SECURITY OF VEHICULAR PLATOONING

by

Soodeh Dadras

A dissertation submitted in partial fulfillment
of the requirements for the degree

of

DOCTOR OF PHILOSOPHY

in

Electrical Engineering

Approved:

Chris Winstead, Ph.D. Major Professor	Todd Moon, Ph.D. Committee Member
Jake Gunther, Ph.D. Committee Member	Don Cripps, Ph.D. Committee Member
David Geller, Ph.D. Committee Member	Richard S. Inouye, Ph.D. Vice Provost for Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2019

ABSTRACT

Security of vehicular platooning

by

Soodeh Dadras, Doctor of Philosophy

Utah State University, 2019

Major Professor: Chris Winstead, Ph.D.
Department: Electrical and Computer Engineering

This dissertation investigates the security of vehicular platooning. It describes the critical challenges in security with a focus on the vulnerabilities of vehicle platooning and points out that exploiting these drawbacks can cause oscillations and collisions in the platoon. These security issues could prove particularly disruptive and dangerous in vehicular platooning by causing severe injuries, a delay in system performance or increase in fuel consumption. This research focuses on the design, detection, and mitigation of attacks in a vehicle platoon. To achieve the secure design, we introduce the possible attacks, that can be implemented by exploiting weaknesses of the platooning algorithms. Furthermore, we explore the attacker's capability to disrupt the typical performance of the platoon which includes the attacker's control over vehicle formation via motion modification and change in control law. Then, we propose a detection algorithm which can identify the attacker in the platoon as a primary step for mitigating the impact of control modification attack in the platoon. In the end, we aim at proposing a resilient scheme which would protect the platoon against undesirable impacts of the attack, like platoon disintegration, collisions, oscillations in vehicles' motion, and inefficient fuel consumption, after the attack.

(134 pages)

PUBLIC ABSTRACT

Security of vehicular platooning

Soodeh Dadras

Platooning concept involves a group of vehicles acting as a single unit through coordination of movements. While Platooning as an evolving trend in mobility and transportation diminishes the individual and manual driving concerns, it creates new risks. New technologies and passenger's safety and security further complicate matters and make platooning attractive target for the malicious minds. To improve the security of the vehicular platooning, threats and their potential impacts on vehicular platooning should be identified to protect the system against security risks. Furthermore, algorithms should be proposed to detect intrusions and mitigate the effects in case of attack. This dissertation introduces a new vulnerability in vehicular platooning from the control systems perspective and presents the detection and mitigation algorithms to protect vehicles and passengers in the event of the attack.

This work is dedicated with love and gratitude to
My wonderful parents,
Best sisters ever,
And
The sweet and adorable young members of my family,
The apples of my eyes,
Who made me a proud aunt.

ACKNOWLEDGMENTS

I wish to express my deepest gratitude to my advisor, Professor Chris Winstead, whose guidance, support, and encouragement have made the completion of this work possible. Professor Winsteads help and trust in my abilities pushed me forward and allowed me to learn more as a student and develop more in my research than I could think.

I would like to thank Professors Todd Moon and Jacob Gunther who inspire me and provided significant help and advice during my time in Utah State University. I also thank my committee members, Professors Todd Moon, Jacob Gunther, Don Cripps, and David Geller for reviewing my work and providing their valuable insights through each step. I am very thankful to wonderful ladies in Electrical and Computer Engineering department Tricia Brandenburg, Kathy Phippen, Diane Buist, and Heidi Harper that helped me throughout every single step in my program. I would like to acknowledge the support I received during my Ph.D. by the National Science Foundation under Grant No. 1410000.

I deeply appreciate the help from my current and previous lab mates for the collaboration and wonderful experiences in the lab. I extend my gratitude to my friend, Aatreyi, for her friendship. I thank all the students and friends who have helped me in one way or another.

Last but not least, I want to thank my exceptional and lovely family, My **Mom**, **Dad**, and **Sisters** for their continuous support, love, and inspiration. I feel extremely fortunate and I am much obliged for their presence. I can not find enough words to thank them for all of the sacrifices they have made to make the completion of this work possible and I am forever in their debt. Moreover, I would like to take this space to thank my mom and dad for their patience, faith in my abilities, and positive words. I admit that their impressive attitudes toward higher education and high quality of life, phenomenal work ethics and remarkable achievements are my all-time and life-long incentives. I give my very special thanks to my sister, Sara, who is my savior, mentor, role model, rock, and source of inspiration. I definitely would not survive a single minute without her extraordinary support,

wisdom, selfless helps, encouragement, and friendship. Thanks to my amazing and super caring family for always being there for me.

Soodeh Dadras

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

CPS	Cyber-Physical Systems
AV	Autonomous Vehicle
CC	Cruise Control
ACC	Adaptive Cruise Control
CACC	Coperative Adptive Cruise Control
PID	Proportional Integral Derivative
PD	Proportional Derivative
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
GPS	Global Positioning System
ITS	Intelligent Transportation System
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
I2V	Infrastructure-to-Vehicle
V2x	Vehicle-to-everything
RSU	Roadside unit
WAVE	Wireless Access for Vehicular Environments
IPv6	Internet Protocol version 6
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
FCC	Federal Communications Commission
IETF	Internet Engineering Task Force
VANET	Vehicular Ad-hoc NETwork
MANETs	Mobile Ad Hoc NETworks
OBU	OnBoard Unit
DGPS	Differential Global Positioning System

CHAPTER 1

Introduction

Since the number of vehicles and vehicular traffic have significantly grown worldwide, platooning has become a topic of considerable interest and has motivated much research in this field. The platooning concept involves a group of vehicles traveling together as shown in Fig. 1.1 to maintain minimum spacing and relative velocity with one leader in the front position for velocity and trajectory reference. Goals for platoon establishment are maximizing highways throughput, greater commuting speeds, enhancing traveling quality and safety in highways, and minimizing fuel consumption [6].

Many companies and projects have been actively involved in vehicle platooning like SARTRE a European platooning project [120]; PATH a California traffic automation program that includes platooning [129]; GCDC a cooperative driving initiative in the Netherlands [103], SCANIA platooning [6] and; Energy ITS a Japanese truck platooning project [135]. The focus of this work will be on security in platooning control and communication.

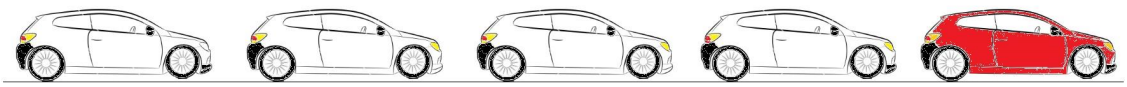


Fig. 1.1: A platooning scenario

1.1 Platoon Control Design

Platoon control can be put in two categories; First, when vehicles are moving in straight

line, longitudinal control is taking care of small spacing and zero relative velocity between vehicles. Second, lateral control prevents unwanted changing lanes and cutting corners for all kind of trajectories [89]. It is worth noting that this work only studies longitudinal control.

In most cases, longitudinal control involves a simple double integrator system.

$$\begin{aligned} \dot{p} &= v \\ \dot{v} &= \frac{1}{M}u \end{aligned} \tag{1.1}$$

where p, v, and u are the position, velocity and control input respectively and M is vehicle mass.

Since the emergence of platooning concept, there have been many pieces of research that pursue and support the platooning goal. The most researched area in driving automation is the vehicle string, stability, and string stability. String stability plays an important role in performance of vehicle formation. A vehicle string is string stable in case of disturbance injection if the error in spacing will attenuate toward the end of the platoon and vehicle distances remain bounded [115, 125].

1.1.1 Platoon strategies

Two strategies are used to control the spacing between vehicles: constant spacing and variable spacing.

Variable spacing usually does not require a lot of data from other vehicles. In addition, it can ensure string stability using onboard information only, but inter-vehicle distances vary with the velocity and can be very large, hence traffic density is low. Constant Time Headway (CTH) is the simplest and most common variable spacing policy. Variable time headway can vary linearly with the velocity, with the relative velocity, or even with vehicle dynamics and road conditions.

Constant spacing can achieve both string stability and high traffic density, sometimes at the cost of inter-vehicle communications. In the Constant Spacing control strategies, the

desired inter-vehicle spacing is independent of the velocity of the controlled vehicle. The tracking requirement is stringent since every controlled vehicle has to match its position, velocity, and acceleration with the vehicle ahead. As a consequence, these strategies require more information to guarantee performance. The achievable traffic capacity is very high in a constant spacing control strategy. There are several solutions for constant spacing strategy: control with information of lead and preceding vehicles, control with information of preceding vehicle (unidirectional), control with information of preceding and following vehicles (bidirectional) are shown in Fig. 1.2 - 1.4 where the arrows show the direction of the information flow [132] and numbering order is from the left side to the right side of the platoons shown in Figs 1.2 - 1.4.

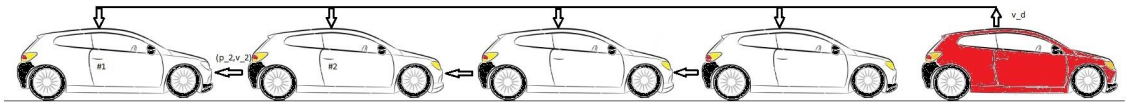


Fig. 1.2: Leader-Predecessor information flow in platoon

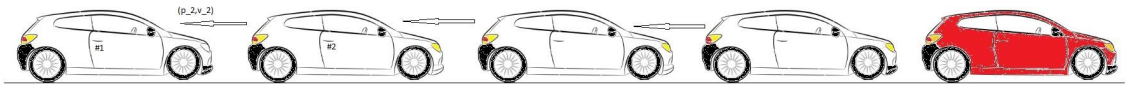


Fig. 1.3: Unidirectional information flow in platoon

Once sufficient information is gathered to understand the state of the vehicle with respect to other vehicles, a control scheme is required. Longitudinal control of platoon has been the topic of many articles [89]; PID control law for longitudinal control of lead

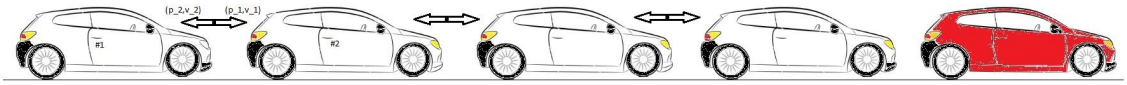


Fig. 1.4: Bidirectional information flow in platoon

vehicle was proposed in [68]. State feedback linearizion used for the control of platoon movement for nonlinear vehicle model in [126]. A simple PD control algorithm is considered in [142] and [59] for different strategies in a platoon where they analyzed platoon as a set of connected mass-spring-damper. In [63] collision avoidance scheme is combined with second-order sliding mode controller where bicycle model vehicles form a platoon. The problem of stability of a vehicle string in the presence of parametric uncertainty is addressed and a Lyapunov-based decentralized adaptive control algorithm to compensate for such parametric variations is presented in [133]. The sliding surface method of controller design is utilized in [118] to guarantee string stability and minimum spacing for leader predecessor strategy. Combined throttle/brake control algorithm using a modified sliding control method designed to control inter-vehicle spacing within a fully automated platoon of vehicles in [76]. The longitudinal control of the vehicles [85] is PD control based on the inter-vehicle distance measured by the laser radar and calculated from the localization data transmitted from the preceding vehicle over the intercommunications. The authors adopt a third-order vehicle model and applied a Lyapunov control method [111] where Lyapunov function is derived based on expected spacing error. In recent years, some advanced platoon control laws have been proposed under the framework of multi-agent consensus control [140], [52] and [122]. Distributed control of a platoon of vehicles with nonlinear dynamics using distributed receding horizon control algorithms is presented in [56] and [57]. Linear and nonlinear event triggered based control are proposed in [93] where every vehicle broadcasts its position and velocity information only at discrete event times and these events are determined by a trigger rule that depends only on the agent's state and time.

This work is mainly based on work presented in [142] where PD control was proposed for different types of information flow in the platoon. The problems which are going to be discussed in this work involve bidirectional, leader-follower and unidirectional with constant time headway information flow where system models are presented in absolute coordinates in equations (1.2), (1.4) and (1.6) and error coordinates in equations (1.3), (1.5) and (1.7).

Platooning model for bidirectional flow of information are presented in (1.2) and (1.3) in absolute and error coordinate frames.

$$
\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= k_{p_n}(x_2 - x_1 - d) + k_{d_n}(v_2 - v_1) \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= k_{p_n}(x_3 - 2x_2 + x_1) + k_{d_n}(v_3 - 2v_2 + v_1) \\
&\vdots \\
\dot{x}_i &= v_i \\
\dot{v}_i &= k_{p_n}(x_n - 2x_{n-1} + x_{n-2}) + k_{d_n}(v_n - 2v_{n-1} + v_{n-2}) \\
\dot{x}_n &= v_n \\
\dot{v}_n &= u_n
\end{aligned}
\tag{1.2}
$$

$$
\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= -2k_p z_1 + k_p z_2 - (k_d) y_1 + k_d y_2 \\
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= k_p z_1 - 2k_p z_2 + k_p z_3 + k_d y_1 - 2k_d y_2 + k_d y_3 \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= k_p z_{n-3} - 2k_p z_{n-2} + k_p z_{n-1} + k_d y_{n-3} - 2k_d y_{n-2} + k_d y_{n-1} \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= k_p z_{n-2} - k_p z_{n-1} + k_d y_{n-2} - k_d y_{n-1} - u
\end{aligned}
\tag{1.3}
$$

Platooning model for leader-predecessor flow of information are presented in (1.4) and (1.5) in absolute and error coordinate frame.

$$
\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= k_{p_n}(x_2 - x_1 - d) + k_{d_n}(v_2 - v_1) + k_{b_n}(v_l - v_1) \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= k_{p_n}(x_3 - 2x_2 + x_1) + k_{d_n}(v_3 - 2v_2 + v_1 + k_{b_n}(v_l - v_2)) \\
&\vdots \\
\dot{x}_{n-1} &= v_i \\
\dot{v}_{n-1} &= k_{p_n}(x_n - 2x_{n-1} + x_{n-2}) + k_{d_n}(v_n - 2v_{n-1} + v_{n-2}) + k_{b_n}(v_l - v_{n-1}) \\
\dot{x}_n &= v_n \\
\dot{v}_n &= u_n
\end{aligned}
\tag{1.4}
$$

$$
\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= -k_p z_1 + k_p z_2 - (k_d) y_1 + k_d y_2 + k_{b_n} y_1 \\
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= -k_p z_2 + k_p z_3 - k_d y_2 + k_d y_3 + k_{b_n} y_2 \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= -k_p z_{n-2} + k_p z_{n-1} - k_d y_{n-2} + k_d y_{n-1} + k_{b_n} y_{n-2} \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= -k_p z_{n-1} - k_d y_{n-1} + k_{b_n} y_{n-1} - u
\end{aligned}
\tag{1.5}
$$

Platooning model for unidirectional flow of information with constant time headway are presented in (1.6) and (1.7) in absolute and error coordinate frame.

$$
\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= k_{p_n}(x_2 - x_1 - hv_1) + k_{d_n}(v_2 - v_1) \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= k_{p_n}(x_3 - x_2 - hv_2) + k_{d_n}(v_3 - v_2) \\
&\vdots \\
\dot{x}_{n-1} &= v_i \\
\dot{v}_{n-1} &= k_{p_n}(x_n - x_{n-1} - hv_{n-1}) + k_{d_n}(v_n - v_{n-1}) \\
\dot{x}_n &= v_n \\
\dot{v}_n &= u_n
\end{aligned} \tag{1.6}
$$

$$
\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= -k_p z_1 + k_p z_2 - (k_d) y_1 + k_d y_2 - k_p h y_1 \\
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= -k_p z_2 + k_p z_3 - k_d y_2 + k_d y_3 - k_p h y_2 \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= -k_p z_{n-2} + k_p z_{n-1} - k_d y_{n-2} + k_d y_{n-1} - k_p h y_{n-2} \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= -k_p z_{n-1} - k_d y_{n-1} - k_p h y_{n-1} y_{n-1} - u
\end{aligned} \tag{1.7}
$$

Where x, v, and $\dot{v}$ represent a vehicle's position, velocity, and acceleration, respectively, k_{p_n} and k_{d_n} the proportional and derivative control gains which are the same for all vehicles for the purpose of simplicity they would refer to as k_p and k_d. Desired spacing between every two vehicles is considered as d. v_l is desired platoon velocity (broadcasted by the system infrastructure or platoon leader) and k_{b_n} the associated control gain for relative velocity between vehicle and the leader, and h is the constant time headway for variable spacing term. u_n is the control input to the leader where it can follow the same rule as

other vehicles in platoon or be zero in normal platooning condition (where there is no attack in the system). The constant time headway is necessary for the input to the leader in unidirectional with constant time headway to form the error coordinate form. The last vehicle would be referred as the first vehicle and the leader would the n_{th} vehicle. i is the vehicle number. Model in absolute coordinates can be transformed into error coordinates by defining two new variables as spacing $z_i = x_{i+1} - x_i - d$ and $y_i = v_{i+1} - v_i$.

The equivalent state-space representation of the linear time-invariant (LTI) system for (1.2), (1.4) and (1.6) defined by (1.8).

$$\begin{aligned} \dot{\mathbf{x}} &= A_n\mathbf{x} + B_n\mathbf{u} \\ \mathbf{y} &= C_n\mathbf{x} \end{aligned} \tag{1.8}$$

Where $\mathbf{x} = [x_1,\ v_1,\ x_2,\ v_2,\ \cdots,\ x_n,\ v_n]^T \in \mathbb{R}^{2n}$ are the states of all the vehicles in the platoon, $A_n \in \mathbb{R}^{2n\times 2n}$, $B_n \in \mathbb{R}^{2n\times 1}$, $C_n \in \mathbb{R}^{2n\times 2n}$. C_n is the identity matrix (because it is assumed that all the vehicle states are measurable), B_n has non-zero entries corresponding to the leader, u_n, and $\mathbf{u} = [u_n]$, for the bidirectional and unidirectional with constant time headway. In leader-predecessor information flow, $B_n \in \mathbb{R}^{2n\times 2}$ has non-zero entries corresponding to the leader, u_n and desired velocity v_l, and $\mathbf{u} = [u_n\, V_l]^\intercal$.

The equivalent state-space representation of the linear time-invariant (LTI) system for (1.3), (1.5) and (1.7) defined by (1.9).

$$\begin{aligned} \dot{\mathbf{x}}_e &= A_e\mathbf{x}_e + B_e\mathbf{u} \\ \mathbf{y}_e &= C_e\mathbf{x}_e \end{aligned} \tag{1.9}$$

Where $\mathbf{x}_e = [z_1,\ y_1,\ z_2,\ y_2,\ \cdots,\ z_{n-1},\ v_{n-1}]^T \in \mathbb{R}^{2n-2}$ are the states of all the vehicles in the platoon, $A_e \in \mathbb{R}^{2n-2\times 2n-2}$, $B_e \in \mathbb{R}^{2n-2\times 1}$, $C_e \in \mathbb{R}^{2n-2\times 2n-2}$. C_e is the identity matrix (because it is assumed that all the vehicle states are measurable), B_e has non-zero entries corresponding to the leader, u_n, and $\mathbf{u} = [u_n]$ for the bidirectional and unidirectional with constant time headway. In leader-predecessor information flow $B_e \in \mathbb{R}^{2n-2\times 2}$ has non-zero

entries corresponding to the leader, u_n and desired velocity v_l, and $\mathbf{u} = [u_n \, v_l]^\intercal$.

1.2 Vehicular Communication network

The information required in each control scenario is provided via onboard sensing like (Radar/Lidar, Camera and Global Positioning System (GPS)) or vehicular communication. A key enabling technology of Intelligent Transportation System (ITS) is wireless communication, covering Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Vehicle (I2V) communications. Collectively, these wireless transactions are referred to as Vehicle-to-everything (V2x) communication are relied on the band of 5.9 GHz ($5.85 - 5.925$GHz).

V2x communication, which involves vehicles exchanging data with each other and the infrastructure for the initial purpose of driver awareness, disseminate warnings and provide real-time traffic information which are well aligned with the capabilities of the technology and has proven to improve traffic safety and increase the efficiency of transportation systems [72]. IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication system and it defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent ITS applications. IEEE 802.11p was designed, from the beginning, to meet every V2x application requirement with the most stringent performance specifications. In 1999, the U.S. Federal Communications Commission (FCC) set aside 75 MHz of bandwidth, in the 5.9 GHz region, for V2x, and the IEEE 802.11p standard operates within this range [84].

United States, Europe, and Japan are the main countries that proposed protocols for standardization landscape for wireless vehicular communication. Dedicated Short Range Communications (DSRC), which is based on IEEE 802.11p, has been the subject of extensive standardization, product development and field trials by many providers, proving its benefit for V2x after it was granted in 2009. Each DSRC-equipped vehicle broadcasts its basic state information, including location, speed, and acceleration, several times per second over a range of a few hundred meters. Each vehicle also receives these safety messages from DSRC-equipped neighbors. A receiving vehicle uses these messages to compute the

trajectory of each neighbor, compares these with its own predicted path, and determines if any of the neighbors poses a collision threat. In addition to V2V communication, vehicles may also communicate to and from DSRC roadside units (RSUs) using safety messages and other types of message. Examples of information a vehicle may learn from an RSU include: the geometry of an approaching intersection, the state of the signals at an intersection, and the existence of a hazard (e.g., disabled vehicle, emergency vehicle, ice, fog). The protocol stack for DSRC communication are briefly pointed out as follows: at the PHY and MAC layers DSRC utilizes IEEE 802.11p Wireless Access for Vehicular Environments (WAVE), a modified version of the familiar IEEE 802.11 (WiFi) standard. In the middle of the stack DSRC employs a suite of standards defined by the IEEE 1609 Working Group: 1609.4 for Channel Switching, 1609.3 for Network Services (including the WAVE Short Message ProtocolVWSMP), and 1609.2 for Security Services. DSRC also supports use of well-known Internet protocols for the Network and Transport layers, i.e., Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). These protocols, defined by the Internet Engineering Task Force (IETF) [88]. Meanwhile in Europe, they adopt ITS-G5 which like DSRC, operates in the 5.9 GHz band. European spectrum allocation is sub-divided into part A to D like ITS-G5A with 30 MHz for safety and traffic efficiency applications, ITS-G5B has 20 MHz for non-safety application. DSCR and ITS-G5 are sharing the same key technology features of IEEE-802.11 for the purpose of compatibility [58].

The network formed by 802.11p compliant devices is known as VANET (Vehicular Adhoc NETwork) a subclass of Mobile Ad Hoc NETworks (MANETs). Vehicles in VANET must be equipped with some sort of radio interface or OnBoard Unit (OBU) that enables short-range wireless ad hoc networks to be formed. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. VANET allows the cars to connect to each other in 100 to 300 meters distant. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication [144].

Although the works are numerous, there are still issues which may be untouched. Specifically the security aspects of the VANET was not considered at the time of standardization.

1.3 Related Works on Security issues in Platooning

Considering a vehicular platoon as the cyber-physical system, the platoon faces security challenges like identifying threats and their countermeasures. Vehicle platoon can be compromised from different aspects such as control and communication. There are many research works investigating vulnerabilities in a platoon which mostly involve communication and network layer threats. The authors in [83] and [1] present complete surveys on attacks that had been performed on communication links. In [3] counted attacks in 5 categories due to their threat to Availability, Confidentiality, Data integrity, Authentication and Non-repudiation where each issue and existent attacks in each domain studied in detail. Authors address accessibility of information at any time to only designated group of users as availability and confidentiality. Data integrity ensures the accuracy and consistency of data from source to endpoint. Authentication as the first line of defense in security would check for the trusted identity. Non-repudiation is the service which ensures that the sending and the receiving parties of the data cannot deny its transmission and reception in the case of dispute. One of most important attack on the network layer, denial of service (DOS) attack is studied in [73] which compromise the availability of the data over the network. Also, authors propose practical countermeasures to secure the VANET and solve the problem causing by attacks. some threats to privacy in VANETs are discussed in [54]. Furthermore, it was pointed out that the degree of privacy depends on user preferences, environmental settings, and application requirements and should therefore be adjustable. [71] identifies internal and external threats to and vulnerabilities of autonomous vehicles in order to identify cyber attacks and countermeasures using a risk management approach. [50] designed a set of insider attacks and abnormal behaviors that occur in a platoon of cars exploiting controller and proposed model-based detection scheme by comparing DSRC (Dedicated Short Range Communications) messages and expected behavior where

switches to non-cooperative ACC (Adaptive Cruise Control), relying solely on radar, to mitigate the impact of the attack. Effects of security attacks on the communication channel as well as sensor tampering of a connected vehicle stream equipped to achieve CACC (Cooperative Adaptive Cruise Control) is studied in [2] and downgrading to ACC mode is proposed as a potential countermeasure. [70] analyzes the effect of the wireless jammer on the stability and the performance of vehicles in a platoon using a specific distributed control algorithm. [28] proves that attacker can create instability or oscillation in platoon using unstable gains. Active and passive attacks against the system are presented in [55] where some members act in a malicious manner with the intent of destabilizing traffic flow. Mitigation algorithm based on modifying an existing control scheme after attack detection to sliding mode control proposed in [121]. The authors in [26] demonstrate their proposed fractional based controller can prevent collisions and oscillation resulting from the attack.

Within the broader work on the security of cyber-physical systems (CPS), the authors of [12] mention that CPSs are uniquely vulnerable to an attack that causes the system to resonate (become unstable), which is one of the goals of the attacker (the other being to wrest control of the platoon from the leader). They do not, however, describe an exact mechanism for carrying out the attack (other than sensor or controller compromise), as such an attack is specific the particular CPS under consideration. Barreto et al. [4] analyzed how an attacker could affect a system, in terms of controllability and stability, when given control over actuators and sensors.

Comparing to a large body of work accomplished in security in cyber physical systems, little amount was specified to security of platoon from control perspective [23,28,50,55,121]. As the control system is a vital part to platooning and automated vehicles, identifying the drawbacks and improving the resilience of this system seems very crucial. Platoon attacks and mitigation algorithm till this date are considered to be model dependent [55] and [50] and lack generality. [8] proposed false data injection attack does not seem quite effective due to attackers limitation which makes the analysis of the attackers' ability and evaluating the efficiency of the attack essential.

1.4 Significance of security in platooning, Contribution and Objectives

The daily increase in the number of vehicles traveling in highways and severity of the injuries and fatalities by accidents, create a strong motivation for platoon formation. Vehicular platooning is in developing phase. Several new applications are enabled by this new technology. A brief overview of the control algorithm and vehicular network that are involved in platooning are described in previous sections. However, as these applications have impact in road traffic safety, strong security requirements must be achieved. Security of platooning should be maintained in the highest level to protect lives of thousands of passengers traveling in vehicles involving in a platoon. New mechanisms have to be developed to deal with the inherent features of vehicles formation for safe and secure performance. Several sources state security as the top concern in platoon realization [9, 77, 119]. In order to guarantee the reliable performance of platooning, the threats to the system should be identified and resiliency against all adversities should be enhanced. The purpose of this work is to emphasize that, apart from typical security needs (e.g. confidentiality), there are other context-specific ones (e.g. trust assurance over reported data and algorithms modification), which require robust secure algorithms. Therefore, the contribution of this work can be highlighted as potential challenges in autonomous vehicles platooning along with fortifying algorithm which equally serve the security of platooning. The focus of this study is provided as follows:

- Identifying threats to vehicle platooning control and vehicular network; where we identify the vulnerability in the platooning control system and devise the destabilizing attack for these systems.

