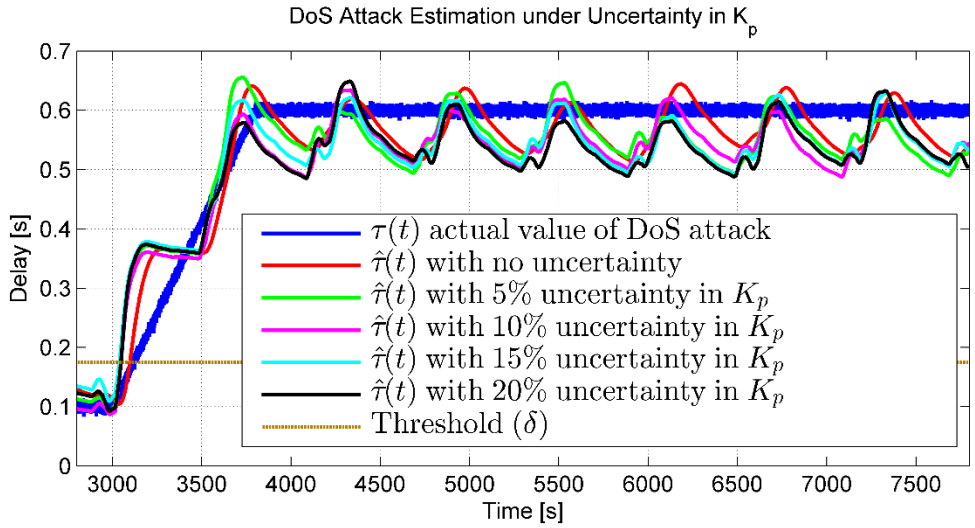

Figure 29: Delay estimation performance under different levels of uncertainties in the parameter k_p. The scenario is based on Case 4.

Case 5: In this scenario, the robustness of the proposed scheme is evaluated under uncertain k_d. To study the effect of uncertainties, we inject 5%, 10%, 15% , and 20% uncertainties to the nominal value of k_d in the model. Same as before, the observers are designed based on the nominal parameter value. Figure. 30 shows the delay estimation for different levels of uncertainties in k_d. As can be inferred from Fig. 30, the DoS detection algorithm can detect the DoS attack despite the uncertainties. However, the presence of

uncertainties affects the accurate delay estimation. For example, there is 15% estimation error under 20% uncertain k_d.

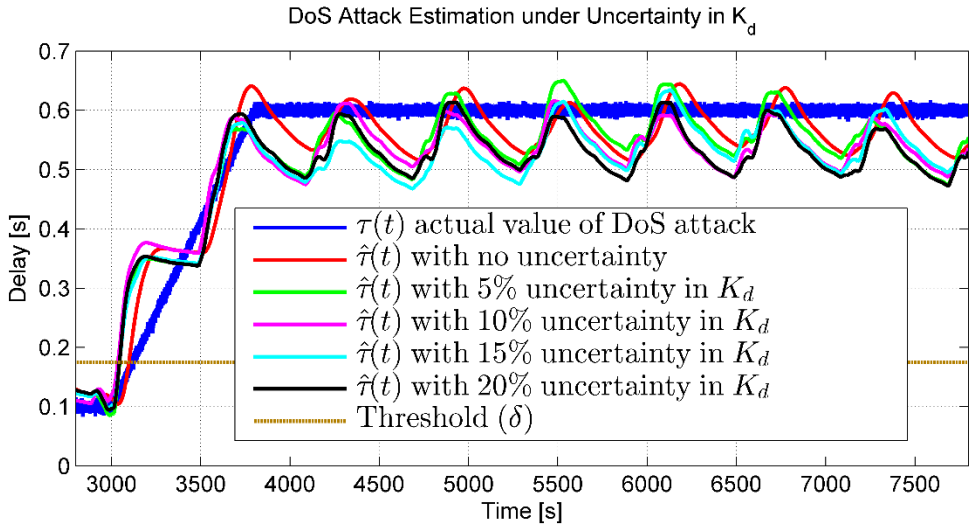

Figure 30: Delay estimation performance under different levels of uncertainties in the parameterk_d. The scenario is based on Case 5.

Case 6: In this case study the effects of measurement noise is discussed. A zero mean Gaussian noise with standard deviation of σ is added to the velocity measurement. To illustrate the robustness of the proposed scheme under measurement uncertainty in V_i, different levels of noises as $\sigma = 0.07, 0.1, 0.14, 0.21$ are added to the velocity measurement. Figure 31 shows the delay estimation for different levels of measurement noises in V_i. It can be seen in Fig. 31 that the DoS detection algorithm detects the DoS attack in all cases. However, the presence of uncertainties affects the accurate delay estimation. For example, there is 25% estimation error under $\sigma = 0.21$.

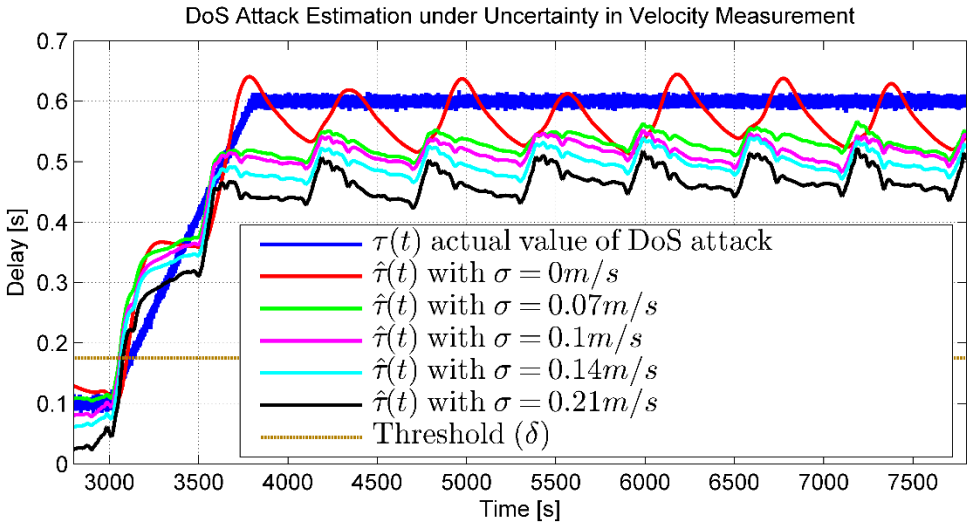

Figure 31: Delay estimation performance under different levels of uncertainties in V_i measurement. The scenario is based on Case 6.

6.3. Strategy Number Three

In this section, we consider a distributed cyber physical system with a shared communication network where the local controller of a sub-system receives measurements with delay. The amount of lumped delay produced by sensor measurements and network communication, is unknown. A new observer-based algorithm is proposed to estimate the states of the system at the time t when only delayed measurements are available. The main contribution of this section of the thesis is the idea of using new observer-based algorithm to estimate an unknown delay and states of a system in the presence of delayed measurements. This study under the condition of unknown delay in the measurements has not been explored in the existing literatures. To address this research gap, a new approach consisting of two observers is presented. i) a PDE-based observer to estimate the unknown delay with adaptive estimation ; and ii) an ODE-based observer to predict the states of the

system using the information from the former observer. Theoretical contributions of this section are devoted to mathematically proving the convergence of estimation error in both ODE delayed observer as well as PDE observer.

Notation: In this section, the following notations are used:

$$z_t(x,t) = \frac{\partial z(x,t)}{\partial t},\ z_x(x,t) = \frac{\partial z(x,t)}{\partial x},\ \|z(.)\| = \sqrt{\int_0^1 z^2(x,t)dx}$$

6.3.1. Problem Statement

Consider a distributed cyber physical system with a shared communication network shown in Fig.32. Each plant as a subsystem of the CPS transfers sensor measurements to the local controller using the communication network.

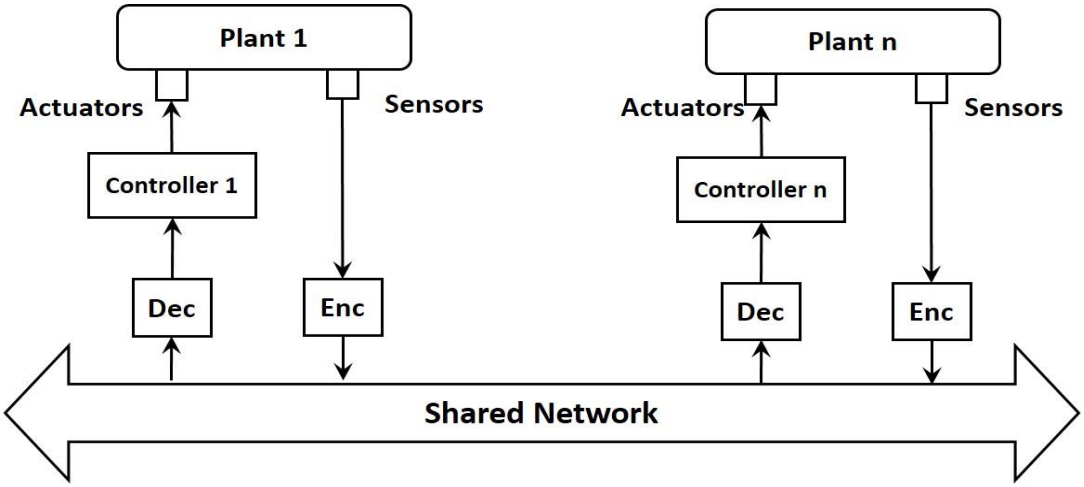

Figure 32. A distributed CPS with a shared network.

For simplicity, we mainly focus on one subsystem of the CPS as it is depicted in Fig.33. In this section, we consider a lumped constant unknown delay, D, between the actual measureable data and the data the controller receives. The system dynamics can be modelled as:

$$\dot{X}(t) = AX(t) + BU(t) \tag{104}$$

$$Y(t) = CX(t - D) \tag{105}$$

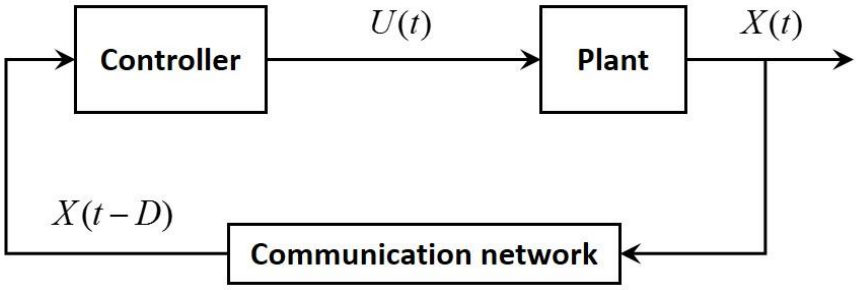

Figure 33. A schematic of a sub-plant of the distributed CPS.

Where $\in \mathbb{R}^n$, $Y \in \mathbb{R}^m$ and $U \in \mathbb{R}^p$ are states, output and input of the system respectively. $A: \mathbb{R}^n \times \mathbb{R}^n, B: \mathbb{R}^n \times \mathbb{R}^p, C: \mathbb{R}^m \times \mathbb{R}^n$ are well defined matrices and all eigenvalues of A have negative real part. $D \in \mathbb{R}^+$, $\underline{D} \leq D \leq \overline{D}$ is a nonzero lumped unknown constant delay where the upper and lower bounds of the delay are known. Dynamics of the delay is modelled with a transport PDE which allows a linear parameterization in the unknown delay [98].

$$Dz_t(x,t) = z_x(x,t) \quad , x \in [0,1] \tag{106}$$

$$z(0,t) = CX(t - D) \tag{107}$$

$$z(1,t) = CX(t) \tag{108}$$

NOTE: Measured value in the plant at time t is $CX(t)$, but the available measurement in the controller is $CX(t - D)$.

Where $z(x,t)$ is the state of communication network in the transport PDE model and only $z(0,t)$ is available as the measurement in the controller.

$$z(x,t) = CX\big(t + D(x-1)\big) \tag{109}$$

Therefore, we can write $z(x,t)$ as the solution of the PDE (106)-(108) and Ordinary Differential Equation (ODE) system (1)-(2) as follows:

$$X(t) = e^{At}X_0 + \int_{t_0}^{t} e^{A(t-\theta)}BU(\theta)d\theta$$

Where, $X_0 = X(t = t_0)$

Considering (6), the solution of the PDE (3)-(5) is derived as:

$$z(x,t) = C\left[e^{AD(x-1)}X(t) - \int_{t+D(x-1)}^{t} e^{A(t+D(x-1)-\theta)}BU(\theta)d\theta\right] \tag{110}$$

The goal of this section is to design a state estimation to predict (t) , while only the delayed measurements, $CX(t-D)$, is available.

6.3.2. Estimation Algorithm

In this section, we will discuss the proposed scheme in detail. As mentioned before, the main objective of this scheme is to estimate the unknown delay, D, and predict the states of the system $X(t)$. From the schematic depicted in Fig. 24, it can be inferred that the algorithm consists of two observers working in cascade manner as follows.

Observer I: This observer is an adaptive observer based on the PDE dynamics of the unknown delay. Using the available measurements affected by the delay, the observer estimates the unknown delay and updates the adaptation law. The estimated delay is fed into the Observer II to predict $X(t)$.

Observer II: The second observer is an ODE based linear observer which is designed using the estimated delay and available system inputs and outputs.

The details of the design of these individual elements are discussed in the subsequent sections.

Remark 14: The presented scheme is designed and implemented in the local controller. Hence, observers only use available information in the controller.

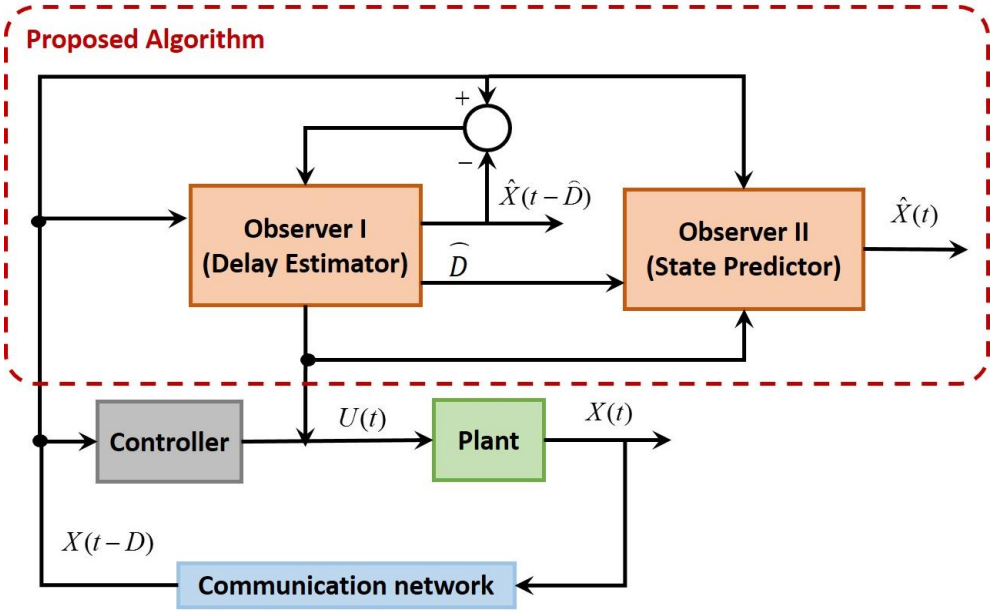

Figure 34. The schematic of the proposed algorithm.

Observer I

We consider the observer dynamics as the following [96]-[97]

$$\dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L_1\widehat{D}\big(Y(t) - \hat{Y}(t)\big) \tag{111}$$

$$\hat{Y}(t) = C\hat{X}(t - \widehat{D}) \tag{112}$$

Where, $\widehat{D}(t)$ is the estimated value of unknown delay, $\hat{X}(t)$ and $\hat{Y}(t)$ are the estimations of $X(t)$ and $Y(t)$ respectively. Similar to the original system, in the observer design, the estimated delay is modelled with a transport PDE:

$$\hat{z}(0,t) = \hat{Y}(t) = C\hat{X}(t - \widehat{D}) \tag{113}$$

$$\hat{z}(1,t) = C\hat{X}(t) \tag{114}$$

where

$$\hat{z}(x,t) = C\hat{X}\left(t + \hat{D}(x-1)\right) = C\left[\hat{X}e^{A\hat{D}(x-1)}\hat{X}(t) - \int_{t+\hat{D}(x-1)}^{t} e^{A(t+\hat{D}(x-1)-\theta)}BU(\theta)d\theta\right] \tag{115}$$

Using (12), dynamic of the estimated delay is given as

$$\hat{D}\hat{z}_t(x,t) = \hat{z}_x(x,t)\left(1 + \dot{\hat{D}}(x-1)\right) + \hat{D}L_1\tilde{z}(0,t) \tag{116}$$

Next, we implement (116) in (111)-(112) to re-write the observer dynamics

$$\dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L_1(\tilde{z}(0,t)) \tag{117}$$

$$\hat{D}\hat{z}_t(x,t) = \hat{z}_x(x,t)\left(1 + \dot{\hat{D}}(x-1)\right) + \hat{D}L_1\tilde{z}(0,t) \tag{118}$$

$$\hat{z}(0,t) = \hat{Y}(t) = C\hat{X}\left(t - \hat{D}\right) \quad , \quad \hat{z}(1,t) = C\hat{X}(t) \tag{119}$$

where, $\tilde{z}(x,t) = z(x,t) - \hat{z}(x,t)$. Defining $\tilde{D} = D - \hat{D}$ as the delay estimation error, $\hat{D}$ in the left side of (118) can be substituted by $\hat{D} = D - \tilde{D}$. Further, (118) as the observer dynamic can be re-written as

$$D\hat{z}_t(x,t) = \tilde{D}\hat{z}_t(x,t) + \hat{z}_x(x,t)\left(1 + \dot{\hat{D}}(x-1)\right) + \hat{D}L_1\tilde{z}(0,t) \tag{120}$$

The standard projector operator is given by

$$\dot{\hat{D}} = \gamma Proj\{\tau(t)\} = \begin{cases} 0, & \hat{D} = \underline{D} \text{ and } \tau < 0 \\ 0, & \hat{D} = \overline{D} \text{ and } \tau > 0 \\ \tau(t), & else \end{cases} \tag{121}$$

Where $\tau(t)$ based on Lyapunov analysis in Theorem 1, is designed as

$$\tau(t) = -\frac{1}{\hat{D}}\tilde{z}(0,t)\hat{z}_x(0,t) \tag{122}$$

And $\gamma > 0$ is the adaptation gain which can be selected as a small enough value. The estimation error dynamics are derived by subtracting (120) from (106),

$$\dot{\tilde{X}}(t) = A\tilde{X}(t) - L_1\tilde{z}(0,t) \tag{123}$$

$$D\tilde{z}_t(x,t) = \tilde{z}_x(x,t) - \frac{\tilde{D}}{\hat{D}}\hat{z}_x(x,t) - \frac{D\dot{\hat{D}}}{\hat{D}}(x-1)\hat{z}_x(x,t) - L_1 D\tilde{z}(0,t) \tag{124}$$

$$\tilde{z}(1,t) = C\tilde{X}(t)$$

$$\dot{\tilde{D}}(t) = -\dot{\hat{D}}(t) \tag{125}$$

Theorem 1: Consider a system described with (104)-(106) and unknown delay dynamics as (107)-(108). For the observer designed as (111)-(114) and adaptive delay estimator of (121), the output estimation error $\tilde{z}(0,t)$ and delay estimation error, $\tilde{D}$, will converge to a bounded area as $t \to \infty$, if the observer gain L_1 is selected large enough to satisfy the following condition,

$$L_1 > \frac{|\tilde{z}_x(0,t)|}{\underline{D}|\tilde{z}(0,t)|}$$

Proof: To analyse the estimation error dynamics, we consider function (126) as Lyapunov candidate

$$W(t) = a_1 D\tilde{z}(0,t)^2 + a_2\tilde{D}^2 \tag{126}$$

Where, $a_1 > 0$, $a_2 > 0$ and $D > 0$, derivate of $W(t)$ with respect to time is given as

$$\dot{W}(t) = a_1 D\frac{\partial}{\partial t}(\tilde{z}(0,t)^2) - 2a_2\tilde{D}\dot{\hat{D}} \tag{127}$$

Therefore,

$$\dot{W}(t) = 2a_1 D\tilde{z}(0,t)\tilde{z}_t(0,t) - 2a_2\tilde{D}\dot{\hat{D}} \tag{128}$$

Substituting $\tilde{z}_t(0,t)$ from (124) at $x = 0$

$$\dot{W}(t) = 2a_1\tilde{z}(0,t)\left(\tilde{z}_x(0,t) - \frac{\tilde{D}}{\hat{D}}\hat{z}_x(0,t) + \frac{D\dot{\hat{D}}}{\hat{D}}\hat{z}_x(0,t) - DL_1\tilde{z}(0,t)\right) - 2a_2\tilde{D}\dot{\hat{D}} \tag{129}$$

The updating rule of $\dot{\hat{D}}$ as given by (121)-(122), simplifies (129) to the following equation

$$\dot{W}(t) = 2a_1\tilde{z}(0,t)\tilde{z}_x(0,t) - 2\tilde{D}\left(a_1\frac{\hat{z}_x(0,t)}{\hat{D}}\tilde{z}(0,t) - a_2\dot{\hat{D}}\right) + 2a_1\tilde{z}(0,t)\frac{D\dot{\hat{D}}}{\hat{D}}\hat{z}_x(0,t) - 2a_1 DL_1\tilde{z}(0,t)^2 \tag{130}$$

Choosing $a_2 = a_1$ and substituting the expressions of (122), we get

$$\dot{W}(t) = 2a_1\tilde{z}(0,t)\tilde{z}_x(0,t) - 2a_1\frac{D}{\hat{D}^2}\tilde{z}(0,t)^2\hat{z}_x(0,t)^2 - 2\,a_1 DL\tilde{z}(0,t)^2 \tag{131}$$

$$\dot{W}(t) \leq 2a_1(|\tilde{z}(0,t)||\tilde{z}_x(0,t)|) - 2a_1\frac{D}{\hat{D}}\tilde{z}(0,t)^2\hat{z}_x(0,t)^2 - 2\,a_1\underline{D}L_1|\tilde{z}(0,t)|^2 \tag{132}$$

$$\dot{W}(t) \leq 2a_1|\tilde{z}(0,t)|\left(|\tilde{z}_x(0,t)| - \underline{D}L_1|\tilde{z}(0,t)|\right) - 2a_1\frac{D}{\hat{D}}\tilde{z}(0,t)^2\hat{z}_x(0,t)^2 \tag{133}$$

As long as we can choose observer gain L_1 to satisfy the following condition,

$$L_1 > \frac{|\tilde{z}_x(0,t)|}{\underline{D}|\tilde{z}(0,t)|} \tag{134}$$

Therefore, we can conclude the negative semi definiteness of $\dot{W}(t)$. Hence, $\dot{W}(t)$ will settle on or within a bounded ball of radius RoC as $t \to \infty$. Note that the magnitude of RoC can be made arbitrarily small by choosing a high value of L_1.

$$RoC: \frac{|\tilde{z}_x(0,t)|}{\underline{D}|\tilde{z}(0,t)|} - L_1 < 0$$

Observer II

Observer II utilizes the estimated delay obtained from Observe I to predict states of the system at time t; while, only the delayed measurements at $t - D$ are available.