- Investigating the impacts and limitations of the attacker in the platoon; where two types of attacks, motion modification and integral attacks, are compared in terms of their impact on platoon and the severity of the damages caused to the platoon under the attack.

- Detection method utilizing system identification methods and anomaly detection is applied to the platoon under the attack in order to locate the attacker(s) in the

platoon.

- Mitigation scheme based on fractional order calculus is proposed to suppress malicious behavior of the attacker compromising the platoon.

It has been detailed that the cybersecurity of autonomous vehicle platooning and their supporting infrastructure is at risk due to security attack on the application layer, network layer, system level, and privacy leakage attack and identifying vulnerabilities seems to be crucial for this flourishing industry. When identified and analyzed, threats and vulnerabilities can be controlled by characterizing countermeasures to ensure that the associated risks and their potential impacts following attacks are mitigated to an acceptable level. The works presented in this dissertation are presented in:

"Dadras, S., Gerdes, R. M., and Sharma, R. (2015, April). Vehicular platooning in an adversarial environment. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 167-178). ACM."

"Dadras, S., Dadras, S., and Winstead, C. (2018, June). Reachable Set Analysis of Vehicular Platooning in Adversarial Environment. In 2018 Annual American Control Conference (ACC) (pp. 5568-5575). IEEE."

"Dadras, S., Dadras, S., and Winstead, C. (2018, June). Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment. In 2018 Annual American Control Conference (ACC) (pp. 5560-5567). IEEE."

"Dadras, S., Dadras, S., and Winstead, C. Resilient Control Design for Vehicular Platooning in an Adversarial Environment. In 2019 Annual American Control Conference (ACC) IEEE."

1.5 Outline of The Dissertation

This dissertation is organized to cover the security of vehicle platooning from attack and defense perspectives. In the two chapters following the introductory chapter, Chapter 2 and Chapter 3, the attacks on stability and string stability of the platoon are formulated and the attacker's capability to drive the platoon to its desired states and create catastrophic

impacts on other vehicles during the attack under input constraint is studied. In Chapter 4, an effective algorithm to detect the attacker in the platoon in the adversarial environment is proposed. In Chapter 5, resilient control is designed to defend the victims in the event of the attack. Finally, the summary of the results and the possible future direction of the research are presented in Chapter 6.

CHAPTER 2

Platoon Stability and String Stability

2.1 Background and Contribution of This Work

The vehicular platooning concept, wherein a group of vehicles act as a single unit through coordination of movements, dates back to at least the 1970s [80], and rose to prominence in the U.S. during the 1990s with the California Partners for Advanced Transit and Highways (PATH) program [127]. It continues to be of interest to academics, governments, and industry [6, 74, 98], and has seen several recent demonstrations [17, 128], in no small part because of its potential benefits, which include increases in safety, roadway capacity, and efficiency [11, 49, 61].

While many aspects of platooning are active areas of research, e.g. transportation impacts, mechanical and control concerns [5, 87, 89], comparatively little work has examined platooning in an adversarial environment. In fact, there are only few such works: [70] examined platooning under the effects of jamming. In this work,it is considered an attacker seeking to destabilize or take control of a platoon through purely local modifications to the control system of the vehicle under their control. The analysis shows that the primary design criterion of platooned systems (stability) can be violated by such means, and that catastrophic accidents, more severe than simply ignoring the control laws, can be effected.

A critical characteristic of vehicle platoons is that they be *string stable*. In the case of a homogeneous platoon of vehicles (i.e. all vehicles have the same performance characteristics), string stability guarantees system stability [18] and, in the absence of particular inflows/outflows, the prevention of traffic flow instability [47, 139]. As it is shown, it is possible for a malicious actor to induce both instability and string instability and, if perpetrated on a large enough scale, it can create traffic flow instability.

An important distinction is also made as to the roles of vehicles in a platoon. Generally,

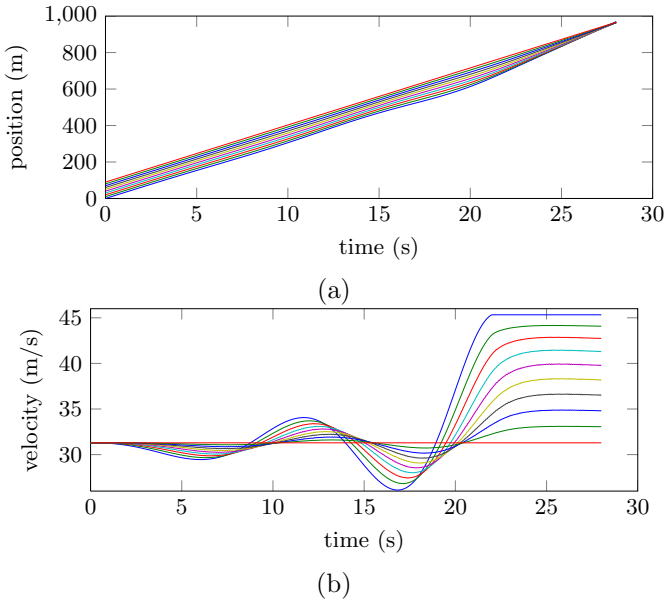


Fig. 2.1: Position and velocity of a platoon under attack. An attacker in the last position leverages instability to cause the platoon to crash into the leader at heightened velocities (time of impact ≈ 27 s).

a platoon will have a leader that is responsible for setting the trajectory and speed of the vehicles behind it. The following vehicles (followers) share a common control algorithm that prescribes how they are to react to perturbations in steady-state operation (e.g. the leader speeding up or slowing down). In this work, the extent to which a malicious actor in control of the following vehicle could subvert the role of the leader and, even more disconcertingly, control the movements (state) of other followers, to an arbitrary degree, are examined.

Finally, while the majority of this work focuses on analyzing the attack against a single controller (proportional-derivative) employed with the particular platooning algorithm (bidirectional), the demonstrated attack is general enough to be applicable to a wide variety of controllers/algorithms. To justify this supposition, it is shown how a non-linear controller, based on sliding mode control, when used with a unidirectional platooning algorithm, can be manipulated to produce similar unstable behavior that can be utilized by an attacker. What attack conveys is that control system designers must consider the possibility that vehicles may attempt to actively undermine the operation of a platoon by targeting the control strategy.

2.1.1 Motivating example

While system instabilities are generally catastrophic, an attacker could also leverage instabilities to target vehicles, in a controlled manner, for crashes with effects far greater than if the instability were not employed. For example, an attacker at the rear of a platoon who wishes to target the leader could simply ignore the control law governing the platoon and accelerate, which would indeed cause preceding vehicles to crash into the leader. The severity of the accident will depend on the relative velocities of the vehicles, with respect to the leader, at the time of impact. However, to maximize relative velocity, the attacker could instead introduce instability and then cause the vehicles to oscillate at the resulting resonant frequency. Each subsequent period of the oscillation will cause the followers to brake more and accelerate more (increasing/decreasing their maximum/minimum velocity). Before the vehicles have crashed into the leader, and while they are at their maximum velocity, the attacker need only stop accelerating to have the other followers maintain their heightened velocities as they crash into the leader (Figure 2.1). It has been found that the mean relative velocities when the attacker leverages instability can be 60% greater than when the attacker simply accelerates, while the kinetic energy at the time of impact can be 160% higher.

2.1.2 Related work

Within the platooning literature, the work that comes closest to examining platooning in an adversarial environment concerns the stability/string stability of heterogenous platoons [125]. In [56, 124], controllers were proposed to maintain the string stability/stability of heterogeneous platoons; however, these controllers were designed without considering the actions of malicious actors. In particular, they assume that vehicles will adhere to the strictures of the control law and that the information provided by vehicles is genuine. Thus, they are unlikely to be able to maintain the integrity of a platoon in the presence of an attacker. The aforementioned work also showed that, in the heterogeneous case, stability does not necessarily imply string stability. Furthermore, it is shown that in the adversarial case neither is implied by the other; i.e. it is possible to have a platoon that is string stable but not stable or one that is stable but not string stable.

Within the broader work on the security of cyber-physical systems (CPS), the authors of [12] mention that CPSs are uniquely vulnerable to an attack that causes the system to resonate (become unstable), which is one of the goals of the attacker (the other being to wrest control of the platoon from the leader). They do not, however, describe an exact mechanism for carrying out the attack (other than sensor or controller compromise), as such an attack is specific the particular CPS under consideration. It has been shown how such an attack could be effected against a platoon by an attacker in control of only a single vehicle. Barreto et al. [4] analyzed how an attacker could affect a system, in terms of controllability and stability, when given control over actuators and sensors. This attack differs in that an attacker alters the state matrix directly and can only know/modify their own control input (though they needn't necessarily use it to carry out the attack).

This attack vector bears some resemblance to an insider version of the replay attack of [114], in that the attacker is part of the CPS and is, therefore, able to inject control inputs legitimately, though the attacker does not need to gain control of sensors to carry out the attack. A single autonomous vehicle was destabilized using a variant of the replay attack that used false-data injection (FDI) in [108]. This attack is effected through malicious vehicle movement/response and FDI is unnecessary.

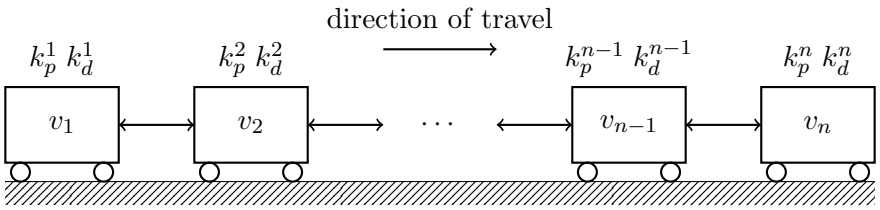
Finally, to the best of author's knowledge, the formalism used to model the attacker was first proposed in [113] to define misbehaving agents in consensus networks. The attack is also unidentifiable in the sense of [113].

2.2 Platoon and threat models

The platooning law of the system under investigation, the rationale for selecting it, and the capabilities and goals of the attacker formally are described.

2.2.1 Platoon model

The analysis focuses on exploiting longitudinal control laws for platooning, which are intended to maintain the separation/velocity of vehicles in a platoon as they follow a straight line. While it may be possible to exploit lateral control laws, too, longitudinal control



(a)

platoon size	3	4	5	6
$k_d \geq$	2.1	2.7	3.3	4.2
platoon size	7	8	9	10
$k_d \geq$	5.1	6	7	7.7

(b)

Fig. 2.2: (a) An n-vehicle platoon employing a bi-directional control law. Arrows represent the flow of information. (b) The minimum derivate gains necessary to guarantee string stability ($k_p = 1$).

represents an inherently coupled system (a CPS), where the movements of one vehicle have the potential to influence others.[1] In addition, vehicles with longitudinal control (in the form of adaptive cruise control) are available from all major auto manufacturers. Thus, it is considered a straight, dedicated platooning lane with a platoon traveling at a constant velocity. All of the vehicles in the platoon are assumed to share the same performance characteristics (i.e. the platoon is homogenous); nonlinearities in vehicle performance can be linearized through feedback linearization techniques [81].

Following the reasoning set forth at the end of the Introduction, of the dozen of control laws available [87, 89], a platooning law that is simple enough for straightforward analysis and presentation is selected, but also has several characteristics deemed desirable by the platooning community. Specifically, the bi-directional (predecessor-follower) proportional-derivative (PD) controller of [142] is used to demonstrate the catastrophic effect a malicious actor can have on platooning operations. This control law is capable of maintaining a constant separation, d, between vehicles, based solely on local sensing. This is important

[1] Even in the case of strictly autonomous vehicles, a control law is needed to maintain separation between vehicle. Thus, a string of such vehicles, employing the same control law, could become coupled in a platoon-like manner.

because it allows us to show that an attacker can affect the platoon solely through malicious movement and needn't rely on interfering with communication between vehicles, as in [70].

Formally, the dynamics of a platoon with n vehicles (Figure 5.1) employing this control law are described by the following system of equations

$$
\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= -k_p^1 x_1 + k_p^1 x_2 - k_p^1 d - k_d^1 v_1 + k_d^1 v_2 \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= k_p^2 x_1 - k_p^2 x_2 + k_p^2 d + k_p^2 x_3 - k_p^2 x_2 - k_p^2 d \\
&\quad + k_d^2 v_1 - 2k_d^2 v_2 + k_d^2 v_3 \\
&\vdots \\
\dot{x}_{n-1} &= v_{n-1} \\
\dot{v}_{n-1} &= k_p^{n-1} x_{n-2} - k_p^{n-1} x_{n-1} + k_p^{n-1} d + k_p^{n-1} x_n - k_p^{n-1} x_{n-1} \\
&\quad - k_p^{n-1} d + k_d^{n-1} v_{n-2} - 2k_d^{n-1} v_{n-1} + k_d^{n-1} v_n \\
\dot{x}_n &= v_n \\
\dot{v}_n &= k_p^n x_{n-1} - k_p^n x_n + k_p^n d + k_d^n v_{n-1} - k_d^n v_n + u
\end{aligned}
\tag{2.1}
$$

where x_i and v_i represent the position and velocity, respectively, of the i^{th} vehicle ($\dot{a}$ denotes the first derivative with respect to time of the variable a) and k_p^i and k_d^i represent their proportional and derivate gains. For normal platooning operations k_p^i and k_d^i are the same for each vehicles (Thus, it is dispensed with the superscript unless referring to the gains for a vehicle in a particular position). k_p is traditionally fixed at one, while k_d varies according to the size of the platoon (Figure 2.2b). Here, u represents the control input for the leader (the n^{th} vehicle). In the steady-state u is generally taken to equal zero; however, it is noted that $k_p^n \neq 0$ and $k_d^n \neq 0$ implies that the followers would be able to influence the leader's movements, unless u is set to cancel out the follower movements, which would effectively set $k_p^n = k_d^n = 0$. In any case, from the security perspective, it seems inadvisable for followers to be able to influence the leader. This ambiguity is of consequence for the controllability

analysis (Section 2.4).

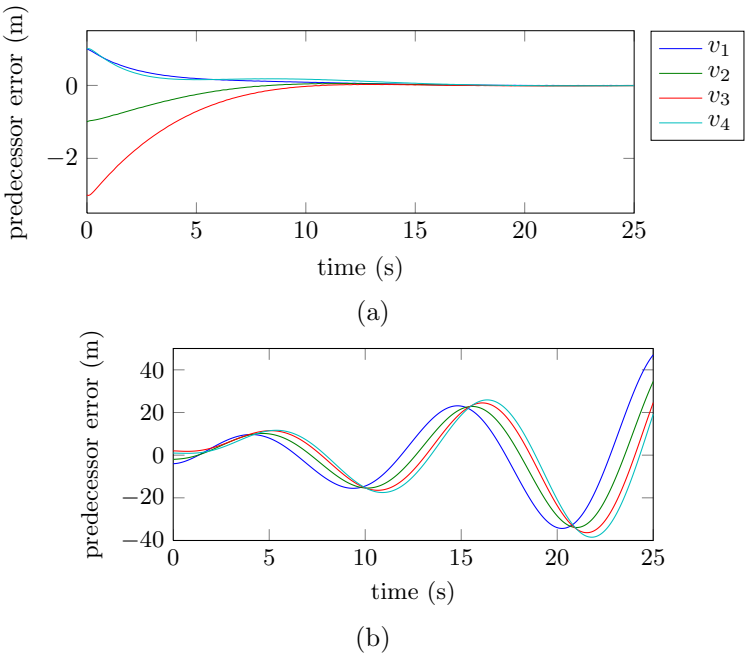


Fig. 2.3: The position error between a vehicle and its predecessor due to initial differences in spacing and velocity for a five vehicle platoon. When the platoon is (a) stable the error reduces to zero, but when (b) unstable the error growth is unbounded.

2.2.2 Threat models

It is examined the case of a single actor in control of a vehicle within an already established platoon, traveling at a constant speed, who attempts to destabilize (Section 2.3) or take control (Section 2.4) of the platoon. In the context of the present work, the attacker may accomplish this by causing the vehicle under their control to subvert or ignore the control law established for maintaining follower separation. This implies that the controller gains of the attacker's vehicle could be modified and should movement in one direction be prescribed by the control law, the vehicle is free to ignore it. The attacker's vehicle is taken to have exactly the same capabilities as the other vehicles in the platoon.

Because it is desired to demonstrate that an attacker is capable of disrupting/controlling platooning operations without being assigned nominal control of the platoon, it is assumed

that the attacker does not act as the leader of the platoon. It is noted, however, that because of the symmetry of the control law (Equation 5.1), any influence that the first vehicle in the platoon is able to effect could be carried out by the leader.

The equivalent state-space representation of the linear time-invariant (LTI) system defined by (5.1) in the presence of an attacker is

$$\begin{aligned} \dot{\mathbf{x}} &= A\mathbf{x} + B\mathbf{u} \\ \mathbf{y} &= C\mathbf{x} \end{aligned} \tag{2.2}$$

where $\mathbf{x} = [x_1,\ v_1,\ x_2,\ v_2,\ \cdots,\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the states of all the vehicles in the platoon, $A \in \mathbb{R}^{2n\times 2n}$, $B \in \mathbb{R}^{2n\times 2}$, $C \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{u} = [u_l\, u_a]^\intercal$. C is the identity matrix (because it is assumed that all the vehicle states are measurable), B has non-zero entries corresponding to the leader and the attacker control, u_l and $u_a = a\sin\omega t$, respectively, where a is the amplitude of the attacker's input and ω is the frequency at which the input oscillates.

The goals and methods of the attacker may be stated formally as: 1) to introduce instability/string instability by modifying the entries in A controlled by the attacker so as to produce instability and then realize a $u_a = a\sin\omega t$ to affect the instability, and 2) to control the platoon by selecting the entries in A and B under their influence to make the system controllable and then derive a controller for u_a that allows them to move the system to the desired state.

2.3 Platoon stability

The stability of an LTI system (5.2) is given by [13]:

Definition 2.3.1 (Marginal and Asymptotic Stability) *The homogeneous LTI system* $\dot{\mathbf{x}} = A\mathbf{x}$ *is said to be marginally asymptotically stable if, for every initial condition* $\mathbf{x}(t_0) = \mathbf{x}_0$*, the homogeneous state-space response* $\mathbf{x}(t) = \Phi(t, t_0)\mathbf{x}_0,\ \ \forall t \geq 0$*, where* $\Phi(t, t_0)$ *is the state transition matrix, is uniformly bounded. The system is asymptotically stable if* $\mathbf{x}(t) \Rightarrow 0$ *as* $t \Rightarrow \infty$.

The homogeneous LTI system is both marginally and asymptotically stable if all the eigenvalues of A have negative real part [13].

Definition 2.3.2 (BIBO Stability) *The homogeneous LTI system (5.2) is said to be bounded input bounded output (BIBO) stable if every bounded input* $\mathbf{u}$ *has a bounded forced response* y.

If a system is asymptotically stable (i.e., if all the eigenvalues of A have a negative real part) then the system is (BIBO) stable [13]. Figure 2.3 shows the response of a five vehicle platoon to initial errors in spacing and velocity when the platoon is asymptotically stable (Figure 2.3a) and unstable (Figure 2.3b).

In what follows, it is proved that by modifying the derivative gain of a single vehicle under their control and applying a sinusoidal acceleration, an attacker can produce both instability and string instability in a platoon. The range of gains and the frequencies corresponding to the resultant unstable modes are discussed.

As per [142], it is assumed that non-attacker (victim) vehicles select the same set of gains, k_p and k_d, chosen based on platoon size, to ensure stability. It is denoted the attacker derivative gain as $\tilde{k}_d$; the attacker uses the same proportional gain as the rest of the vehicles in the platoon.

2.3.1 String instability

The stability/string stability condition in the homogeneous case states that spacing errors between vehicles should attenuate as they move upstream. Allowing $z_i = x_i - x_{i+1}$ to represent the spacing error between the i^{th} and i^{th}+1 vehicles, the string stability criterion may be stated as [142]

$$|G_i(s)| = \left| \frac{z_i}{z_{i+1}} \right| < 1 \text{ for } i = 1, \ldots, n-2 \tag{2.3}$$

where $s = \jmath\omega$ and ω is the angular frequency. $|G_i(s)|$ represents the magnitude of the (error) transfer function between the i^{th} and i^{th}+1 vehicles. The transfer function varies according to the relative position of the vehicles and their gains; thus the effects of an

attacker changing their gain, in an attempt to violate (2.3), will depend upon the relative position of the attacker. To understand the attacker's impact requires that it is derived the form of the transfer function for an attacker at each possible position. The requisite derivation for an attacker at the first position is performed here and then simply provide the expressions for the remainder of the positions.

Transfer function derivation

To aid in this task, first the system dynamics given in (5.1) is transformed to error coordinates

$$\begin{aligned} z_1 &= x_1 - x_2 \\ y_1 &= \dot{z}_1 = v_1 - v_2 \\ z_2 &= x_2 - x_3 \\ y_2 &= \dot{z}_2 = v_2 - v_3 \\ &\vdots \\ z_{n-2} &= x_{n-2} - x_{n-1} \\ y_{n-2} &= \dot{z}_{n-2} = v_{n-2} - v_{n-1} \\ z_{n-1} &= x_{n-1} - x_n \\ y_{n-1} &= \dot{z}_{n-1} = v_{n-1} - v_n \end{aligned} \tag{2.4}$$

The resulting equations in error coordinates for an attacker at the first position are then

$$\begin{aligned} \dot{z}_1 &= y_1 \\ \dot{y}_1 &= -2k_p z_1 + k_p z_2 - (k_d + \tilde{k}_d) y_1 + k_d y_2 \end{aligned}$$

$$
\begin{aligned}
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= k_p z_1 - 2k_p z_2 + k_p z_3 + k_d y_1 - 2k_d y_2 + k_d y_3 \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= k_p z_{n-3} - 2k_p z_{n-2} + k_p z_{n-1} \\
&\quad + k_d y_{n-3} - 2k_d y_{n-2} + k_d y_{n-1} \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= k_p z_{n-2} - 2k_p z_{n-1} + k_d y_{n-2} - 2k_d y_{n-1} + u
\end{aligned}
\tag{2.5}
$$

To find $|G_1(s)| = \left|\frac{z_1}{z_2}\right|$ is transformed that

$$
\begin{aligned}
&\dot{y}_1 = z_2 - 2z_1 + k_d y_2 - (\tilde{k}_d + k_d) y_1 \\
&\Rightarrow \ddot{z}_1 = z_2 - 2z_{n-1} + k_d \dot{z}_2 - (\tilde{k}_d + k_d)\dot{z}_1 \\
&\Rightarrow s^2 z_1 + s(\tilde{k}_d + k_d) z_1 + 2z_1 = z_2 + k_d s z_2 \\
&\Rightarrow (s^2 + s(\tilde{k}_d + k_d) + 2) z_1 = (1 + k_d s) z_2
\end{aligned}
$$

which results in

$$
|G_1(s)| = \left|\frac{z_1}{z_2}\right| = \left|\frac{1 + k_d s}{s^2 + s(\tilde{k}_d + k_d) + 2}\right| \tag{2.6}
$$

Similarly, for $|G_2(s)| = \left|\frac{z_2}{z_3}\right|$

$$
\begin{aligned}
&\dot{y}_2 = z_3 - 2z_2 + z_1 + k_d y_3 - 2k_d y_2 + k_d y_1 \\
&\Rightarrow \ddot{z}_2 = z_3 - 2z_2 + z_1 + k_d \dot{z}_3 - 2k_d \dot{z}_2 + k_d \dot{z}_1 \\
&\Rightarrow s^2 z_2 + 2k_d s z_2 + 2z_2 = z_3 + k_d s z_3 + z_1 + k_d s z_1 \\
&\Rightarrow (s^2 + 2k_d s + 2) z_2 = (1 + k_d s) z_3 + (1 + k_d s) z_1 \\
&\Rightarrow (s^2 + 2k_d s + 2) z_2 = (1 + k_d s) z_3 \\
&\quad + (1 + k_d s) \frac{1 + k_d s}{s^2 + s(\tilde{k}_d + k_d) + 2} z_2 \\
&\Rightarrow (s^2 + 2k_d s + 2 - (1 + k_d s) \frac{1 + k_d s}{s^2 + s(\tilde{k}_d + k_d) + 2}) z_2 \\
&\quad = (1 + k_d s) z_3
\end{aligned}
$$

yields

$$
|G_2(s)| = \left|\frac{z_2}{z_3}\right| = \left|\frac{\frac{1+k_d s}{s^2+2k_d s+2}}{1 - \frac{1+k_d s}{s^2+2k_d s+2} G_1}\right| \tag{2.7}
$$

to simplify the transfer functions it is defined

$$
\begin{aligned}
g_1 &= \frac{1 + \tilde{k}_d s}{s^2 + s(\tilde{k}_d + k_d) + 2} \quad g_2 = \frac{1 + k_d s}{s^2 + s(\tilde{k}_d + k_d) + 2} \\
g_3 &= \frac{1 + k_d s}{s^2 + 2k_d s + 2}
\end{aligned}
$$

$|G_3(s)|$ to $|G_{n-2}(s)|$ follow a similar pattern as $|G_2(s)|$; thus, the transfer functions for the platoon when an attacker is in the first position may be stated as

$$
\begin{aligned}
&|G_1(s)| = |g_2|, |G_2(s)| = \left|\frac{g_3}{1 - G_1 g_3}\right|, \cdots, \\
&|G_i(s)| = \left|\frac{g_3}{1 - G_{i-1} g_3}\right|, \cdots, |G_{n-2}(s)| = \left|\frac{g_3}{1 - G_{n-3} g_3}\right|
\end{aligned} \tag{2.8}
$$

The reader is refered to [27] for the definitions of the transfer functions for the remaining attacker positions.

String instability analysis

To violate the string stability condition an attacker must select a gain, $\tilde{k}_d$, such that the inequality of (2.3) is reversed. Even though the attacker gain may appear in more than one transfer function, the attacker need only cause a single $|G_i(s)| = \left|\frac{z_i}{z_{i+1}}\right| > 1$ to breach the stability criterion. In what follows is the demonstration of how an attacker in the first position should select their gain to achieve this; Then an algorithm that generalizes the procedure for the remaining positions is offered.

Beginning from the analysis given above, it has been shown

$$|G_1(s)| = \sqrt{\Re(G_1)^2 + \Im(G_1)^2} \tag{2.9}$$

where $\Re(\cdot)$ and $\Im(\cdot)$ denote the real and imaginary parts, respectively, of $G_1(s)$. Considering each separately, it has been shown

$$\begin{aligned} \Re &= \frac{(-1 + k_d\tilde{k}_d + (k_d)^2)w^2 + 2}{w^4 + w^2((k_d)^2 + (\tilde{k}_d)^2 + 2k_d\tilde{k}_d - 4) + 4} \\ \Im &= \frac{(-k_d w^3 + w(k_d - \tilde{k}_d))}{w^4 + w^2((k_d)^2 + (\tilde{k}_d)^2 + 2k_d\tilde{k}_d - 4) + 4} \end{aligned} \tag{2.10}$$

The attacker wishes to satisfy $\sqrt{\Re(G_1)^2 + \Im(G_1)^2} > 1$. Using (2.10) this condition is transformed as

$$\alpha(\tilde{k}_d)^2 + \beta(\tilde{k}_d) + \gamma > 0 \tag{2.11}$$

where $\alpha = 1$, $\beta = 2k_d$ and $\gamma = \dfrac{w^4 - 4w^2 + 3}{w^2}$. To make (2.11) greater than zero for some value of $\tilde{k}_d$ requires that $\Delta = \beta^2 - 4\alpha\gamma > 0$, which results in

$$(k_d)^2 > \frac{w^4 - 4w^2 + 3}{w^2} \tag{2.12}$$

Thus, to make the system string unstable an attacker should choose a $\tilde{k}_d$ that lies between the roots of (2.12); i.e. $k_d - \sqrt{(k_d)^2 - \frac{w^4-4w^2+3}{w^2}} < \tilde{k}_d < k_d + \sqrt{(k_d)^2 - \frac{w^4-4w^2+3}{w^2}}$. It is noted that if k_d is selected such that $(k_d)^2 < \frac{w^4-4w^2+3}{w^2}$ the system is string stable and cannot be made string unstable. However, a k_d smaller than the minimum values given in Figure 2.2b

would compromise string stability for other vehicles, and furthermore, as it has been shown in Section 2.3.2, small values of k_d make it easier for an attacker to destabilize the platoon.

Beyond an attacker in the first position, symbolic analysis becomes tedious. Therefore, an algorithm for numerically determining $\tilde{k}_d$ for a platoon of size n that uses a derivate gain of k_d, at a given ω (Algorithm 1) is proposed. The general procedure for an attacker at the i^{th} position is to evaluate the real and imaginary parts of the first transfer function, G_i, where $\tilde{k}_d$ appears and arrange the results into the form of (2.11). Table 2.1 provides the range of gains, as a function of attacker position, that make a ten vehicle platoon unstable for $\omega = \{\pi/4, \pi/2, \pi, 2\pi\}$. It is noted that, in general, the lower the frequency of string instability, the higher the attacker gain can be to effect it.

Algorithm 1: Finding the attacker gain to make the platoon string unstable.

Input : k_d, n and ω (a normal vehicle gain, platoon size, and frequency)
Output: $\tilde{k}_d$ (gain for the attacker which makes the platoon string unstable)
$i \leftarrow$ first transfer function affected by attacker;
$\alpha(\tilde{k}_d)^2 + \beta(\tilde{k}_d) + \gamma > 0 \leftarrow \Im(G_i)^2 + \Re(G_i)^2 > 1$;
$\Delta \leftarrow \beta^2 - 4\alpha\gamma$;
if $\alpha > 0$ *and* $\Delta > 0$ **then**
  $\tilde{k}_d$ should be chosen between $\frac{-\beta \pm \sqrt{\Delta}}{2\alpha}$;
else if $\alpha < 0$ *and* $\Delta > 0$ **then**
  $\tilde{k}_d$ should be chosen out of $\frac{-\beta \pm \sqrt{\Delta}}{2\alpha}$;
else if $\alpha < 0$ *and* $\Delta < 0$ **then**
  an attacker can not make the platoon string unstable;
else if $\alpha = 0$ **then**
  $\tilde{k}_d < \frac{-\gamma}{\beta}$;
else
  platoon is always string unstable;
end

2.3.2 Instability

An attacker can make the platoon asymptotically and BIBO unstable only by changing the eigenvalues of A (by making real part of at least one eigenvalue positive). First, it has

Table 2.1: Attacker gains to guarantee string instability for a ten vehicle platoon, with respect to attacker position and frequency. $\tilde{k}_d$ must be within the given intervals; $k_d = 7.7$.

ω \ position	1	2	3	4	5	6	7	8	9
2π	$> -12.59, < -2.81$	< -6.16	< -8.41	< -10.24	< -10.22	< -10.06	< -10.03	< -10.04	< -10.04
π	$> -15.03, < -0.37$	< -4.25	< -3.45	< -4.42	< -5.15	< -5.28	< -5.21	< -5.15	< -5.13
$\pi/2$	$> -15.58, < 0.18$	< -3.83	< -2.02	< -1.75	< -1.98	< -2.30	< -2.5	< -2.55	< -2.54
$\pi/4$	$> -15.92, < 0.52$	< -3.95	< -1.83	< -1.04	< -0.62	< -0.42	< -0.38	< -0.44	< -0.52

been proved that an attacker can introduce an instability into a platoon, and then show that this instability can be effected through malicious movements on the part of the attacker.

Attacker gain derivation

To prove that an attacker can cause a platoon to become unstable by changing its derivative gain (i.e. $\tilde{k}_d \neq k_d$), the error coordinates formulation given by (2.4) is used. For an n vehicle platoon, the state matrix, $A \in \mathbb{R}^{2(n-1)\times 2(n-1)}$, for the error coordinates will, however, depend on the position of the attacker.

The general form of A, in the absence of an attacker, is given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -2k_p & -2k_d \end{bmatrix} \tag{2.13}$$

Allow $A(i,j)$ to represent access to the element at the i^{th} row and j^{th} column of A. When an attacker is present at the first position, only $A(2,2) = -k_d - \tilde{k}_d$ of (5.3) needs to be changed. An attacker in the i^{th} position, $1 < i < n-1$, will change the following elements

of (5.3)

$$\begin{aligned} A(2(i-1),2(i-1)) &= -k_d - \tilde{k}_d,\ A(2(i-1),2i) = \tilde{k}_d \\ A(2i,2(i-1)) &= \tilde{k}_d,\ A(2i,2i) = -k_d - \tilde{k}_d \end{aligned} \tag{2.14}$$

When the attacker position is $i = n-1$, only $A(2(i-1),2(i-1)) = -k_d - \tilde{k}_d$ of (5.3) is changed.

lemma 1 *A platoon cannot be stable if the real part of a single eigenvalue of A is greater than zero. An attacker who selects a derivative gain $\tilde{k}_d < -k_d$ will cause A to have at least one eigenvalue with a positive, real part and therefore make the platoon unstable.*

proof 1 *The non-symmetric matrix A will necessarily have an eigenvalue with a positive, real component if an $x \in \mathbb{R}^{2(n-1)}$ can be found such that $x^\intercal Ax > 0$. The gains in the absence of an attacker are selected to ensure that the state matrix of (5.3) will produce $x^\intercal Ax < 0$ for every x and that the eigenvalues of (5.3) will have only negative, real components. Thus, for an attacker to create instability, the vector x must contain at least one element such that the product $x^\intercal Ax$ includes $\tilde{k}_d$.*

For an attacker in the first position $x = [0\ 1\ 0\ \cdots\ 0]^\intercal$ with $A(2,2) = -k_d - \tilde{k}_d$ are selected

$$x^\intercal Ax = A(2,2) = -k_d - \tilde{k}_d > 0 \Rightarrow \tilde{k}_d < -k_d \tag{2.15}$$

Similarly, for an attacker in the i^{th} position, $1 < i < n$, $x(2(i-1)) = 1$ with the remaining elements of x set to zero are selected and the modifications to A given by (2.14) (it is noted that that for $i = n-1$ only $A(2(i-1),2(i-1))$ is changed)

$$x^\intercal Ax = A(2(i-1),2(i-1)) = -k_d - \tilde{k}_d > 0 \Rightarrow \tilde{k}_d < -k_d \tag{2.16}$$

$\therefore \forall \tilde{k}_d < -k_d$ will make a platoon unstable, independent of the position of the attacker.

It is noted that the above analysis does not necessarily determine the maximum attacker gain that will result in instability. In fact, it gives a necessary rather than sufficient value

for the attacker gain; i.e. $\tilde{k}_d > -k_d$ may still produce instability. To find the maximum attacker gain, the gain margin of the characteristic equation for platoons of size $n = [3, 10]$, is calculated using attacker positions of $i = 1, \cdots, n-1$. Figure 2.4a gives the maximum attacker gains to produce instability, as a function of platoon size and attacker position.

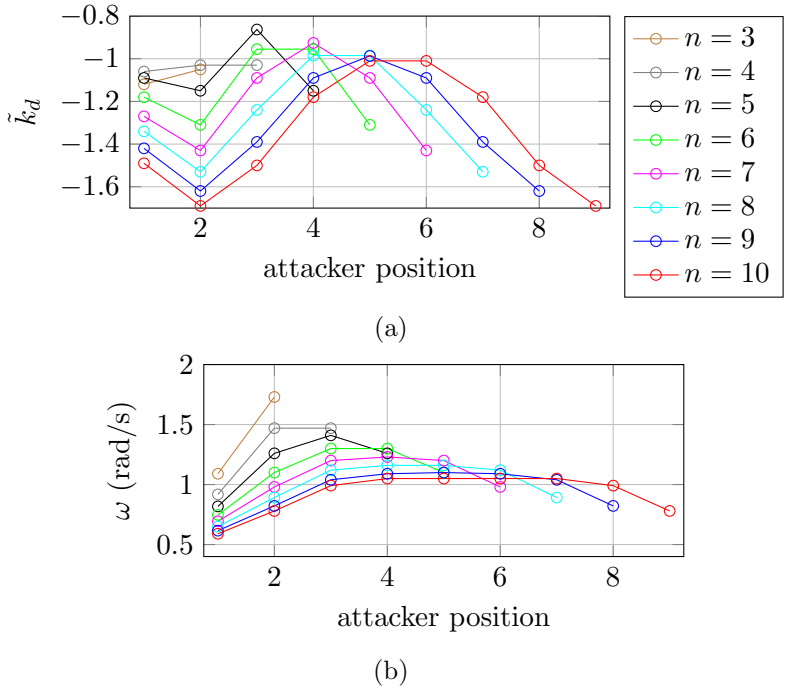


Fig. 2.4: (a) Maximum attacker gains that produce instability, as function of attacker position and platoon size, n. (b) The frequencies of instability corresponding to maximum attacker gains.

Frequency response of the platoon

It has been demonstrated that it is possible for an attacker, through judicious selection of their derivative gain, to cause a platoon to violate the stability criterion. It is not, however, sufficient for the system to contain a potential unstable mode: the attacker must be able to affect the instability through the movement of their vehicle (i.e. accelerate/brake in an oscillatory fashion). This requires that an attacker, in reference to (5.2), either realize a control input at the frequency of the instability ω or introduce a position/velocity error. In either case, the vehicles in the platoon must be capable of oscillating at ω. For the

attack to be feasible, it has been stipulated that the frequency of the instability be less than or equal to one hertz ($\omega \leq 2\pi$); also, this condition for string instability (Table 2.1) has been applied. Figure 2.4b gives the unstable frequency for the maximum attacker gain that causes instability, with respect to attacker position and platoon size, found in Section 2.3.2; at every position the attack is feasible. Figure 2.5 further demonstrates that an attacker can meet the feasibility constraint for a wide range gains, at every position in ten vehicle platoon (when an attacker gain resulted in multiple instabilities, the one with the highest frequency) is selected.

The exact response of the system to the instability introduced by the attacker may be calculated as follows. The solution of the LTI state-space system (5.2) with $u = a \sin \omega_t$ can be written as $\mathbf{x}(t) = \mathbf{x}_h(t) + \mathbf{x}_f(t)$, where $\mathbf{x}_h(t) = e^{At}\mathbf{x}_0$ is the zero-input or homogeneous solution and $\mathbf{x}_f(t) = a\alpha \sin(\omega_t + \phi)$ is the zero-state or forced response [13]. In the forced response α is the magnitude of the transfer function $\hat{g}(s) = C(sI - A)^{-1}B$, computed at $s = j\omega$, and ϕ is the phase angle of the transfer function, computed at $s = j\omega$. Referring to the stability conditions discussed earlier, it can be said that if all the eigenvalues of A have negative real parts, the homogeneous part $\mathbf{x}_h(t) \to 0$ and $\mathbf{x}(t)$ is then equal to the forced response $\mathbf{x}_f(t)$. In other words, the LTI system response oscillates with the attacker's frequency ω. The oscillations, in this case, are bounded, not fulfilling the attacker's objectives.

In order to create growing (unbounded) oscillations, the attacker has to change the eigenvalues of A (i.e. make the real part of at least one eigenvalue positive) by changing $\tilde{k}_d$, as shown in the previous section. Changing $\tilde{k}_d$ can result in two types of behavior, depending on the k_d used by the platoon.

1) *If the attacker selects $\tilde{k}_d < -k_d$ and k_d is near the minimum value given in Figure 2.2b* then in addition to making the real parts of up to two eigenvalues positive, imaginary parts to some of the remaining eigenvalues of A may also be introduced. This will result in oscillating $\mathbf{x}_h(t)$ with growing amplitude (caused by the negative damping introduced by the attacker) and with frequency $\omega_d = \omega_n\sqrt{1-\zeta^2}$ with growing amplitude, where ω_n is the

natural frequency of the platoon, and ζ is the damping coefficient. The natural frequency ω_n is the magnitude of the poles with an imaginary part. This implies that the time response of the platoon states, $\mathbf{x}(t) = \mathbf{x}_h(t) + \mathbf{x}_f(t)$, is the sum of two signals oscillating at two different frequencies ω_d and ω and that the amplitude of the oscillations grows with time.

2) *If the attacker selects $\tilde{k}_d < -k_d$ and k_d is much greater than the minimum value given in Figure 2.2b* then, unlike the above scenario, the attacker is only able to make the real parts of up to two eigenvalues positive, but not introduce imaginary parts to any eigenvalues of A. This will result in exponentially growing $\mathbf{x}_h(t)$ (caused by the negative damping introduced by the attacker) without any oscillations. This implies that the time response of platoon states, $\mathbf{x}(t) = \mathbf{x}_h(t) + \mathbf{x}_f(t)$, grows with time and oscillates at the attacker's frequency ω.

2.3.3 Comparing string stability and stability

In the case of a homogeneous platoon, string stability (SS) will ensure stability (S); however, in the adversarial case, neither implies the other. To prove that $SS \not\Rightarrow S$ and $S \not\Rightarrow SS$, it is sufficient to find one example in which the system is stable but not string stable and another example in which it is string stable but not stable. For the former case, $n = 20$, $k_d = 14$ are selected, and an attacker at position one with $\tilde{k}_d = -0.2$, which results in stability/string instability at $\omega = 2.1$, while for the latter $n = 3$, $k_d = 2.5$ are used, and an attacker at position one with $\tilde{k}_d = -5$ to produce instability/string stability at $\omega = 0.474$ (Figure 2.6 depicts the string stable/string unstable regions vs. $\tilde{k}_d$ for these cases).

2.4 Platoon controllability

In this section, the controllability of the platoon from an attacker's perspective; i.e. whether an attacker can cause other vehicles in the platoon to take on arbitrary states and by doing so fully control their movements (separation between neighboring vehicles and velocity) has been investigated.

Definition 2.4.1 (Controllability) *A system is said to be controllable if and only if it is*

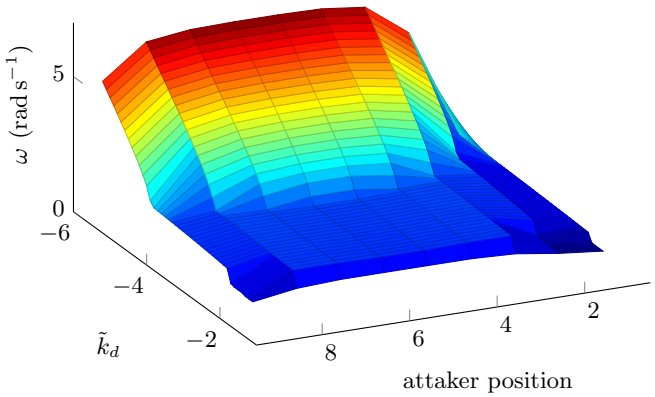


Fig. 2.5: Frequencies at which a ten vehicle platoon can be made unstable, with respect to attacker position and gain.

possible, by means of the input, to transfer the system from one state to another state in finite time.

A LTI system represented by

$$\dot{x} = Ax + Bu \tag{2.17}$$

where $x \in \mathbb{R}^n$, $A \in \mathbb{R}^{n\times n}$, $u \in \mathbb{R}^m$, and $B \in \mathbb{R}^{n\times m}$. is controllable if the controllability matrix

$$\mathcal{C} = \begin{bmatrix} B & AB & A^2B & \cdots & A^{n-1}B \end{bmatrix} \tag{2.18}$$

is full rank (i.e $rank(\mathcal{C}) = n$) [13].

In what follows, a controllability analysis to determine an attacker's ability to control the states (position and velocity) of other vehicles in the platoon is performed. A general controllability framework for dynamic systems was investigated from a security perspective in [4]. The author is specifically interested in whether an attacker can control the states of all the other vehicles or only some vehicle states in a platoon. To comment on the controllability of the vehicle platoon with an attacker planning malicious control, a five vehicle platoon using error coordinates is considered. Due to the regularity of the state matrix, only three attacker positions need to be examined. Because of the ambiguity in

how the control law is to be applied (end of Section 2.2.1), controllability for two different leader behaviors is investigated: 1) the leader is not affected by followers and 2) the leader responds to the perturbations of followers as any other vehicle in the platoon would.

2.4.1 Lead vehicle unaffected by followers

In this scenario, the lead vehicle is not applying the vehicle platooning control law and moves at a constant speed ($k_p^n = k_d^n = 0, u_l = 0$). Equations of motion for the lead vehicle (5th vehicle) can be written as

$$\dot{x}_5 = v_5$$
$$\dot{v}_5 = 0.$$

Relative equations of motion for controllability analysis are used. Under this scenario, controllability of three cases for the attacker at first, second, and third position are investigated.

Attacker at 1st position. A and B matrices for the LTI system in (2.17) for a five vehicle platoon with attacker in the first position can be written as

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & k_p & k_d & -2k_p & -2k_d & k_p & k_d \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & k_p & k_d & -k_p & k_d \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^\top.$$

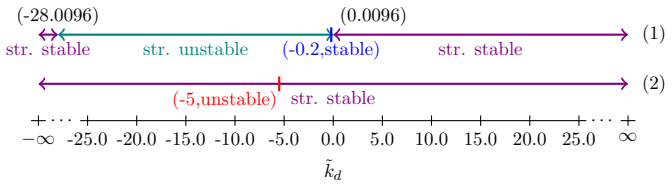


Fig. 2.6: Attacker at position one. (1) system stable but not string stable. (2) system string stable but not stable.

The controllability matrix $\mathcal{C}$ for the above system can be computed using (2.18). It can be verified that

$$\det(\mathcal{C}) = k_p^{12} \neq 0$$

Therefore, it can be said that $rank(\mathcal{C}) = 8$ meaning that system is controllable and the attacker can control relative position and velocity between all the vehicles.

Attacker at 2nd position. A and B matrices for the LTI system in (2.17) for a five vehicle platoon with attacker in the second position can be written as

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & k_p & k_d & -2k_p & -2k_d & k_p & k_d \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^\top.$$

The controllability matrix $\mathcal{C}$ for the above system can be computed using (2.18). It can be verified that

$$\det(\mathcal{C}) = 0$$

It can be verified that $rank(\mathcal{C}) = 6 < 8$ meaning that system is not fully controllable when the attacker is at second position.

To find out uncontrollable states similarity transformation is performed to bring the controllability matrix into Row Reduced Echelon Form (RREF) which is given by

$$RREF(\mathcal{C}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & a_1 & a_2 \\ 0 & 0 & 0 & 1 & 0 & 0 & a_3 & a_4 \\ 0 & 0 & 0 & 0 & 1 & 0 & a_5 & a_6 \\ 0 & 0 & 0 & 0 & 0 & 1 & a_7 & a_8 \end{bmatrix} \tag{2.19}$$

where $a_1 = -3k_p^2$, $a_2 = 12k_dk_p^2$, $a_3 = -6k_dk_p$, $a_4 = 24k_d^2k_p - 3k_p^2$, $a_5 = -3k_d^2 - 4k_p$, $a_6 = 12k_d^3 + 10k_pk_d$, $a_7 = -4k_d$, $a_8 = 13k_d^2 - 4k_p$. The six controllable states can then be written as

$$X_{cont} = \begin{bmatrix} z_1 \\ y_1 \\ z_2 + a_1z_4 + a_2y_4 \\ y_2 + a_3z_4 + a_4y_4 \\ z_3 + a_5z_4 + a_6y_4 \\ y_3 + a_7z_4 + a_8y_4 \end{bmatrix}$$

where $z_1 = x_1 - x_2$, $y_1 = v_1 - v_2$, $z_2 = x_2 - x_3$, $y_2 = v_2 - v_3$, $z_3 = x_3 - x_4$, $y_3 = v_3 - v_4$, $z_4 = x_4 - x_5$, and $y_4 = v_4 - v_5$ are relative position and velocity coordinates.

Attacker at 3rd position. A and B matrices for the LTI system in (2.17) for a five vehicle platoon with attacker in the third position can be written as

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & k_p & k_d & -2k_p & -2k_d & k_p & k_d \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \end{bmatrix}^\top.$$

The controllability matrix $\mathcal{C}$ for the above system can be computed using (2.18). It can be verified that

$$\det(\mathcal{C}) = k_p^{12} \neq 0$$

Therefore, it can be said that $rank(\mathcal{C}) = 8$ meaning that system is controllable and the attacker at the third position can control relative position and velocity between all the vehicles.

2.4.2 Lead vehicle affected by followers

In this scenario the lead vehicle is also applying the vehicle platooning control law meaning the attacker can also affect the leader's motion in this case ($k_p^n = k_p, k_d^n = k_d, u_l = 0$). Equations of motion for the lead vehicle (5th vehicle) can be written as

$$\dot{x}_5 = v_5$$

$$\dot{v}_5 = k_p(x_4 - x_5) + k_d(v_4 - v_5).$$

Under this scenario, the controllability for the three cases of an attacker at first, second, and third position are investigated, as above. Table 2.2 summarizes the controllability analysis results for the two types of leader behavior. Note: an attacker in the third position for the second case is able to control four states, which are a combination of several individual vehicle states, as in the case of an attacker in the second position in the first case.

Based on the analysis it can be concluded that the symmetry of an attacker's position makes the system uncontrollable, from the attacker's perspective. For an attacker to completely control the platoon, the attacker must be situated at certain positions, which are determined by how the leader implements the platooning control law; partial control (which may or may not allow an attacker to control other vehicle states individually) is possible from every position in the platoon.

Having determined which states an attacker can control, the next step is to create a controller for u_a that allows an attacker to control its own motion in such a way as to regulate distance and velocity between two adjacent vehicles. It is considered the feasibility of designing such controllers in Section 2.5.2. This type of attack is distinct from, and more powerful than, an attack in which the attacker's gains are changed to destabilize the platoon, as it provides more flexibility (individual states, or a subset of vehicle states, may be controlled, to a perhaps arbitrary) and safety to the attacker (the attacker needn't be affected by the attack).

2.5 Discussion

The security/safety implications of the findings presented in Sections 2.3 and 2.4 are discussed.

2.5.1 Stability

An attacker able to violate string stability on a large enough scale (i.e. an attacker in control of several compromised vehicles) and in the right conditions (i.e. high traffic densities) could affect traffic flow instability; e.g. the creation of phantom traffic jams. Within a single platoon, violations of string stability would lead to greater than anticipated

Table 2.2: Five vehicle controllability results

Case	Position#1	Position#2	Position#3
1 ($\dot{v}_5 = 0$)	Cont	Uncont	Cont
2 ($\dot{v}_5 \neq 0$)	Cont	Cont	Uncont

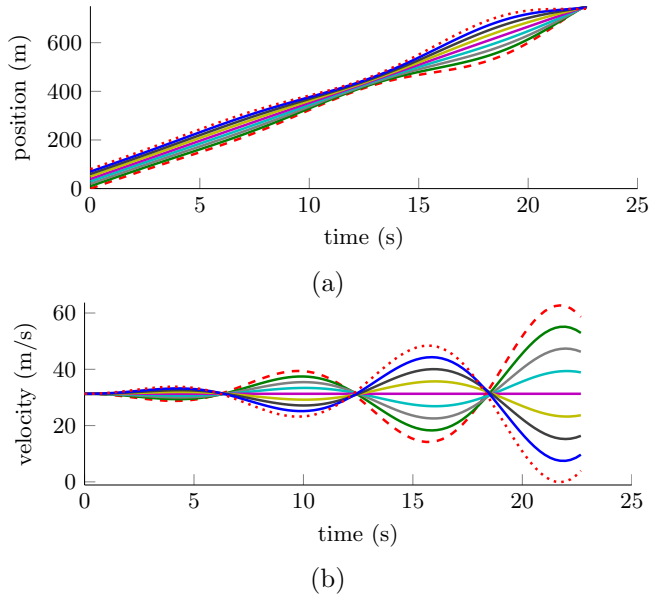


Fig. 2.7: Position and velocity of a platoon under attack. (a)/(b) Two attackers cause the platoon to collapse in on itself by oscillating at the resonant frequency, but 180° out of phase.

vehicle separations, which would possibly negate the fuel savings of the platoon, or allow an attacker to carry out the attack of more effectively.

The example given in Section 2.1.1 illustrates how a single attacker can leverage instability to target the leader of a platoon. By changing the threat model slightly, in order accommodate an attacker in control of two vehicles or two colluding attackers, also it can be illustrated how a single, non-leader vehicle can be targeted. In this case the two attackers are positioned at the first and ninth position of a ten vehicle platoon. They begin to accelerate and brake contrariwise (one breaks while the other accelerates) at an unstable frequency. Vehicles following the fifth vehicle will brake at the same time vehicles preceding the fifth accelerate (and vice versa); the fifth vehicle will not be disturbed. Eventually the oscillation produced grows so great that the vehicles collide at the center point of the

platoon; i.e. the platoon collapses in on the fifth vehicle (Figure 2.7). By employing different amplitudes for their respective oscillations, the attackers could target vehicles at other positions for the same attack.