Assumption 15: The signal $X(t)$ is at least once differentiable with respect to time. Furthermore, the derivative is bounded by some finite value, i.e. $\left|\dot{X}(t)\right| < X_{dmax}$, $\forall\, t > 0$.

Considering the system dynamics (104)-(105), we design the second observer as follows

$$\dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L_2\left(Y(t) - \hat{Y}(t)\right)$$

$$\hat{Y}(t) = C\hat{X}(t - \widehat{D}) \qquad (135)$$

Where $\widehat{D}(t) \in \left[\underline{D}, \overline{D}\right]$ is the estimated delay derived from the Observer I.

Remark 15: Referring to (121), $\widehat{D}(t)$ has a bounded derivative with respect to time.

Substituting the (135) in the dynamic of Observer II is given as,

$$\dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L_2\left(Y(t) - \mathrm{C}\hat{X}(t - \widehat{D}(t))\right) \qquad (136)$$

Next, by subtracting (136) from first equation of (134), the estimation error dynamic is derived as

$$\dot{\tilde{X}}(t) = A\tilde{X}(t) - L_2 C\left(\tilde{X}(t - \hat{D}(t))\right) + M(t) \tag{137}$$

where, L_2 is the second observer's gain and $M(t)$ is the bounded uncertainty due the delay estimation error.

With initial condition as $\tilde{X}(t_0) = \tilde{X}_0$, $\tilde{X}(s) = 0$, $s < t_0$, we will apply the following Lyapunov-Krasovskii functional for delay-dependent analysis of (137)

$$V(t, \tilde{X}, \dot{\tilde{X}}) = \tilde{X}^T(t) P \tilde{X}(t) + \int_{t-\overline{\mathrm{D}}}^{t} e^{a(s-t)} \tilde{X}^T(s) S \tilde{X}(s) ds$$
$$\int_{t-D}^{t} e^{a(s-t)} \tilde{X}^T(s) E \tilde{X}(s) ds$$
$$+\overline{\mathrm{D}} \int_{-\overline{\mathrm{D}}}^{0} \int_{t+\theta}^{t} e^{a(s-t)} \dot{\tilde{X}}^T(s) R \dot{\tilde{X}}(s) ds \, d\theta \tag{138}$$

where $a > 0, b > 0 \; and \; n \times n - matrices \; P > 0, S > 0, E > 0 \; and \; R > 0$

Preposition 1: The error dynamics represented in (34) is stable and converges to a bounded region exponentially, if there exist $L_2 > 0$ and $a > 0, b > 0 \; and \; n \times n - matrices \; P > 0, S > 0, E > 0 \; and \; R > 0$ matrix such that along trajectories of (137), the Lyapunov-Krasovskii function (138) satisfies the following condition [99]-[100].

$$W_2 \triangleq aV - b|M|^2 + \dot{V} < 0 \tag{139}$$

Then, the solution of (124) with initial condition of $\tilde{X}(t_0) = \tilde{X}_0$ satisfies the inequality

$$\tilde{X}^T(t) P \tilde{X}(t) < e^{-a(t-t_0)} \tilde{X}_0^T P \tilde{X}_0 + \left[1 - e^{-a(t-t_0)}\right] \frac{b}{a} \left| M_{[t_0, t_\infty]} \right|_\infty^2 \tag{140}$$

Proof: Applying comparison principle [99], we have

$$\tilde{X}^T(t)P\tilde{X}(t) \leq V\left(t,\tilde{x}_t,\dot{\tilde{x}}_t\right) < e^{-a(t-t_0)}V\left(t,\tilde{x}_{t0},\dot{\tilde{x}}_{t0}\right) + \int_{t_0}^{t} e^{-a(t-s)}b|M(s)|^2 ds$$

(141)

Lyapunov candidate V can be written as (142) as a positive definite function

$$V\left(t,\tilde{X},\dot{\tilde{X}}\right) = V_1 + V_2 + V_3 + V_4 \tag{142}$$

where

$$V_1 = \tilde{X}^T(t)P\tilde{X}(t) \tag{143}$$

$$V_2 = \int_{t-\overline{\mathrm{D}}}^{t} e^{a(s-t)}\tilde{X}^T(s)S\tilde{X}(s)ds \tag{144}$$

$$V_3 = \int_{t-\mathrm{D}}^{t} e^{a(s-t)}\tilde{X}^T(s)E\tilde{X}(s)ds \tag{145}$$

$$V_4 = \overline{\mathrm{D}}\int_{-\overline{\mathrm{D}}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{X}}^T(s)R\dot{\tilde{X}}(s)ds\,d\theta \tag{146}$$

Making derivative of V with respect to time,

$$\dot{V}_1 = 2\tilde{X}^T(t)P\dot{\tilde{X}}(t) \tag{147}$$

$$\dot{V}_2 = \frac{\partial}{\partial t}\left[e^{-at}\int_{t-\overline{\mathrm{D}}}^{t} e^{as}\tilde{X}^T(s)S\tilde{X}(s)ds\right]$$

$$= -ae^{-at}\left(\int_{t-\overline{\mathrm{D}}}^{t} e^{as}X^T(s)S\tilde{X}(s)ds\right) + \tilde{X}^T(t)S\tilde{X}(t)$$

$$+ e^{-\overline{D}t}\tilde{X}^T\left(t-\overline{D}\right)S\tilde{X}\left(t-\overline{D}\right)$$

(148)

Similarly,

$$\dot{V}_3 = -ae^{-at}\left(\int_{t-\mathrm{D}}^{t} e^{as}\tilde{X}^T(s)E\tilde{X}(s)ds\right) + \tilde{X}^T(t)E\tilde{X}(t) + e^{-Dt}\tilde{X}^T(t-D)E\tilde{X}(t-D)$$

(149)

$$\dot{V}_4 = -a\overline{D}\left(\int_{-\overline{\mathrm{D}}}^{0}\int_{t+\theta}^{t} e^{a(s-t)}\dot{\tilde{X}}^T(s)R\dot{\tilde{X}}(s)ds\,d\theta\right) + \overline{D}^2\dot{\tilde{X}}^T(t)R\dot{\tilde{X}}(t)$$

$$-\overline{D}\int_{t-\overline{\mathrm{D}}}^{t} e^{-a(s-t)}\dot{\tilde{X}}^T(s)R\dot{\tilde{X}}(s)ds$$

(150)

Substituting (142)-(146) and (147)-(150) in (139), we find

$$W_2 \le 2\tilde{X}^T(t)P\dot{\tilde{X}}(t) + a\tilde{X}^T(t)P\tilde{X}(t) - bM^T(t)M(t)$$

$$+\overline{D}^2\dot{\tilde{X}}^T(t)R\dot{\tilde{X}}(t) - \overline{D}e^{-a\overline{D}}\int_{t-\overline{D}}^{t}\dot{\tilde{X}}^T(s)R\dot{\tilde{X}}(s)ds + \tilde{X}^T(t)S\tilde{X}(t) + \tilde{X}^T(t)[S$$

$$+E]\tilde{X}(t) - \tilde{X}^T\left(t-\overline{D}\right)S\tilde{X}(t-\overline{D}) + [\tilde{X}^T(t-D)E(\tilde{X}(t-D)]e^{-a\overline{D}}$$

(151)

Next, applying the standard arguments we obtain that

$$W_2 \le \eta^T(t)\Phi\eta(t) < 0 \qquad \forall\eta(t) \ne 0 \tag{152}$$

where, $\eta(t) = col\left\{\tilde{X}(t), \dot{\tilde{X}}(t), \tilde{X}\left(t-\overline{D}\right), \tilde{X}(t-D), M(t)\right\}$ if the matrix inequality

$$\Phi = \begin{bmatrix} \phi_{11} & \phi_{12} & 0 & -P_2^T L_2 C + \mathrm{Re}^{-a\overline{D}} & P_2^T \\ * & \phi_{22} & 0 & -P_3^T L_2 C & P_3^T \\ * & * & -(S+R)e^{-a\overline{D}} & Re^{-a\overline{D}} & 0 \\ * & * & * & -(2R+E)e^{-a\overline{D}} & 0 \\ * & * & * & * & -bI \end{bmatrix} < 0 \quad (153)$$

is feasible, where

$$\phi_{11} = A^T P_2 + P_2^T + aP + S + E - \mathrm{Re}^{-a\overline{D}} \quad (154)$$

$$\phi_{12} = P - P_2^T + A^T P_3 \quad (155)$$

$$\phi_{22} = -P_3 - P_3^T + \overline{D}^2 R \quad (156)$$

Thus, the following results will be obtained

Lemma 1: Given $a > 0, b > 0$, $and\ \ \overline{D} > 0$, let there exist $n \times n\ matrices\ P > 0, P_2, P_3,\ S > 0, E > 0\ and\ R > 0$ such that the LMI (153) with notation given in (154)-(156) holds. Then, the solution of (137) satisfies (140) for all delays $\underline{D} \leq D \leq \overline{D}$. Moreover, the ellipsoid

$$\chi_\infty = \left\{ \tilde{X} \in R^n :\ X^T(t) P \tilde{X}(t) < \frac{b}{a} K^2 . \Delta^2 \right\} \quad (157)$$

is exponentially attractive with the decay rate $a/2$ for all $|M(t)|^2 \leq K^2 . \Delta^2$. ■

6.3.3. Simulation Results and Discussion

To evaluate the effectiveness of the proposed scheme, we conducted simulation study on a general system with the following dynamics.

$$\begin{bmatrix}\dot{X}_1\\ \dot{X}_2\end{bmatrix}=\begin{bmatrix}-0.5 & 0\\ 6 & -5\end{bmatrix}\begin{bmatrix}X_1\\ X_2\end{bmatrix}+\begin{bmatrix}1\\ 0\end{bmatrix}U \tag{158}$$

$$Y=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}X_1\\ X_2\end{bmatrix} \tag{159}$$

Where, U is the system input as

$$U=3\sin(\frac{\pi}{2}t) \tag{160}$$

To illustrate the impact of the delay in the system, we simulate the system in two cases of no delay and 0.9 sec delay in the measurements in Fig. 35. The outputs of the system with no delay are plotted in solid blue lines; while, the outputs of the system with delay are shown with red dashed lines.

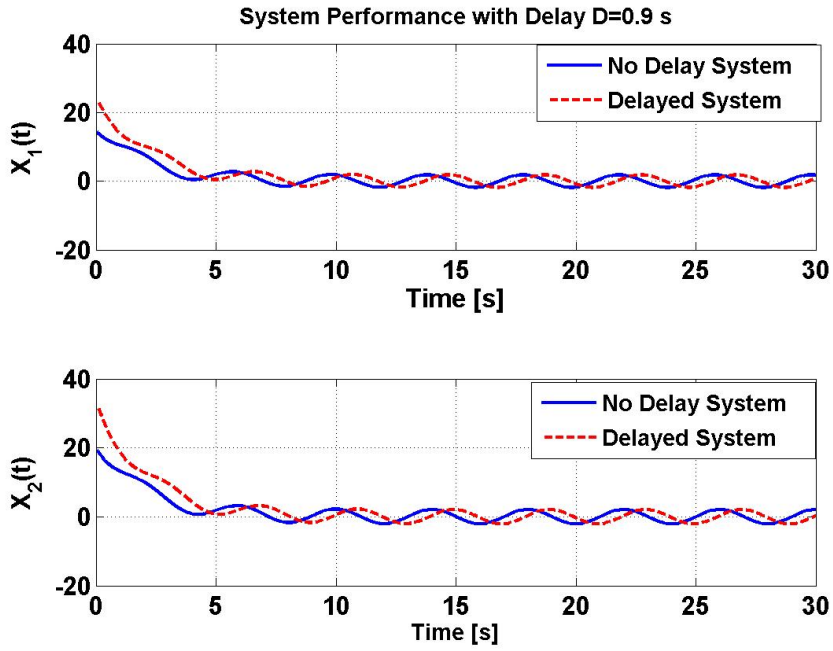

Figure 35. System performance in presence of delay

To estimate the delay and states of the system in the presence of the injected delay, two observers are designed based on the proposed algorithm.

Observer I

A constant delay of $D = 0.9\,sec$ is injected to system output measurements in (159), therefore, available measurements are as follows:

$$Y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} X_1(t-D) \\ X_2(t-D) \end{bmatrix} \tag{161}$$

We model the delay with a transport PDE model where the boundary conditions of the PDE are related to the system dynamics. To design the observer we assume the known boundaries of delay as $D \in \left[\underline{D}, \overline{D}\right] = [0.1, 1.5]$. The gain L_1 is designed as $L_1 = \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix}$, therefore, referring to (20) the error dynamics is

$$\begin{bmatrix} \dot{\tilde{X}}_1 \\ \dot{\tilde{X}}_2 \end{bmatrix} = \begin{bmatrix} -0.5 & 0 \\ 6 & -5 \end{bmatrix} \begin{bmatrix} \tilde{X}_1 \\ \tilde{X}_2 \end{bmatrix} - \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix} \begin{bmatrix} \tilde{u}_1(0,t) \\ \tilde{u}_2(0,t) \end{bmatrix} \tag{162}$$

Choosing L_1 large enough to satisfy (134), and initial guess of $\widehat{D} = 0.5\,s$ for the delay, the observer estimates on delay and outputs $C\hat{X}\left(t - \widehat{D}\right) = \hat{z}(0,t)$ are provided in Fig. 4 and Fig. 5 respectively. To verify the convergence of Observer I, initial condition for states are $\hat{z}_1(0,0) = 13,\ \hat{z}_2(0,0) = 16.5$. Furthermore, we will quantify the convergence performance of the estimates in terms of convergence time defined as the time taken to reach within ±2% band of the true value starting from the incorrect initial condition. The delay estimation in Fig. 36 and delay estimation error in Fig. 37 prove that the estimated value of delay converges to the exact value of 0.9 after 15 s.

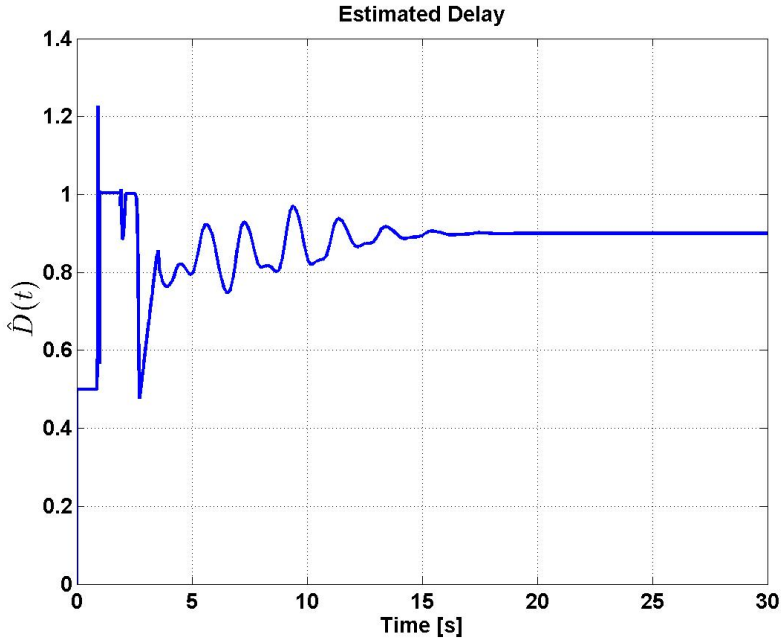

Figure 36. Estimated delay.

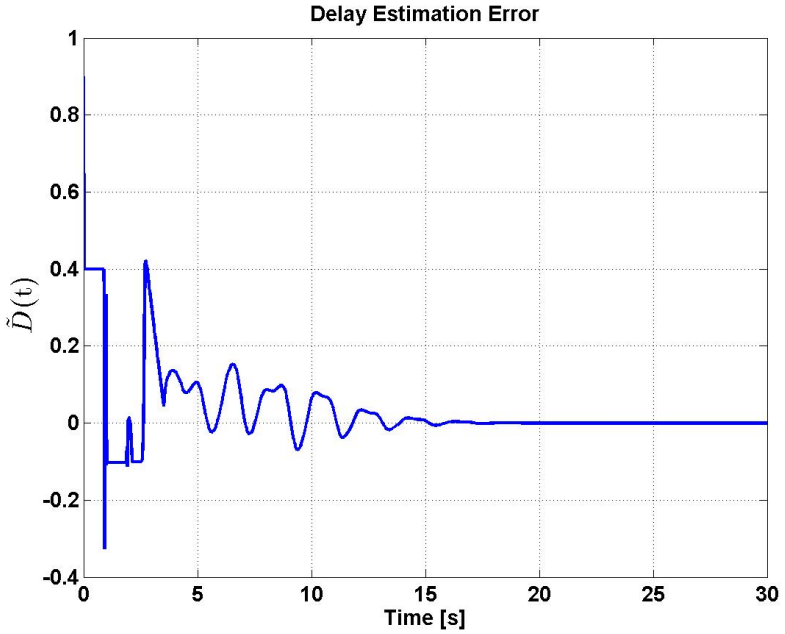

Figure 37. Delay estimation error

Observe I also estimates the available outputs of the system, $\hat{z}(0,t) = C\hat{X}(t-\hat{D})$.

Fig. 38, shows the estimates of the outputs considering the on-line estimated value of delay.

The actual outputs of the system which is can be measured in the controller are drawn with solid blue lines and the estimated values are shown with red dashed lines.

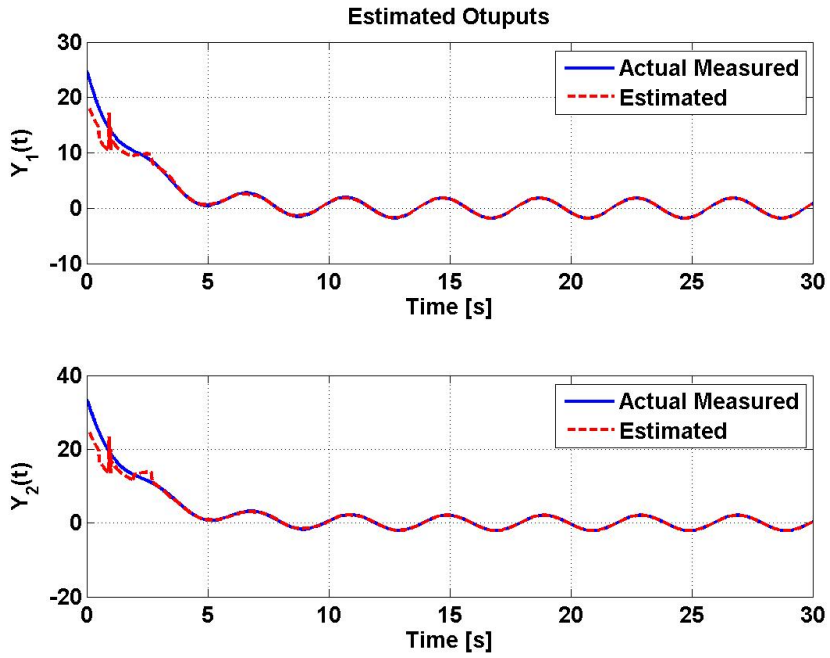

Figure 38. Measured and estimated output.