It is noted that countering such attacker-induced instabilities is not a simple matter of damping out the normal modes of the system. Figure 2.8 shows the position/velocity gain for the ninth vehicle in a platoon due to a perturbation from an attacker situated at the first position of the platoon. The wide bandwidth of the gain shows that even if the attacker doesn't oscillate at the natural frequency of the system, they can still cause significant deviations in velocity/position for the victim (essentially each subsequent period of oscillation by the attacker will cause position/velocity deviations at least twice as great as the last for the victim). Additionally, while constraining allowable vehicle behavior (e.g. maximum velocity) decreases the effect of the attack, limits per se cannot prevent it from being deployed to increase the severity of accidents. For example, if the vehicles in the above two-attacker example are limited to a maximum velocity of 35 and accelerations in the range of ± 5, a collision resulting from an instability would still see relative velocities 35% greater, and kinetic energy 81% greater, at time of impact than if the attackers had simply decelerated/accelerated at ± 5.

Generality of attack

To demonstrate the widespread applicability of the attack, a platoon is considered following a unidirectional algorithm [142] employing a second order sliding mode controller [62]. The control objective in this instance is to make the velocities of the following vehicles converge to that of the leader's; only information about the preceding vehicle is used. Again, assuming an ideal vehicle model, the dynamics of the i^{th} vehicle are given by:

$$\begin{aligned} \dot{x}_i &= v_i \\ \dot{v}_i &= a_i \\ \dot{a}_i &= \frac{1}{h}(-W_M sign[s_i(t) - \frac{1}{2}s_{max,i}]) \end{aligned} \tag{2.20}$$

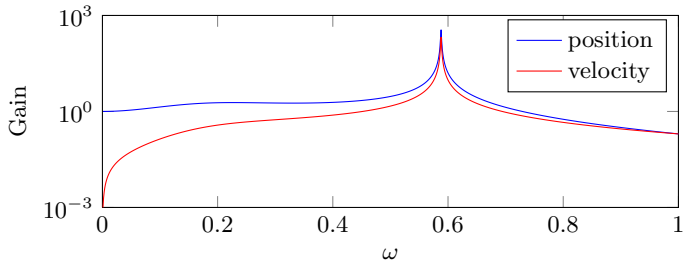


Fig. 2.8: Position/velocity gains of the ninth vehicle in ten vehicle platoon for attacker in the first position. The attacker can cause significant changes to the vehicle even when not oscillating at the resonant frequency.

where x_i, v_i, and a_i denote the position, velocity, and acceleration of the vehicle, W_M is a gain taken to be greater than four times the maximum vehicle acceleration, a_{max}, and $s_{max,i}$ is the extremal value of the signal of $s_i = x_i - x_{i+1} + s_{d0} + hv_i$, with s_{d0} being a desired minimum vehicle spacing at rest and h a "headway time".

As in the case of PD control, the attacker must first be able to make the system unstable through a change of gain(s). The resulting resonant frequency must then be achievable by the other vehicles in order to affect the attack. First, it has been proved that an attacker can make the platoon unstable, and then has been shown that the resulting frequencies for some gain changes satisfy the feasibility condition ($\omega \leq 2\pi$).

lemma 2 *The states of the system will not converge to the desired value of* $s_i = 0$ *(i.e. an attacker can make the system unstable) if the attacker selects for its gain,* W_M*, in* $(0, 4a_{max})$.

proof 2 *In [62], convergence is proved via the contraction property. Should an attacker choose their gain such that it violates the contraction property, the state trajectory will not converge to the origin of the state plane. The contraction property holds for the system if* $\frac{2a_{max}}{W_M - 2a_{max}} < 1$. *If* W_M *is chosen from* $(0, 4a_{max})$ *the strict inequality is violated. This holds for all initial conditions.*

By varying the attacker's gain and simulating the system response ($W_M = 5a_{max}$ was used for victim vehicles), it has been found that the platoon will resonate at feasible frequencies for attacker gains over the range $(0, 1.2a_{max})$ (Figure 2.9). The location of the attacker in the platoon does not affect the resonant frequency, but, because of the

unidirectional nature of the platooning algorithm, the attacker is only able to force following vehicles to oscillate. All vehicles oscillate at the same frequency.

2.5.2 Controllability

As it has been shown in Section 2.4, it is theoretically possible for an attacker to control the states of individual vehicles in the platoon, assuming they are at the proper position. However, controlling states of other vehicles just by controlling an attacker's motion falls under single input multiple output (SIMO) control, which has not been addressed in the controls literature very extensively. The SIMO control problem has been solved for slow dynamic systems, such as control of a dam river system, where the action variable is the upstream discharge and the controlled variable the downstream discharge [95, 96]. In an extension of this work, the solution to the SIMO control problem in order to design a controller that allows an attacker to control their motion to regulate other vehicles' position and velocity will be proposed. The results of the controllability analysis presented above should thus been seen as the uncovering of a new vulnerability in vehicle platooning. For an attacker to exploit this vulnerability will require advances in the area of SIMO control.

Another problem in designing SIMO attacker control is the conditionality of the control matrix. Even when the system is fully controllable (full rank), the controllability matrix is badly conditioned (very high condition number). This means even though the attacker can theoretically control all the other vehicle states, to practically design a controller it may be required to change the structure of the A and B matrices to improve the condition number of the controllability matrix. In future work, the use of false data injection to accomplish this will be explored.

While it is not possible to offer a general-purpose controller that would allow an attacker to control arbitrary vehicle states, a controller that gives an attacker arbitrary control over preceding vehicles' separation, without changing the attacker's gain(s) can be provided.

lemma 3 *Vehicles preceding an attacker will be separated by an amount equal to the attacker's desired spacing.*

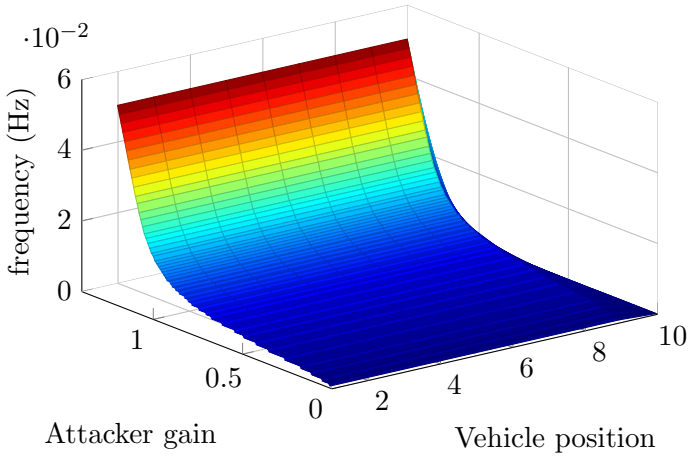


Fig. 2.9: Frequencies at which each vehicle in a ten vehicle platoon will resonate; non-linear controller used for each vehicle, with unidirectional platoon algorithm. Attacker at position nine.

proof 3 *Allow d_{atk} to be the attacker's desired spacing for the platoon and d the desired platoon spacing in the absence of an attacker. Using these values with (5.1) for an attacker in the first position (rear of the platoon), it has been shown that at steady state (i.e. $\dot{v}_1 = \dot{v}_2 = \cdots = \dot{v}_n = 0$ and $v_1 = v_2 = \cdots = v_n$):*

$$\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= -k_p x_1 + k_p x_2 - k_p d_{atk} = 0 \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= k_p x_1 - k_p x_2 + k_p d \\
&\quad + k_p x_3 - k_p x_2 - k_p d = 0 \\
&\vdots \\
\dot{x}_{n-1} &= v_{n-1} \\
\dot{v}_{n-1} &= k_p x_{n-2} - k_p x_{n-1} + k_p d \\
&\quad + k_p x_n - k_p x_{n-1} - k_p d = 0 \\
\dot{x}_n &= v_n \\
\dot{v}_n &= 0
\end{aligned} \tag{2.21}$$

Rearranging and canceling terms for $\dot{v}_1$, it has been found that $x_2 - x_1 = d_{atk}$. Substituting this value recursively into the subsequent $\dot{v}_i$ equations yields $x_i - x_{i-1} = d_{atk}$ for $1 < i < n-1$. Following the same procedure for an attacker in the j^{th} position, it can be shown that $x_{i+1} - x_i = d$ for $1 < i < j$ and $x_{i+1} - x_i = d_{atk}$ for $j < i < n-1$.

$\therefore$ For all vehicles preceding them, the attacker is able to specify the spacing policy.

The utility of this attack lies in an attacker being able to set $d_{atk} \leq 0$, which results in the platoon collapsing in on itself (more negative values of d_{atk} will cause this to happen at greater relative velocities). By setting $d_{atk} \sim \sin \omega t$ an attacker would cause vehicles in the platoon to oscillate back and forth in a controlled manner that would not invite collisions. Such movements would force vehicles to brake and accelerate, continuously, which would cause excess energy expenditure (i.e. wasting of fuel).

2.6 Summary

In this chapter, it has been shown that a single, maliciously controlled vehicle can destabilize a vehicular platoon, to catastrophic effect, through local modifications to the prevailing control law. Specifically, by combining changes to the gains of the associated law with the appropriate vehicle movements, the attacker can cause the platoon to oscillate at a resonant frequency, causing accidents that could result in serious injury or death. The range of gains and their corresponding frequencies, that allow an attacker to violate the string stability and stability criteria at different positions in the platoon are determined. Furthermore, it is proved that the attack can be successful at any position in the platoon and at frequencies that can be realized by the other vehicles in the platoon. This work implies that neither the string stability nor stability conditions, when used singly, ensure proper platoon operation, and that neither can be used to ensure the other. Finally, it is shown that an attacker is theoretically capable of gaining control over the individual position and velocity (states) of other vehicles in the platoon; two attacks are demonstrated for this vulnerability.

CHAPTER 3

Reachability Analysis of the Vehicular Platooning

3.1 Background and Contribution of This Work

Platooning, also known as Cooperative Adaptive Cruise Control (CACC), is characterized as a group of vehicles with coordinated movement. Platooning has been investigated for around 4 decades [87]. The main objective of platooning is to reduce the inter-vehicle distance significantly compared to what is considered advisable during manual driving. Among the potential benefits are a better use of the road infrastructure by allowing more vehicles to use a given stretch of road, improved energy efficiency by reducing aerodynamic drag, increased highway safety due to the reduction of human mistakes, and reduced traffic congestion [136]. Huge body of research involves longitudinal and lateral control of vehicle platoon [20, 75, 118, 126, 129, 132]. The main concept in platoon control is *string stability*. String stability deals with how errors are propagated through the vehicle string due to disturbances or the reference trajectory of the formation lead. A string-stable control form means that spacing errors between adjacent vehicles do not grow or amplify along the vehicle string [90, 125].

While many features of platooning are active areas of research, e.g. transportation impacts, environmental, mechanical and control concerns [29, 87, 94, 99, 138], comparatively little work has examined platooning in an adversarial environment and among those, most papers challenge platoon security from communication aspect [86]. A few works that performed security analysis on control in platooning can be grouped into categories of attack design [28, 44–46] and mitigation strategies [24]. It has been verified by recent studies that attacks on platooning components may cause physical damages and threaten their normal functions. Research works are mostly seeking the drawbacks in controls and trying to manipulate the vulnerabilities like modification of control law such that attacker can create

catastrophic impacts on platoon. This type of impacts included, but are not limited to, collision in high relative velocity to maximize the damage or oscillation to cause passenger discomfort and increase fuel consumption [28, 44, 50]. A scenario wherein a group of malicious vehicles on a highway perform a cooperative attack for creating undesirable wave effects among other vehicles are investigated. The mathematical analysis to choose the undesirable wave is presented in [67]. This investigation helps to understand the effect of drivers behavior on traffic formation. In [28] attacker changes its gains such that system becomes unstable and authors, at the end, briefly introduce the controllability of attacker over platoon. To investigate this idea thoroughly, reachability of the platoon in presence of attacker is studied, which can give clear picture of attacker capability in affecting position and velocity of other vehicles in platoon, with its own motion involving acceleration or deceleration. However, the research works mentioned above focus on only designing attacks and disrupting the platoon. The important challenge remaining is to provide guarantees for successful attack. Two intriguing questions in this context are: *(a) Will the attacker be able to carry out the attack successfully? (b) Will the vehicles collide under control constraints?* This problem implies that the attack should be designed with a more comprehensive analysis.

This work is devoted to the analysis of reachability properties of vehicular platooning under attack. Reachability analysis determines the set of states that the system can possibly visit within finite or infinite time when started from a bounded set of possible input and parameter values. The Exact reachable set can be computed for special cases with few states. Except for the simplest of examples, analytic verification of reachable set for continuous and hybrid systems is rarely possible. With the goal of broadening the applicability and automating the process, numerical methods for verifying or validating such properties have been the subject of much study. Several papers in the literature deal with approaches for reachability set computation. Reachable sets and the optimal time to reach a target for a controlled nonlinear system is characterized using Hamilton Jacobi equation with state constraints in [10]. An algorithm which can numerically compute the backward reachable

set for a two player, nonlinear differential game with a general target set is proposed in [104]. This algorithm is based on a formulation of reachability in terms of the viscosity solution of a time-dependent Hamilton-Jacobi-Bellman partial differential equation. Hamilton-Jacobi methods to reach-avoid problems with time-varying dynamics, targets, and constraint have applications in game theory and optimal control problems. Hamilton-Jacobi methods for such applications including pursuit-evasion, differential games, and safety certificates for dynamical systems are extended in [64]. Any reachability analysis performed so far on vehicle platoon or any vehicular formation was for the purpose of collision avoidance [14, 15, 19] or fuel consumption minimization [53].

Approximation of reachable sets is one major category of numerical methods. Reachable set can be over or under-approximated. Obviously, over-approximated reachable states can contain states which are not practically achievable and minimizing over-approximation results in high computational cost. Hence, under-approximation techniques are more reliable approach.

Currently, the analysis of the vehicle platoon systems cannot tractably provide the exact reachable set if the number of vehicles is large. In this work, under approximated reach set for platoon of vehicles under attack is studied. For the longitudinal control, the Proportional Derivative (PD) control for Bidirectional information flow [142] is used to produce a sequence that minimizes spacing, relative velocity and the cost of traveling from an origin to any destination. The extent of performance disruption of the platoon facing attack is studied using ellipsoidal method and the attacker's goal satisfaction are analyzed using homogeneous model for all vehicles. First, reachable states for a single motion change attack, is studied. Then, in the event of the integral attack (motion and gain modification), potential impacts are investigated. We demonstrate the platoon states whilst facing two representative attack scenarios and discuss the attacker's control over platoon performance in each scenario.

To the best of my knowledge, reach set computation for the attacker has not been investigated in the literature. In this work, the attacker's capabilities, based on its position

in the platoon and the type of attack are discussed and detailed examination of reachable set for two attack scenarios under input constraints are presented. This study gives a profound knowledge of what the attacker is really capable of accomplishing, under physical constraints in practical cases.

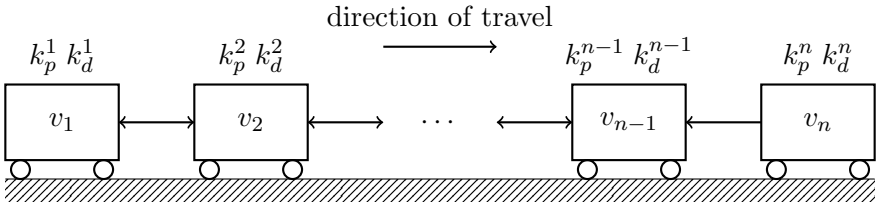


Fig. 3.1: An n-vehicle platoon employing a bi-directional control law. Arrows represent the flow of information.

3.2 Preliminaries

Reachability analysis computes all possible states a system can attain, and in this sense provides knowledge about the system with completeness, or coverage, that a finite number of simulation runs cannot deliver, due to its inherent complexity.

Reachability analysis is concerned with the computation of the reachable set in a way that can effectively meet some types of requests. These requests include [65]: (a) determination of non-empty intersection of the reach set and the target set; (b) finding a feasible initial condition; (c) control that steers the system from this initial condition to the given reachable state in given time.

Several methods in the literature propose algorithms to calculate the reachable set of the system like methods based on ellipsoidal representations [92], techniques using support functions [69], and applying Hamilton Jacobi Isac (HJI) equations to differential equations [104]. As the number of the states increases, it becomes harder to calculate the exact reachable set of the system by admissible inputs. Hence, some of the existing methods suggest some approximation algorithms to find the reachable set.

Ellipsoidal method is proposed for calculating reachable set for continuous time linear

system under input constraints in [91] and [16]. In [91], the authors proposed that they can estimate the reachable tube for the general linear time invariant system described in (3.1),

$$\dot{x} = Ax + Bu \quad t_0 \leq t \leq T \tag{3.1}$$

where $x \in R^n$, $u \in R^m$, $A \in R^{n\times n}$, and $B \in R^{n\times m}$ are states, inputs, and matrices describing dynamic of the system, respectively.

Definition 3.2.1 *The reachable set $R[x,T] = R(T,t_0,X_0)$ of the system (3.1) at time T from a set of initial states X_0 and time t_0 is the set of all points x for which there exists a trajectory $x(s,t_0,X_0)$, $x_0 \in X_0$ that transfers the system from (t_0,x_0) to (T,x), $x = x(T)$, while satisfying the associated constraints [145].*

Similarly, the reachable tube is the set of all reachable sets over a time interval.

Definition 3.2.2 *The reachable tube is all values (3.1) can meet during $[t_0,T]$ and is mathematically defined as $Tu(x,T) = \bigcup_{t\in[t_0,T]} R(t,t_0,X_0)$ [145].*

Assuming some constraints on the input, the admissible set of inputs is $u(t) \in P(t)$, where $P(t)$ is non-degenerate ellipsoid continuous in t,

$$\begin{aligned} P(t) &= \xi(q(t),Q(t)) \\ &= \{u(t) : (u-q(t)), Q^{-1}(t)(u-q(t)) \leq 1\} \end{aligned} \tag{3.2}$$

where $q(t) \in R^m$ is the center and positive definite matrix $Q(t) \in R^{m\times m}$ is matrix of ellipsoid.

The response of the system can be obtained using

$$x(t) = \exp(A(t-t_0))x_0 + \int_{t_0}^{T} (\exp(A(t-\tau))Bu(\tau)d\tau). \tag{3.3}$$

Extending (3.3) to ellipsoidal calculation for reachable set results in

$$x(t) \in R[T, t_0, X_0] = \exp(A(t - t_0))\xi(x_0, X_0) + \int_{t_0}^{T} (\exp(A(t - \tau))B\xi(q(\tau), Q(\tau))d\tau). \tag{3.4}$$

Above, the reachable set computation using Ellipsoidal toolbox is described.

3.3 Problem statement

The analysis focuses on exploiting longitudinal control laws and input of the vehicles in platoon, which are intended to maintain desired separation and velocity as they follow straight line. Assuming all vehicles are traveling in one dimension, attacker gets the chance to influence other vehicles' motion via manipulating longitudinal control algorithm.

3.3.1 Platoon Model

The bi-directional (predecessor-follower) proportional-derivative (PD) controller is used to demonstrate the impact of a malicious actor on platooning operations. This control law is capable of maintaining a constant separation, d, between vehicles, based solely on local sensing. This is important because it allows us to show that an attacker can affect the platoon solely through malicious movement and need not rely on interfering with inter-vehicle communication. Formally, the dynamics of a platoon with n vehicles employing this control law for the leader are described by the following system of equations,

$$\begin{aligned}
\dot{x}_1 &= v_1, \\
\dot{v}_1 &= k_p^1(x_2 - x_1 - d) + k_d^1(v_2 - v_1), \\
\dot{x}_2 &= v_2, \\
\dot{v}_2 &= k_p^2(x_1 - x_2 + d) + k_p^2(x_3 - x_2 - d), \\
&\quad + k_d^2(v_1 - v_2) + k_d^2(v_3 - v_2), \\
&\vdots
\end{aligned}$$

$$
\begin{aligned}
\dot{x}_{n-1} &= v_{n-1}, \\
\dot{v}_{n-1} &= k_p^{n-1}(x_{n-2} - x_{n-1} + d) + k_p^{n-1}(x_n - x_{n-1} - d), \\
&\quad + k_d^{n-1}(v_{n-2} - v_{n-1}) + k_d^{n-1}(v_n - v_{n-1}), \\
\dot{x}_n &= v_n, \\
\dot{v}_n &= k_p^n x_{n-1} - k_p^n x_n + k_p^n d + k_d^n v_{n-1} - k_d^n v_n + u_l
\end{aligned}
\tag{3.5}
$$

where x_i and v_i represent the position and velocity of the i_{th} vehicle, respectively ($\dot{a}$ denotes the first derivative with respect to time of the variable a), and k_p^i and k_d^i represent their proportional and derivative gains, respectively. For normal platooning operations k_p^i and k_d^i are the same for each vehicles (thus the superscripts are ignored unless referring to the gains for a vehicle in a particular position). k_p is traditionally fixed at 1, while k_d varies according to the size of the platoon [28]. Here, u_l represents the control input for the leader (n_{th} vehicle). In the steady-state u_l is generally taken to be equal to zero; however, it is noted that $k_p^n \neq 0$ and $k_d^n \neq 0$ implies that the followers would be able to influence the leader's movements, unless u_l is set to cancel out the follower movements, which would effectively set $k_p^n = k_d^n = 0$. In any case, from the security perspective it seems inadvisable for followers to be able to influence the leader.

3.3.2 Threat Models

The behavior of platoon in presence of malicious vehicle and the scope of deviation from its normal performance, traveling at a constant speed with constant spacing are studied. Two attack scenarios are investigated: In the first attack, the attacker attempts to take control of all the states and brings them to desired and arbitrary states solely through its motion. This raises a question about how probable is it that the attacker will successfully accomplish his goal. In this attack, attacker chooses its gains, as other vehicles in the platoon but it uses its own acceleration/deceleration to influence other vehicles states. The attacker's vehicle is considered to have exactly the same capabilities as the other vehicles in the platoon.

In the second attack scenario, the attacker implements an integral attack where attacker takes advantage of motion modification while it modifies its control algorithm. The attacker's capability during the integral attack is analyzed. The attack model would be similar to (5.2) and the corresponding row to the attacker in A matrix would be modified like [28].

In order to, demonstrate the extent of the attacker's capability of controlling platooning operations with being assigned nominal control of the platoon, it is assumed that the attacker does not act as the leader of the platoon.

The equivalent state-space representation of the linear time-invariant (LTI) system defined by (5.1) in the presence of an attacker is

$$\begin{aligned} \dot{\mathbf{X}} &= A\mathbf{X} + B\mathbf{U} \\ \mathbf{Y} &= C\mathbf{X} \end{aligned} \tag{3.6}$$

where $X = [x_1,\ v_1,\ x_2,\ v_2,\ \cdots,\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the states of all the vehicles in the platoon and Y is the output, which in this case is similar to states, $A \in \mathbb{R}^{2n\times 2n}$, $B \in \mathbb{R}^{2n\times 2}$, $C \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{U} = [u_l\, u_a]^\intercal$. C is the identity matrix (because it is assumed that all the vehicle states are measurable), B has non-zero entries corresponding to the leader and the attacker control, u_l and u_a, respectively, where u_a is the attacker's input in order to achieve the desired states for both attacks.

$$\begin{aligned} z_i &= x_i - x_{i+1} + d \\ y_i &= \dot{x}_i - \dot{x}_{i+1} = v_i - v_{i+1} \end{aligned} \tag{3.7}$$

The states to be controlled by the attacker are relative position and relative velocity. So, the system of equation, (5.1) is transformed to (3.8), where attacker is in i_{th} position in the platoon. In case there are n vehicles in the platoon, number of states in absolute coordinate (5.1) is $2n$ for positions and velocities. On the other hand, using error coordinate (3.7) and (3.8), there are $2n-2$ states, z_i and y_i, which are spacing and relative velocity,

respectively. Leader of the platoon would be counted as the n_{th} vehicle in platoon, as shown in Fig. 5.1, and it is assumed that all vehicles in platoon follow the normal control law in motion modification attack described in (3.8).

$$
\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= -2k_p z_1 + k_p z_2 - 2k_d y_1 + k_d y_2 \\
\dot{z}_2 &= y_2 \\
\dot{y}_2 &= k_p z_1 - 2k_p z_2 + k_p z_3 \\
&\quad + k_d y_1 - 2k_d y_2 + k_d y_3 \\
&\vdots \\
\dot{z}_{i-1} &= y_{i-1} \\
\dot{y}_{i-1} &= k_p z_{i-2} - 2k_p z_{i-1} + k_p z_i \\
&\quad + k_d y_{i-2} - 2k_d y_{i-1} + k_d y_i - u_a \\
\dot{z}_i &= y_i \\
\dot{i}_2 &= k_p z_{i-1} - 2k_p z_i + k_p z_{i+1} \\
&\quad + k_d y_{i-1} - 2k_d y_i + k_d y_{i+1} + u_a \\
\dot{z}_{i+1} &= y_{i+1} \\
\dot{y}_{i+1} &= k_p z_i - 2k_p z_{i+1} + k_p z_{i+2} \\
&\quad + k_d y_i - 2k_d y_{i+1} + k_d y_{i+2} \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= k_p z_{n-3} - 2k_p z_{n-2} + k_p z_{n-1} \\
&\quad + k_d y_{n-3} - 2k_d y_{n-2} + k_d y_{n-1}
\end{aligned}
\tag{3.8}
$$

$$\dot{z}_{n-1} = y_{n-1}$$

$$\dot{y}_{n-1} = k_p z_{n-2} - k_p z_{n-1} + k_d y_{n-2} - k_d y_{n-1} - u_l$$

Then, A and B matrices using error coordinate can be formed as (3.9) and (5.3). The attacker in the first attack scenario only implements motion modification where the B matrix is modified. Single attacker only tries to control platoon by its own motion in which B matrix is described as a single-column with entries 1 at $2i_{th}$ and -1 at $2i-1_{th}$ rows, where i is the place of the attacker in the platoon. If the second vehicle is considered to be the attacker, B matrix can be written as:

$B =$

$$\begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{3.9}$$

In the integral attack, attacker combines the motion modification in the former attack with its gains modification and applies the changes to its corresponding row of A matrix.

$A =$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix} \tag{3.10}$$

The changes to A matrix is described as follows: Allow $A(i, j)$ to represent access to the element at the i_{th} row and j_{th} column of A. When an attacker is present at the first position,

$$\begin{aligned} A(2,1) &= -k_p - \tilde{k_p} \\ A(2,2) &= -k_d - \tilde{k_d} \end{aligned} \tag{3.11}$$

An attacker in the i_{th} position, $1 < i < n-1$, changes the following elements of (5.3)

$$\begin{aligned} A(2(i-1), 2(i-1)-1) &= k_p - \tilde{k_p}, \\ A(2(i-1), 2i-1) &= \tilde{k_p}, \\ A(2i, 2(i-1)-1) &= \tilde{k_p}, \\ A(2i, 2i-1) &= -k_d - \tilde{k_p} \\ A(2(i-1), 2(i-1)) &= k_d - \tilde{k_d}, \\ A(2(i-1), 2i) &= \tilde{k_d}, \\ A(2i, 2(i-1)) &= \tilde{k_d}, \\ A(2i, 2i) &= -k_d - \tilde{k_d} \end{aligned} \tag{3.12}$$

When the attacker's position is $i = n-1$,

$$\begin{aligned} A(2(i-1), 2(i-1)-1) &= k_p - \tilde{k_p} \\ A(2(i-1), 2(i-1)) &= k_d - \tilde{k_d} \end{aligned} \tag{3.13}$$

Where derivative and proportional gains of the attacker shown using $\tilde{k_d}$ and $\tilde{k_p}$.

3.4 Reachability Analysis and Simulation Results

In this section, the attacker's capability to disrupt the stable navigation of the platoon is analyzed and the efficiency of the attack is measured through reachable set. Efficiency of the attack would be measured through attacker's power to cause collisions between vehicles or cause the stop-then-go motion, which causes discomfort to passengers and increase in fuel consumption. Alinear model (5.2) is considered for the platoon where attacker modifies input set while it follows the platoon control law using stable gains or it compromises the platoon via changing entries in A and u_a. In spite of system controllability analysis, which indicates platoon would be able to reach any arbitrary states proposed in [28] for the vehicle platoon, it can be clearly evidenced that attack is not feasible in stable case. This infeasibility stems from the small controllability grammian matrix determinant, which results in a huge control effort. Furthermore, when attacker changes its gains to unstable or marginally stable ones, it can actuate platoon to more diverse desired states. To clarify the difference of the two scenarios described in (5.2) - (5.5), the reachable sets of the system in both cases are computed and demonstrated for a small size platoon.

3.4.1 Reachability Analysis of the Platoon During Motion Modification Attack

A set of states for vehicles in platoon where attacker can steer states of vehicles towards them through its own constrained motion is investigated. More specifically, given that platoon already reached its desired constant spacing and velocity before the attack starts, the most severe impact that the attacker can cause when its acceleration and deceleration are bounded the $u_a \in [u_{a_{min}}, u_{a_{max}}]$ is desired. This analysis is for the purpose of verifying

attacker's capability to compromise the system. As explained, let the initial states and input sets of attacker be the ellipsoids. Initial set $\xi(x_0, X_0)$ for the (3.7), $x_0 = 0$ and X_0 is a very small deviation around 0 and admissible input set for the single attacker $\xi(q(\tau), Q(\tau))$ is a line stretched between $[u_{a_{min}}, u_{a_{max}}]$.

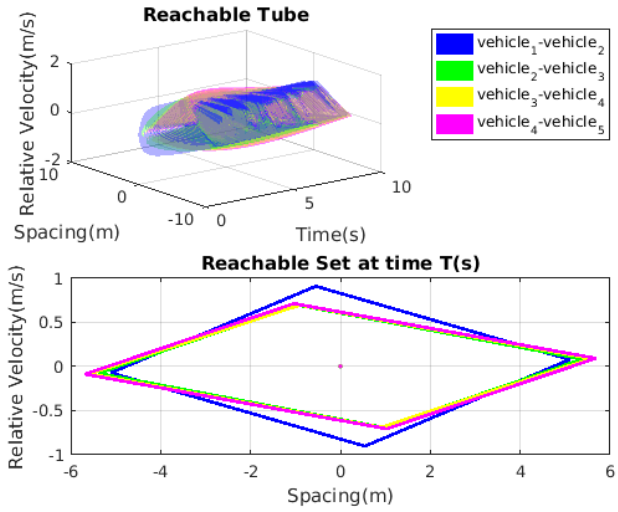


Fig. 3.2: Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the first place.

3.4.2 Reachability Analysis of the Platoon During Integral Attack

During integral attack, attacker adds the control law modification attack on top of its erratic acceleration and deceleration to make more impact. The rationale is, changing gain for the attacker causes the platoon system to lose its symmetric structure, and even become more controllable from attacker perspective. In some cases, such control offers the attacker a broader range of impact. Therefore, attacker carries out motion modification attack with same setting described in previous attack while it modifies the A matrix as represented in (3.11) - (5.5).

3.4.3 Simulation Results

The reachable sets for motion modification and integral attack scenarios are demonstrated for the 5-vehicle platoon model. The reachable sets using Ellipsoid toolbox are computed.

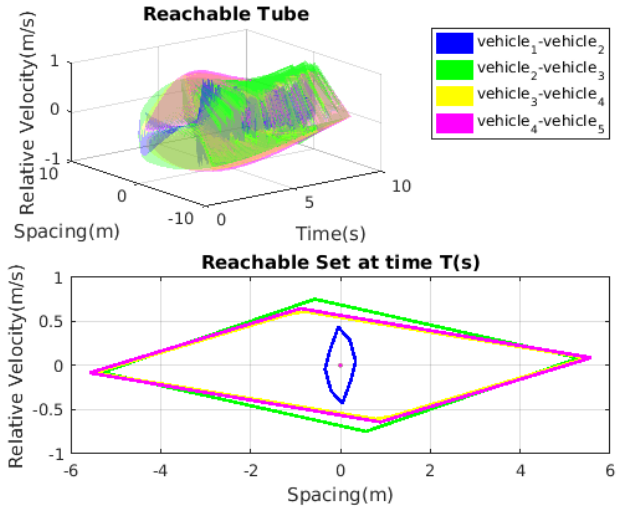


Fig. 3.3: Platoon reachable set and tube for T(s) duration of motion modification attack, when attacker is in the second place.

First, the reach set for the motion modification attack is shown. The attack happens when platoon already reached the steady state utilizing stable gains $k_p = 1$ and $k_d = 3.3$. 5-Vehicle platoon model involves 8 states which makes it hard to present the reachable sets graphically. Therefore, a projection for the demonstration purposes is applied to the results. In each case the reach tube and reach set for time $T = 10(s)$ is provided, where input limits for the attacker are considered to be $[-5, 5]$. Reachable sets and tubes of the platoon for different positions of the attacker using a motion modification attack are presented in Figs. 3.2, 3.3, ,3.4 and 3.5. Reachable relative velocity values are shown versus spacing values in each figure.

The reach set demonstration gives us a clear understanding of the extent that attacker, in each position is able to deviate platoon from its normal vehicle following motion and the

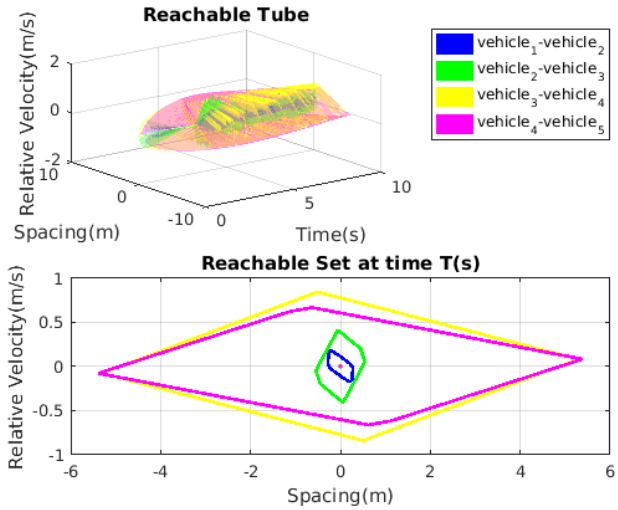


Fig. 3.4: Platoon reachable set and tube for T(s) duration of motion modification attack, when the attacker is in the third place.

severity of the attack in case of accidents. The analysis to determine whether the attacker is able to cause any collision between vehicles is based on (3.7). Collision happens when following vehicle hits or passes predecessor while moving in the same lane. Necessary and sufficient condition for the collision occurrence is presented as (5.19),

$$z_i \geq d. \tag{3.14}$$

Comparing desired spacing with the reachable set for the spacing, the instances of collision can be recognized.

For clarification, it is assumed that $d = 4m$, comparing (5.19) with Figs. 3.2 - 3.5, attacker in all positions is able to cause collisions between vehicles in front, but not the following ones. Observing the relative velocity values for all cases, it is shown that the collision happens when $v_i = v_{i+1} \pm 0.2$, which barely cause any damage to the vehicles. Higher relative velocity during collisions results in more severe damages. Reachable tubes present a constant pattern after $7(s)$ and reachable set for longer attack duration than $7(s)$ remain the same.

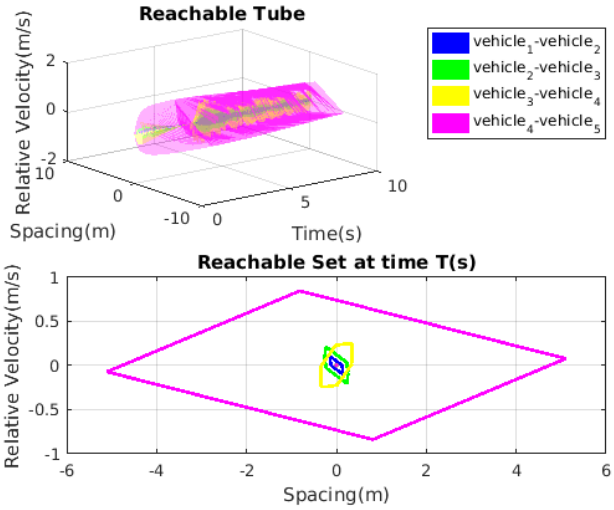


Fig. 3.5: Platoon reachable set and tube for T(s) duration of motion modification the attack, when the attacker is in the fourth place.

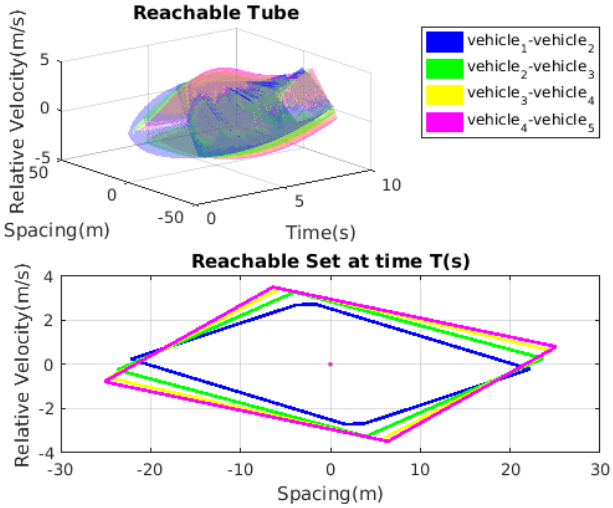


Fig. 3.6: Platoon reachable set and tube for T(s) duration of integral attack, when the attacker is in the first place.

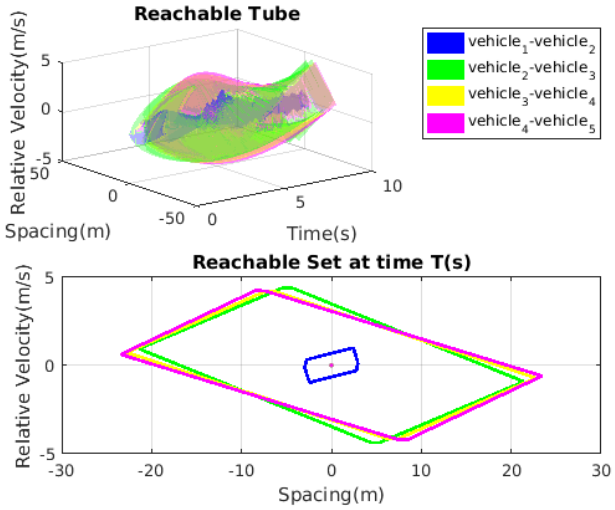


Fig. 3.7: Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the second place.

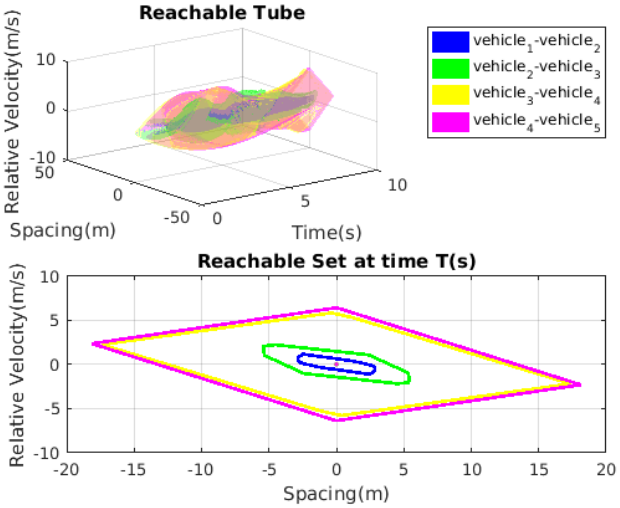


Fig. 3.8: Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the third place.

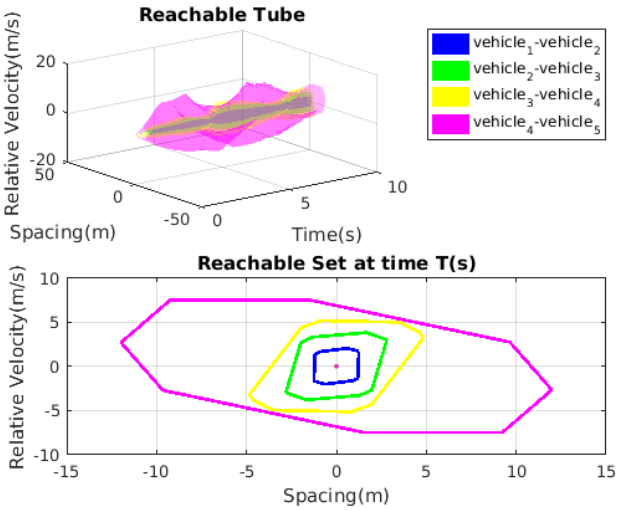


Fig. 3.9: Platoon reachable set and tube for T(s) duration of integral attack, when attacker is in the fourth place.

, Attacker randomly selects stable gains $\tilde{k_p} = 0.4$ and $\tilde{k_d} = -0.1$, such that all system eigenvalues remain in left half plane. Attacker uses the same range of input $[-5, 5]$ as motion modification attack to carry out integral attack. Corresponding reach set and tube for attacker in first position are presented in Fig. 3.6. Comparing the results for the same position of the attacker in two attack scenarios, Fig. 3.2 and Fig. 3.6, the attacker has broader range of impact in latter case, where attacker can cause collision in speed of $v_i = v_{i+1} \pm 3$. Attacker reach set grows as position of the attacker moves toward the leader of platoon as shown in Figs. 3.7 - 3.9, where attacker collide into leader in speed of $v_i = v_{i+1} \pm 5$. Reachable tube in Fig. 3.9 represents oscillatory movement which causes passenger discomfort and increases fuel consumption.

3.4.4 Discussion and Future work

Reachability analysis is proven useful to learn destructive attacks against vehicular platooning. Through the investigation, several points regarding reach set are surfaced, which are briefly pointed out as follows: In attacks involving motion modification, attacker states has the largest reachable set among other members and it grows larger as position

of the attacker moves towards leader in integral attack. While moving away from attacker the impact decreases on victims in both direction, and decreasing rate in direction pointing to the first vehicle is greater than the rate towards the leader. Duration of integral attack affects the reach set and in case of utilizing unstable gains, platoon reach set is very large and grows exponentially with time.

3.5 Summary

In this chapter, a method based on reachable set theory to investigate adversarial behavior in automated vehicle platoons is proposed. Vehicular platoons have been developed to increase highway throughput and safety, and to enhance driving comfort. The resulting deployment of Cyber-physical technology in critical infrastructure is increasingly attractive to both hackers and security researchers. To ensure safety and privacy of vehicle occupants, it is essential to identify the vulnerabilities of platoon systems. In this chapter, the attacker's capabilities under input constraints during two types of attack are studied: motion modification and integral attacks. Using ellipsoidal techniques, the extent of an attacker's ability to manipulate the control variables and states of a platoon resulting in oscillatory motion or collision is shown. At the end,the outcomes of the analysis are demonstrated by an example.

CHAPTER 4

Detection of the Attacker in Vehicular Platooning under Attack

4.1 Background and Contribution of This Work

Information and communication technologies have had a rapid development over the last few years and attracted many interests to their application in real-world processes. This expansion has led to the emergence of closed-loop systems involving strong integration and coordination of physical and cyber (computational and communication) components, often referred to as Cyber-Physical Systems (CPS). Actually, the key feature of these systems is their ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control. CPS applications range from daily life usage such as healthcare and smart grid systems to large-scale industrial applications and critical infrastructures such as water and transportation.

Cyber-physical systems are prone to failures and attacks on their physical infrastructure, and cyber attacks on their data management and communication layer. These attacks can vary in complexity and their target and can cause faults and failures in the physical process of the system. Increasing dependence on CPS in vital infrastructures and critical processes have risen the concern and demand for CPS to be inevitably secure, robust, reliable and trustworthy.

However, CPS suffer from specific vulnerabilities which do not affect classical control systems, and for which appropriate detection and identification techniques need to be developed. This realization led to the emergence of security challenges that are distinct from traditional network security. On the other hand, current information security methods, such as authentication, access control, and message integrity, are not powerful enough to completely secure and protect CPS.

In literature, several possible attacks against the control structure of cyber-physical

systems have been formulated with a focus on integrity attacks where an adversary alters a subset of control inputs, sensor measurements or control laws including replay [106], false data injection [97], zero dynamics [114], covert [131] and destabilizing [28] attacks.

In general, the attacks on CPS affecting communication can be classified into two categories [79]. These attacks share some common features with attacks on control. The first class of the attacks includes the attacks that prevent the exchange of information like jamming and DOS attacks while the second class of the attacks incorporates the false data injection in information packets. The second class is more difficult to identify and hence they are more detrimental to CPS security.

Due to the rising interest in improving the reliability of CPS, a significant research effort has been carried out to overcome the limitations of security algorithms in CPS and detect and handle failures in control systems. In recent years, few methods are being developed which are capable of tolerating component malfunctions whilst still maintaining desirable performance.

However, a key challenge in cyber-physical defense is a fast online detection and localization of faults and intrusions without prior knowledge of the failure type. Few attack detection algorithms have been proposed in the literature that can automatically detect and mitigate targeted attacks and failures. Authors in [114] studied detectability and identifiability of the attack based on changes that attacker can cause to the output and analyzed fundamental monitoring limitations for cyber-physical systems under attack modeled by linear time invariant descriptor systems with exogenous inputs. Yet, the attack is unidentifiable and undetectable when it excites zero dynamics.

Active detection methods to reveal stealthy attacks via manipulation of control inputs and dynamics have been proposed in [109]. In [109], a method of physical watermarking to authenticate the nominal behavior of a control system is proposed. Specifically, in this approach, a known noisy control input is purposely injected to detect replay attacks by analyzing the output of the system. The problem of secure state estimation, i.e. capability of reconstructing the state when CPS of interest is under attack, has been studied in [110,

130, 143]. Under the assumption of linear systems subject to an unknown but bounded number of false-data injection attacks, the problem for a noise-free system has been cast into an l_0-optimization problem, which can be relaxed as a more efficient convex problem [60], and later adapted to systems with bounded noise [112]. A model-based detection scheme that leverages the broadcast nature of dedicated short range communication (DSRC) is designed in [50] to detect a set of insider attacks in the vehicular platoon. Each car uses DSRC messages from other cars in the platoon to model the expected behavior of the car directly preceding it. If the expected behavior and actual behavior differ for the monitoring vehicle, the vehicle would be flagged as an attacker.

This work belongs to the family of studies that addresses gain modification and destabilizing attacks against Cyber-Physical System. The focus in this study is on less explored Cyber-security concerns in CPS and proposing an attack detection scheme. In terms of the methodology used in this work, the identification method and thresholding/clustering method, which is novel in detection field are combined. The proposed method is also computationally efficient, unlike most of the previously proposed approaches. To the best of author's knowledge, only in [82], an identification method for destabilizing attacks on power systems is proposed. Authors proposed an Unscented Kalman Filter (UKF) to identify the compromised buses in power systems. The proposed method can be considered as an effective method for the cyber-physical systems like vehicular platooning and power systems under not only destabilizing attack but also any gain modification attack in presence of noise. Moreover, the detection method is only based on prior knowledge on order of each subsystem and it does not require any further knowledge of the normal and adversarial parameters, number and place of attackers. The efficiency of the proposed algorithm is proved through illustrative example on vehicle platooning in an adversarial environment.

4.2 Problem Statement

In this section, models for Cyber-Physical Systems in presence of attack are introduced. In threat model, attacker capability to manipulate the system model to create an attack is described.

4.2.1 System Model

Cyber physical system is considered to be a linear time-invariant system. The equivalent state-space representation of the linear-time-invariant (LTI) system in discrete time is defined by (4.1):

$$\begin{aligned} \mathbf{x}_{k+1} &= A\mathbf{x}_k + B\mathbf{u}_k + w_k \\ \mathbf{y}_k &= C\mathbf{x}_k + v_k \end{aligned} \tag{4.1}$$

where $x_k \in R^n$ is the state vector at time instant k and $u_k \in R^m$ is control input. $y_k \in R^p$ is the vector of sensor measurements. w_k is the independent and identically distributed (IID) process noise with the probability distribution given by $w_k \sim N(0, Q)$ where $Q > 0$. Meanwhile, v_k is the IID measurement noise with distribution given by $v_k \sim N(0, R)$ where $R > 0$. It is assumed that (A, C) is detectable. Additionally, (A, B) and $(A, Q^{1/2})$ are assumed to be stabilizable. The set of measurements y are sent to the infrastructure in order to monitor the performance of the process.

Cyber-Physical Systems can be described as distributed systems in which each subsystem dynamic can be defined as a part of the larger system where its dynamic depends on its own states and other subsystems in the network. Hence, (4.1) can be reformulated as:

$$\begin{aligned} \mathbf{x_i}_{k+1} &= A_i\mathbf{x_i}_k + A_j\mathbf{x_j}_k + B_i\mathbf{u_i}_k + w_{i_k} \\ \mathbf{y_i}_k &= C_i\mathbf{x_i}_k + v_{i_k} \end{aligned} \tag{4.2}$$

where i index shows the matrices and states of each subsystem and $j \neq i$ is corresponding to other parts of the complex system and can refer to multiple subsystems.

4.2.2 Attack Model

The case of a single (or multiple) malicious actor(s) in control of interconnected systems, who attempts to destabilize or create oscillatory behavior in the system is examined. Attacker may accomplish this by causing the subsystem under its control to subvert or ignore the control law established for maintaining the normal performance of the system.

This implies that controller gains of the attackers could be modified [28, 44, 55, 82]. Therefore, the attacker is capable of disrupting the normal operation of the system via altering assigned nominal control parameters. An attacker can implement a gain modification attack via state feedback and modify the corresponding rows in A in (4.1).

Furthermore, applying linear feedback control changes rows of A_i and A_j in (4.2). System matrices in (4.2) are modified by the attacker as $A_i = A_i - B_i K_i$ and $A_j = A_j - B_i K_j$ where K_i and K_j are the state feedback gains with matching dimensions, B_i has nonzero entries for the external input to the corresponding subsystem. The subsystem equations (4.2) can be rearranged in the new set of equations (4.3), where A_i only can be defined for the states of the subsystem itself and all other variables affecting the subsystems' dynamics are counting as the input. So, (4.2) can be reformulated as

$$\begin{aligned} \mathbf{x_i}_{k+1} &= A_i \mathbf{x_i}_k + B_{n_i}[\mathbf{u_{i_k}}, \mathbf{x_{j_k}}] + w_{i_k} \\ \mathbf{y_i}_k &= C_i \mathbf{x_i}_k + v_{i_k} \end{aligned} \tag{4.3}$$

where B_{n_i} is formed by a combination of B_i and A_j matrices. The states of the other subsystem (coupling between subsystems) are considered as a new set of input to the subsystem.

4.3 Detection method

In section 4.2.2, it is discussed how attackers influence system by changing their control algorithms via their gains. Gain modification directly affects the system parameters and results in different parameters for the attackers' subsystems, i.e. parameters of the transfer function or state space representation, comparing to other subsystems. The proposed detection algorithm involves the following steps: 1)collecting the set of input-output data of each subsystem 2)identifying the parameters of each subsystem 3)comparing parameters/eigenvalues of all subsystems, and 4)detecting set of parameters/eigenvalues which do not follow the major pattern.

Two different approaches are applied to find each subsystem characteristics described in (4.3): 1)State Space Identification approach 2) Transfer Function Identification approach.

The former approach is dealing with the state space representation of the system and provides system matrices. For the detection purpose, A_i is chosen. This method is known as subspace identification. The latter method is an alternative method for identification of the system where parameters of the transfer function are estimated. The order of the system is known and fitting a model to input and output data is out of the scope of this work.

4.3.1 Identification Methods

Well matured area of system identification is comprised of various modeling techniques. Modeling is the abstraction of a real process to characterize its behavior. Although most of the analysis is in the interest of the continuous-time process, measurements are provided in the discrete form. Hence, discrete time system identification is chosen due to the access to discretized input and output data. In many cases, it is assumed that a signal x is set to a value $x(k)$ at time t_k (where t_k is the discrete time steps $t_k = kT_s$ and T_s is sampling period where k is an integer) and remains at that value until the next time step t_{k+1} (zero-order hold (ZOH) discretization). Equation (4.4) can be reformulated as (4.1) using Euler's forward approximation of the first derivative of a continuous signal x that is sampled at discrete time steps.

$$\begin{aligned} \dot{\mathbf{x}}(t) &= A_{CT}\mathbf{x}(t) + B_{CT}\mathbf{u}(t) + w(t) \\ \mathbf{y}(t) &= C_{CT}\mathbf{x}(t) + v(t) \end{aligned} \tag{4.4}$$

where $A = A_{CT}T_s + I$, $B = B_{CT}T_s$ and $C = C_{CT}$, I is the identity matrix with the same dimension as A_{CT}. Transfer function identification in continuous time is the process of modeling input and output relations in the Laplace domain. For continuous-time system (4.4), transfer function can be obtained $G(s) = C_{CT}(SI - A_{CT})^{-1}B_{CT}$ and for the discrete time system (4.1), using Z transform the transfer function would be $G(Z) = C(ZI -$

$A)^{-1}B$. Following, the system identification method for discrete time state space and transfer function representation of the system are discussed.