Fig. 39 shows the estimation error, $\tilde{z}(0,t) = [\tilde{z}_1(0,t) \quad \tilde{z}_2(0,t)]^T$, for our case study. The estimation error converges to a small bounded area of ±2% band of the true value after 5 seconds. Along with output estimation from Observer I, Fig.40 depicts the original $z(x,t) = [z_1(x,t) \quad z_2(x,t)]^T$ and estimated signals $\hat{z}(x,t) = [\hat{z}_1(x,t) \quad \hat{z}_2(x,t)]^T$.

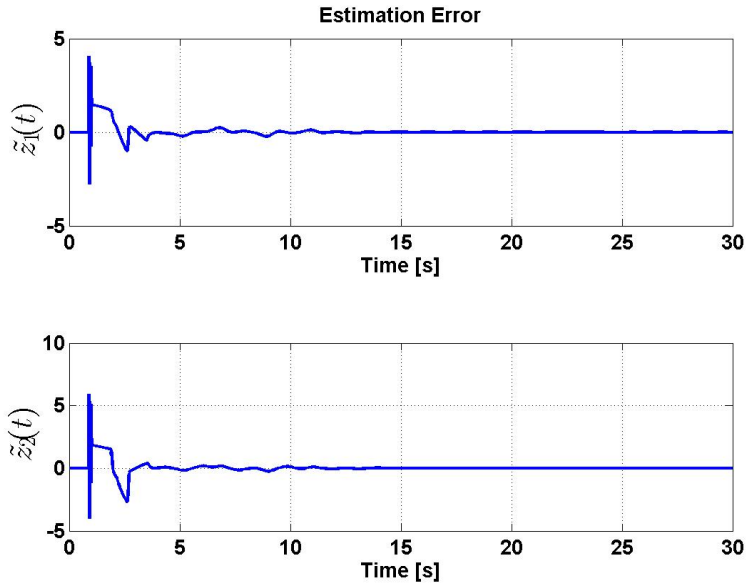

Figure 39. Estimation error

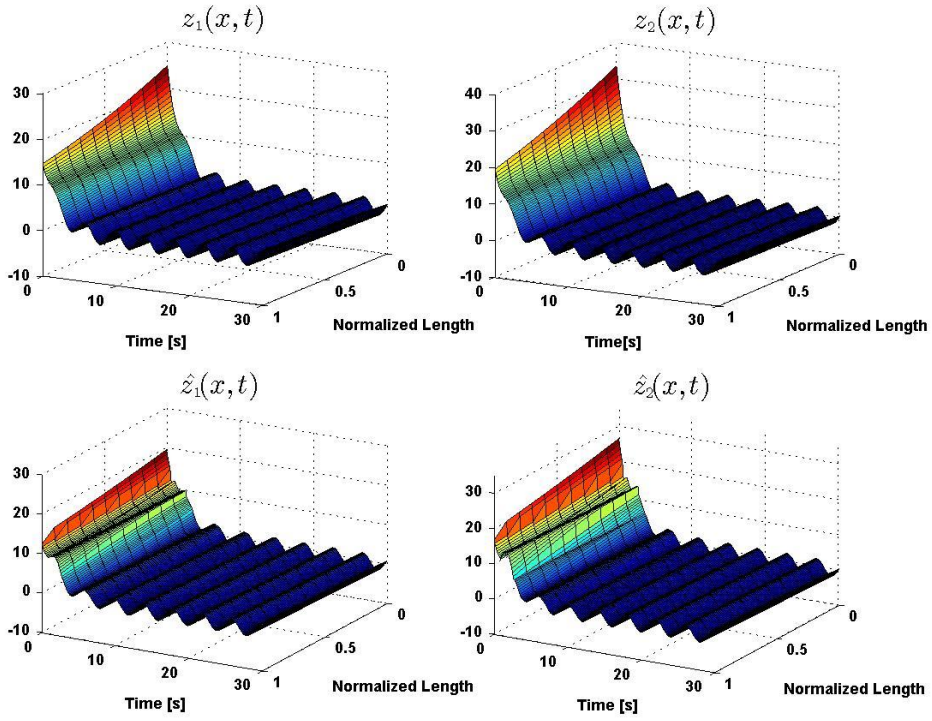

Figure 40. Original and estimated values of $z(x,t) = [z_1(x,t) \quad z_2(x,t)]^T$

Observer II

Considering the estimated delay, obtained from Observer I, the predicted states of the system are derived via the second observer. To design the second observer, the parameters $a > 0, b > 0$ are chosen as:

$$a = 1\,, b = 2$$

These values are selected such that the LMI in (153) is satisfied and matrix Φ is negative definite. Solving the LMI the following positive definite matrixes are obtained.

$$L_2 = \begin{bmatrix} 0.2 & 0.15 \\ 0.25 & 0.2 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 25.25 & -19.66 \\ -19.66 & 15.30 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 25.98 & -19.75 \\ -19.75 & 15.25 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 3.78 & 4.80 \\ 4.80 & 6.2525 \end{bmatrix}$$

$$S = \begin{bmatrix} 42.5256 & -32.811 \\ -32.811 & 25.3183 \end{bmatrix}$$

$$R = \begin{bmatrix} 4.0867 & 5 \\ 5 & 6.3 \end{bmatrix}$$

$$E = \begin{bmatrix} 21.45 & -16.55 \\ -16.55 & 12.77 \end{bmatrix}$$

Therefore, the states of the system at time t can be predicted as it is shown in Fig. 41. Both states are initialized with incorrect values to test the convergence properties of the observer. The solid blue lines are the real states of the system before being transmitted through the network communication and the red dashed lines represent the predicted states

via the proposed algorithm. As it can be demonstrated from the results, after 10 seconds, the predicted values converge to actual values of the states with a bounded error. The estimation error for both states are given in Fig. 42.

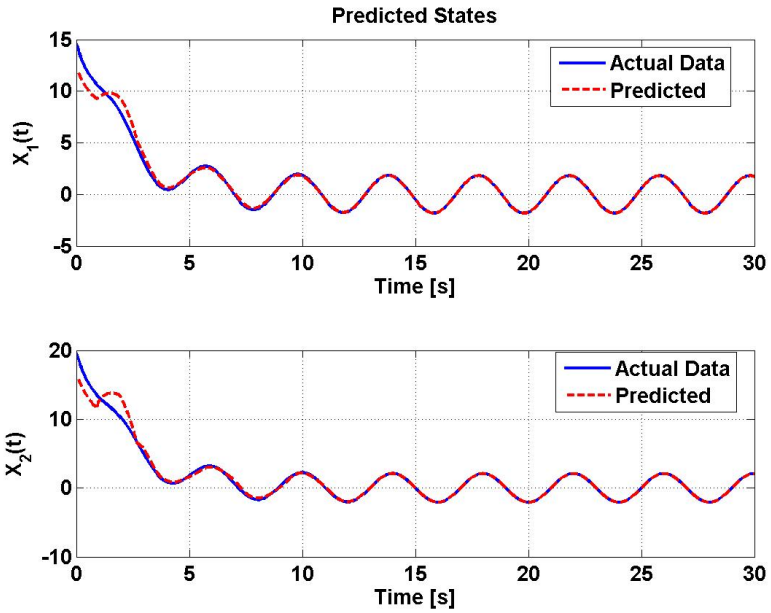

Figure 41. Predicted states of the system at time t.

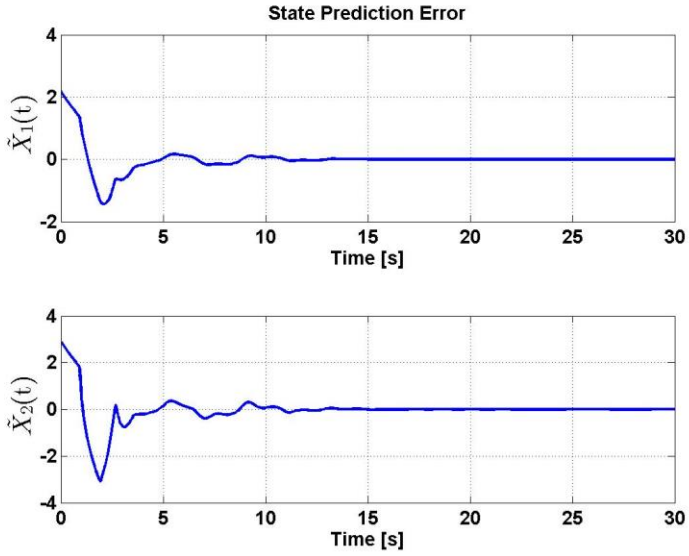

Figure 42. Prediction errors of Observer II

CHAPTER SEVEN

RESILIENT STRATEGY TOWARD FALSE DATA INJECTION ATTACK

The contribution and novelty of this chapter is three fold. First, we develop a continuous model of connected vehicles equipped with CACC algorithm using the PDE approximation inspired by the extensive literature on traffic dynamics [7], [13]; The PDE model simplifies the analysis regarding to system behavior and attack detection. Furthermore, stability analysis regarding to delay and perturbation proportion is further easy for PDE modeling comparing to ODE model of connected vehicles. The results of this chapter are obtained by analyzing the PDE; they are then validated by simulation of a dynamic equations of a platoon of 15 vehicles.

Second, we model an intelligent false data injection attack in the DSRC with fake vehicle identities. The fake (ghost) vehicles in the platoon disrupt the smooth vehicle density by corrupting desire the inter-vehicle distances. The ghost vehicles following the same dynamics of CACC strategy. Hence, the false data injected attack studied in this chpater, is not possible to detect with current attack detection methods developed based on sensor faults detection methodologies.

Third, we propose a novel diagnosis scheme using active control concept to detect false data injection attack in the vehicle platooning system. The proposed diagnosis algorithm consist of a series of PDE observers to provide information of the location of the injected ghost vehicles in the platoon. The most significant advantage of using a PDE based analysis is that the PDE reveals perturbations, better than the discrete equations do. The proposed scheme is capable of (1) detecting the occurrence of false data injection;

and (2) determining the position of fake data injected into the platoon as fake (ghost) vehicles. It is worth mentioning that we don't apply the centralized controller to connected vehicle. Indeed, each individual vehicle has its own decentralized CACC strategy with works as its ODE version. However, we develop just one centralized observer into the leader vehicle to identify the false data injection attack.

7.1. PDE Modeling of the Platoon (Combine with attack)

The notation in this section is a little different from the rest of the thesis. Therefore, we redefine parameters of the platoon as follows.

Consider a homogeneous platoon of connected vehicles equipped with CACC strategy. The vehicles follow their leader in a single lane (see Fig.43). Each vehicle in the platoon is equipped with on-board sensors to measure the relative distance and velocity with respect to its preceding. In addition, each vehicle receives the acceleration information of the preceding vehicle through Dedicated Short Range Communication (DSRC) network [30].

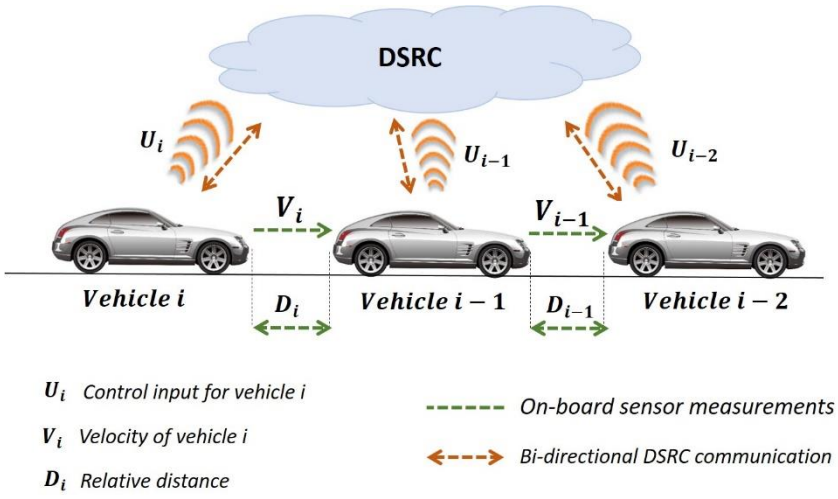

Figure 43 : A platoon of CACC.

Remark 16: In this study, the leader vehicle follows a constant velocity profile with a perturbation for diagnosis purposes. Hence, the velocity profiles of the vehicles in the platoon are not constant.

Dynamics of vehicle i in the platoon is given by [105]:

$$\begin{bmatrix} \dot{D}_i \\ \dot{V}_i \end{bmatrix} = \begin{bmatrix} V_{i-1} - V_i \\ U_i \end{bmatrix}, i \in S_m \setminus \{1\} \tag{163}$$

Where $S_m = \{i \in N | 1 \leq i \leq m\}$ is the set of all vehicles in the platoon of length of m, $D_i = q_{i-1} - q_i + L_i + d_s$ is the distance between vehicle i and $i-1$, q_i and q_{i-1} are the rear bumper position of vehicles i and $i-1$. The length of vehicle i is presented by L_i, d_s is the minimum safety distance between two vehicles, V_i denotes the velocity of vehicle i. Moreover, U_i is the desired acceleration and acts as the vehicle control input [30].

The control strategy regarding to the inter-vehicle spacing obtains as follows

$$D_{r,i}(t) = hV_i(t), i \in S_m \setminus \{1\} \tag{164}$$

where $D_{r,i}(t)$ is the desire relative distance between vehicles i and $i-1$ and h is the time headway. Without losing the generality, to simplify the analysis, we consider $d_s = 0$ and $L_i = 0$. The main objective of platooning is to regulate the D_i to $D_{r,i}$, i.e.

$$E_i(t) = D_i(t) - D_{r,i}(t) \to 0 \quad \text{as} \quad t \to \infty \tag{165}$$

Substituting (164) and $D_i = q_{i-1} - q_i$ in (165), the error is re-written as:

$$E_i(t) = q_{i-1}(t) - q_i(t) - hV_i(t) \tag{166}$$

The vehicle control input of each vehicle in the platoon (U_i) except the leader one depends on the preceding vehicle control input (U_{i-1}). Hence, this architecture employ a decentralized control scheme. Next, we consider the following dynamic controller to achieve the zero regulation error:

$$\dot{U}_i = -\frac{1}{h}U_i + \frac{1}{h}(K_P E_i + K_D \dot{E}_i) + \frac{1}{h}U_{i-1} \tag{167}$$

where U_{i-1} and V_{i-1} are the desired acceleration and velocity of the preceding vehicle received through DSRC network. The parameters K_P, K_D>0 are controller gains designed such that (i) the inter-vehicle distance is maintained to $D_{r,i}$ and, (ii) U_i changes smoothly and remains bounded.

Remark 17: Referring to (167), the control signal of vehicle i (U_i) which is obtained from CACC algorithm, depends on (1) states of vehicle i (D_i, V_i, and U_i), and (2) the transmitted information from the preceding vehicle (U_{i-1}).

Next, we make the following assumptions:

Assumption 16: We consider a homogeneous platoon of vehicles. Therefore, all vehicles in the platoon are identical and have the same parameters e.g. mass, inertia, rolling resistance coefficient.

Assumption 17: Each vehicle in the platoon measures relative distance with respect to preceding vehicle D_i.

Remark 18: Vehicle i measures the relative velocity via radar and hence can compute the absolute velocity V_{i-1} of vehicle $i-1$. Vehicle i also receives acceleration U_{i-1}

information of vehicle $i-1$ via DSRC network. Both these measurements are subjected to measurement noises and uncertainties.

The leader vehicle in the platoon follows a fixed constant velocity trajectory. Hence, the desired velocity and relative distance between vehicles are V_d and $D_{s,r} = hV_d = \Delta$ respectively. By imposing constant velocity trajectories, the position of each vehicle in the platoon is obtained as $q_1(t) = V_d t$ and $q_m(t) = V_d t - (m-1)\delta$. Therefore, each vehicle trys to regulate its relative distance from its preceding vehicle to Δ using CACC strategy.

Next, we develop a new coordinate as "Normalized Coordinate" to facilitate the analysis [103],

$$y_i = \frac{q_i(t) - V_d t + L}{L}$$
$$v_i = \frac{V_i(t) - V_d}{L}$$
$$u_i = \frac{U_i - U_d}{L} = \frac{U_i}{L}$$

where $L = m \times \Delta$ denotes the platoon length. Fig. 44(b) presents the schematic of the platoon in the new coordinates. In the normal coordinate we get, $y_i(t) \in [0,1], y_1(t) \equiv 1$, and $y_m(t) \equiv 0$, where $y_1(t)$ and $y_m(t)$ refer to leader's and last vehicle's positions respectively. Here, we have implicitly assumed that the deviations of the vehicle positions and velocities from their desired values are small.

The dynamics of the vehicle i in the normalized coordinate are given by

$$\ddot{y}_i = u_i \tag{168}$$

$$\dot{y}_i = v_i \tag{169}$$

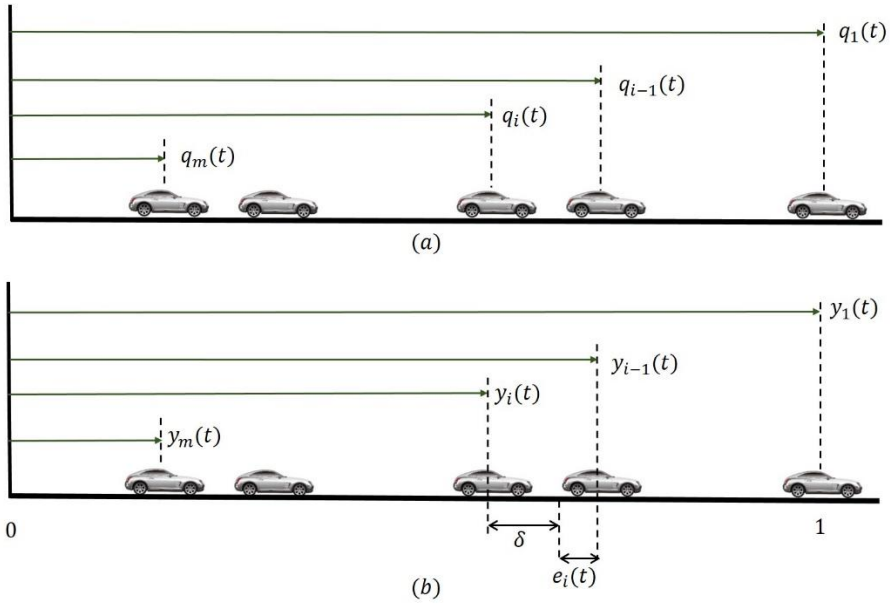

Figure 44: Platoon with vehicles moving in a single lane (a) A platoon with leader and follower vehicles. (b) Same platoon in y coordinates.

where $u_i = \frac{U_i}{L}$. The desired spacing and velocities are

$$\delta = \frac{\Delta}{L}, \quad v_d = \frac{V_d - V_d}{L} = 0, \quad u_d = 0 \tag{170}$$

and the desired position of the vehicle i is

$$y_{d,i}(t) \equiv 1 - \delta \times i \tag{171}$$

The position and velocity errors for the *ith* vehicle in the normalized coordinate are given by

$$\overline{y}_i(t) = y_i(t) - y_{d,i}(t) \tag{172}$$

$$\overline{v}_i(t) = v_i(t) - v_d = v_i(t) \tag{173}$$

$$\overline{u}_i(t) = u_i(t) - u_d = u_i(t) \tag{174}$$

Also, regarding to (167), it is useful to introduce the front relative position errors for the *ith* vehicle:

$$e_i(t) = \frac{E_i(t)}{L} = \frac{q_{i-1}(t) - q_i(t) - \Delta}{L} = y_{i-1} - y_i - \delta \tag{175}$$

$$\dot{e}_i(t) = \frac{\dot{E}_i(t)}{L} = \frac{V_{i-1} - V_i}{L} = v_{i-1} - v_i \tag{176}$$

For $= 1, \ldots, m$. The quantities $e_i(t)$ and $\dot{e}_i(t)$ denote the relative position and relative velocity errors between the *ith* and its predecessor $i - 1$ vehicle.

Therefore, (167) in the normal coordinate will be as

$$\dot{u}_i = \frac{1}{h}(u_{i-1} - u_i) + \frac{k_p}{h} e_i + \frac{k_d}{h} \dot{e}_i \tag{177}$$

The relative errors, including the velocity error, are computed by on-board devices such as GPS, radars, and speed sensors. Consistent with the decentralized linear control architecture, the dynamics of control signal u_i of the vehicle i is assumed to depend on 1) its acceleration u_i, 2) its preceding acceleration, u_{i-1} which is received through DSRC network, 3) relative velocity, 2) the relative position errors between itself and its preceding vehicle.

PDE Model of Platoon

In this section, we develop a continuous PDE approximation of the discrete platoon dynamics modelled in section II. Note that the discrete platoon dynamics refers to the model of platoon explained with ODE set of equations (168)-(177). This model is discrete with respect to space and is continuous with respect to time. The PDE is derived with respect to

a scaled spatial coordinate explained in section II with lower case states $y_i(t), v_i(t),$ and $u_i(t)$. Hence, to make the spatially discrete ODE based model to a continuous model, we define a new position parameter $x \in [0,1]$. In effect, the two symbols x and y correspond to the same coordinate representation but, are used here to distinguish the continuous and discrete formulations [103].

The first step to develop the PDE model is to define the continuous approximation. Referring to normalized coordinate, every car is nominally assumed to lie within an interval of length Δ (see Fig. 44(b)). For the purpose of a continuous approximation, we expand each vehicle over its interval to have a constant mean density (vehicles per unit length) as (178) for m vehicles in the platoon.

$$\rho_0 = \frac{1}{\delta} = m \tag{178}$$

Furthermore, we assume the following approximation for the velocity in each vehicle's interval

$$v(x,t) = \begin{cases} v_i(t) & \text{for } x = y_i \\ y_i \dfrac{v_i - v_{i-1}}{y_i - y_{i-1}} \times (x - y_{i-1}) + v_{i-1} & \text{for } x \in [y_{i-1}, y_i) \end{cases} \tag{179}$$

This approximation grantees that velocity profile in the PDE approximation changes smoothly in the length of platoon (x).

Next, we define the density of the platoon, $\rho(x,t)$, represents the quantity regarding to vehicles per unit of length. Local density of, $\rho(x,t)$, at spatial coordinate $x \in [0,1]$ and

time $t \in [0, \infty)$ relates to the velocity $v(x,t)$ using the continuity equation of the macroscopic continuous models of the traffic flow as follows [107]-[108]

$$\frac{\partial \rho}{\partial t} + \frac{\partial (\rho v)}{\partial x} = 0 \tag{180}$$

As it can be interpreted from (180), the perturbation in the density causes by the dynamics of the individual vehicles in the platoon. Local density $\rho(x,t)$ increases (decreases) as the cars move closer (apart). In order to analyze small perturbations about the mean values (equilibrium point of the system), we define the perturbed quantities $\bar{\rho}$, $\bar{v}$ as

$$\rho(x,t) = \rho_0 + \bar{\rho}(x,t), v(x,t) = v_0 + \bar{v}(x,t), \tag{181}$$

Therefore, for small perturbations around mean values we can linearized (181) to

$$\frac{\partial \rho_0}{\partial t} + \frac{\partial \bar{\rho}}{\partial t} = \frac{\partial}{\partial t}\left(\rho_0 v_0 + \bar{\rho} v_0 + \rho_0 \bar{v} + \bar{\rho}\bar{v}\right) \tag{182}$$

recalling (169), we have the mean velocity equals to zero, $v_0 = v_d = 0$ and we know ρ_0 is constant. Thus, we can re-write (182) as

$$\frac{\partial \bar{\rho}}{\partial t} + \rho_0 \frac{\partial \bar{v}}{\partial x} = 0 \rightarrow \frac{\partial \bar{\rho}}{\partial t} = -\rho_0 \frac{\partial \bar{v}}{\partial x} \tag{183}$$

This equation is consistent with the physical intuition whereby a positive gradient in velocity (due to say the predecessor speeding up or the follower slowing down) will cause the local density to decrease. In order to study density perturbations, one thus needs to specify the velocity which arises due to the linearized momentum balance:

$$\frac{\partial \bar{v}(x,t)}{\partial t} = \bar{u}(x,t) = u(x,t) \tag{184}$$

where $u(x,t)$ is the control signal developed by CACC strategy and equals to acceleration of the vehicle. To develop the continuous approximation of the acceleration, $u(x,t)$, we consider two terms of (172) and approximate each term separately in the rest of this section. First term in (172) as

$$\frac{\bar{u}_{i-1}-\bar{u}_i}{\delta}=\frac{u_{i-1}-u_i}{\delta}=\left[\frac{\partial}{\partial x}u(x,t)\right]_{x=y_i} \tag{185}$$

second term is

$$e_i(t)=y_{i-1}(t)-y_i(t)-\delta=(1-\frac{\delta}{y_{i-1}-y_i})(y_{i-1}-y_i) \tag{186}$$

$$e_i(t)\approx\int_{y_i}^{y_{i-1}}(1-\frac{\rho(x)}{\rho_0})dx \tag{187}$$

$$e_i(t)\approx-\frac{1}{\rho_0}\int_{y_i}^{y_{i-1}}\bar{\rho}(x,t)dx=-\frac{1}{\rho_0}\bar{\rho}(x^+,t)\delta \tag{188}$$

by the Mean Value Theorem [103]-[104], where $x^+\in[y_i,y_{i-1}]$. Therefore, we can approximate (188) with

$$e_i(x,t)=-\frac{1}{\rho_0}\bar{\rho}(x^+,t)\delta \tag{189}$$

Thus, referring to (177), we will construct a PDE approximation of discrete dynamics in terms of these continuous approximations as

$$\left[\dot{u}(x,t)\right]_{x=y_i}=\left[\frac{1}{h\rho_0}(\frac{\partial}{\partial x}u(x,t))\right]_{x=y_i}-\left[\frac{k_p}{h\rho_0}\bar{\rho}(x,t)\delta\right]_{x=y_i}-\left[\frac{k_d}{h\rho_0}\dot{\bar{\rho}}(x,t)\delta\right]_{x=y_i} \tag{190}$$

where, k_p and k_d are used to denote continuous approximations of discrete gains K_P and K_D respectively. Then, we arrive at the partial differential equation (PDE) as a model of the discrete platoon dynamics by

$$\frac{\partial}{\partial t}u(x,t)=\frac{1}{h\rho_0}(\frac{\partial}{\partial x}u(x,t))-\frac{k_p}{h\rho_0}\bar{\rho}(x,t)\delta-\frac{k_d}{h\rho_0}\dot{\bar{\rho}}(x,t)\delta \tag{191}$$

applying (182) into the last term of (191), we get

$$\frac{\partial}{\partial t}u(x,t)=\frac{1}{h\rho_0}(\frac{\partial}{\partial x}u(x,t))-\frac{k_p}{h\rho_0}\bar{\rho}(x,t)\delta+\frac{k_d}{h}\frac{\partial}{\partial x}v(x,t)\delta \tag{192}$$

using the following notation

$$\begin{aligned}
&v_t(x,t)=\frac{\partial v(x,t)}{\partial t},v_x(x,t)=\frac{\partial v(x,t)}{\partial x}\\
&\bar{\rho}_t(x,t)=\frac{\partial\bar{\rho}(x,t)}{\partial t},\bar{\rho}_x(x,t)=\frac{\partial\bar{\rho}(x,t)}{\partial x}\\
&u_t(x,t)=\frac{\partial u(x,t)}{\partial t},u_x(x,t)=\frac{\partial u(x,t)}{\partial x}
\end{aligned} \tag{193}$$

The state space representation for PDE model of a platoon of vehicles equipped with CACC strategy is given as

$$v_t\left(x,t\right)=u\left(x,t\right) \tag{194}$$

$$\bar{\rho}_t(x,t)=-\rho_0 v_x(x,t) \tag{195}$$

$$u_t(x,t)=\frac{1}{h\rho_0}u_x(x,t)-\frac{k_p}{h\rho_0^2}\bar{\rho}(x,t)+\frac{k_d}{h\rho_0}v_x(x,t) \tag{196}$$

In this section, we assume that the attacker has knowledge about dynamics of vehicles into the platoon. Therefore, to implement a non-trivial attack, the attacker designs the fake vehicle dynamics similar the dynamics other real vehicles in the platoon. Indeed, this fake

vehicle does not provide wrong sensor/actuator information and can not be detected with aforementioned methodologies. Injecting fake vehicles into the platoon, directly impacts the density perturbation in the string. Hence, we can express the effect of fake vehicles as false data injection attack by

$$\bar{\rho}_a(x,t) = \bar{\rho}(x,t) + \Delta\rho(x_a, t_a) \tag{197}$$

where, $\Delta\rho(x_a, t_a)$ presents the effect of fake vehicles injection at position $x = x_a$ and time $t = t_a$ in the platoon. In this attack scenario, apart from detecting the attack occurrence, isolating the injection point of the attack is crucial and requires more analysis. Furthermore, the injection point of the attack determines which vehicles in the platoon are the fake (ghost) vehicles. In this chapter, to detect the exact position of the false data injection attack, we take advantages of (i) cascading nature of the platoon which makes delay in responding to any perturbation in the driving profile. (ii) PDE modeling of the whole platoon to develop a centralize health monitoring option for platoon.

Therefore, as an overview for the proposed scheme in this chapter to detect the false data injection attack, the following guideline is provided:

Remark 19: False data injection attack as fake vehicles does not occur in the leader and last vehicle of the platoon. Hence, the first and last vehicles in the platoon are real vehicles.

7.2. Diagnostics Approach

In this section, we develop a novel diagnosis scheme based on PDE model of the platoon to detect and isolate the false data injection attack. The isolation of false data injection attack in a platoon of connected vehicles equals to identifying the position of the fake

(ghost) vehicle in the string. The proposed diagnosis algorithm works based on the following guideline:

Step-1: Model the attack as injected fake vehicles in the platoon changing the density parameter in the platoon PDE model;

Step-2: Design PDE-based observer to estimate the states of the system in no attack scenario;

Step-3: Derive two residuals using the estimates and measured values of velocity and acceleration of the vehicles in the platoon;

Step-4: Analyse residuals behavior in both no attack and under attack scenario to develop unique signature for each case;

We design the state estimation scheme to estimate all states of the PDE model consisting of $\bar{\rho}(x,t), v(x,t), u(x,t)$ using available information. The observer is designed and implemented in the leader vehicle to monitor whole platoon performance using just one observer. We assume information regarding to velocity and acceleration of all vehicles in the platoon is available in the leader vehicle.

Assumption 18: All vehicles in the platoon share their acceleration and velocity information through the DSRC network with the leader vehicle since the DSRC is a broad casting shared network.

Remark 20: Available information through the DSRC network are subjected to network uncertainties and measurement noise.

Estimation Scheme

Considering *assumption 18*, in the observer design we have access $v(x,t)$ and $u(x,t)$ for whole platoon for $\forall\ t > 0$. The following structure is chosen for the PDE observer which is implemented into the leader vehicle.

$$\hat{v}_t(x,t) = \hat{u}(x,t) + L_{11}(\tilde{v}(x,t)) + L_{12}(\tilde{u}(x,t)) \tag{198}$$

$$\hat{\bar{\rho}}_t(x,t) = -\rho_0 \hat{v}_x(x,t) + L_2(\tilde{u}(x,t)) \tag{199}$$

$$\hat{u}_t(x,t) = \frac{1}{h\rho_0}\hat{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\hat{\bar{\rho}}(x,t) + \frac{k_d}{h\rho_0}\hat{v}_x(x,t) + L_3(\tilde{u}(x,t)) \tag{200}$$

with the following boundary conditions derived from leader vehicle

$$\hat{v}(1,t) = v(1,t), \qquad \hat{u}(1,t) = u(1,t) \tag{201}$$

where, $\hat{v}(x,t)$, $\hat{\bar{\rho}}(x,t)$,, and $\hat{u}(x,t)$ are estimates of $v(x,t)$, $\bar{\rho}(x,t)$, and $u(x,t)$ respectively. L_{11}, L_{12} L_2 and L_3 are observer gains to be determined.

Remark 21: Considering each vehicle in the platoon as a point. We have point measurement based on ODE model of the platoon. However, we used PDE approximation in section II to develop a continuous mode. Similar approximations and assumptions are applied for the observer design.

Furthermore, estimation error parameters including $\tilde{v}(x,t)$, $\tilde{\bar{\rho}}(x,t)$ and $\tilde{u}(x,t)$ are defined as

$$\begin{aligned}
&\tilde{v}(x,t) = v(x,t) - \hat{v}(x,t),\\
&\tilde{\bar{\rho}}(x,t) = \bar{\rho}(x,t) - \hat{\bar{\rho}}(x,t),\\
&\tilde{u}(x,t) = u(x,t) - \hat{u}(x,t)
\end{aligned} \tag{202}$$

Subtracting (194)-(196) from (198)-(200),the error dynamics of the observer are given by

$$\tilde{v}_t(x,t) = \tilde{u}(x,t) - L_{11}(\tilde{v}(x,t)) - L_{12}(\tilde{u}(x,t)) \tag{203}$$

$$\tilde{\tilde{\rho}}_t(x,t) = -\rho_0 \tilde{v}_x(x,t) - L_2(\tilde{u}(x,t)) \tag{204}$$

$$\tilde{u}_t(x,t) = \frac{1}{h\rho_0}\tilde{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\tilde{\tilde{\rho}}(x,t) + \frac{k_d}{h\rho_0}\tilde{v}_x(x,t) - L_3(\tilde{u}(x,t)) \tag{205}$$

with boundary condition of

$$\tilde{v}(1,t) = 0, \tilde{u}(1,t) = 0 \tag{206}$$

Theorem 1: Consider system modeled by (194)-(196) and the observer designed as (198)-(200). There exist observer gains L_{11}, L_{12} L_2 and L_3 such that the error dynamics (203)-(205), converges to bounded area in finite time, in the presence of no faults and cyber-attacks.

Proof: we provide the proof for this theorem in two stages using Lyapunov analysis method. First, we start with analysing (203) by choosing (207) as the Lyapunov function candidate [96].

$$V_1(t) = \| \tilde{v}(x,t) \|^2 = \int_0^1 \tilde{v}^2(x,t)dx \tag{207}$$

As it can be inferred from (207), for $\forall\, x > 0$ and $\forall\, t > 0$, $V_1(t) > 0$ when $\tilde{v}(x,t) \neq 0$. Taking the time derivative of $V_1(t)$ along the state trajectories, we get

$$\dot{V}_1(t) = \int_0^1 \tilde{v}(x,t)\tilde{v}_t(x,t)dx \tag{208}$$

$$\dot{V}_1(t) = \int_0^1 \tilde{v}(x,t)\big(\tilde{u}(x,t) - L_{11}\tilde{v}(x,t) - L_{12}\tilde{u}(x,t)\big)dx \tag{209}$$

choosing $L_{12} = 1$ and $L_{11} > 0$, (209) converts to

$$\dot{V}_1(t) = \int_0^1 -\tilde{v}^2(x,t)dx = -L_{11}V_1(t) \tag{210}$$

Considering any positive initial value of $V_1(t=0) = V_1(0) > 0$ we can write

$$V_1(t) = V_1(0)e^{-L_{11}t} \tag{211}$$

Hence, $V_1(t) \to 0$ as $t \to \infty$ asymptotically with the weight of L_{11}. Consequently, $\tilde{v}(x,t) \to 0$ as $t \to \infty$. Next, we analyze the error dynamics (204)-(205) using the following Lyapunov function candidate

$$V_2(t) = \frac{1}{2}\int_0^1 \tilde{\bar{\rho}}^2(x,t)dx + \frac{b_1}{2}\int_0^1 \tilde{u}^2(x,t)dx \tag{212}$$

where $b_1 > 0$. Differentiating the Lyapunov function candidate along the solution of (203)-(205) we obtain

$$\dot{V}_2(t) = \int_0^1 \tilde{\bar{\rho}}(x,t)\bar{\rho}_t(x,t)dx + b_1\int_0^1 \tilde{u}(x,t)\tilde{u}_t(x,t)dx \tag{213}$$

Substituting $\tilde{\bar{\rho}}_t(x,t)$ and $\tilde{u}_t(x,t)$ by (204) and (205) respectively, we have

$$\begin{aligned}\dot{V}_2(t) = &\int_0^1 \tilde{\bar{\rho}}(x,t)\Big(-\rho_0\tilde{v}_x(x,t) - L_2(\tilde{u}(x,t))\Big)dx + \\ &b_1\int_0^1 \tilde{u}(x,t)\Big(\frac{1}{h\rho_0}\tilde{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\tilde{\bar{\rho}}(x,t) + \frac{k_d}{h\rho_0}\tilde{v}_x(x,t) - L_3(\tilde{u}(x,t))\Big)dx\end{aligned} \tag{214}$$

For simplicity, we drop (x,t) term from the functions

$$\begin{aligned}\dot{V}_2(t) = &\int_0^1 -\rho_0\tilde{\bar{\rho}}\tilde{v}_x dx - \int_0^1 \tilde{\bar{\rho}}\tilde{u}\Big(L_2 + b_1\frac{k_p}{h\rho_0^2}\Big)dx \\ &+b_1\frac{k_d}{h\rho_0}\int_0^1 \tilde{u}\tilde{v}_x dx + \frac{b_1}{h\rho_0}\int_0^1 \tilde{u}\tilde{u}_x dx - b_1L_3\int_0^1 \tilde{u}^2 dx\end{aligned} \tag{215}$$

Choosing L_{11} large enough which assures a fast convergence of $\tilde{v}(x,t) \to 0$, we can conclude that $v(x,t) \to \hat{v}(x,t)$ and $v_x(x,t) \to \hat{v}_x(x,t)$. Hence, we can neglect terms related to v_x in (215) and simplify it to

$$\dot{V}_2(t) = -\int_0^1 \tilde{\rho}\tilde{u}\left(L_2 + b_1 \frac{k_p}{\rho_0^2}\right)dx + \frac{b_1}{h\rho_0}\int_0^1 \tilde{u}\tilde{u}_x dx - b_1 L_3 \int_0^1 \tilde{u}^2 dx \tag{216}$$

Selecting the observer gain, L_2 as

$$L_2 = -\frac{b_1 k_p}{h\rho_0^2} \tag{217}$$

The fisrt term in the right hand side of (216) equals to zero. Therefore, the derivative of V_2 obtains as

$$\dot{V}_2(t) = \frac{b_1}{h\rho_0}\int_0^1 \tilde{u}\tilde{u}_x dx - b_1 L_3 \int_0^1 \tilde{u}^2 dx \tag{218}$$

Now integrating the first term of the right hand side of (218) we have

$$\int_0^1 \tilde{u}\tilde{u}_x dx = \frac{1}{2}\tilde{u}(x,t)^2\Big]_0^1 = \frac{1}{2}\left(|\tilde{u}(1,t)|^2 - |\tilde{u}(0,t)|^2\right) = -\frac{1}{2}|\tilde{u}(0,t)|^2 \tag{219}$$

Next, considering (219) and applying the definition of norm on the second term of right hand side of (218), we get

$$\dot{V}_2(t) = -\frac{b_1}{2h\rho_0}|\tilde{u}(0,t)|^2 - b_1 L_3 \int_0^1 \tilde{u}^2 dx \tag{220}$$

$$\dot{V}_2(t) = -\frac{b_1}{2h\rho_0}|\tilde{u}(0,t)|^2 - b_1 L_3 \| \tilde{u}(t) \|^2 \leq 0 \tag{221}$$

Choosing $L_3 > 0$ and $b_1 > 0$, $\dot{V}_2(t) \leq 0 \quad \forall t \geq 0$ which describe the decaying behavior of $V_2(t)$. Hence, if we restrict the initial conditions so that $V_2(t=0) = V_2(0)$ is bounded,

the Lyapunov function $V_2(t) \leq V_2(0)$ remains bounded for all $t \geq 0$. Therefore, we obtain the uniformly boundedness of $\|\tilde{u}\|^2$and $\|\tilde{\rho}\|^2$ are bounded [98]. Further, to prove the regulation of the $\dot{V}_2(t)$ which equals to $V_2(t) \to 0$ as $t \to \infty$ we define function $M(t)$ as

$$M(t) = -b_1 L_3 \int_0^1 \tilde{u}^2 dx \tag{222}$$

Therefore, from (220) and (222) we can conclude

$$\dot{V}_2(t) \leq M(t) \tag{223}$$

Differentiating (222) with respect to time, we get

$$\ddot{V}_2(t) \leq \dot{M}(t) = -b_1 L_3 \int_0^1 \tilde{u}\tilde{u}_t dx \tag{224}$$

Substituting $\tilde{u}_t$ from (215), and using fact that $\tilde{v}(x,t) \to 0$ and $\tilde{v}_x(x,t) \to 0$, (222) , we get

$$\dot{M}(t) = -\frac{b_1 L_3}{h\rho_0} \int_0^1 \tilde{u}\tilde{u}_x dx + \frac{b_1 L_3 K_p}{h\rho_0^2} \int_0^1 \tilde{u}\tilde{\rho} dx + b_1 L_3^2 \int_0^1 \tilde{u}^2 dx \tag{225}$$

$$\dot{M}(t) \leq \frac{b_1 L_3}{h\rho_0} |\tilde{u}(0,t)|^2 + \frac{b_1 L_3 K_p}{h\rho_0^2} (\left(\| \tilde{u} \| + \| \tilde{\rho} \|\right) + b_1 L_3 \| \tilde{u} \| \tag{226}$$

Since we have measurement on $u(0,t)$ we can select $\hat{u}(0,t)$ close to actual value with error of measurement noise. Therefore, $|\tilde{u}(0,t)|$ is bounded. Also, we know $\|\tilde{u}\|^2$and $\|\tilde{\rho}\|^2$ are uniformly bounded. Therefore, referring to (226) we can conclude $\dot{M}(t)$ is bounded and equivalently proves the boundedness of $\ddot{V}_2(t)$ as

$$\ddot{V}_2(t) \leq \dot{M}(t) < \infty \tag{227}$$

Furthermore, the boundedness of $\ddot{V}_2(t)$ concludes that $\dot{V}_2(t)$ is uniformly continuous. Hence, applying Barbalat lemma [92]on $\dot{V}_2(t)$ along with the fact that $V_2(t)$ is bounded,

we obtain $\dot{V}_2(t) \to 0$ as $t \to \infty$. At this point, we proved the stability of the estimation error dynamics which converges to zero as $t \to \infty$.