State Space Identification

Subspace identification methods are used to identify the parameters (matrices) of LTI state space model from the input and output data. Parameters of the identified linear system are obtained from the row or the column subspace of a matrix, which is formed from the input and output data. Using the sequence of input and output data, Hankel matrix can be formed to use geometric and mathematical tools to find system matrices. Input blocks for Hankel matrices are defined using,

$$U_p = \begin{bmatrix} u_0 & u_1 & \dots & u_{j-1} \\ u_1 & u_2 & \dots & u_j \\ \vdots & \vdots & \ddots & \vdots \\ u_{i-1} & u_i & \dots & u_{i+j-2} \end{bmatrix} \tag{4.5}$$

and

$$U_f = \begin{bmatrix} u_i & u_{i+1} & \dots & u_{i+j-1} \\ u_{i+1} & u_{i+2} & \dots & u_{i+j} \\ \vdots & \vdots & \ddots & \vdots \\ u_{i+h-1} & u_{i+h} & \dots & u_{i+h+j-2} \end{bmatrix}. \tag{4.6}$$

The matrix of Hankel associated to input U is given by

$$U_{0|2i-1} = \begin{bmatrix} U_p \\ - - - \\ U_f \end{bmatrix} \tag{4.7}$$

$$\begin{aligned} X_p &= \begin{bmatrix} x_0 & x_1 & \dots & x_{j-1} \end{bmatrix} \\ X_f &= \begin{bmatrix} x_i & x_{i+1} & \dots & x_{i+j-1} \end{bmatrix} \end{aligned} \tag{4.8}$$

The subscripts p and f refer to *past* and $future$, respectively. The number of block rows i is a user-defined index which should at least be larger than the maximum order of the system one wants to identify. The number of columns j is typically equal to $s-i-h+1$, which implies that all given data samples (s) are used where it is assumed $s \to \infty$ and $h = i$. Output block Y is constructed using the same method as input block. The instrumental variable matrix (or Hankel matrix of past data) is given by

$$W_p = (U_p^T \; Y_p^T)^T. \tag{4.9}$$

The extended observability and reversed extended controllability matrices are defined as:

$$\begin{aligned} \Gamma_i &= (C^T \quad (CA)^T \quad \dots \quad (CA^{i-1})^T)^T \\ \Delta_i &= ((A^{i-1}B)^T \quad (A^{i-2}B)^T \quad \dots \quad B^T)^T \end{aligned} \tag{4.10}$$

and the block Toeplitz matrix, H_i, is developed as

$$H_i = \begin{bmatrix} D & 0 & \dots & \dots & 0 \\ CB & D & 0 & \dots & 0 \\ CAB & CB & D & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ CA^{i-2}B & CA^{i-3}B & \dots & CB & D \end{bmatrix}. \tag{4.11}$$

N4SID method [134, 137] is used to find system matrices. The key step of this method is the oblique projection of subspaces generated by the block Hankel matrices formed by input/output data of the system using (4.5) - (4.8). Mathematical and geometrical tools like SVD (Singular Value Decomposition) are used to extract the order of the system and the observability matrix which contain the parameters of the estimated model. N4SID algorithm is explained as following. (4.1) can be extended as

$$\begin{aligned} \mathbf{X}_f &= A^i \mathbf{X}_p + \Delta_i \mathbf{U}_p \\ \mathbf{Y}_p &= \Gamma_i \mathbf{X}_p + H_i \mathbf{U}_p \\ \mathbf{Y}_f &= \Gamma_i \mathbf{X}_f + H_i \mathbf{U}_f \end{aligned} \tag{4.12}$$

It is assumed that the order of system is known. Hence, the steps for determining the order of the system are skipped. In N4SID method, two weighting matrices are used where W_1 usually is an identity matrix and W_2 should be chosen such that satisfies $rank(W_p) = rank(W_p W_2)$. O_i is the oblique projection:

$$O_i = \frac{Y_f}{U_f} W_p \tag{4.13}$$

and applying SVD decomposition,

$$W_1 O_i W_2 = [U_1 \ U_2] \begin{bmatrix} S_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_1^T \\ V_2^T \end{bmatrix} = U_1 S_1 V_1^T \tag{4.14}$$

The extended observability matrix Γ_i is given

$$\begin{aligned} \Gamma_i &= W_1^{-1} U_1 S_1^{\frac{1}{2}} T \\ X_f W_2 &= T^{-1} S_1^{\frac{1}{2}} V_1^T \\ X_f &= \Gamma_i^{\dagger} O_i \end{aligned} \tag{4.15}$$

where T is a non-singular similarity transformation matrix. System matrices can be derived using equations in (4.15). Matrix C is extracted directly from the first l rows of Γ_i where is l is equal to number of outputs. The matrix A is determined from the shift structure of Γ_i. Denoting

$$\underline{\Gamma}_i A = \overline{\Gamma}_i \tag{4.16}$$

where $\underline{\Gamma}_i$ is the Γ_i without last p rows where $y_k \in R^p$, equation (4.16) can be rewritten as

$$A = \underline{\Gamma}_i^{\dagger}\overline{\Gamma}_i \tag{4.17}$$

If Y_f in equation (4.12) multiplied by $\Gamma_i^{\perp}$ at left and at right by $U_f^{\dagger}$ and $\Gamma_i^{\perp}\Gamma_i = 0$, and can be obtained as follows:

$$\begin{aligned} \Gamma_i^{\perp} Y_f U_f^{\dagger} &= \Gamma_i^{\perp} H_i \\ L &= \Gamma_i^{\perp} \\ M &= \Gamma_i^{\perp} Y_f U_f^{\dagger} \end{aligned} \tag{4.18}$$

$$M = LH_i \tag{4.19}$$

A system of equations (4.19) which are function of B and D is resolved by a linear regression algorithm.

Transfer Function Identification

The basic relationship between the input and outputs is the linear difference equation

$$\begin{aligned} y(k) + a_1 y(k-1) + \ldots + a_n y(k-n) = \ldots \\ b_1 u(k-1) + \ldots + b_m u(k-m) + v(k) \end{aligned} \tag{4.20}$$

Equation (4.20) describes a linear, discrete-time system with transfer function,

$$\begin{aligned} G(z) &= \frac{b_1 z^{n-1} + b_2 z^{n-2} + \ldots + b_m z^{n-m}}{z^n + a_1 z^{n-1} + \ldots + a_n} \\ H(z) &= \frac{z^n}{z^n + a_1 z^{n-1} + \ldots + a_n} \end{aligned} \tag{4.21}$$

where system is causal ($n \geq m$). The approach to calculate values of parameters of the system, a_i and b_i, from observed data is needed. There are two inputs considered to the system, one is the normal input as $u(k)$ and the other is noise $v(k)$. Therefore, there are two transfer functions, $G(z)$ which shows the relations between y and u and the other one $H(z)$ demonstrates how v would affect the output y. We choose ARX (Autoregressive with exoge-

nous input) as the best fit for the system. If there is colored noise in the system, ARMAX is more appropriate model. ARX takes advantage of optimization methods to estimate the parameters of the system $[a_i \ b_j]$, such that the error between the real measurement and output with estimated value get close to zero.

4.3.2 Detection and Localization of the Attacker

Once the parameters of each subsystem is identified, a measure is applied to distinguish misbehaving subsystem from other subsystems. The proposed schemes to determine the attacker, Clustering and Thresholding, are applied to the parameters of system obtained from identification step.

Recall from the attack model, attacker changes at least one of its gains in order to affect the characteristics of the system. This modification leads to different system matrices or transfer function with unlike parameters than normal subsystems. Hence, a malicious agent is traceable via its different eigenvalues or parameter using former or latter identification approaches. Sometimes, the attacker targets the stability of the system causing instability or oscillation in the system. It can be safely concluded any subsystem has eigenvalues or poles out of or on the unit circle is the attacker's subsystem.

Clustering

K-means clustering algorithm is employed to automate the process of detecting anomalies. K-means Clustering aims to partition n observations into a certain number of clusters like k in which each observation belongs to the cluster with the nearest mean, serving as a prototype of the cluster. This algorithm is based on minimizing the cost function

$$J(v) = \sum_{i=1}^{n} \sum_{j=1}^{c_i} (\|x_i - v_j\|)^2 \tag{4.22}$$

where, $\|x_i - v_j\|$ is the Euclidean distance between x_i data points (eigenvalues or transfer function coefficients) and v_j center of each set. In this method, c is the number of clusters which is randomly chosen and c_i is the number of data points in the i_{th} cluster. K-means

clustering can be summarized as following steps: Let $X = x_1, x_2, \ldots, x_n$ be the set of data points and $V = v_1, v_2, \ldots, v_c$ be the set of centers. 1) Randomly select c cluster centers, 2) Calculate the distance between each data point and cluster centers, 3) Assign the data point to the cluster center whose distance from the cluster center is minimum of all the cluster centers, 4) Recalculate the new cluster center using: $v_i = \frac{1}{c_i} \sum_{j=1}^{c_i} x_i$, 5) Recalculate the distance between each data point and new obtained cluster centers and 6) If no data point was reassigned then stop, otherwise repeat from step 3).

Thresholding

Once the parameters of the system are identified, the anomaly detection method is applied to the set of estimated data.. The main idea of anomaly detection algorithm is to detect data instances in a data set, which deviate from the norm. The proposed method is alternate approach to clustering in order to find the outliers. In statistics, an outlier is an observation point that is distant from other observations and in the system, adversary related parameters fall out of normal set. This method relies on statistical properties like mean and standard deviation of the data points. The boundaries for the benign data points are set to lie within k standard deviations of the mean. The normal data domain is defined as $d = \mu \pm k\sigma$ where, $\mu = E[X] = \frac{1}{n} \sum_{i=1}^{n} x_i$ is the mean value of observations and $\sigma = \sqrt{E[(X-\mu)^2]}$ is the standard deviation. k is the coefficient which can be obtained by trial and error. The attacker is detected using,

$$Attacker = \underset{i}{\text{argmax}}(|parameter(i) - \mu|, \sigma). \tag{4.23}$$

4.4 Illustrative Example

In recent years, realization of secure vehicular platoon has been introduced as a new challenge in the field of cyber-physical systems [25, 28, 44–46]. Platooning is characterized by a tight coupling between vehicle's physical dynamics (mobility) and the computing and communications aspects of the vehicle. With rising public concern about transportation issues such as roadway capacity, traffic congestion, and highway safety, interest in vehicle

platoon has been increasing and automated driving vehicles have been the subject of active research over the last decade. However, the biggest concern regarding vehicle platoon and autonomous vehicles is safety and reliability. In order to realize a safe and trustful vehicle platoon system, using a reliable attack detection algorithm is a key enabling technology. In this section, proposed methods are applied to the vehicular platooning in presence of the adversary and the detection results are demonstrated.

4.4.1 Platoon and Threat Models

In attack scenario, which is under investigation, the attacker focuses on the exploitation of longitudinal control schemes, which are intended to allow an automated vehicles to maintain a desired separation/velocity from vehicles' immediate neighbor as they travel a straight path. A coupled and cooperative system of vehicles traveling on a straight trajectory at a constant velocity is considered. Vehicle convoy is assumed to be homogeneous in terms of performance characteristics and utilize the same control law for all participants. There is a central unit present as an essential infrastructure of the intelligent highway system to monitor the vehicle performance and has access to all vehicles' data, i.e., velocity and position.

Control laws govern how a vehicle should behave with respect to the movements of the preceding vehicle. Due to this interaction, the system of cooperative vehicles can be described using coupled differential equations. A stream of n vehicles can be described as follows:

$$\begin{aligned} \dot{x}_1 &= v_1 \\ \dot{v}_1 &= k_p(x_2 - x_1 - h\dot{x}_1) + k_d(\dot{x}_2 - \dot{x}_1) \\ &\vdots \end{aligned} \tag{4.24}$$

$$\dot{x}_{n-1} = v_{n-1}$$
$$\dot{v}_{n-1} = k_p(x_n - x_{n-1} - h\dot{x}_{n-1}) + k_d(\dot{x}_n - \dot{x}_{n-1})$$
$$\dot{x}_n = v_n$$
$$\dot{v}_n = u.$$

The equivalent state-space model of the linear-time-invariant (LTI) system defined by (4.24) is represented by (4.4): where $x(t) = [x_1,\ v_1,\ x_2,\ v_2, ...,\ x_{n-1},\ v_{n-1},\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the vehicle states, $A_{CT} \in \mathbb{R}^{2n\times 2n}$, $B_{CT} \in \mathbb{R}^{2n\times 2}$, $C_{CT} \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{u}$ is a scalar input. Because all the vehicle states are assumed to be measurable, C_{CT} is an identity matrix. B_{CT} has one non-zero entry for the lead vehicle's input and k_p, k_d, and h represent system gains.

Attack plot [55] involves a multi-attacker scenario where one active attacker directly controls vehicles' traveling by its motion and using modified gains for its control algorithm (4.25) and it is placed behind the leader of the platoon. Additionally, one or multiple passive attackers, following a modified control law (4.26), are present in the stream of vehicles as shown in Fig.4.1. Gains of passive attackers are determined deliberately to cause oscillation in the desired acceleration. The passive attacker vehicles could be colluding with other vehicles as a result of the exploit. All other vehicles in the platoon are considered victim vehicles. The leader of the platoon is denoted as a n_{th} vehicle. Stability of the system under attack is investigated in [55].

$$\dot{v}_a = k_{p_a}(x_{a+1} - x_a - h_a v_a) + k_{d_a}(v_{a+1} - v_a) + u_a \tag{4.25}$$

The active attacker, indicated by subscript $_a$, changes its gains to k_{p_a}, k_{d_a} *and* h_a and modifies its motion using u_a . Subscript $_{a+1} =_n$ refers to the leader of the platoon. k_{p_p}, k_{d_p} and h_p are passive attackers' selected gains,

$$\dot{v}_i = k_{p_p}(x_{i+1} - x_i - h_p v_i) + k_{d_p}(v_{i+1} - v_i) \tag{4.26}$$

The goal of the attackers is to introduce instability by modifying the elements of A_{CT} in (4.4) corresponding to each attacker so as to produce an unstable system, and then perturb the system to ensure the system is forced out of steady state equilibrium. The overall effect of the attack is a reduction in traffic flow stability and secondary impact is the possible occurrence of collisions.

In order to present the detection problem in the form of (4.3), the whole platoon is divided into the identification of one vehicle as the subsystem. The states and inputs of each vehicle (subsystem) are described as $X = [x_i, v_i]^T$, $u = [p_{i+1}, v_{i+1}]^T$, and y is the output vector that consists of all states of the vehicle. The measurement noise is n, where $n \sim N(0, R^n)$. A_i, B_i *and* $C_i = I$ are matrices of each vehicle in discrete time as follows,

$$A_i = \begin{bmatrix} 1 & T_s \\ -k_{p_i}T_s & (-k_{d_i} - k_{p_i}h_i)T_s + 1 \end{bmatrix}$$

$$B_i = \begin{bmatrix} 0 & 0 \\ k_{p_i}T_s & k_{d_i}T_s \end{bmatrix}$$

These matrices have the same structure for all passive attackers and normal vehicles and in each case, entries are substituted by attackers' or normal gains, respectively. A and C matrices are the same for the active attacker and B matrix has another column for the external input to active attacker u_a.

The Two-input-Two-output system for each vehicle is considered and state space identification approach is applied to the set of inputs and outputs to identify the entries of the matrix A_i and calculate eigenvalues from resulted matrix entries.

Since attacker mainly affects platoon through its gains and the system's parameters vary with different gains, system identification is a basic step in the detection approach. Each vehicle input-output relation is described using 4 different transfer functions. Each

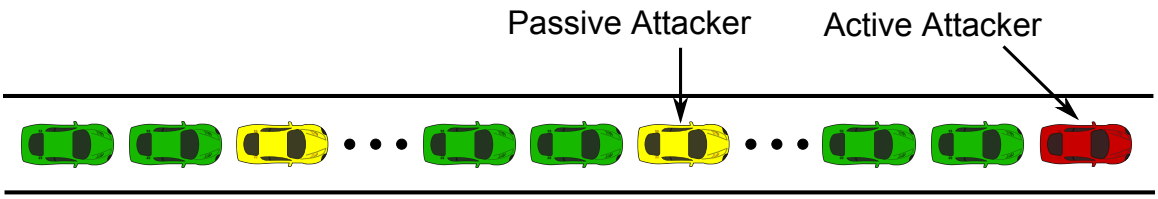


Fig. 4.1: System of automated vehicles in the presence of attackers

output according to superposition property of linear systems is the summation of the responses of the system to two inputs. Transfer functions have the similar form as

$$G_x(z) = \frac{b_{x_1} + b_{x_2} Z^{-1}}{1 + a_{x_2} Z^{-1} + a_{x_3} Z^{-2}} \tag{4.27}$$

with one zero and two poles which describe the relation between position and velocity of the preceding vehicle as inputs and the position and velocity of each vehicle as outputs.

In next step, to identify the attacker, the parameters $a_{x_{2,3}}$ and $b_{x_{1,2}}$, coefficients of numerator and denominator of (4.27) using transfer function identification approach are estimated.

Remark 1 *As attacker mainly affects the relations between positions and velocities as inputs and outputs by changing gains,the same model considered for all vehicles (normal, active and passive attacker) is considered. Given that, the external input to active attacker does not influence the analysis.*

4.4.2 Detection Results

As the second step to detect attacker, the parameters are estimated and the most affected parameters from gain alteration scenario are identified. To test the efficiency of the proposed detection approach, 1000 data sets of 101-vehicle platoon under the described attack for various positions and numbers of attackers created using Monte Carlo simulation are utilized. To demonstrate the efficiency of the method, a sample data set where $k_p = 1,\ k_d = 1.2746\ and\ h = 1.166$ is chosen. In this data set, the variance of noise on measurements are 0.1 and attackers' positions are [8 9 11 51 76 77 87 100] where vehicle 100 is the active attacker $k_{d_a} = -2$ and the rest are passive attackers $k_{d_p} = -0.8929$. Vehicle

101 is the leader and leader's parameters are not included in the analysis. The sampling period T_s is 1 second. The results of transfer identification approach are presented in Fig. 4.2 - Fig. 4.5. In Fig. 4.2, estimated parameters for $\frac{x_i}{x_{i+1}}$ transfer function are shown. Moreover, the thresholding results are included in each figure. Blue line shows the mean and green line is the standard deviation from the mean. It can be concluded from Fig. 4.2 that attackers are distinguishable as their identified values are far from normal estimated values and we consider the parameters a_{1_2}, a_{1_3} and b_{1_1} of $\frac{x_i}{x_{i+1}}$ transfer function dependable measures to identify the attackers.

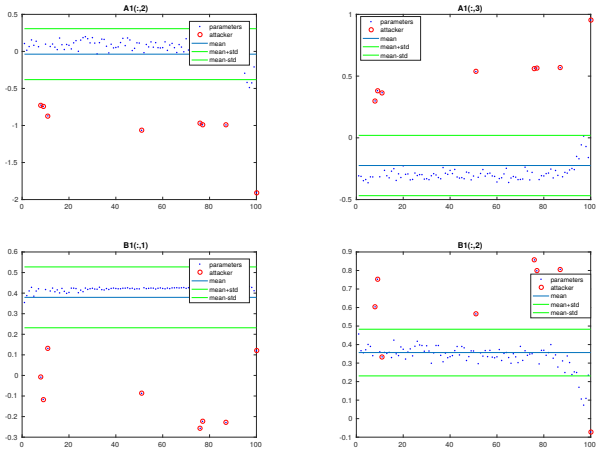


Fig. 4.2: Parameters for the $\frac{x_i}{x_{i+1}}$ transfer function

Estimated parameters for $\frac{x_i}{v_{i+1}}$ demonstrated in Fig. 4.3 are not revealing noticeable difference between victims and attackers. Thus, these parameters are not reliable measures to detect the attackers. Identification parameter's deviation for $\frac{v_i}{x_{i+1}}$ and $\frac{v_i}{v_{i+1}}$ shown in Figs. 4.4 and 4.5 are very small and it is not trustworthy measure to assess the benevolence of each vehicle.

Comparing the results from Figs. 4.2 - 4.5, the parameters of $\frac{x_i}{x_{i+1}}$ transfer function to determine the attackers' vehicles are determined. There are two important factors in detection scheme: 1) parameter that reflects difference in all data sets and 2) the number of sample points included in attack detection window. The parameters a_{1_2}, a_{1_3} and b_{1_1},

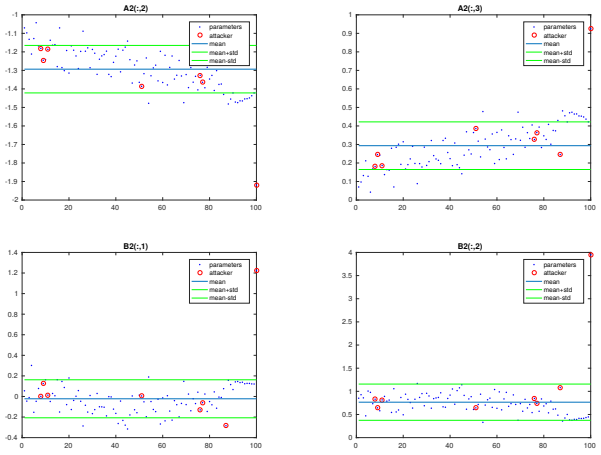


Fig. 4.3: Parameters for the $\frac{x_i}{v_{i+1}}$ transfer function

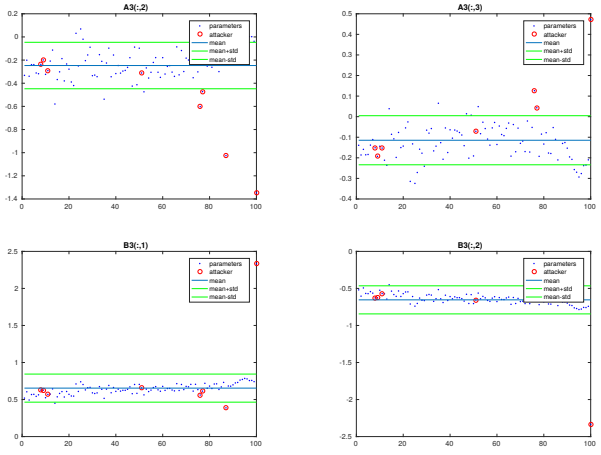


Fig. 4.4: Parameters for the $\frac{v_i}{x_{i+1}}$ transfer function

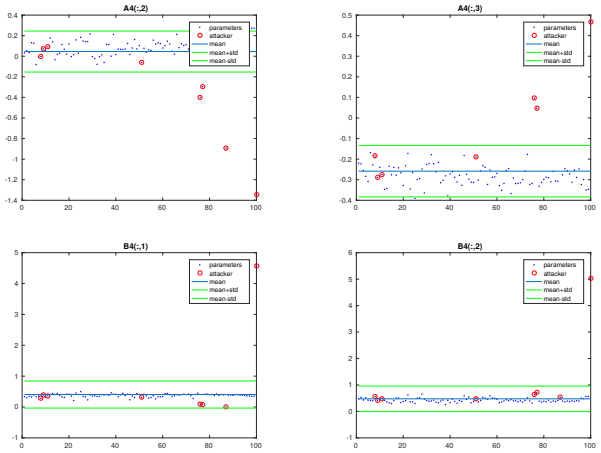


Fig. 4.5: Parameters for the $\frac{v_i}{v_{i+1}}$ transfer function

together and individually, and different duration for parameter identification are deployed to achieve best true positive and false positive rates on data sets. Duration of each data set is $1200(s)$ and best result is for $[60(s) - 180(s)]$. It is worth noting that in all the data sets, attack has already started or going to happen in this duration and system is not in steady state. The best true positive and false positive rates as presented in Table 4.1 are for the case we set threshold on $b1_1$. The identified parameter belongs to the attacker if $b_{1_1}(i) \notin \mu(b_{1_1}) \pm \sigma(b_{1_1})$.

True positive rate (TPR) and false positive rate (FPR) using b_{1_1} for the different level of noise in measurements are presented in Table. 4.1.

Table 4.1: Detection rates using transfer function (TF) and State Space (SS) attacker detection scheme

Noise Variance	TPR (TF)	TPR (SS)	FPR (TF)	FPR (SS)
0	100	100	0	0
0.1	91.2	94.4	0.86	0.69
0.5	85.3	89.7	1.13	1.03
1	61.5	73.6	1.74	1.55

State space identification approach and detection algorithm are applied to same sample

data set and computed eigenvalues and detection results are presented in Figs.4.6 and 4.7. Using state space identification results of A matrix, the eigenvalues of the system are computed. Changing gains in the system results in the variation of eigenvalues which is the key factor in detecting the attacker. This helps the clustering algorithm to categorize the eigenvalue of the vehicle in two different groups and it is assumed that the attackers are minority in vehicular platoon. Result of clustering is presented in Fig. 4.7. The results illustrate that the proposed detection method is able to detect all attackers of platoon successfully. Comparison of the detection rate for two proposed approaches is presented in Table 4.1 and results indicate that state space identification approach combined with clustering method is more efficient in detecting adversaries in platoon.

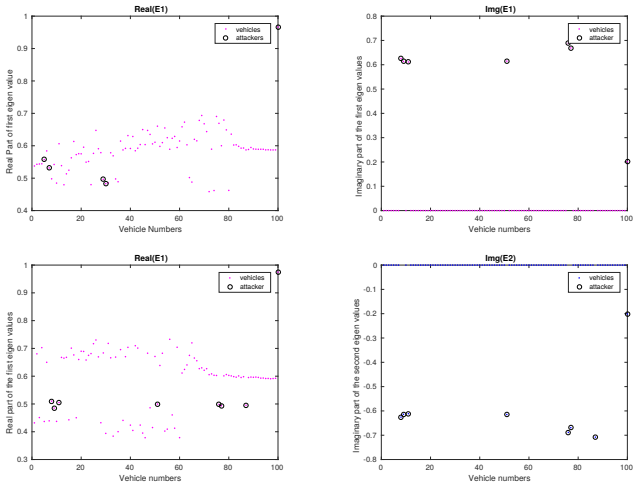


Fig. 4.6: Eigenvalues of the system calculated from state space identification method

4.5 Summary

Cyber-Physical Systems (CPS) are systems with tight coupling between integration of physical, computational and networking components. Control systems play an important role to help these systems to adhere to their desired performance. Having a reliable and secure control system which can cope with high risk situations and various attacks is one of the bottlenecks for real-world Cyber-physical systems. It has been proven that using

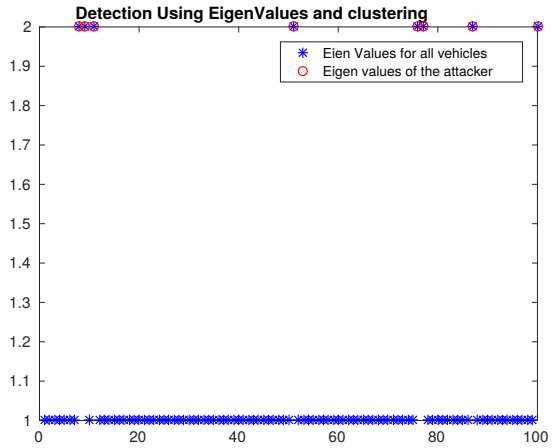


Fig. 4.7: Attack detecting result using state space identification and clustering methods

control modification attack, where the adversary modifies the sensor information or the control law, can disrupt the desired performance of the system. In this chapter, a novel scheme is presented to detect and identify the attacker in control systems. The detection algorithm is the combination of the system identification method and machine learning technique which effectively recognizes the malicious actors. The proposed algorithm is efficient, viable, and simply adequate to address the challenges posed by complex Cyber-physical systems. Finally, the efficiency of the presented method is verified with the case of platooning in an adversarial environment.