7.3. Attack Diagnostics

The main idea behind attack diagnosis in this chapter is using the perturbation in velocity profile to poke the inherent effects of the attack which makes the detection easier. Indeed, the ghost vehicles develop disturbances (changes) in the local density of the platoon. The leader vehicle perform a small perturbation on the constant velocity profile to detect the attack and isolate the injected point of the attack in the platoon. Next, we explain in detail how the attack is diagnosed using the PDE model and the aforementioned idea.

Applying the selected observer gains into the estimation error dynamics explained in(203)-(205), we get

$$\tilde{v}_t(x,t) = -L_{11}(\tilde{v}(x,t)) \tag{228}$$

$$\tilde{\tilde{\rho}}_t(x,t) = -\rho_0 \tilde{v}_x(x,t) + \frac{b_1 k_p}{h\rho_0^2}(\tilde{u}(x,t)) \tag{229}$$

$$\tilde{u}_t(x,t) = \frac{1}{h\rho_0}\tilde{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\tilde{\tilde{\rho}}(x,t) + \frac{k_d}{h\rho_0}\tilde{v}_x(x,t) - L_3(\tilde{u}(x,t)) \tag{230}$$

with boundary condition of

$$\tilde{v}(1,t) = 0, \tilde{u}(1,t) = 0 \tag{231}$$

Since, velocity and acceleration of vehicles in the platoon are the two available measurements of the PDE system, we define two following residuals for attack detection strategy

$$r_1(x,t) = \tilde{v}(x,t) = v(x,t) - \hat{v}(x,t)$$
$$r_2(x,t) = \tilde{u}(x,t) = u(x,t) - \hat{u}(x,t) \quad (232)$$

We have analysed the stability of estimation errors dynamics in section V. Under no false data injection attack, we proved that the estimation error dynamics converge to zero as $t \to \infty$. Equivalently, with no attack in the platoon, both residuals $r_1(x,t)$ and $r_2(x,t)$ converge to zero. This signature of two residuals is considered as no attack signature.

Next, we analyse the behavior of the residuals in the occurrence of false data injection attack. In case the attack formulated in (197), $\tilde{v}(x,t)$ will converge to zero with same Lypupanov analyse. However, dynamics of the acceleration perturbation in (230) changes to

$$\tilde{u}_t(x,t) = \frac{1}{h\rho_0}\tilde{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\tilde{\tilde{\rho}}(x,t) + \frac{k_d}{h\rho_0}\tilde{v}_x(x,t) - L_3(\tilde{u}(x,t)) - \frac{k_p}{h\rho_0^2}\Delta\rho(x_a,t_a) \quad (233)$$

So, the derivation of Lyupanov function$V_2(t)$ will have additional term in (221) as the effect of $\Delta\rho(x_a,t_a)$ in acceleration perturbation dynamics

$$\dot{V}_2(t) = -\frac{b_1}{2h\rho_0}|\tilde{u}(0,t)|^2 - b_1 L_3 \|\tilde{u}(t)\|^2 + \|\Delta u(x_a,t_a)\| \quad (234)$$

Therefore, under false data injection attack scenario, the second Lyapunov function $V_2(t)$ for analysing convergence of $\tilde{u}(x,t)$ and $\tilde{\tilde{\rho}}(x,t)$ will converge to a bounded region. Equivalently, $\tilde{u}(x,t)$ and consequently, residual $r_2(x,t)$ converges to a bounded area.

Finally, we can conclude that, in the presence of the false data injection attack, first residual, $r_1(x,t)$, will not change; while, the second residual, $r_2(x,t)$, will converge to a bounded non-zero value. This signature of the residuals is considered as false data injection attack signature.

One of the possible ways to deal with attack detection using residual values is to use nonzero threshold set based on no attack behavior of the system. Hence, in the next step, we select constant threshold values for the obtained residuals in no-attack situation using the probability distribution method. In this method, first we need to collect residual data, $r_i(x,t), \quad i \in \{1,2\}$ under no attack scenario of platoon operation. Next, using the probability distribution characteristics such as mean and standard deviation, we set a constant threshold for each residual. The constant thresholds $\gamma_i, \quad i \in \{1,2\}$ as selected such that the probability of false alarms calculated with are acceptable. where, γ_i is the selected constant threshold on residual r_i.

$$P_{FAi} = \int_{-\infty}^{-\gamma_i} p_0(x)dx + \int_{\gamma_i}^{\infty} p_0(x)dx, \tag{235}$$

where, P_{FAi} i is the probability of attack false alarm in , γ_i is the selected threshold for false data injection attack and $p_0(x)$ is the $r_i(x,t)$ probability distribution under no attack in the platoon. The goal here is to select $\gamma_i$which will yield an acceptable P_{FAi}.

Finally, we can conclude the residual analysis in both no-attack and under attack scenarios with the following remark.

Remark 22: The residuals signature is evaluated to determine if false data injection attack occurs into the connected vehicle platoon. In case of no attack in the system, the signature of residuals is $|r_1(x,t)| < \gamma_1$, and $|r_2(x,t)| < \gamma_2$; when the residual signature shows $|r_1(x,t)| < \gamma_1$ and $|r_2(x,t)| > \gamma_2$ it determines a false data injection attack is detected in the system.

7.4. Results and Discussion

In this section, we evaluate the effectiveness of the proposed algorithm using the simulation studies. We consider a platoon of fifteen ($m = 15$) identical vehicles equipped with CACC strategy. Most of the simulation parameter of the platoon are taken similar to existing literature [30],[64]. The controller gains are constant for all vehicles, i.e., $k_p(x) = K_P = 0.7$ and $k_d(x) = K_D = 2.5$ and the headway is selected as $h = 0.2\ s$. The desired inter-vehicle distance is considered as $\Delta = hV_d$ and desired velocity is $V_d = 20\ m/s$. The initial velocity of all vehicles was chosen as the desired velocity and the initial position of the vehicle was determined as $q_i(t) = V_d t + (i-1)\Delta$. As a result, the initial relative position error and velocity error of every vehicle was zero except for the first vehicle. The first vehicle has a velocity perturbation of $v(1,t) = v_0(t) = 0.24sin(t)$ which cause an acceleration perturbation as $u(1,t) = u_0(t) = 0.24cos(t)$ with respect to the desired velocity $V_d = 20\ m/s$ and desired acceleration $U_d = 0\ m/s^2$.

Since the controller gains K_P and K_D are constant, the controller gains in the continuous PDE model are the same. Based upon the Lyapunov analysis discussed in section V, the observers gain are selected as $L_{11} = 700, L_{12} = 1, L_2 = -\frac{2k_p}{h\rho_0^2}$ and $L_3 = 50$. As it is mentioned in assumption 18, the leader vehicle receives information of velocity and acceleration of each vehicle in the platoon. To analysis a realistic scenario, we consider zero mean Gaussian noises as measurement noise for all available velocity and acceleration measurements. Velocity measurement noises have standard deviation of $\sigma_v = 2c\ m/s$ and acceleration measurement noises have standard deviation of $\sigma_u = 3c\ m/s^2$ [109]. To test the convergence properties, observers in the proposed scheme are initialized with incorrect values except for the leader vehicle. Since, the PDE observers are designed and implemented in the leader vehicle, the observers have access to the exact measured data of velocity and acceleration of the leader vehicle as it is formulated in (201).

Next we illustrate the effectiveness of the proposed approach under the following cases. **Case 1**: The scenario that the platoon operates in normal condition with no false data injection attack; and **Case 2**: the case study in which false data injection attack occurred into the system by injecting fake vehicles using fake identity. For each case, the simulation is run for 70 seconds and the obtained results are further discussed in more details.

Case 1: No Fault Scenario

In this case we consider an ideal communication network in the platoon with no false data injection attack. The velocity perturbation in the whole platoon is demonstrated in Fig. 44. Referring to PDE formulation (194)-(196), the leader vehicle is placed at $x = 1$ while the last vehicle in the platoon is represented at $x = 0$. Fig.45 depicts the minimum velocity

perturbation in the leader vehicle at $x = 1$. However, as it is expected, the perturbation is propagated through the length of platoon as we have the largest perturbation in the last vehicle on the string. The velocity perturbation in the leader vehicle is $v(1,t) = 0.24\,sin(t)$ with maximum amplitude of $0.24\,m/s$. This value is almost tripled in last vehicle in the platoon with maximum of $0.64\,m/s$.

An overshoot in the transient behavior of the vehicles in the platoon is noticeable in the velocity perturbation simulation results. Note that, each vehicle in the platoon receives information of the preceding vehicle as inputs. Therefore, the velocity of each vehicle is an output to the receiving information and has transient phase which will propagate through the platoon. The initial overshoot which is more detectable in the last vehicle of the platoon (at $x = 0$) is because of step response to receiving perturbation.

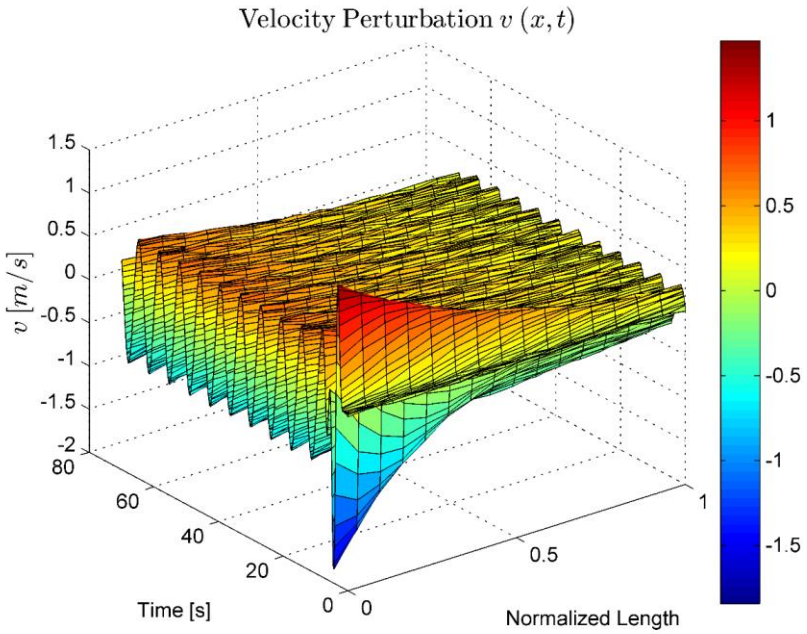

Figure 45: Velocity perturbation in the platoon

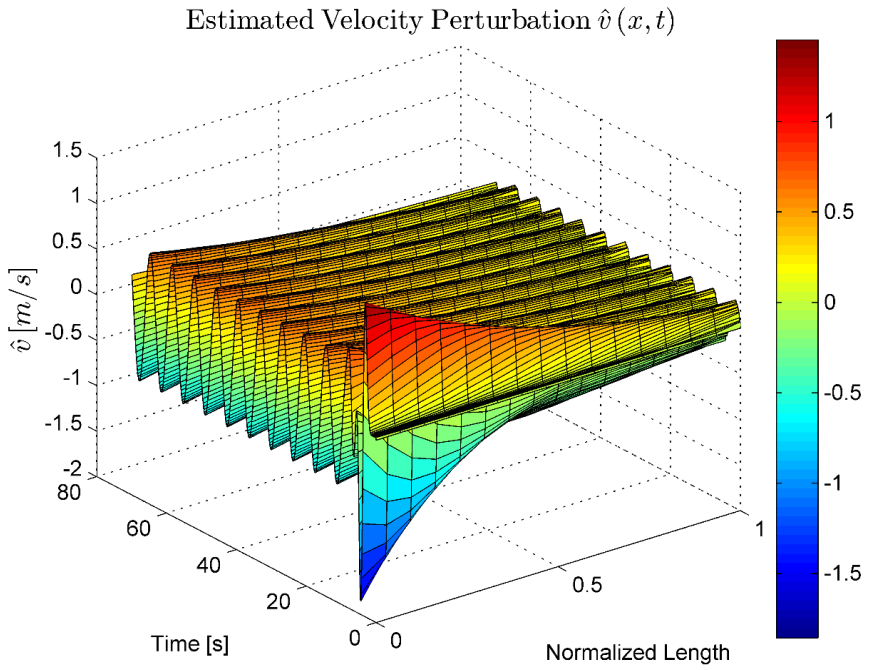

Figure 46: Estimated velocity perturbation in the platoon

Fig. 46 shows the estimate value of velocity perturbation for whole platoon which is obtained with the observers designed in section V. To verify the convergence properties of the proposed scheme, observers are initialized with incorrect values of velocity perturbation, acceleration perturbation and density perturbation. The estimation error of the velocity perturbation is given in Fig. 47. As it can be inferred, the estimate value converges to actual value of velocity perturbation. The estimation error converges to zero asymptotically with the rate of $L_{11} = 700$ with measurement noise.

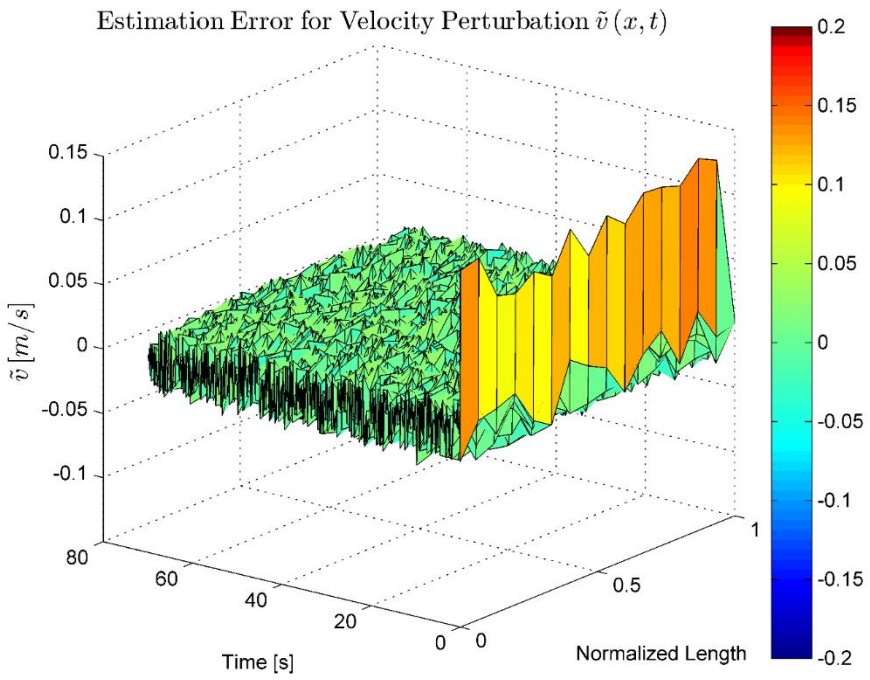

Figure 47: Estimation error for velocity perturbation in the platoon

Fig. 48 represents the actual acceleration perturbation in vehicles in our case study platoon. As it can be demonstrated from this plot, the acceleration perturbation also propagates through the platoon from the leader to the last follower in the string. The acceleration perturbation of the leader vehicle is $u(1,t) = 0.24\,cos(t)$ with maximum amplitude of $0.24\,m/s^2$, while the maximum acceleration perturbation in the vehicle in the platoon reaches to $0.64\,m/s^2$. Similar to the velocity perturbation, the transient response of the acceleration perturbation settles into the steady state within less than 5 seconds.

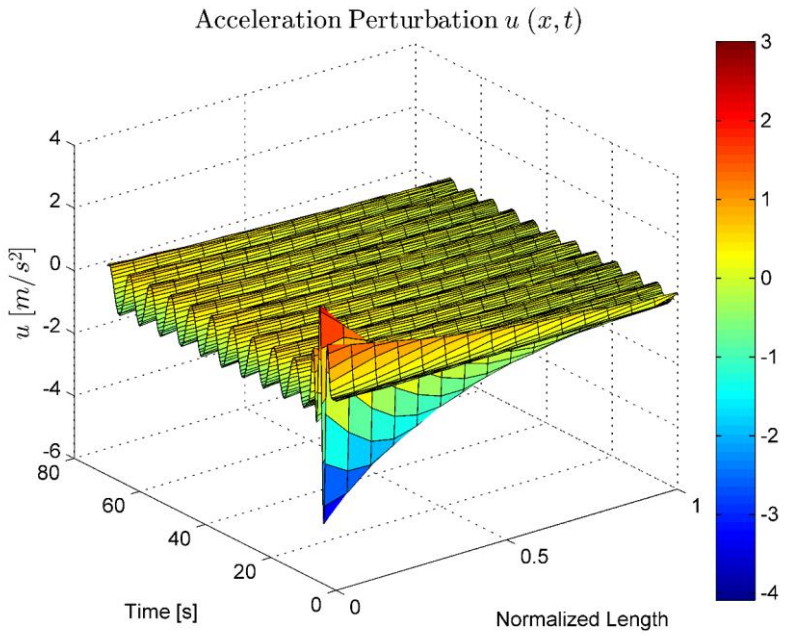

Figure 48: Actual acceleration perturbation in the platoon

The estimate value of acceleration perturbation in the platoon is give by Fig. 49. Except for the leader vehicle, the initial acceleration perturbation values for all vehicles in the platoon is chosen incorrectly to test the convergence properties of observers. Fig. 50 presents the error between actual measured acceleration permutation and the estimate values in the whole platoon. As it is shown in the plot, the estimation error converges to a bounded area in finite time.

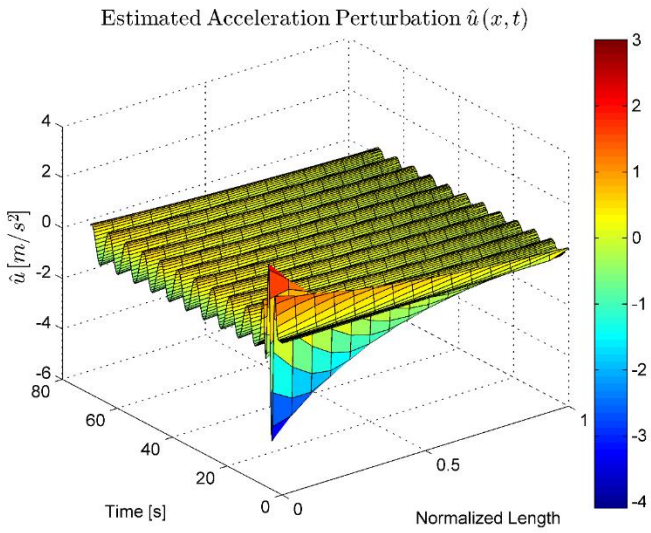

Figure 49: Estimated acceleration perturbation in the platoon

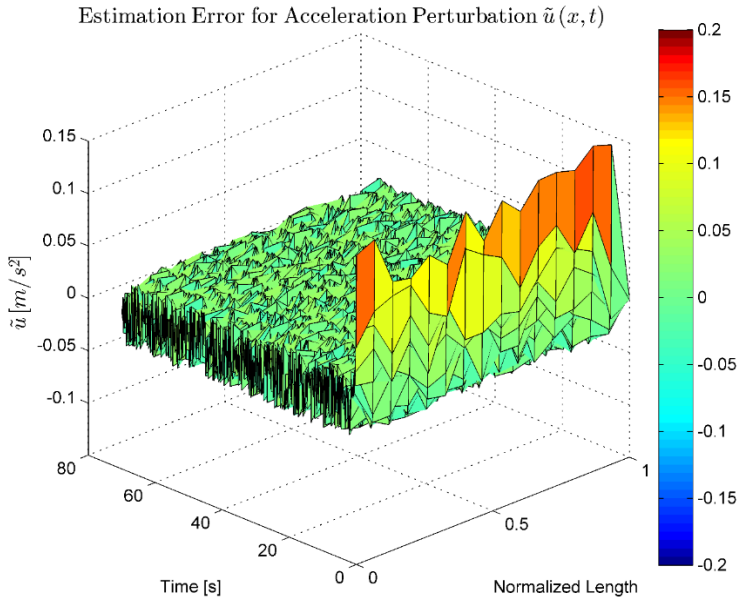

Figure 50: Estimation error for acceleration perturbation in the platoon

Density perturbation in the platoon, $\rho\ (x,t)$ is represented in Fig. 51 as function of position (vehicle in the platoon) and time. The leader vehicle has a density perturbation value of

$\rho\,(1,t) = -3.6\,cos(t)$. As it is expected the perturbation is propagated into the platoon and the last vehicle in the platoon has a maximum density perturbation of 10.3. Since the perturbation is a function of velocity, the initial transient response reaches to steady state in less than 5 seconds.

The estimate value of density perturbation for whole platoon is depicted in Fig. 52 and the estimation error is given by Fig. 53. As it can be inferred from the plot, the estimated density perturbation converges to its actual value in finite time. The error of the estimation remains less than 0.5 which verifies convergence properties proved in Section V using Lyapunov method. The value of $\tilde{\rho}(1,t)$ represents the estimation error of density perturbation in leader vehicle. Since the observer is designed in the leader vehicle, both estimate value and actual value of density perturbation in position of leader vehicle, $x = 1$ are same. Hence, $\tilde{\rho}(1,t) = 0$, however, for the rest of the platoon, due to the existence of measurement noise in velocity and acceleration, and incorrect chosen initial values of $\hat{v}(x,0), \hat{u}(x,0)$, and $\hat{\rho}(x,0)$.

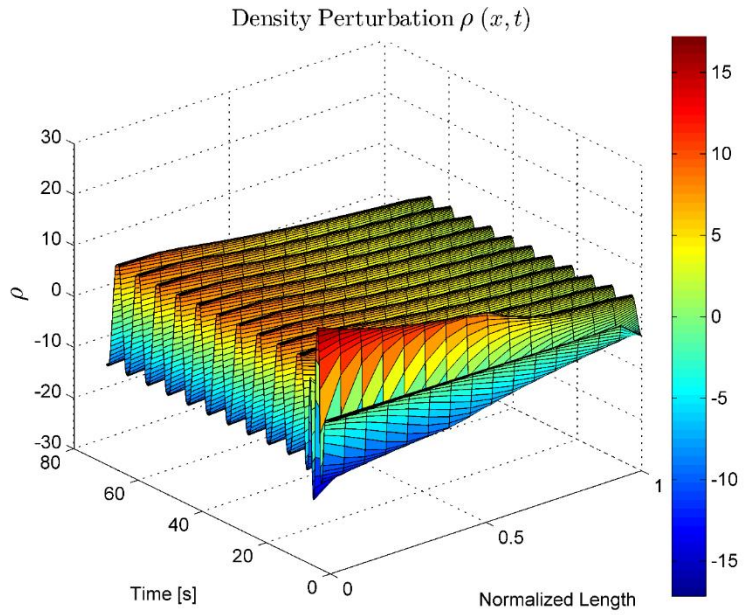

Figure 51: Actual density perturbation in the platoon

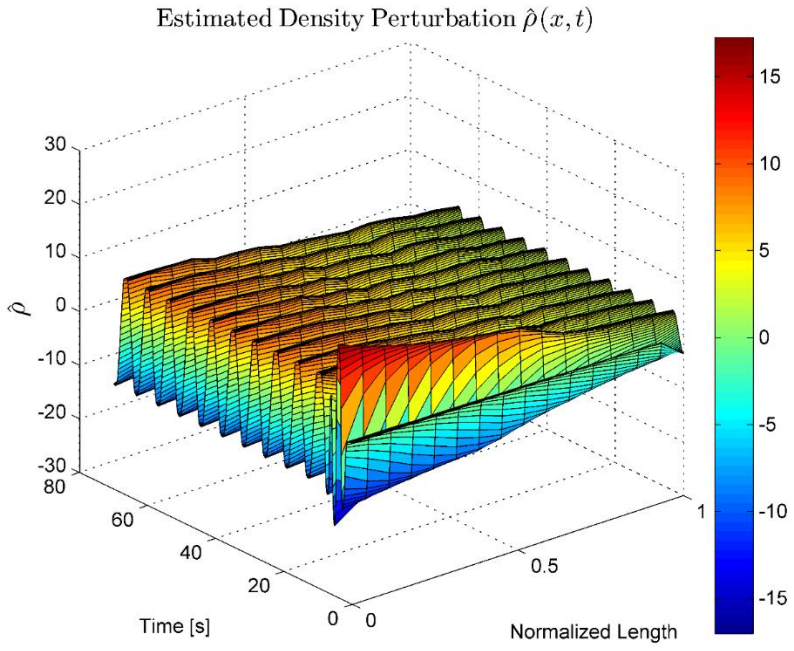

Figure 52: Estimated density perturbation in the platoon

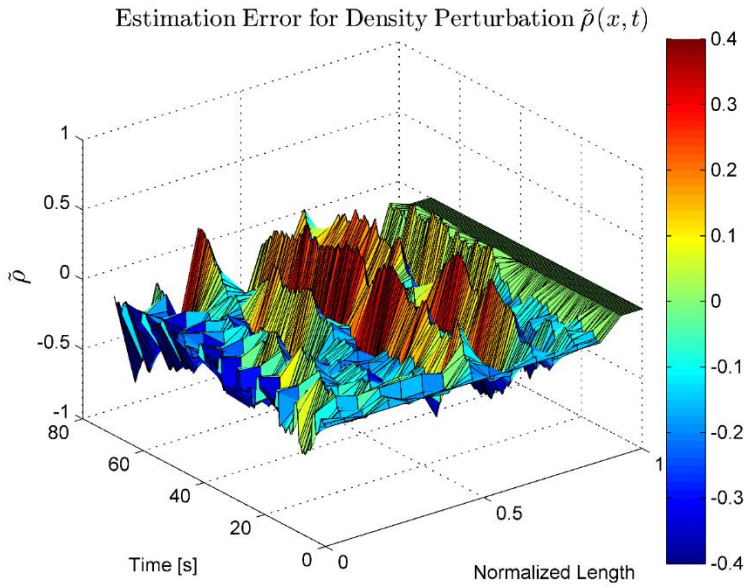

Figure 53: Estimation error for density perturbation in the platoon

Next, we define two constant thresholds for the obtained residuals, $r_1(x,t) = \tilde{v}(x,t)$ and $r_2(x,t) = \tilde{u}(x,t)$using the concept explained in section V. Since only second residual $r_2(x,t)$ is critical to determine the false data injection attack, we mainly focus on this residual. Analysing the obtained data for $\tilde{u}(x,t)$ in this section under no attack , we select $|\gamma_2(x,t)| = 0.03$ to determine the boundary for threshold as shown in Fig. 54. Therefore, if the residual $r_2(x,t)$ exceed the threshold $|\gamma_2(x,t)|$ we interpret the event as false data injection attack occurrence.

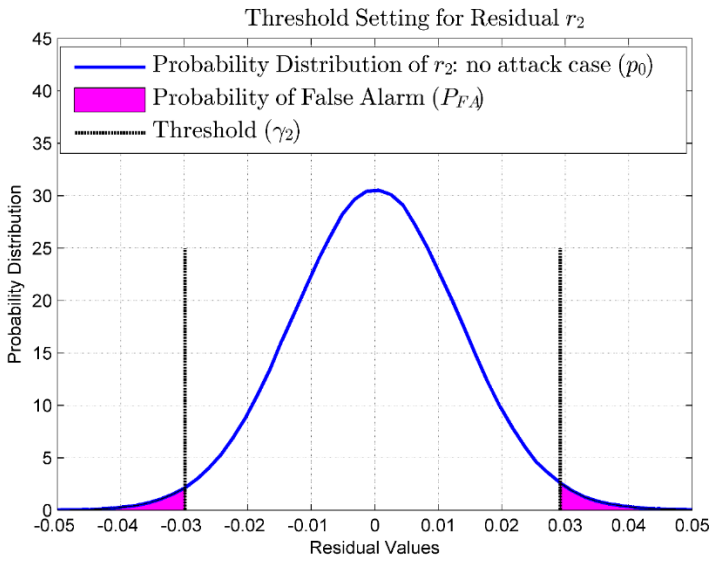

Figure 54: Residual probabilty desnity for thereshold setting

Case 2: Fault Data Injection Scenario

In this scenario, we inject the fake vehicles as false data injection attack into the platoon. We consider two fake vehicles to be injected in the middle of the platoon between vehicle number 7 and 8. These fake vehicles add additional density into the platoon in the injected point. Hence, the estimated density perturbation will not match with the actual density perturbation in the disrupted point in the platoon. The proposed algorithm is capable of detecting the density disruption as well as identifying the position of the attack in the platoon system. Fig. 55 depicts the first residual, $r_1(x,t)$ equivalent to estimation error for velocity perturbation, $\tilde{v}(x,t)$ under false data injection attack scenario. As it is discussed in Subsection B of Section V, we destined the observers such that the first residual does not show the effect of the attack. However, the second residual, $r_2(x,t)$ corresponding to

estimation error for acceleration perturbation has non-zero value when attack occurs into the system. Fig. 56 represent estimation error of acceleration perturbation for the whole platoon. As it can be inferred, the estimation error converges to a has non-zero bounded value at $x = 0.5$ corresponding to 7^{th} vehicle of the platoon representing of attack occurrence. Since the attack remains in the system for whole time of the simulation, the non-zero value of the estimation error remains for all time of the simulation $t \in [0,80]$. To illustrate the attack detection using the pre-defined threshold, Fig. 46 shows the residual $r_2(x,t)$ with the constant threshold, $\gamma_2(x,t) = 0.03$. The pre-defined threshold $\gamma_2(x,t)$ is depicted via pink surfaces at $r_2(x,t) = 0.03$ and $r_2(x,t) = -0.03$. It can be inferred from the Fig.57, in the occurrence of the false data injection attack, the residual $r_2(x,t)$ surpasses the set threshold declaring that the attack is happening in the system.

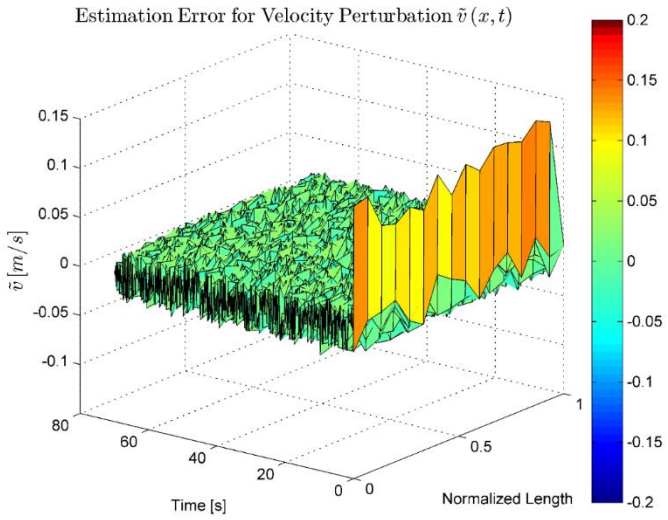

Figure 55: Estimation error for velocity perturbation under false data attack injection

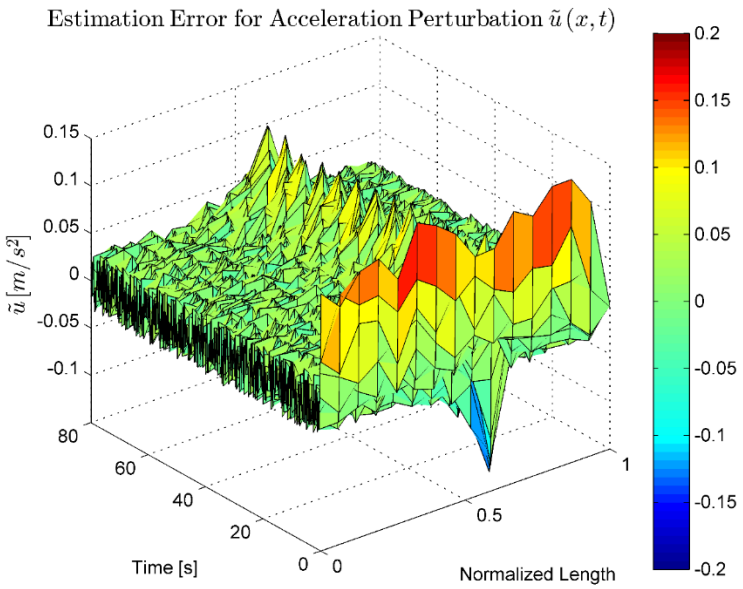

Figure 56: Estimation error for acceleration perturbation under false data attack injection

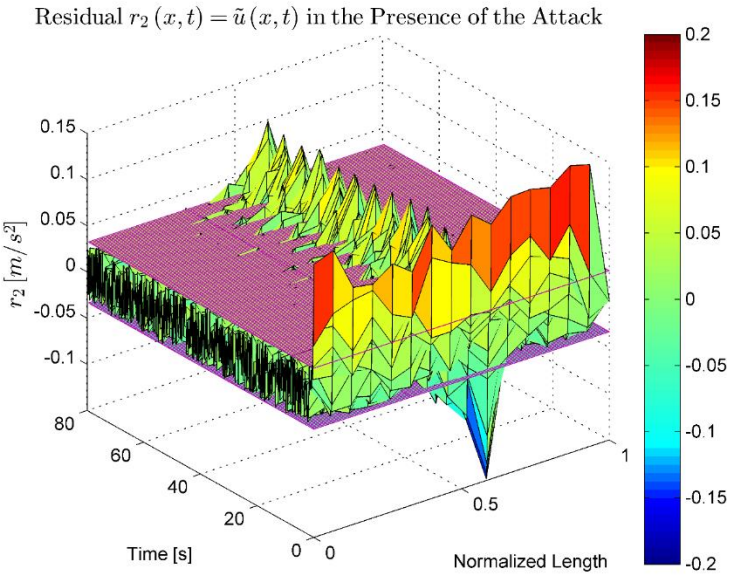

Figure 57: Estimation error for acceleration perturbation as residual $r_2(x,t)$ under false data attack injection

CHAPTER EIGHT

DECISION MAKING

To combine the aformationed strategies in an integrated control strategy, a hybrid format controller is required to determine which types of cyber-attacks is happening in the system and what is the coresponiding strategy to minimize the effect of that specific attack. To achive this objective, we design a descion maker using optimum control algorithm to choose the best control signal among the avialbable choices. We formulate the optimization problem with a MPC problem in which the cost function penalize the agresive driving profile as well as selecting safest relative distance to avoid collision.

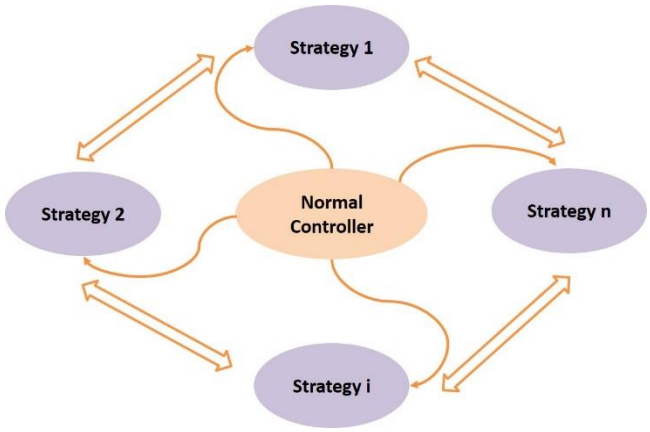

Figure 58: Hybrid system scheme

8.1. Problem Formulation

In this section, we refere to the two strategeis proposed in chapter five and chapter seven for packet dorpping and denial of service attack respectively. We develop a scenario including both packet dropping phenomena and DoS attack to illustrate the effectiveness

of the decision making algorithm in selecting right strategy. Indeed, in each sample time, the decsion making block receives three choices of control signal as

1- Actual Control Signal: This is the actual control singal obtained from the CACC algorithm while actual information received through the DSRC network. The information received through DSRC network is subjected to packet dropping and DoS attack. In fact, the Actual Control signal is the control signal without applying any resilient strategy. We refer to this control signal as u_{actual}
2- Packet Dropout Control Signal: This control singal is the output of the modified CACC while the strategy of the packet dropping phenomena is applied into the system. We refer to this control signal as $u_{Packet\_Applied}$
3- Denial of Service Control Signal: This control singal is the output of the modified CACC while the strategy of the denial of srvice attack is applied into the system. We refer to this control signal as $u_{DoS\_Applied}$

Intuitively, we expect that, the packet dorpping srategy acts better than DoS attack strategy when there is packet dropping phenomena in the communicaiton network. In contrast, we expect that the strategy of the DoS attack has a better perfoamnce comparint to the packet dropping strategy when there is actually a DoS attack in the DSRC network.

We formulate the MPC problem as

$$\min_{u_i \in U} J = \sum_{i=1,\dots,N} \omega_1 {d_i}^2 + \omega_2 {u_i}^2 \quad (236)$$

where, $U = \{u_{actual}, u_{Packet\_Applied}, u_{DoS\_Applied}\}$

8.2. Simulation results

For the simulation scenario, we consider a US06 driving cycle as the velocity profile for the leader vehicle. Similar to the rest of the simulation scenarios in this research we consider a platoon of vehicles equipped with CACC strategy. To illustrate the effectiveness of the proposed algorithm we discuss the performance of *Vehicle 3* in the platoon as an example.

The simulation run for 600 seconds, the first 50 seconds the communication network works ideally with no packet dropping or delay. At t=50 for 250 seconds we inject the DoS attack with an effect of $= 5\ s$. After the DoS attack, we consider the network works ideally again for another 100 seconds. At time t= 400 s, we inject packet dropping failure into the DSRC network with $\lambda = 0.3$ (the probability of losing data) which remains till the end of the simulation time. Fig. 59 shows the relative distance of *Vehicle 3* with respect to its predecessor vehicle (d_3) under different strategies with the explained attack in the communication network. The ideal behavior of the *Vehicle 3* when there is no attack or packet dropping in DSRC is depicted with blue curve as a criteria for comparison. The actual relative distance d_3 is shown with solid black curve. The actual signal represents the actual behavior of the *Vehicle 3* under DoS attack and packet dropping while there is no strategy applied in the controller. As we can see in more visualized plot in Fig. 60, in 5 points of the plot, the relative distance is less than zero representing accident with the preceding car. Next, we apply only the packet dropping strategy on the controller and the result is shown with dashed green curve. Similarly, we only apply the DoS attack strategy and the result of the *Vehicle 3* relative distance is shown via dashed red line. As it can be

inferred from Fig. 59, the packet dropping algorithm help the *Vehicle 3* to behave very close to its ideal performance in part of the simulation when packet dropping occurs in the DSRC network. However, the packet dropping strategy fails to help the *Vehicle 3* when DoS attack is happening the communication network. In contrast, DoS attack strategy acts very well in the time slot that actually DoS attack is injected in the DSRC network while, it is not resilient toward packet dropping phenomena. The acceleration data is also provided in Fig. 61, illustrating similar argument results.

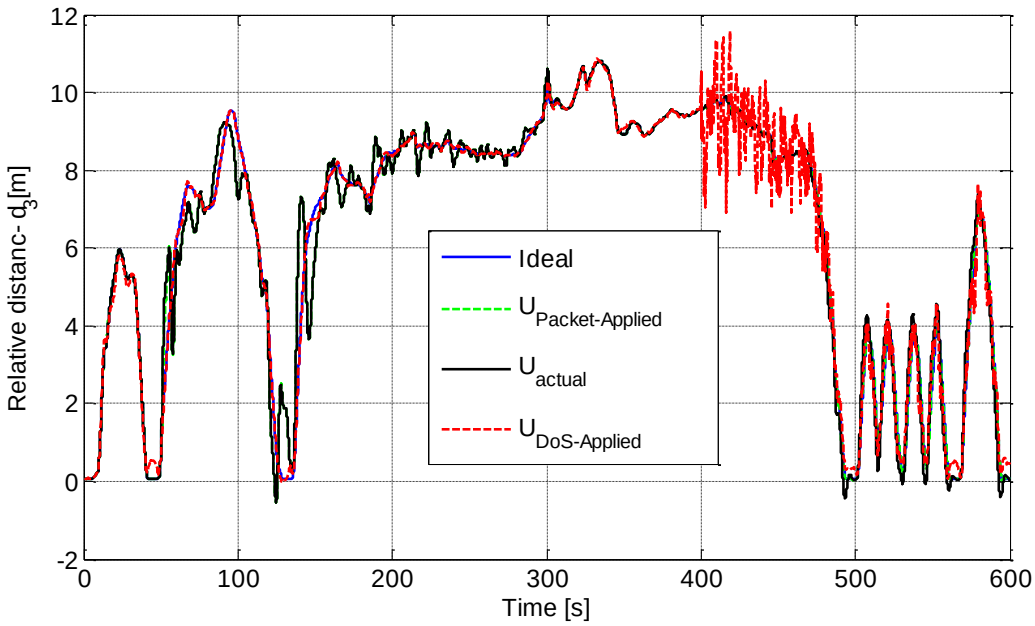

Figure 59: Relative distance of the *Vehicle 3* under ideal DSRC network (blue), DSRC under attack while packet dropping strategy applied (dashed green), DSRC under attack and no strategy applied (black) and DSRC under attack while DoS attack strategy applied (dashed red).