CHAPTER 5

Resilient Control for the Platooning in Adversarial Environment

5.1 Background and Contribution of This Work

Recent efforts in automotive industry point in the direction of increased content of electronics, computers, and controls with an emphasis on the improved functionality, automation and overall system robustness. These endeavors result in emerging technologies in the field of autonomous vehicles and Intelligent Transportation Systems (ITS) i.e. platooning. The platooning concept involves a group of vehicles acting as a single unit through coordination of movements. While vehicle platooning can benefit human beings in various aspects like decrease in the number of collisions due to human error, minimization of traffic congestion as a result of the increase in highways throughput, and reduced fuel consumption, there is a particular interest in security of vehicular platooning. It is an essential part to this field and complicates the integration of this technology in real world.

There are three types of security challenges in CPS control systems. The first issue deals with the security attacks and threats. In literature, several possible attacks against control structure of Cyber-Physical Systems have been formulated with a focus on the attacks where an adversary alters a subset of control inputs, sensor measurements or control laws including replay [107], false data injection [97,105], zero dynamics [114], covert [131] and destabilizing [28] attacks. The second challenge in securing the CPS against cyber attacks is to provide the CPS with an attack detection algorithm. There exist several investigations on modeling and detection of cyber attacks from network security and control systems perspectives. The current state of the art methods used for cyber attack detection are Intrusion Detection Systems (IDS) where they continuously monitor the system or network and generate alarms to inform the system administrator of suspicious events [66, 123]. Authors in [114] studied detectability and identifiability of the attack based on changes that attacker can cause to the

output and analyzed fundamental monitoring limitations for cyber-physical systems under attack modeled by linear time invariant descriptor systems with exogenous inputs. Yet, the attack is unidentifiable and undetectable when it excites zero dynamics. Active detection methods to reveal stealthy attacks via manipulation of control inputs and dynamics have been proposed in [141]. A model-based detection scheme that leverages the broadcast nature of dedicated short range communication (DSRC) is designed in [50] to detect a set of insider attacks in the vehicular platoon. Novel detection approach based on system identification and clustering for gain modification attack is proposed in [24]. The presented approach estimates the parameters of each subsystem and locates all attackers through their parameter when they deviate from mainstream. As the last but very crucial challenge of cybersecurity in CPS, attack resiliency is of utmost importance to maintain the functional CPS in the presence of cyber attacks. Authors comprehensively survey the concept and strategies for building resilient and integrated cyber-physical systems in [78]. Mitigation technique based on sliding mode controller coupled with an attack detection scheme, that ensures that deviations from desired inter-vehicle separations remain low, is designed in [121]. Sliding surface is designed based on errors in desired values for relative spacing and velocity. Authors in [7] investigate resilient control under Denial of Service (DoS) attack in connected vehicles application. Estimation scheme is added to the conventional Cooperative Adaptive Cruise Control (CACC) control strategy to make the platoon resilient to DoS attack.

One of the possibilities to enhance the performance of control algorithms and make them robust against uncertainties is to extend its integer order element to fractional order [36,37,39,100–102]. An increasing number of studies can be found related to the application of fractional controllers in many areas of science and engineering [21, 22, 31, 33, 38, 41–43]. Podlubny [117] has proposed a generalization of the PID controller, namely the $PI^{\lambda}D^{\mu}$ controller, involving an integrator of order and differentiator of order (the orders may assume real noninteger and nonnegative values). However, to the best knowledge of the authors, the resilient control of Cyber-physical systems under attack using the fractional order controllers

has not yet been studied.

The aim of this work is to propose an effective method to mitigate the attacker's impacts on the platoon under attack. This work falls under the category of resilient control design for the platoon against the gain modification attacks. To cope with the security challenges and threats, a novel fractional calculus-based technique is proposed to eliminate collisions and undesired oscillations in the platoon under the gain modification and destabilizing attacks. The aforementioned attacks not only can cause collisions in high relative velocities, which result in catastrophic damages to vehicles in a platoon, but also can increase fuel consumption due to oscillatory behavior. Hence, finding an effective way to reduce such impacts can be of great importance. Considering the platoon dynamics in presence of the adversary, in this study a fractional order controller is put forth to alleviate attacker's influence. The proposed approach is decentralized and the attacker can be controlled locally after being detected. In this work, a stabilizing controller is designed to obtain a robustly stable closed-loop system. The main contribution of this work is to propose a simple design of a robust stabilizing fractional order controller for the systems under attack. While the common and frequently used techniques to tackel the gain variation in classic control system are sliding mode control and adaptive control [30,32,34,35,40] they are not efficient for the system under the attack.The closest work to the proposed contribution is [121] where two different controllers are considered for the platoon. There is switching between the control in presence of attack and normal platooning control algorithm, which state is determined based on attack detection algorithm. The drawback of this approach is the drastic change between linear control and sliding mode control is not considered. The other issue regarding [121] is that upon attack detection the configuration of the platoon is changed which is not advisable and, in some cases, unfeasible in practice.

5.2 Problem statement

The controller design focuses on strengthening longitudinal control laws of the vehicles in platoon, which are intended to maintain desired separation and velocity as they follow straight line. Assuming all vehicles are traveling in one dimension, attacker gets the chance

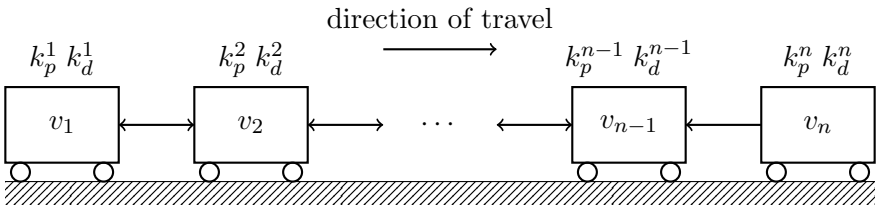


Fig. 5.1: An n-vehicle platoon employing a bi-directional control law. Arrows represent the flow of information.

to influence other vehicles' motion via manipulating longitudinal control algorithm.

5.2.1 Platoon Model

The bi-directional (predecessor-follower) proportional-derivative (PD) controller is used to demonstrate the impact of a malicious actor on platooning operations. This control law is capable of maintaining a constant separation, d, between vehicles, based solely on local sensing. This is important because it allows us to show that an attacker can affect the platoon solely through malicious movement. Formally, the dynamics of a platoon with n vehicles employing this control law for the leader are described by the following system of equations,

$$
\begin{aligned}
\dot{x}_1 &= v_1, \\
\dot{v}_1 &= k_p^1(x_2 - x_1 - d) + k_d^1(v_2 - v_1), \\
\dot{x}_2 &= v_2, \\
\dot{v}_2 &= k_p^2(x_1 - x_2 + d) + k_p^2(x_3 - x_2 - d), \\
&\quad + k_d^2(v_1 - v_2) + k_d^2(v_3 - v_2), \\
&\vdots \\
\dot{x}_{n-1} &= v_{n-1}, \\
\dot{v}_{n-1} &= k_p^{n-1}(x_{n-2} - x_{n-1} + d) + k_p^{n-1}(x_n - x_{n-1} - d), \\
&\quad + k_d^{n-1}(v_{n-2} - v_{n-1}) + k_d^{n-1}(v_n - v_{n-1}),
\end{aligned}
$$

$$\begin{aligned} \dot{x}_n &= v_n, \\ \dot{v}_n &= k_p^n x_{n-1} - k_p^n x_n + k_p^n d + k_d^n v_{n-1} - k_d^n v_n + u_l \end{aligned} \tag{5.1}$$

where x_i and v_i represent the position and velocity of the i_{th} vehicle, respectively ($\dot{a}$ denotes the first derivative with respect to time of the variable a), and k_p^i and k_d^i represent their proportional and derivative gains, respectively. For normal platooning operations k_p^i and k_d^i are the same for each vehicles (the superscript is omitted unless referring to the gains for a vehicle in a particular position). The proportional gain k_p is traditionally fixed at 1, while k_d varies according to the size of the platoon [28]. Here, u_l represents the control input for the leader (n_{th} vehicle). In the steady-state u_l is generally taken to be equal to zero; however, it is noted that $k_p^n \neq 0$ and $k_d^n \neq 0$ implies that the followers would be able to influence the leader's movements, unless u_l is set to cancel out the follower movements, which would effectively set $k_p^n = k_d^n = 0$. In any case, from the security perspective it seems inadvisable for followers to be able to influence the leader.

5.2.2 Threat Models

The mitigation scheme for the platoon in presence of malicious vehicle is proposed. The controller is designed for the platoon states, where attacker implements an attack through modifying its control algorithm. A technique to eliminate the undesired effects of attack on the platoon is proposed. The attack model would be similar to (5.2) and the corresponding row to the attacker in A matrix would be modified like [28]. It is assumed that the attacker does not act as the leader of the platoon.

The equivalent state-space representation of the linear time-invariant (LTI) system defined by (5.1) in the presence of an attacker is

$$\begin{aligned} \dot{\mathbf{X}} &= A\mathbf{X} + B\mathbf{U} \\ \mathbf{Y} &= C\mathbf{X} \end{aligned} \tag{5.2}$$

where $X = [x_1,\ v_1,\ x_2,\ v_2,\ \cdots,\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the states of all the vehicles in the

platoon and Y is the output, which in this case is similar to states, $A \in \mathbb{R}^{2n\times 2n}$, $B \in \mathbb{R}^{2n\times 1}$, $C \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{U} = [u_l]^\intercal$. C is the identity matrix (because it is assumed that all the vehicle states are measurable), B has the non-zero entries corresponding to the leader and the attacker control. A matrix using (5.1) can be formed as (5.3).

$A =$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -k_p & -k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix} \tag{5.3}$$

Leader of the platoon would be counted as the n_{th} vehicle in the platoon, as shown in Fig. 5.1, and it is assumed that all vehicles in platoon follow the normal control law in motion modification attack described in (5.2) before the attack. In the gain modification attack, the attacker applies the changes to its corresponding row of A matrix. The changes to A matrix is described as follows: Allow $A(i, j)$ to represent access to the element at the i_{th} row and j_{th} column of A. When an attacker is present at the first position,

$$\begin{aligned} A(2,1) &= -\tilde{k_p}, \\ A(2,3) &= \tilde{k_p}, \\ A(2,2) &= -\tilde{k_d}, \\ A(2,4) &= \tilde{k_d}. \end{aligned} \tag{5.4}$$

An attacker in the i_{th} position, $1 < i < n$, changes the following elements of (5.3)

$$\begin{aligned} A(2i, 2(i-1)-1) &= \tilde{k_p}, \\ A(2i, 2i-1) &= -2\tilde{k_p}, \\ A(2i, 2i+1) &= \tilde{k_p}, \\ A(2i, 2(i-1)) &= \tilde{k_d}, \\ A(2i, 2i) &= -2\tilde{k_d}, \\ A(2i, 2(i+1)) &= \tilde{k_d} \end{aligned} \tag{5.5}$$

where derivative and proportional gains of the attacker are shown using $\tilde{k_d}$ and $\tilde{k_p}$.

5.3 Attack Mitigation Algorithm Design

To recover platoon from gain modification and destabilizing attacks, the use of fractional order controller is suggested. The stability criterion is expanded by fractional order calculus and make system robust against destabilizing attack. The proposed controller improves system performance in presence of the adversary and reduce the number of collisions and undesired oscillatory movement caused by the attacker. Fractional order controller guarantees speedy recovery from attack and least damages to the vehicles in the platoon. The mitigation algorithm is incorporated into the system based on the detection scheme proposed in [24]. The detection is based on system identification and machine learning algorithm. The infrastructure receives all measurements (velocities and positions of each vehicle) and estimate the parameter of each vehicle using adjacent vehicles' measurement as input and the velocity and position of the vehicle as output. Clustering is applied to the estimated parameters of the system, resulted from system identification, to detect anomalies. The controller is designed such that, it stabilizes the system and enables the defending cars to maintain the safe distance with the other vehicles. In the controller design, it is assumed there is a communication link between vehicles, where the defender can inject the control input to the attacker's controller.

5.3.1 Fundamentals of fractional calculus and fractional order systems

Fractional-order integration and differentiation is the generalization of the integer-order ones. Efforts to extend the specific definitions of the traditional integer order to the more general arbitrary order context led to different definitions for fractional derivatives [48]. Two of the most commonly used definitions are the Riemann-Liouville and Caputo definitions.

Definition 5.3.1 *Riemann-Liouville integration([116]) The n_{th} fractional-order Riemann-Liouville integral (n real positive) of a function $f(t)$ is defined by the relation*

$$I_n(f(t)) = \frac{1}{\Gamma(n)} \int_0^t (t-\tau)^{n-1} f(\tau) d\tau \tag{5.6}$$

Definition 5.3.2 *([116]) One of the basic functions of the fractional calculus is Eulers Gamma function which is defined by*

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt \tag{5.7}$$

which converges in the right half of the complex plane, i.e. $Re(z) > 0$.

Definition 5.3.3 *([116]) The αth-order RiemannLiouville fractional derivative of function $f(t)$ with respect to t and the terminal value 0 is given by*

$$\frac{d^\alpha f(t)}{dt^\alpha} = \frac{1}{\Gamma(m-a)} \frac{d^m}{dt^m} \int_0^t \frac{f(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau \tag{5.8}$$

where m is the first integer larger than α, i.e. $m-1 \leq \alpha < m$ and Γ is the Gamma function

Definition 5.3.4 *([116]) The Caputo fractional derivative of order α of a continuous function $f : R_+ \to R$ is defined as follows*

$$\frac{d^\alpha f(t)}{dt^\alpha} = \begin{cases} \frac{1}{\Gamma(m-\alpha)} \int_0^t \frac{f^m(\tau)}{(t-\tau)^{\alpha-m+1}} d\tau & m-1 < \alpha < m \\ \frac{d^m}{dt^m} f(t) & \alpha = m \end{cases} \tag{5.9}$$

Theorem 1 *[51] Consider the following n-dimensional linear fractional order system*

$$\begin{aligned} \frac{d^{\alpha_1} x_1(t)}{dt^{\alpha_1}} &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}, \\ \frac{d^{\alpha_2} x_2(t)}{dt^{\alpha_2}} &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}, \\ &\vdots \\ \frac{d^{\alpha_n} x_n(t)}{dt^{\alpha_n}} &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}, \end{aligned} \tag{5.10}$$

where all $0 < \alpha_i \leq 1$. Assume M is the lowest common multiple of the denominators ud_i's of α_i's, where $\alpha_i = vd_i/ud_i, (ud_i, vd_i) = 1, ud_i, vd_i \in Z^+$, for $i = 1, 2, \cdots, n$. By defining

$$\Delta(\lambda) = \begin{bmatrix} \lambda^{M\alpha_1} - a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & \lambda^{M\alpha_2} - a_{22} & -\cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & \lambda^{M\alpha_1} - a_{nn} \end{bmatrix} \tag{5.11}$$

Then the zero solution of system (5.11) is globally asymptotically stable in the Lyapunov sense if all roots λ 's of the equation $det(\Delta(\lambda)) = 0$ satisfy $|arg(\lambda)| > \pi/2M$. $\Delta(s)$ is called the characteristic matrix and $det(\Delta(s))$ is called the characteristic polynomial of system (5.11) [51].

In case of $\alpha_1 = \alpha_2 = \cdots = \alpha_n = \alpha$, Fig. 5.2 shows the stable region for $0 < \alpha < 1$.

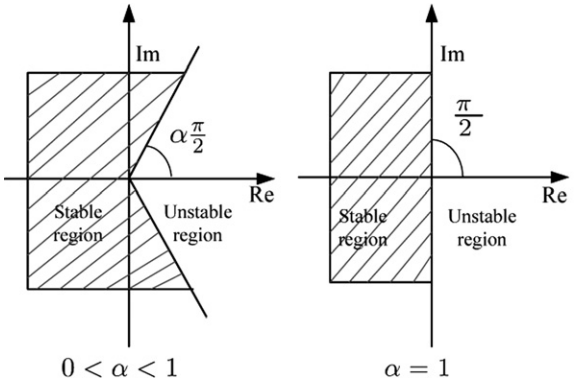


Fig. 5.2: Stability region of fractional system.

5.3.2 Controller Design

In the control design, the aim is to add a robust stabilizing controller on top of the normal controller of the platoon in order to stabilize the platoon and prevent collisions. Without loss of generality, the controller design procedure is described for 5-vehicle platoon where attacker is in the

third position (5.12) and changes its gains from k_d to $\tilde{k_d}$.

$$
\begin{aligned}
\dot{x}_1 &= v_1, \\
\dot{v}_1 &= k_p(x_2 - x_1 - d) + k_d(v_2 - v_1), \\
\dot{x}_2 &= v_2, \\
\dot{v}_2 &= k_p(x_1 - x_2 + d) + k_p(x_3 - x_2 - d), \\
&\quad + k_d(v_1 - v_2) + k_d(v_3 - v_2), \\
\dot{x}_3 &= v_3, \\
\dot{v}_3 &= k_p(x_2 - x_3 + d) + k_p(x_4 - x_3 - d), \\
&\quad + \tilde{k}_d(v_2 - v_3) + \tilde{k}_d(v_4 - v_3), \\
\dot{x}_4 &= v_4, \\
\dot{v}_4 &= k_p(x_3 - x_4 + d) + k_p(x_5 - x_4 - d), \\
&\quad + k_d(v_3 - v_4) + k_d(v_5 - v_4), \\
\dot{x}_5 &= v_5, \\
\dot{v}_5 &= u_l
\end{aligned}
\tag{5.12}
$$

The proposed controller is applied to the vehicle under attacker's control in order to tackle the attacker effect on the platoon system,

$$
\begin{aligned}
\dot{x}_1 &= v_1, \\
\dot{v}_1 &= k_p(x_2 - x_1 - d) + k_d(v_2 - v_1), \\
\dot{x}_2 &= v_2, \\
\dot{v}_2 &= k_p(x_1 - x_2 + d) + k_p(x_3 - x_2 - d), \\
&\quad + k_d(v_1 - v_2) + k_d(v_3 - v_2), \\
\dot{x}_3 &= v_3, \\
\dot{v}_3 &= k_p(x_2 - x_3 + d) + k_p(x_4 - x_3 - d), \\
&\quad + \tilde{k}_d(v_2 - v_3) + \tilde{k}_d(v_4 - v_3) - k_i D^{\alpha} v_3 + D(v_3),
\end{aligned}
\tag{5.13}
$$

$$
\begin{aligned}
\dot{x}_4 &= v_4, \\
\dot{v}_4 &= k_p(x_3 - x_4 + d) + k_p(x_5 - x_4 - d), \\
&\quad + k_d(v_3 - v_4) + k_d(v_5 - v_4), \\
\dot{x}_5 &= v_5, \\
\dot{v}_5 &= u_l
\end{aligned}
$$

The controller term is shown as $Dv_3 - k_i D^{\alpha} v_3$ which includes a fractional order differentiator and α (the differentiation order) is the design parameter. From (5.13), one can conclude

$$
\begin{aligned}
\dot{x}_1 &= v_1, \\
\dot{v}_1 &= k_p(x_2 - x_1 - d) + k_d(v_2 - v_1), \\
\dot{x}_2 &= v_2, \\
\dot{v}_2 &= k_p(x_1 - x_2 + d) + k_p(x_3 - x_2 - d), \\
&\quad + k_d(v_1 - v_2) + k_d(v_3 - v_2), \\
\dot{x}_3 &= v_3, \\
D^{\alpha} v_3 &= k_{cp}(x_2 - x_3 + d) + k_{cp}(x_4 - x_3 - d), \\
&\quad + \tilde{k}_{cd}(v_2 - v_3) + \tilde{k}_{cd}(v_4 - v_3), \\
\\
\dot{x}_4 &= v_4, \\
\dot{v}_4 &= k_p(x_3 - x_4 + d) + k_p(x_5 - x_4 - d), \\
&\quad + k_d(v_3 - v_4) + k_d(v_5 - v_4), \\
\dot{x}_5 &= v_5, \\
\dot{v}_5 &= u_l
\end{aligned}
\tag{5.14}
$$

where $k_{cp} = k_p/k_i$ and $k_{cd} = \tilde{k}_d/k_i$. Due to control law applied to the system (5.13), v_3 involves fractional order term in the closed loop system. In order to analyze the closed loop system stability, considering $\alpha = p/q$, system (5.14) can be rewritten as

$$
\begin{aligned}
Dx_1 &= f_1(x, v), \\
Dv_1 &= f_2(x, v), \\
Dx_2 &= f_3(x, v), \\
Dv_2 &= f_4(x, v), \\
Dx_3 &= f_5(x, v), \\
D^{(p/q)}v_3 &= f_6(x, v), \\
&\vdots \\
Dx_5 &= f_9(x, v), \\
Dv_5 &= f_{10}(x, v, u_l).
\end{aligned}
\tag{5.15}
$$

It can be inferred that q is the lowest common multiple of the denominators in (5.15). According to Theorem (1), and comparing (5.10) with (5.15), the equilibrium point of the system (5.15) is asymptotically stable if:

$$
|arg(\lambda)| > \pi/2q, \tag{5.16}
$$

for all roots λ_i s of (5.17),

$$
\det(diag([\lambda^q \cdots \lambda^p \cdots \lambda^q]) - J) = 0, \tag{5.17}
$$

where

$$
\begin{aligned}
J &= \partial f/\partial x|_{x^*, v^*}, \\
f &= \begin{bmatrix} f_1 & f_2 & \cdots & f_n \end{bmatrix}^T.
\end{aligned}
\tag{5.18}
$$

By tuning the design parameter α, poles and zeros that were in the right half plane and causing instability in the system, are now within the stable area for the fractional order system based on Theorem (1) and Fig. 5.2. Hence, the closed loop system dynamics become stable. In other words, by increasing flexibility in the tuning strategy, i.e. using fractional order differentiator to design control input, the instability issue is fixed and collisions can be avoided.

5.4 Simulation and Results

To demonstrate the effectiveness of the proposed approach, a five-vehicle platoon with the attacker at position three is considered. In simulation, gains of the controller are considered to be $k_p = 1$, $k_d = 3.3$ and $\tilde{k_d} = -2$, respectively. In Fig. 5.3, Fig. 5.4 and Fig. 5.5, the performances of the platoon under attack are demonstrated. In Fig. 5.3, it is shown that collision happens among all vehicles in the platoon. To provide more evident proof of collision in, Fig. 5.4, spacing between vehicles (z_i) are shown. Necessary and sufficient condition for the collision occurrence is presented as (5.19),

$$z_i \leq 0. \tag{5.19}$$

The oscillation in velocities of vehicles in the platoon resulting from successful destabilizing attack are pointed out in Fig. 5.5.

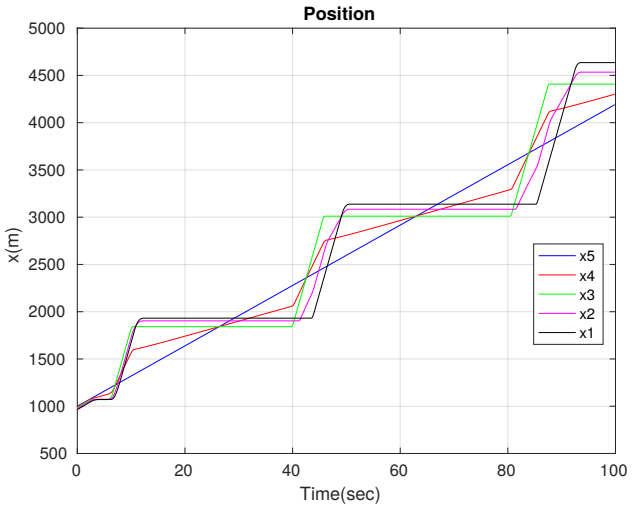


Fig. 5.3: Positions of the vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in the place three, without mitigation scheme.

Performance of the proposed mitigation scheme is evaluated in Fig. 5.6, Fig. 5.7 and Fig. 5.8. It is shown that the controller is able to prevent collisions. Positions of vehicles shown in Fig. 5.6 clearly, demonstrate the efficiency of the control design. It can be seen that in the first 37 seconds after the attack, detection controller brings the attacker and its following vehicles to stop

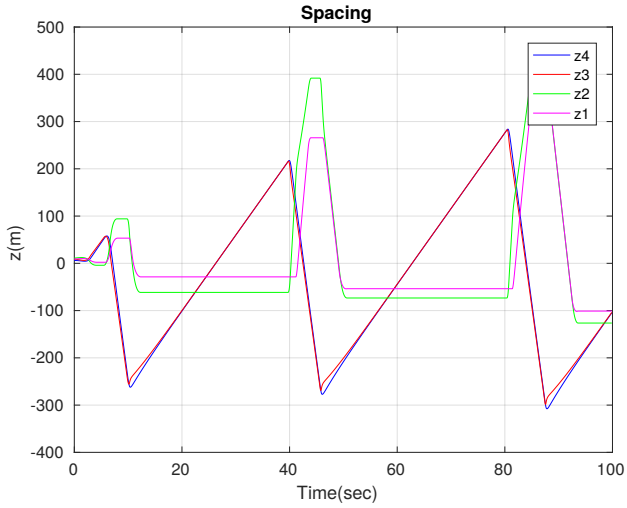


Fig. 5.4: Spacing between vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in the place three, without mitigation scheme.

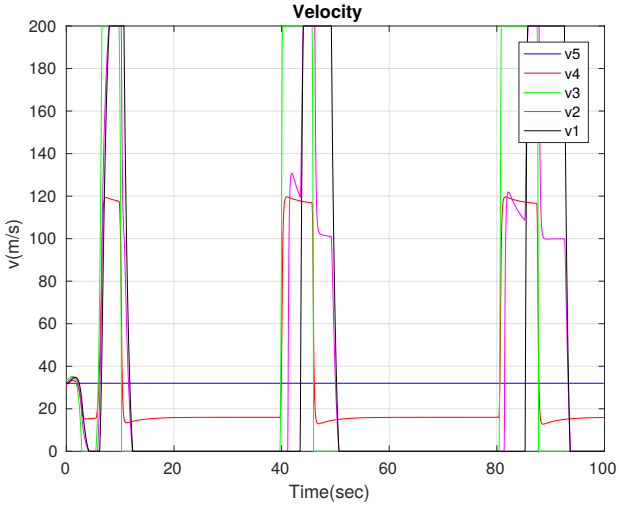


Fig. 5.5: Velocities of the vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in the place three, without mitigation scheme.

and platoon gradually recovers from the attack. Also, the attacker's preceding vehicle slows down. In this simulation leader of the platoon is not affected by other vehicles' motion. Due to this cause, the differences in spacings and velocities are justifiable. The mitigation scheme is able to protect the platoon against undesirable effects of the attack, but the attacker can cause disruption in platoon performance. Results show that after applying the mitigation controller, platoon becomes stable and all vehicles are able to follow the leader.