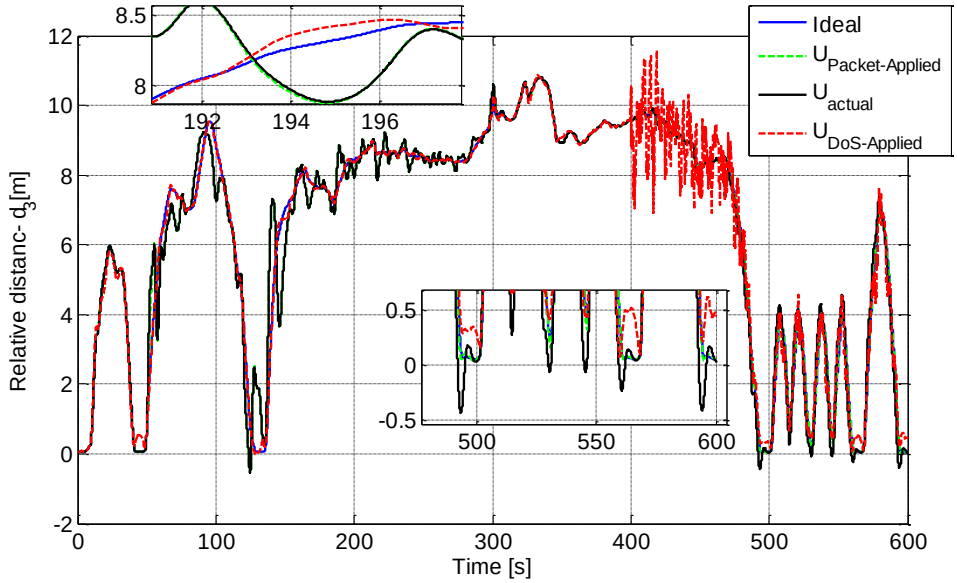

Figure 60: Visulaized relative distance of the *Vehicle 3* under ideal DSRC and under attack.

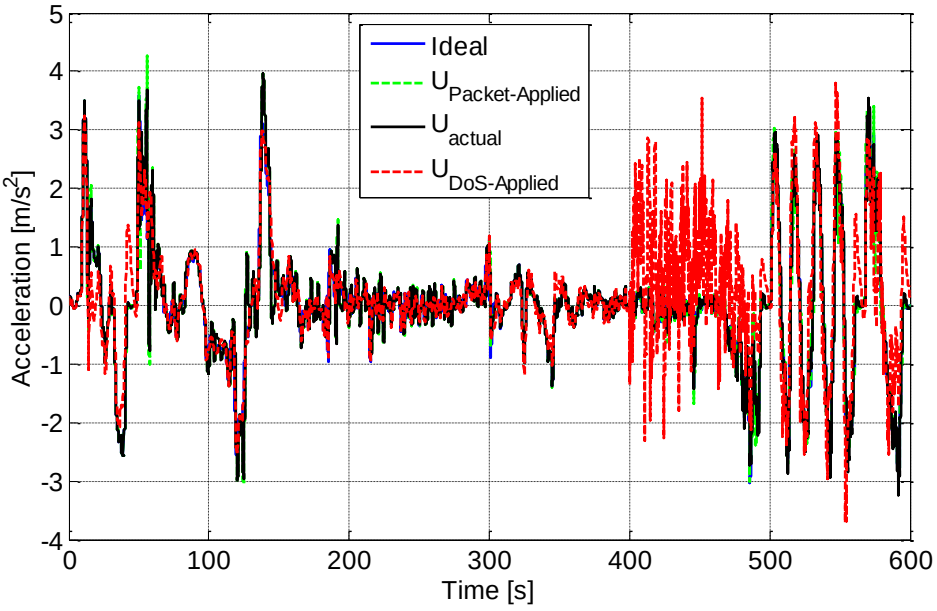

Figure 61: Acceleration the *Vehicle 3* (control signal) under ideal DSRC and under attack while packet dropping strategy applied (dashed green), DSRC under attack and no strategy applied (black) and DSRC under attack while DoS attack strategy applied (dashed red).

The provided results for this scenario, validates the necessity of essential decision making algorithm for choosing write strategy corresponding to the existing attack/network failure in the CPS. To achieve this objective along with maintaining the smooth driving profile, we developed the MPC strategy as (236) which provides the following results

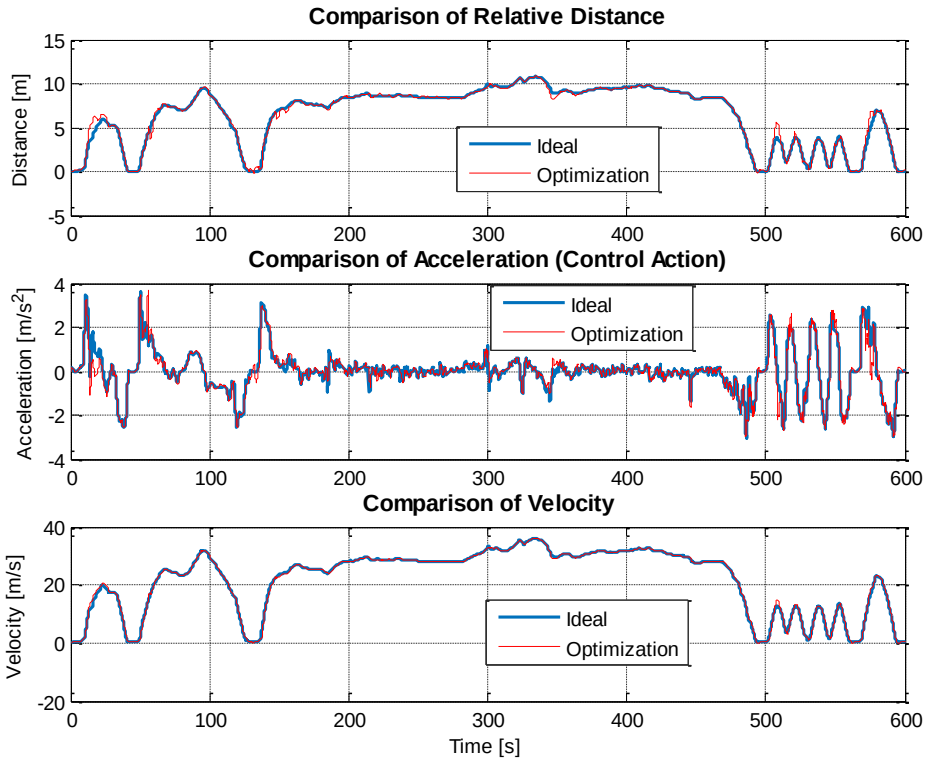

Figure 62: Behavior of the Vehicle 3 under ideal DSRC network (blue), and DSRC under attack scenario with resilient control strategies applied via optimum decision making algorithm (red).

As it can be inferred from Fig. 62, the optimum decision making algorithm chooses suitable decision to have the keep the performance of the platoon close to the normal. Furthermore, the decision guarantees the safe relative distance as well as smooth driving

behavior which is similar to deriving profile when the DSRC has ideal communication. The selected control action in each sample time is shown in Fig. 63.

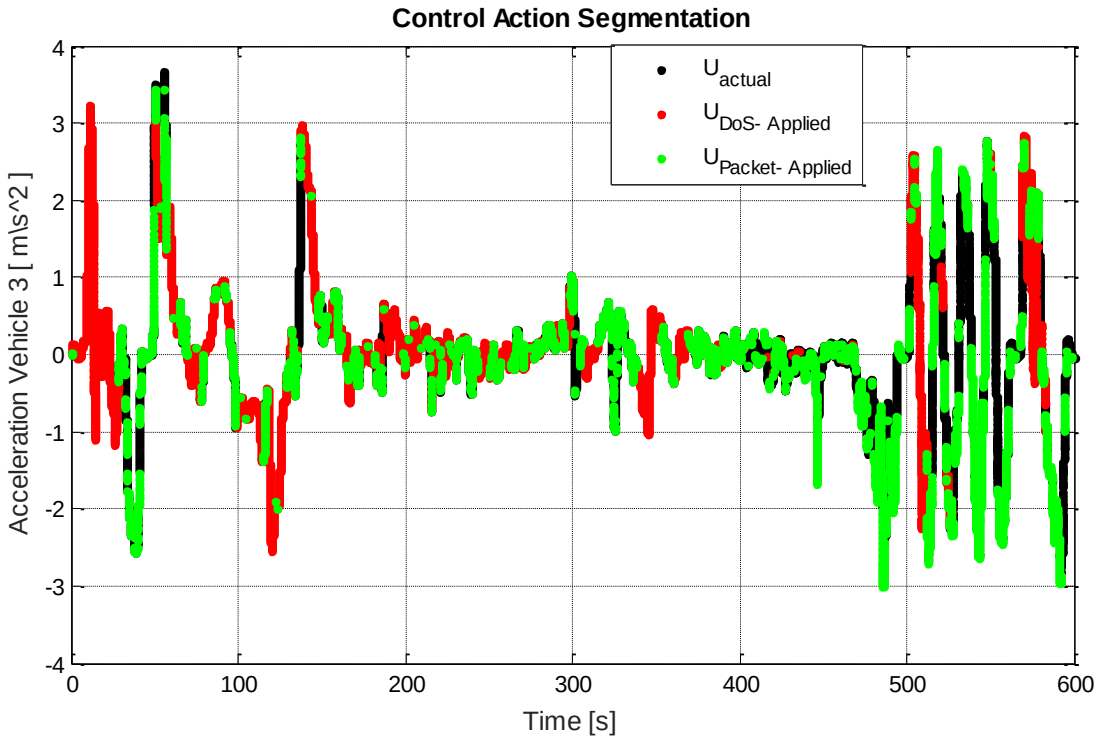

Figure 63: Selected control action during US06 driving cycle via decision making block.

As it can be inferred from Fig. 63, in the first part of the driving cycle, when the DoS attack occurs in the DSRC network, the decision making block mainly chooses DoS strategy specially for critical points where Collison could happen such as $t = 110s$ or $t = 118\ s$, where we have higher acceleration or deceleration in the driving profile. However, after $t = 400\ s$ when packet dropping is happening in the DSRC, the decision making chooses mainly packet dropping strategy to modify control strategy of the platoon.

CHAPTER NINE

SUMMARY AND FUTURE WORKS

9.1. Dissertation Summary

This dissertation is concerned with security of cyber physical systems with particular focus on connected vehicles. Despite being widely applicable in various industries and infrastructures, cyber physical system suffer from issues regarding to safety, security and reliability. To improve the performance of the CPS, these issues should be addressed which requires good knowledge on attack modeling, cyber-attack detection and attack resilient strategies. Along with cyber-attacks, CPS also requires physical health monitoring with regard to physical faults as well as network failures. Motivated by this scenario, this dissertation proposed a set of hybrid strategies to make cyber physical systems resilient toward cyber-attacks as well as physical faults and network failures. These strategies are based on control/systems theory tools and physical models of the CPS that would be beneficial for maintaining the performance and functionality of the CPS in the presence of malfunction and cyber-attacks.

In Chapter 2, a brief introduction has been given on working principle of connected vehicles and modeling of the connected vehicles equipped with Cooperative Adaptive Cruise Control (CACC). Next, in Chapter 3 we have a state- of- art- literature review on cyber-attacks modeling and security in cyber physical systems in occurrence of common cyber-attacks. The chapter also includes a brief review over diagnostics and observer design tools.

In Chapter 4, a sensor/actuator fault diagnosis problem is explored for a connected vehicle system under CACC. The diagnostic scheme has two sliding mode observers to detect, isolate and estimate different sensor faults in the individual vehicles; the CACC controller uses this estimated fault information to reconstruct the control signal. Therefore, inclusion of the diagnostic scheme essentially supplies the controller with more accurate information which in turn improves the overall safety of the connected vehicles. Simulation studies are presented which confirm the effectiveness of the diagnostic scheme.

In Chapter 5, the diagnostic scheme has two components: 1) A sample hold strategy and 2) A Kalman filter-based estimation scheme to reconstruct the data under packet drop outs; the filter provides an improved estimate of the data received via communication network, which is in turn used by the CACC controller to construct the control signal.

In Chapter 6, we proposed three algorithms to estimate the effect of denial of service attack as time delay. The first algorithm considers the statistic time delay as the effect of DoS attack, while, the latter two algorithms model DoS attack as the saturated attack with constant unknown delay. In first section of proposed research, an observer-based algorithm is presented for state estimation for vehicle platooning. The proposed algorithm consists of three main components including a Luenberger observer operates for ideal case of no attack in the system and a model-based observer and delay estimator for under-attack situation. This scheme is capable to detect DoS attack in DSRC communication network as well as estimating states of preceding vehicle for each car. Therefore, the modified CACC using estimated states can avoid potential dangers and present better performance. As future work, the scheme should be validated with experimental data.

In the second algorithm, we propose a real-time scheme for diagnosis of Denial of Service (DoS) cyber-attack in connected vehicles. Under DoS, the attacker keeps the communication network busy by sending fake requests and hence the network is unable to respond to legitimate requests from the real users. Specifically, the proposed scheme can potentially (i) detect the occurrence of DoS, and (ii) estimate its effect on the connected vehicle system. We model the effect of the attack by a time delay in the information processing via communication network. The main goal of the proposed scheme is to track this delay in information processing. The proposed scheme consists of a set of observers designed via sliding mode theory and adaptive observer theory. Simulation case studies are provided to verify the effectiveness of the proposed scheme. Furthermore, the robustness of the scheme is verified (i) under several forms of parametric uncertainties, and (iii) several measurement noise scenarios.

In the third algorithm, we consider a more general problem with delay (as the effect of DoS attack) in cyber physical systems. Hence, an observer-based algorithm is presented to estimate the current states of a distributed cyber physical system while, only delayed measurements are available. The existing delay in the system measurements is a constant unknown value. The proposed scheme consists of two separate components: (1) a PDE model- based adaptive observer to estimate the unknown constant delay in the system and (2) a Luenburger observer to predict the states of the system based on an estimated delay obtained from the first observer. This scheme is capable of detecting and estimating unknown constant delay in cyber physical systems and estimate the correct states of the system despite delay. Hence, it is a valuable method for precise health monitoring

applications in CPS and for modifying the controller of the system to compensate the effects of the delay. As for future works, the scheme can be used to modify the control strategy of the system to compensate the impact of the delay in cyber physical and networked control systems.

In Chapter 7, we considered a platoon of vehicles equipped with CACC strategy. The vehicles moving in a single straight line following their leader in a constant velocity and specific inter-vehicle distance. A continuous model using PDE approximation is developed to describe the dynamics of the platoon. Further, we modeled the false data injection attack in the platoon with injected ghost vehicles disturbing the local density perturbation characteristics of the platoon. To detect and isolate the false data injection attack into the platoon, we develop an observer based diagnostics algorithm. The proposed diagnostics scheme is developed based on PDE model and available measurements on velocity and acceleration of the vehicles in the platoon. Two residuals are derived from the presented scheme using the pre-define constant thresholds. The residuals behaviors are studied in both no attack and under attack scenarios and unique signature is developed for each scenario. Two case studies are conducted in the simulation results to illustrate the effectiveness of the presented algorithm. The results of these two scenarios verify the convergence of the PDE observer and demonstrate the capability of the algorithm to detect and isolate the injection point of the false data injection attack.

Finally, in Chapter 8 we presented an MPC based algorithm to select among available control strategies based on (1) smooth driving and (2) safe relative distance to

compensate the effect of existing network failures/ cyber-attacks in the communication network.

9.2. Future Works

Experimental validation: None of the presented algorithms are validated with the experimental test due to the lack of suitable hardware to create the platoon of vehicle (or robots) sharing their information through the commination network. These algorithms should be validated by experimental studies. However, to do the same, new experimental methods should be developed based on CACC control strategy and DSRC network characteristics.

Observer design for more comprehensive models: In the proposed algorithms and observer design, mainly we have assumed linear model of the platoon of connected vehicles. Although majority of the presented algorithms are based on control theories which are applicable to nonlinear systems e.g. sliding mode observer design, adaptive observer design, it would be good extension to apply the proposed tools to nonlinear model of platoon.

More comprehensive attack modeling: Some of the modeling of the cyber-attacks or network failure can be more complicated from what is used in this thesis such as Morkov model for packet dropping and DoS model.

Stochastic decision making strategy: The inherent of the cyber-attacks is not deterministic. Therefore, it will be more efficient to provide a stochastic decision making scenario to switch among the strategies e.g. game theory based algorithms.

REFERENCES

[1] Workshop Report by the Cyber Security Research Alliance, “Designed-In Cyber Security for Cyber- Physical Systems”, April 2013 in Githersburg, Maryland.

[2] S. Amin, X. Litrico, S. Sastry, and A. Bayen, “Cyber Security of Water SCADA Systems_Part I: Analysis and Experimentation of Stealthy Deception Attack”, IEEE Transaction on Control Systems Technology, vol. 21, no.5, pp: 1963-1970, 2012.

[3] S. Amin, X. Litrico, S. Sastry, and A. Bayen, “Cyber Security of Water SCADA Systems_Part II: Attack Detection Using Enhanced Hydrodynamic Models”, IEEE Transaction on Control Systems Technology, vol. 21, no. 5, pp: 1679-1693, 2013.

[4] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen, and K. Zhao, “Cyber-Physical-social-System in Intelligent Transportation”, IEEE/CAA Journal of Automatica Sinica, vol. 2, no.3, pp:320-333.

[5] Challenges for control research, “Resilient Cyber Physical Systems”.

[6] C. Basile, M. Gupta, Z. Kalbarczyk, and R. Iyer, “An Approach for Detecting and Distinguishing Errors versus Attacks in Sensor Networks”, Proceedings of the 2006 International Conference on Dependable Systems and Network, IEEE 2006.

[7] Y. Zhou, J.Li, L. Lamont and C.A. Rabbath” Modeling of Packet Dropout for UAV Wireless Communications”, International Conference on Computing, Networking and Communications Invited Position Paper Track, 2012, pp. 667-682.

[8] M. Huang, and S. Dey, “Stability of Kalman Filtering with Markovian Packet Loses”, Automatica, vol. 43, pp: 598-607, 2007.

[9] A. A. Cardenas, S. Amin, and S. Sastry," Secure Control: Towards Survivable Cyber-Physical Systems", IEEE 28th International Conference on Distributed Computing Systems, pp: 495-500, 2008.

[10] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, T. Basar, "Resilient Control of Cyber-Physical Systems against Denial of Service Attack", IEEE pp: 54-59, 2013.

[11] Y. Mo, B. Sinopoli, "Secure Control Against Replay Attacks", IEEE 57th Annual Allerton Conference, pp: 911-918, 2009.

[12] E. Wang, Y. Yu, X. Xu, S. Yin, L. Hui, and K. Chow, "Security Issues and Challenges for Cyber Physical System", IEEE/ACM International Conference on Green Computing and Communication & International Conference on Cyber Physical and Social Computing, pp:733-738, 2010.

[13] U. E. Larson, and D. K. Nilsson, "Securing Vehicles against Cyber Attacks", CSIIRW'08 Proceedings of the 4th annual workshop on Cyber security and information intelligence research, pp.1-3, 2008.

[14] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An Approach to Specification-based Attack Detection for In-Vehicle Networks", IEEE Intelligent Vehicles Symposium, pp.220 -225, 2008.

[15] W.B. Qin, M. M. Gomez, and G. Orosz, "Stability Analysis of Connected Cruise Control with Stochastic Delay", 2014 American Control Conference (ACC), 2014, pp. 4624-4629.

[16] W. Qin, and G. Orosz, “Digital Effects and Delays in Connected Vehicles: Linear Stability and Simulations”, Proceeding of the ASME 2013 Dynamics Systems Control Conference, DSCC 2013.

[17] D. K. Nilsson, and U. E. Larson, “Simulated Attacks on Can Buses: Vehicle Virus”, Proceedings of the Fifth IASTED International Conference, Communication Systems and Networks (AsiaCSN), pp. 66-72, 2008.

[18] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage ,“Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, pp. 447 – 462, 2010.

[19] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno,” Comprehensive Experimental Analyses of Automotive Attack “, USENIX Security, August 10–12, 2011.

[20] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”, 31st IEEE Symposium on Security and Privacy, 05/2010.

[21] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, “A survey of inter-vehicle communication protocols and their applications,” IEEE Communications Surveys Tutorials, vol. 11, pp. 3–20, Second 2009.

[22] X. Yang, L. Liu, N. H. Vaidya, and F. Zhao, “A vehicle-to-vehicle communication protocol for cooperative collision warning,” in Mobile and Ubiquitous Systems:

Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on,pp.114–123,IEEE, 2004.

[23] S. Lee and A. Lim, “An empirical study on ad hoc performance of dsrc and wi-fi vehicular communications,” International Journal of Distributed Sensor Networks, vol. 2013, 2013.

[24] P. G. Gipps, “A behavioral car-following model for computer simulation”, Transportation Research Part B: Methodological, vol. 15, no. 2, pp: 105-111, 1981.

[25] B. HomChauduri, A. Vahidi, and P. Pisu, “A Fuel Economic Model Predictive Control Strategy for a Group of Connected Vehicles in Urban Roads”, American Control Conference, 2015.

[26] M. Brackstone, and M. McDonald, “Car-following: a historical review”, Transportation Research Part F, vol. 2, pp: 181-196, 1999.

[27] M. Persson, F. Botling, E. Hesslow, and R. Johansson, “ Stop & Go Controller for Adaptive Cruise Control”, Proceedings of the 1999 IEEE International Conference on Control Applications, pp: 1692-1699 1997.

[28] C. Park, and N. Jeon, “A Study of Adaptive Cruise Control System to Improve Fuel Efficiency”, Proceeding of the World Congress on New Technologies, pp: 202.1-202.6, 2015.

[29] F. Bu, H. Tan, and J. Huang, “Design and field testing of a cooperative adaptive cruise control system”, 2010 American Control Conference, pp: 4416-4421, 2010.

[30] J. Ploeg, N. Wouw, and H. Nijmeijer, “Lp String Stability of Cascaded Systems: Application to Vehicle Platooning”, IEEE Transactions on Control Systems Technology, vol. 22, no. 2, 2014, pp: 786-793.

[31] S. Oncu, J. Ploeg, N. Wouw, and H. Nijmeijer, “Cooperative Adaptive Cruise Control: Network-Aware Analysis of String Stability”, IEEE Transaction on Intelligent Transpiration Systems, Vol. 15, No. 4, pp: 1527-1538, 2014.

[32] D. Cody, F. Bu, S. Dickey, D. Nelson, J. Spring, C. Nowakowski, and S. Shladover,” Effects of Cooperative Adaptive Cruise Control on Traffic Flow: Testing Drivers’ Choices of Following Distances”, California Path Program Institute of Transpiration Studies University of California, Berkeley, 2008.

[33] T. Stanger, and L. Re, “ A Model Predictive Cooperative Adaptive Cruise Control Approach”, 2013 American Control Conference, pp:1374-1379, 2013.

[34] Pisu, P, AuE 826 Vehicle Diagnostics: Lecture Notes, 2012.

[35] [70] P. M. Frank, “Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results,” Automatica, vol. 26, no. 3, pp. 459-474, 1990.

[36] J. Luo, K. Pattipati, L. Qiao, and S. Chigusa, “An Integrated Diagnostic Development Process for Automotive Engine Control System”, IEEE Transaction system, Man and Cybernetics, Part C: Application and Reviews, vol. 37, no.6, pp: 1163-1173, 2007.

[37] K. Krishnaswami, G. Luh, and G. Rizzoni, "Nonlinear Parity Equation based Residual Generation for Diagnostics of Automotive Engine Faults", Contr.Eng.Practice, vol.3, no.10, pp: 1385-1392, 1995.

[38] Y. Zhang, G. Gantt, M. Rychlinski,, R. Edwards, J. Correia, and C. Wolf, " Connected Vehicle Diagnostics and Prognostics, Concept, and Initial Practice", IEEE Transactions on Reliability, vol. 58, no.2, pp:286-294, 2009.

[39] Z. H. Pang, G. Liu, and Z. Dong, "Secure Networked Control Systems under Denial of Service Attacks", 18th IFAC world Congress, pp: 8908-8915, 2011.

[40] A. Housholder, A. Manion, L. Pesante, G. Weaver, and R. Thomas, " Managing the Threat of Denial of Service Attack", Carnegie Mellon CERT Coordination Center, Pittsburgh, PA, Available: http://www.cert.org/archive/pdf/Managing_DoS.pdf

[41] S. Amin, A. Cardenas, and S. Sastry, "Safe and Secure Networked Control Systems under Denial of Service Attacks", HSCC 2009, LNCS 5469, pp. 31–45, 2009.

[42] M. Long, C. Wu, and J. Hung, "Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation", IEEE Transaction on Industrial Information, vol. 1, no. 2, pp: 85-96, 2005.

[43] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 226–231, IEEE, 2010.

[44] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on, pp. 911–918, IEEE, 2009.

[45] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, “Stealthy deception attacks on water scada systems,” in Proceedings of the 13th ACM international conference on Hybrid systems: computation and control, pp. 161–170, ACM, 2010.

[46] K. Ingols, M. Chu, R. Lippmann, S. Webster, S.Boyer , “Modeling Modern Network Attacks and Countermeasures Using Attack Graphs”,IEEE, 2009 Annual Computer Security Applications Conference, pp:117-126.

[47] S. A. Camtepe and B. Yener, “Modeling and Detection of Complex Attacks”, 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops, pp. 234 – 243, 2007.

[48] J. Wu, L. Yin, Y. Guo, “Cyber Attacks Prediction Model Based on Bayesian Network”, 2012 IEEE 18th International Conference on Parallel and Distributed Systems, pp: 730 – 731.

[49] T. Chen, J. Carlos Sanchez, and J. Buford,“Petri Net Modeling of Cyber-Physical Attacks on Smart Grid”, IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, pp: 741-749, DECEMBER 2011,

[50] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo “Identifying Cyber Attacks via Local Model Information”, Decision and Control (CDC), 2010 49th IEEE Conference on, 2010, pp. 5961 – 5966.

[51] Y.Mo and B.Sinopoli, “Integrity Attacks on Cyber-Physical Systems”, *HiCoNS’12,* April 17–18, 2012, Beijing, China.

[52] Y.Mo and B.Sinopoli, “Secure Control Against Replay Attacks”, Forty-Seventh Annual Allerton Conference, pp: 911-918, Allerton House, UIUC, Illinois, USA, September 30 - October 2, 2009

[53] C.Kwon, W.Liu and I.Hwang “Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks”, 2013 American Control Conference (ACC), Washington, DC, USA, June 17-19, 2013,pp: 3344-3349.

[54] B. Sinopoli, L. Schenato, M. franceschetti, K. Poolla, M. I. Jordan, S. Sastry, “Kalman Filtering with Intermittednt Observation”, IEEE Transaction on Automatic Control, vol. 49, no. 9, 2004, pp. 1453-1664.

[55] N. Erzhuo, W. Qing, D. Chaoyang, “Robust Fault Detection and Optimization for a Network of Unmanned Vehicles with Imperfect Communication Channels”, Chinese Journal of Astronautics, vol.27, no.1, 2014, pp. 65-75.

[56] N. Meskin, K. Khosravani, and C. A. Rabbath, “Fault Diagnosis in a Network of Unmanned Aerial Vehicles with Imperfect Communication Channels”, AIAA Guidance, Navaigation, and Control Conference, August 2009, pp. 1-18.

[57] J. Hespanha, P. Naghshtabrizi, and Y. Xu, “A survey of recent results in networked control systems,” *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[58] N. Nahi, “Optimal recursive estimation with uncertain observation,” *IEEE Trans. Inf. Theory*, vol. 15, no. 4, pp. 457–462, 1969.

[59] O. C. Imer, S. Yuksel, and T. Basar, “Optimal control of dynamical systems over unreliable communication links,” *Automatica*, vol. 2, no. 9, pp. 1429–1440, Sep. 2006.

[60] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE,* vol. 95, no. 1, pp. 163–187, Jan. 2007.

[61] V. Gupta, B. Hassibi, and R. M. Murray, "Optimal LQG Control Across Packet-Dropping Links", Journal of Systems and Control Letters, vol. 56, pp: 439-446, 2007.

[62] Z. Jin, V. Gupta, R. M. Murray, "State Estimation Over Packet Dropping Networks Using Multiple Description Coding", Automatica, vol. 42, pp:1441-1452, 2006.

[63] L. Shi, M. Epstein, and R. M. Murray, "Kalman Filtering Over a Packet-Dropping Network: A Probabilistic Perspective", IEEE Transaction on Automatic Control, vol. 55, no.3, pp: 594- 606.

[64] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. Wouw, and H. Nijmeijer, "Graceful Degradation of CACC Performance Subject to Unreliable Wireless Communication", Proceedings of the 16th International IEEE Annual Conference on Intelligent Transportation Systems (ITSC 2013), The Hague, The Netherlands, October 6-9, 2013.

[65] A. Housholder, A. Manion, L. Pesante, G. Weaver, and R. Thomas, " Managing the Threat of Denial of Service Attack", Carnegie Mellon CERT Coordination Center, Pittsburgh, PA, Available: http://www.cert.org/archive/pdf/Managing_DoS.pdf

[66] S. Amin, A. Cardenas, and S. Sastry, "Safe and Secure Networked Control Systems under Denial of Service Attacks", HSCC 2009, LNCS 5469, pp. 31–45, 2009.

[67] M. Long, C. Wu, and J. Hung, "Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation", IEEE Transaction on Industrial Information, vol. 1, no. 2, pp: 85-96, 2005.

[68] F. Pasqualetti, F. Drfler, F. Bullo, “Attack Detection and Identification in Cyber-Physical Systems”, IEEE. Trans. Automatic Control, vol. 58, no. 11, pp: 2715-2729, 2013.

[69] Y. Yan, Y. Qian, H. Sharid, and D. Tipper,” A Survey on Cyber Security for Smart Grid Communications”, IEEE Communication surveys & Tutorials, vol. 14, no.4, pp:998-1010, 2012.

[70] B. Zhu, A. Joseph, and S. Sastry, “A Taxonomy of Cyber Attacks on SCADA Systems”, 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp. 380-388, 2011.

[71] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets,” in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 226–231, IEEE, 2010.

[72] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in Preprints of the 1st workshop on Secure Control Systems, pp. 1–6, 2010. [29]

[73] F. Pasqualetti, F. D¨orfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729, 2013.

[74] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, “Cyber security analysis of state estimators in electric power systems,” in 49th IEEE conference on decision and control (CDC), pp. 5991–5998, IEEE, 2010.

[75] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 1, p. 13, 2011.

[76] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks with incomplete information against smart power grids,” in Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 3153– 3158, IEEE, 2012.

[77] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (IDPS)”, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, NIST special publication 800-94, 2007.

[78] P. G. Teodoroa, J. D. Verdejoa, G. M. Fernandeza, and E. Vazquezb, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” Computer & Security, vol. 28, no. 1, pp. 18 – 28, 2009.

[79] L. Spitzner, Honeypots: Tracking Hackers, 1st edition. Addison-Wesley, Boston,MA, 2002.

[80] R. Chen, and K. A. Loparo,” Identification of Time Delays in Linear Stochastic Systems”, International Journal of Control, vol.57, no.6, 1993, pp.1273-1291.

[81] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. Proceedings of the VDE Congress, Berlin, 2004.

[82] A. Teixeria, H. Sandberg, and K. Johansson, “Networked Control Systems under Cyber Attacks with Applications to Power Networks”, American Control Conference, pp: 3690-3696, 2010.

[83] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, “A survey of fault detection, isolation, and reconfiguration methods,” IEEE Transactions on Control Systems Technology, vol. 18, no. 3, pp. 636-653, 2010.

[84] J. Chen, R. J. Patton, and H. Y. Zhang, “Design of unknown input observers and robust fault-detection filters,” Int. J. Control, vol. 63, no. 1, pp. 85–105, 1996.

[85] R. K. Mehra and J. Peschon, “An innovations approach to fault detection and diagnosis in dynamic systems,” Automatica, vol. 7, pp. 637–640, 1971.

[86] J. Gertler, “Fault detection and isolation using parity relations,” Control Eng. Practice, vol. 5, no. 5, pp. 653–661, 1997.

[87] R. Isermann, “Process fault detection based on modeling and estimation methods: A survey,” Automatica, vol. 20, no. 4, pp. 387–304, 1984.

[88] V. Utkin, J. Guldner, and J. Shi, Sliding mode control in electromechanical systems. CRC press, 1999.

[89] F. L. Lewis, “Optimal Estimation”, Wiley, New York, 1986.

[90] Y. Zheng, H. Fang, and H. Wang, “Takagi-Sugeno Fuzzy-Model-Based Fault Detection for Networked Control Systems with Markov Delays”, IEEE Transactions on Systems, Man, and Cybernetics_Part B, vol. 36, no.4, pp:924-929, 2006.

[91] M. D. Greenberg, Advanced engineering mathematics. Prentice-Hall, 1988.

[92] K. S. Narendra and A. M. Annaswamy, Stable adaptive systems. Courier Corporation, 2012.

[93] W. H. van Willigen, M. C. Schut, and L. J. Kester, “Approximating safe spacing policies for adaptive cruise control strategies,” in Vehicular Networking Conference (VNC), 2011 IEEE, pp. 9–16, IEEE, 2011.

[94] W. van Willigen, L. Kester, E. van Nunen, and E. Haasdijk, “Safety in the face of uncertainty: Critical headway estimation in cooperative adaptive cruise control,” International Journal of Intelligent Transportation Systems Research, vol. 13, no. 2, 2015.

[95] K. C. Dey, L. Yan, X. Wang, Y. Wang, H. Shen, M. Chowdhury, L. Yu, C. Qiu, and V. Soundararaj, “A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (cacc),” IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 2, pp. 491–509, 2016.

[96] M. Krstic and A. Smyshlyaev, Boundary control of PDEs: A course on backstepping designs, vol. 16. Siam, 2008.

[97] Bresch-Pietri. D, and Krstic. M, (2009), "Adaptive trajectory tracking despite unknown input delay and plant parameters." *Automatica* 45.9 (2009): 2074-2081.

[98] Bresch-Pietri. D, and Krstic. M, (2010), "Delay-adaptive predictor feedback for systems with unknown long actuator delay." *IEEE Transactions on Automatic Control* 55.9 (2010): 2106-2112.

[99] E. Fridman, and M. Dambrine, “Control under quantization, saturation and delay: An LMI approach”, Automatica, vol. 45, 2009, pp. 2258-3364.

[100] Han, X. R., Fridman. E, Spurgeon, S. K, Edwards. C, (2009), "On the design of sliding-mode static-output-feedback controllers for systems with state delay." *IEEE Transactions on Industrial Electronics* 56.9 (2009): 3656-3664.

[101] Han. X, Fridman. E, and Spurgeon. S.K, (2012), "Sliding mode control in the presence of input delay: A singular perturbation approach." *Automatica*48.8 (2012): 1904-1912.

[102] H. Hao and P. Barooah, "Approximation error in pde-based modelling of vehicular platoons," International Journal of Control, vol. 85, no. 8, pp. 1121–1129, 2012.

[103] P. Barooah, P. G. Mehta, and J. P. Hespanha, "Mistuning-based control design to improve closed-loop stability margin of vehicular platoons," IEEE Transactions on Automatic Control, vol. 54, no. 9, pp. 2100–2113, 2009.

[104] P. Barooah and J. P. Hespanha, "Error amplification and disturbance propagation in vehicle strings with decentralized linear control," in Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC'05. 44th IEEE Conference on, pp. 4964–4969, IEEE, 2005.

[105] G. Naus, R. Vugts, J. Ploeg, R. van de Molengraft, and M. Steinbuch, "Cooperative adaptive cruise control, design and experiments," in Proceedings of the 2010 American Control Conference, pp. 6145–6150, IEEE, 2010.

[106] G. J. Naus, R. P. Vugts, J. Ploeg, M. J. van de Molengraft, and M. Steinbuch, "String-stable cacc design and experimental validation: A frequency-domain approach," IEEE Transactions on Vehicular Technology, vol. 59, no. 9, pp. 4268–4279, 2010.

[107] D. Helbing, “Traffic and related self-driven many-particle systems,” Reviews of modern physics, vol. 73, no. 4, p. 1067, 2001.

[108] P. Barooah, P. G. Mehta, and J. P. Hespanha, “Control of large vehicular platoons: Improving closed loop stability by mistuning,” in American Control Conference, 2007. ACC’07, pp. 4666–4671, IEEE, 2007.

[109] J. Ryu and J. C. Gerdes, “Integrating inertial sensors with global positioning system (gps) for vehicle dynamics control,” TransactionsAmerican Society of Mechanical Engineer Journal of Dynamic System Measurement and Control, vol. 126, no. 2, pp. 243–254, 2004.

[110] F. Bai, and H. Krishnan, “Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications”, Proceedings of the IEEE ITSC, pp: 355-363, 2006.

[111] I. Hassan, H. Vu, and T. Sakurai, “Performance Analysis of the IEEE 802.11 MAC Protocol for DSRC Safety Applications”, IEEE Transactions on Vehicular Technology, pp: 1-15, 2011.

[112] F. Hu, Y. Lu, A. Vasilakos, Q. Hao, R. Ma, and Y. Patil, “Robust Cyber Physical Systems: Concept, model and implementation”, Journal of Future Generation Computer Systems, vol. 56, pp: 449-475, 2016.

[113] C. D. Persis, and P. Tesi, “On Resilient Control of Nonlinear Systems under Denial of Service”, 53rd IEEE Conference on Decision and Control, 2014, pp. 5254-5259.

[114] Y. Niu, and D. Ho, “Robust Observer Design for Ito Stochastic Time-Delay Systems via Sliding Mode Control”, Journal of Systems & Control Letters, vol. 55, pp:781-793, 2006.

[115] J. Fischer, A. Hekler, and U. Hanebeck, “State Estimation in Networked Control Systems”.

[116] Y. Zhang, X. Zhang, K. Liang, “Observer-based Fault Detection for Stochastic Delayed Systems in Network Environment”, Proceeding of the 11th World Congress on Intelligent Control and Automation, pp: 5706-5701, 2014.

[117] Y. Zheng, H. Fang, and H. Wang, “Takagi-Sugeno Fuzzy-Model-Based Fault Detection for Networked Control Systems with Markov Delays”, IEEE Transactions on Systems, Man, and Cybernetics_Part B, vol. 36, no.4, pp:924-929, 2006.

[118] H. Fang, H. Ye, M. Zhong, “Fault Diagnosis of Networked Control Systems”, Annual Reviews in Control, vol. 31, pp: 57-68, 2007.

[119] Z. Mao, B. Jian, P. Shi, “H_∞ Fault Detection Filter Design for Networked Control Systems Modelled by Discrete Markovian Jump Systems”, IET Control Theory Application, vol. 1, no. 5, pp: 1336-1343.

[120] Y. Ge, Q. Chen, and M. Jian, “Modeling and Estimation of Networked Control Systems with Time Delays Based on CTHMM”, Proceedings of the IEEE International Conference on Mechatronics and Automation, pp: 4649-2654, 2009.

[121] G. Qzveren and A. Willsky, “Observability of Discrete Event Dynamic Systems”, IEEE Trans. On Automatic Control, vol. 35, pp: 797-806, 1990.

[122] A. Balluchi, L. Benvenuti, M.D. Benedetto, C. Pinello, and A. L. Vincentelli, “Automotive Engine Control and Hybrid Systems: Challenges and Opportunities”, Proceedings of the IEEE, 88, “Special Issue on Hybrid Systems”, vol.7, pp: 888-912, 2000.

[123] A. Alessandri, and P. Coletta, “Design of Luenberger Observers for a Class of Hybrid Linear Systems”, In Hybrid Systems: Computation and Control, vol. 2034 of LNCS, pp: 7-18, 2001.

[124] A. Balluchi, L. Benvenuti, M. Benedetto, and A. L. Vincentelli,, “ Design of Observers for Hybrid Systems”

[125] R. Goebel, R. Sanfelice, and A. Teel, “Hybrid Dynamical Systems: Modeling, Stability, and Robustness”, Princeton University Press.

[126] F. Ferrante, F. Gouaisbaut, R. Sanfelice and S. Tarbouriech, “A Hybrid Observer with a Continuous Intersample Injection in the Presence of Sporadic Measurements”, IEEE 54th Annual Conference on Decision and Control (CDC), pp: 5654-5459, 2015.