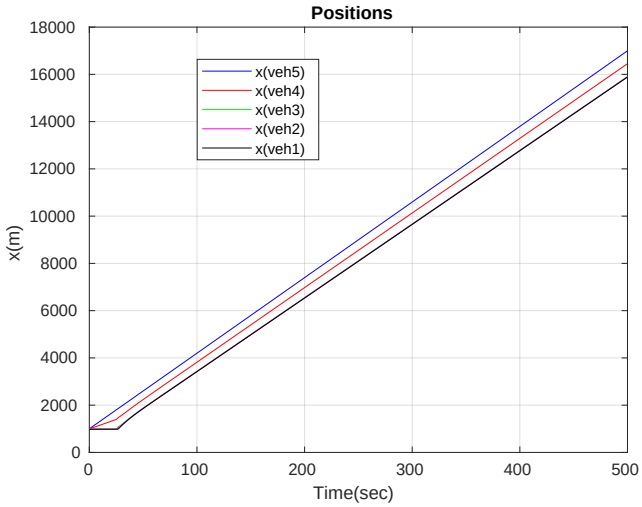


Fig. 5.6: Positions of the vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in the place three, with mitigation scheme.

5.5 Discussion

In this chapter, the fractional order differentiator (5.13) is applied to the vehicular platoon under attack. The mitigation technique is applicable to the system after the detection of the attacker, and the attacker is controlled through its front vehicle. As it is shown in (5.1), each vehicle's inputs are the states of the adjacent vehicle. The defender uses this link to inject the control input to the attacker and control its motion. The proposed method performance is superior to the method which isolates the attacker upon detection as it prevents the attacker to disintegrate the platoon. The simulation results demonstrate that the proposed algorithm efficiently reduces the damages and prevents collisions. The alternative approach can be taken based on detection of the attack, not an attacker where similar control law (i.e. $D(v_i) - k_i D^{\alpha} v_i$) can be applied to all v_i equations

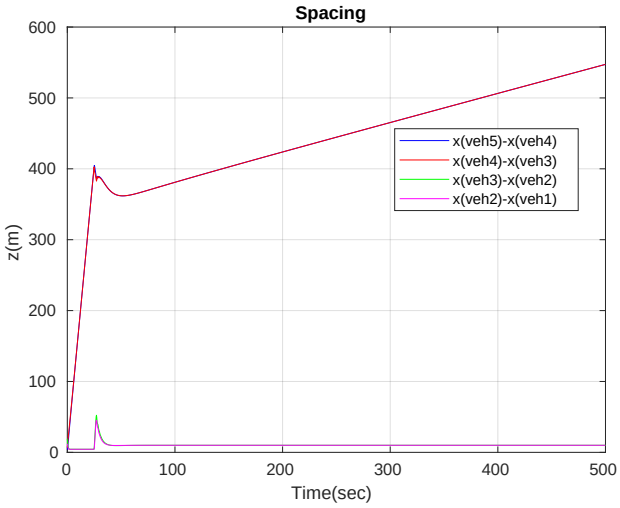


Fig. 5.7: Spacing between vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in the place three, with mitigation scheme.

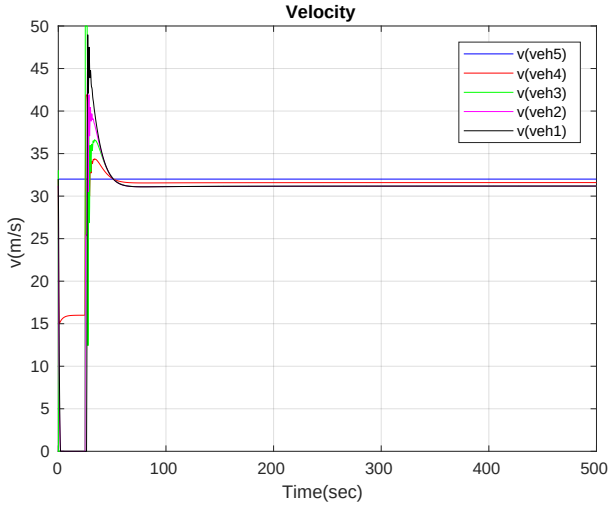


Fig. 5.8: Velocities of the vehicles in 5-vehicle platoon under gain modification attack, when the attacker is in place three, with mitigation scheme.

without prior knowledge of the attacker's position. This implies that in the event of the attack and its detection, all vehicles apply fractional order controller to the following vehicle.

5.6 Summary

In this chapter, a mitigation scheme to prevent an attacker from causing collisions in a vehicular platoon under a gain modification attack is proposed. A control algorithm, based on fractional-order calculus and using only local sensor information is shown to significantly alleviate the impact of the attacker. The control is incorporated into the system when attacker(s) is(are) detected. It has been proved that once the stream has been destabilized and its states continually deviate from the desired trajectories, the attacker can be interrupted by another member of the platoon. Simulations demonstrate that by applying the proposed control method, collisions are eliminated despite the attacker maliciously altering its gain such that the system becomes unstable or shows oscillatory behavior.

CHAPTER 6

Conclusion and Future Work

6.1 Summary of This Work

This work is the first of its kind to investigate the security of the platooning system from the control perspective in a comprehensive manner. First, the vulnerabilities of the existing upper-level controller algorithms are identified, then the control modification attack targeting the stability and string stability of the system under study is devised. Following that, the capabilities of the attacker under actuator saturation and the reachable states of the platoon during the attack are studied. At last, effective detection and mitigation algorithms are proposed.

The designed attack has been demonstrated that a vehicle with a modified control system, operated by a maliciously minded actor, can destabilize a platoon employing a PD controller that uses predecessor and follower distances and velocities to maintain a constant separation. This work demonstrates the need for creators of future platooning control laws to consider the presence of an adversary in the design process. Additionally, it has been proved that an attacker can theoretically control the relative position and velocity of surrounding vehicles.

Reachability of platoon to determine feasible attacks with destructive impact is presented in Chapter 3. The proposed approach provides new insight to the security of control in CPS, specifically platooning. This method is proved that the attacker has a very limited capability to disrupt platoon, only utilizing acceleration and deceleration when all vehicles in platoon follow normal control law. Therefore, the attacker's attempt would not result in severe damage and present control law has proven to be robust to such attacks. On the other hand, when the attacker combines, the motion modification and control law alteration, it can be shown that this type of attack is more disruptive and can cause collisions between one to all vehicles. Although the attacker's motion is bounded, gain changing empowers attacker to create collisions with more physical damages in platoon.

In Chapter 4, the problem of detecting attackers in Cyber-Physical Systems under the gain modification or destabilizing attack is addressed. This algorithm is capable of distinguishing the misbehaving units by identifying corresponding parameters and differentiating them from the normal group of parameters using the basic machine learning algorithm. Using the presented scheme, it can be distinguished which subsystems are compromised. The proposed method does not require prior

knowledge of the number of attackers or the system's parameters. This results are highly applicable to attack detection in CPS. A case study of compromised CPS, vehicle platooning in adversarial environment, is presented to evidence the efficiency of the proposed strategy. In vehicular platooning, where attackers alter their gains to different values than the normal set of gains, the detection algorithm is capable of pinpointing all attackers. This goal can be achieved by using position and velocity of the vehicle in-front as the inputs and the vehicle's own position and velocity as the outputs to identify each vehicle's control parameters. The infrastructure, which has access to all measurements is responsible for the algorithm implementation. Then, victims can be separated from malicious actors utilizing the thresholding method or classifiers. Vehicle Platooning example illustrates that the presented detection scheme successfully identifies all attackers participating in the attack scenario in a small time window after the attack and more importantly, detection is accurate.

A fractional order control scheme is designed in Chapter 5 for collision avoidance in adversarial platooning environment. Proposed fractional order calculus-based technique is applied to attacker's vehicle through the vehicle in front of the attacker. The main purpose in the control design is to stabilize platoon after the attacker destabilizes system through gain modification attack. Simulation results show that the proposed scheme can effectively eliminate the collisions caused by the attacker. The mitigation algorithm is capable of preventing damages and stopping undesired impacts of the attack in a timely manner. This approach is mainly based on attacker detection and is applied to the platoon under attack after attacker identification. While the approach is effective in protecting platoon against damages, platoon falls short in recovering and returning to the normal performance regarding constant spacing and zero relative velocity.

6.2 Future Works

Future work will focus on the designing of countermeasures, including the possible use of dynamic gain scheduling for vehicles in a platoon. It is hoped that by obfuscating the exact gains of other vehicles, an attacker would be prevented from calculating their own gain to achieve resonance. Furthermore, the performance of the controller and platoon in presence of adversary will be improved. Also the susceptibility of platooning/platooning-like laws that rely only on predecessor information and/or employ communication to relay information (e.g. adaptive and cooperative adaptive cruise control systems), which are already present in or are under development for, commercial systems will be examined. Moreover, the impacts of the attacks in different attack scenarios like

jamming attack, and the replay attack will be investigated and compared to the control modification attack.

Bibliography

[1] M. S. Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pages 1–9. IEEE, 2012.

[2] M. Amoozadeh, A. Raghuramu, C. n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, June 2015.

[3] M. Azees, P. Vijayakumar, and L. J. Deborah. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, 10(6):379–388, 2016.

[4] C. Barreto, A. A. Crdenas, and N. Quijano. Controllability of dynamical systems: Threat models and reactive security. In S. Das, C. Nita-Rotaru, and M. Kantarcioglu, editors, *Decision and Game Theory for Security*, volume 8252 of *Lecture Notes in Computer Science*, pages 45–64. Springer International Publishing, 2013.

[5] L. D. Baskar, B. De Schutter, J. Hellendoorn, and Z. Papp. Traffic control and intelligent vehicle highway systems: a survey. *IET Intelligent Transport Systems*, 5(1):38–52, 2011.

[6] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa. Overview of platooning systems. In *Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012)*, 2012.

[7] Z. A. Biron, S. Dey, and P. Pisu. Resilient control strategy under denial of service in connected vehicles. In *American Control Conference (ACC), 2017*, pages 4971–4976. IEEE, 2017.

[8] B. Biswas. *Analysis of False Data Injection in Vehicle Platooning*. PhD thesis, UTAH STATE UNIVERSITY, 2014.

[9] bloomberg. Cybersecurity is biggest risk of autonomous cars, survey finds, July 19, 2016.

[10] O. Bokanowski, N. Forcadel, and H. Zidani. Reachability and minimal times for state constrained nonlinear problems without any controllability assumption. *SIAM Journal on Control and Optimization*, 48(7):4292–4316, 2010.

[11] J. Carbaugh, D. N. Godbole, and R. Sengupta. Safety and capacity analysis of automated and manual highway systems. *Transportation Research Part C: Emerging Technologies*, 6(1):69–99, 1998.

[12] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, 2009.

[13] C.-T. Chen. *Linear system theory and design*. Oxford University Press, Inc., 1995.

[14] M. Chen, Q. Hu, J. F. Fisac, K. Akametalu, C. Mackin, and C. J. Tomlin. Reachability-based safety and goal satisfaction of unmanned aerial platoons on air highways. *Journal of Guidance, Control, and Dynamics*, 2017.

[15] M. Chen, Q. Hu, C. Mackin, J. F. Fisac, and C. J. Tomlin. Safe platooning of unmanned aerial vehicles via reachability. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 4695–4701. IEEE, 2015.

[16] F. L. Chernousko. *State estimation for dynamic systems*. CRC Press, 1993.

[17] E. Coelingh and S. Solyom. All aboard the robotic road train. *IEEE Spectrum*, November 2012. [Online; accessed 30-Sept-2013].

[18] P. Cook. Conditions for string stability. *Systems & Control Letters*, 54(10):991–998, 2005.

[19] C. Dabadie, S. Kaynama, and C. J. Tomlin. A practical reachability-based collision avoidance algorithm for sampled-data systems: Application to ground robots. In *Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on*, pages 4161–4168. IEEE, 2014.

[20] S. Dadras. Path tracking using fractional order extremum seeking controller for autonomous ground vehicle. In *SAE Technical Paper*. SAE International, 03 2017.

[21] S. Dadras, S. Dadras, H. Malek, and Y. Chen. A note on the lyapunov stability of fractional-order nonlinear systems. In *ASME 2017 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, pages V009T07A033–V009T07A033. American Society of Mechanical Engineers, 2017.

[22] S. Dadras, S. Dadras, and H. Momeni. Linear matrix inequality based fractional integral sliding-mode control of uncertain fractional-order nonlinear systems. *Journal of Dynamic Systems, Measurement, and Control*, 139(11):111003, 2017.

[23] S. Dadras, S. Dadras, and C. Winstead. Collaborative attacks on autonomous vehicle platooning. In *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 464–467, Aug 2018.

[24] S. Dadras, S. Dadras, and C. Winstead. Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment. In *2018 American Control Conference (ACC)*, June 2018.

[25] S. Dadras, S. Dadras, and C. Winstead. Reachable set analysis of vehicular platooning in adversarial environment. In *2018 Annual American Control Conference (ACC)*, pages 5568–5575. IEEE, 2018.

[26] S. Dadras, S. Dadras, and C. Winstead. Resilient control design for vehicular platooning in an adversarial environment. In *2019 Annual American Control Conference (ACC)*. IEEE, 2019.

[27] S. Dadras, R. M. Gerdes, and R. Sharma. Transfer functions for string instability. Technical report, http://www.eng.usu.edu/ece/faculty/rgerdes/papers/tech/transferSI.pdf, 2015.

[28] S. Dadras, R. M. Gerdes, and R. Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, pages 167–178, New York, NY, USA, 2015. ACM.

[29] S. Dadras, H. Jamshidi, and S. Dadras. Novel stop sign detection algorithm based on vehicle speed profile. In *2019 Annual American Control Conference (ACC)*. IEEE, 2019.

[30] S. Dadras and H. R. Momeni. Control uncertain genesio–tesi chaotic system: Adaptive sliding mode approach. *Chaos, Solitons & Fractals*, 42(5):3140–3146, 2009.

[31] S. Dadras and H. R. Momeni. A novel three-dimensional autonomous chaotic system generating two, three and four-scroll attractors. *Physics Letters A*, 373(40):3637–3642, 2009.

[32] S. Dadras and H. R. Momeni. Adaptive sliding mode control of chaotic dynamical systems with application to synchronization. *Mathematics and Computers in Simulation*, 80(12):2245–2257, 2010.

[33] S. Dadras and H. R. Momeni. Control of a fractional-order economical system via sliding mode. *Physica A: Statistical Mechanics and its Applications*, 389(12):2434–2442, 2010.

[34] S. Dadras and H. R. Momeni. Four-scroll hyperchaos and four-scroll chaos evolved from a novel 4d nonlinear smooth autonomous system. *Physics Letters A*, 374(11-12):1368–1373, 2010.

[35] S. Dadras and H. R. Momeni. Generating one-, two-, three-and four-scroll attractors from a novel four-dimensional smooth autonomous chaotic system. *Chinese Physics B*, 19(6):060506, 2010.

[36] S. Dadras and H. R. Momeni. Fractional sliding mode observer design for a class of uncertain fractional order nonlinear systems. In *Decision and control and european control conference (CDC-ECC), 2011 50th IEEE conference on*, pages 6925–6930. IEEE, 2011.

[37] S. Dadras and H. R. Momeni. A new fractional order observer design for fractional order nonlinear systems. In *ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, pages 403–408. American Society of Mechanical Engineers, 2011.

[38] S. Dadras and H. R. Momeni. Fractional terminal sliding mode control design for a class of dynamical systems with uncertainty. *Communications in Nonlinear Science and Numerical Simulation*, 17(1):367–377, 2012.

[39] S. Dadras and H. R. Momeni. Passivity-based fractional-order integral sliding-mode control design for uncertain fractional-order nonlinear systems. *Mechatronics*, 23(7):880–887, 2013.

[40] S. Dadras, H. R. Momeni, and S. Dadras. Adaptive control for ship roll motion with fully unknown parameters. In *Control and Automation, 2009. ICCA 2009. IEEE International Conference on*, pages 270–274. IEEE, 2009.

[41] S. Dadras, H. R. Momeni, and V. J. Majd. Sliding mode control for uncertain new chaotic dynamical system. *Chaos, Solitons & Fractals*, 41(4):1857–1862, 2009.

[42] S. Dadras, H. R. Momeni, and G. Qi. Analysis of a new 3d smooth autonomous system with different wing chaotic attractors and transient chaos. *Nonlinear Dynamics*, 62(1-2):391–405, 2010.

[43] S. Dadras, H. R. Momeni, G. Qi, and Z.-l. Wang. Four-wing hyperchaotic attractor generated from a new 4d system with one equilibrium and its fractional-order form. *Nonlinear Dynamics*, 67(2):1161–1173, 2012.

[44] S. Dadras and C. Winstead. Cybersecurity of autonomous vehicle platooning. 2017.

[45] S. Dadras and C. Winstead. Collaborative attacks on vehicular platooning. 2018.

[46] S. Dadras and C. Winstead. Insider vs. outsider threats to autonomous vehicle platooning. 2018.

[47] S. Darbha and K. Rajagopal. Intelligent cruise control systems and traffic flow stability. *Transportation Research Part C: Emerging Technologies*, 7(6):329–352, 1999.

[48] S. Das. *Functional fractional calculus*. Springer Science & Business Media, 2011.

[49] A. Davila, E. del Pozo, E. Aramburu, and A. Freixas. Environmental benefits of vehicle platooning. *Human Factors*, 2012:05–17, 2012.

[50] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague. Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, page 22. ACM, 2015.

[51] W. Deng, C. Li, and J. Lü. Stability analysis of linear fractional differential system with multiple time delays. *Nonlinear Dynamics*, 48(4):409–416, 2007.

[52] M. di Bernardo, A. Salvi, and S. Santini. Distributed consensus strategy for platooning of vehicles in the presence of time-varying heterogeneous communication delays. *IEEE Transactions on Intelligent Transportation Systems*, 16(1):102–112, 2015.

[53] J. Ding, J. Sprinkle, S. S. Sastry, and C. J. Tomlin. Reachability calculations for automated aerial refueling. In *Decision and Control, 2008. CDC 2008. 47th IEEE Conference on*, pages 3706–3712. IEEE, 2008.

[54] F. Dötzer. Privacy issues in vehicular ad hoc networks. In *International Workshop on Privacy Enhancing Technologies*, pages 197–209. Springer, 2005.

[55] D. Dun. *Attacker-induced traffic flow instability in a stream of automated vehicles*. UTAH STATE UNIVERSITY, 2015.

[56] W. B. Dunbar and D. S. Caveney. Distributed receding horizon control of vehicle platoons: Stability and string stability. *IEEE Transactions on Automatic Control*, 57(3):620 – 633, 2012.

[57] W. B. Dunbar and R. M. Murray. Distributed receding horizon control for multi-vehicle formation stabilization. *Automatica*, 42(4):549–558, 2006.

[58] D. Eckhoff, N. Sofra, and R. German. A performance study of cooperative awareness in etsi its g5 and ieee wave. In *Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on*, pages 196–200. IEEE, 2013.

[59] J. EYRE, D. YANAKIEV, and I. KANELLAKOPOULOS. A simplified framework for string stability analysis of automated vehicles. *Vehicle System Dynamics*, 30(5):375–405, 1998.

[60] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, 2014.

[61] C. Featherstone and M. Lowson. Viability and benefits of platooning in automated transport systems. http://www.cybercars.org/docs/CTF%20Lowson%20Report.pdf, 2004. [Technical report; online; accessed 04-June-2014].

[62] A. Ferrara and C. Vecchio. Sliding mode control for automatic driving of a platoon of vehicles. In *International Workshop on Variable Structure Systems, 2006. VSS'06.*, pages 262–267. IEEE, 2006.

[63] A. Ferrara and C. Vecchio. Second order sliding mode control of vehicles with distributed collision avoidance capabilities. *Mechatronics*, 19(4):471 – 477, 2009. Robotics and Factory of the Future, New Trends and Challenges in MechatronicsINCOM 2006.

[64] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry. Reach-avoid problems with time-varying dynamics, targets and constraints. In *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, pages 11–20. ACM, 2015.

[65] R. Gagarinov and A. Kurzhanski. Ellipsoidal toolbox, 2014.

[66] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 28(1-2):18–28, 2009.

[67] M. Ghanavati, A. Chakravarthy, and P. Menon. Pde-based analysis of automotive cyber-attacks on highways. In *2017 American Control Conference (ACC)*, pages 1833–1838, May 2017.

[68] D. N. Godbole and J. Lygeros. Longitudinal control of the lead car of a platoon. *IEEE Transactions on Vehicular Technology*, 43(4):1125–1135, 1994.

[69] C. L. Guernic and A. Girard. Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems*, 4(2):250 – 262, 2010. {IFAC} World Congress 2008.

[70] J. J. Haas. The effects of wireless jamming on vehicle platooning, 2009.

[71] M. Haddrell. Towards an autonomous vehicle enabled society: cyber attacks and countermeasures.

[72] H. Hartenstein and L. Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications magazine*, 46(6), 2008.

[73] H. Hasbullah, I. A. Soomro, et al. Denial of service (dos) attack and its possible solutions in vanet. *World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, 4(5):813–817, 2010.

[74] HDT Truckinginfo. Project to test 'platooning' trucks. http://www.truckinginfo.com/channel/fuel-smarts/news/story/2013/10/project-to-test-platooning-trucks.aspx, 2013. [Online; accessed 04-June-2014].

[75] J. Hedrick. Constant spacing strategies for platooning in automated highway systemsˆ. 1999.

[76] J. K. Hedrick, D. McMahon, V. Narendran, and D. Swaroop. Longitudinal vehicle controller design for ivhs systems. In *American Control Conference, 1991*, pages 3107–3112, June 1991.

[77] C. Hempfield. Why a cybersecurity solution for driverless cars may be found under the hood, Feb 18, 2017.

[78] F. Hu, Y. Lu, A. V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, and N. N. Xiong. Robust cyber–physical systems: concept, models, and implementation. *Future Generation Computer Systems*, 56:449–475, 2016.

[79] A. Humayed, J. Lin, F. Li, and B. Luo. Cyber-physical systems securitya survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

[80] P. Ioannou. *Automated Highway Systems*. Springer, 1997.

[81] A. Isidori. *Nonlinear Control Systems*. Number v.1 in Communications and Control Engineering. Springer, 1995.

[82] M. Izbicki, S. Amini, C. R. Shelton, and H. Mohsenian-Rad. Identification of destabilizing attacks in power systems. In *American Control Conference (ACC), 2017*, pages 3424–3429. IEEE, 2017.

[83] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen. A survey on platoon-based vehicular cyber-physical systems. *IEEE Communications Surveys & Tutorials*, 18(1):263–284, 2015.

[84] D. Jiang and L. Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

[85] S. Kato, S. Tsugawa, K. Tokuda, T. Matsui, and H. Fujii. Vehicle control algorithms for cooperative driving with automated vehicles and intervehicle communications. *IEEE Transactions on Intelligent Transportation Systems*, 3(3):155–161, Sep 2002.

[86] M. Kaur, J. Martin, and H. Hu. Comprehensive view of security practices in vehicular networks. In *Connected Vehicles and Expo (ICCVE), 2016 International Conference on*, pages 19–26. IEEE, 2016.

[87] P. Kavathekar and Y. Chen. Draft: Vehicle platooning: A brief survey and categorization. In *Proceedings of The ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, volume 2011, pages 829–845. ASME, 2011.

[88] J. B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[89] A. Khodayari, A. Ghaffari, S. Ameli, and J. Flahatgar. A historical review on lateral and longitudinal control of autonomous vehicle motions. In *2010 International Conference on Mechanical and Electrical Technology*, 2010.

[90] R. Kianfar, P. Falcone, and J. Fredriksson. A control matching model predictive control approach to string stable vehicle platooning. *Control Engineering Practice*, 45:163 – 173, 2015.

[91] A. B. Kurzhanski and P. Varaiya. On ellipsoidal techniques for reachability analysis. part i: external approximations. *Optimization methods and software*, 17(2):177–206, 2002.

[92] A. Kurzhanskii and I. Valyi. *Ellipsoidal calculus for estimation and control*. Nelson Thornes, 1997.

[93] S. Linsenmayer and D. V. Dimarogonas. Event-triggered control for vehicle platooning. In *2015 American Control Conference (ACC)*, pages 3101–3106. IEEE, 2015.

[94] T. Litman. Autonomous vehicle implementation predictions. 2017.

[95] X. Litrico. Robust imc flow control of simo dam-river open-channel systems. *Control Systems Technology, IEEE Transactions on*, 10(3):432–437, 2002.

[96] X. Litrico and J. Pomet. Nonlinear modelling and control of a long river stretch. In *European Control Conference, Cambridge, UK*, 2003.

[97] 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)*, 14(1):13, 2011.

[98] X.-Y. Lu, S. E. Shladover, and C. Nowakowski. Partial automation for truck platooning. http://www.automatedvehiclessymposium.org/callforposters/partial-automation, 2014. [Poster presented at TRB Automated Vehicle Symposium 2014; accessed 04-June-2014].

[99] K. J. Malakorn and B. Park. Assessment of mobility, energy, and environment impacts of intellidrive-based cooperative adaptive cruise control and intelligent traffic signal control. In *Sustainable Systems and Technology (ISSST), 2010 IEEE International Symposium on*, pages 1–6. IEEE, 2010.

[100] H. Malek, S. Dadras, and Y. Chen. A fractional order maximum power point tracker: Stability analysis and experiments. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 6861–6866. IEEE, 2012.

[101] H. Malek, S. Dadras, and Y. Chen. Fractional order equivalent series resistance modelling of electrolytic capacitor and fractional order failure prediction with application to predictive maintenance. *IET Power Electronics*, 9(8):1608–1613, 2016.

[102] H. Malek, S. Dadras, and Y. Chen. Performance analysis of fractional order extremum seeking control. *ISA transactions*, 63:281–287, 2016.

[103] J. Mårtensson, A. Alam, S. Behere, M. A. A. Khan, J. Kjellberg, K.-Y. Liang, H. Pettersson, and D. Sundman. The development of a cooperative heavy-duty vehicle for the gcdc 2011: Team scoop. *IEEE Transactions on Intelligent Transportation Systems*, 13(3):1033–1049, 2012.

[104] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin. A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on automatic control*, 50(7):947–957, 2005.

[105] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5967–5972. IEEE, 2010.

[106] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 911–918. IEEE, 2009.

[107] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 911–918. IEEE, 2009.

[108] Y. Mo and B. Sinopoli. Integrity attacks on cyber-physical systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, HiCoNS '12, pages 47–54, New York, NY, USA, 2012. ACM.

[109] Y. Mo, S. Weerakkody, and B. Sinopoli. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, 35(1):93–109, 2015.

[110] Y. Nakahira and Y. Mo. Dynamic state estimation in the presence of compromised sensory data. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5808–5813. IEEE, 2015.

[111] T. S. no, K.-T. Chong, and D.-H. Roh. A lyapunov function approach to longitudinal control of vehicles in a platoon. *IEEE Transactions on Vehicular Technology*, 50(1):116–124, Jan 2001.

[112] M. Pajic, P. Tabuada, I. Lee, and G. Pappas. Attack-resilient state estimation in the presence of noise. 2015.

[113] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *Automatic Control, IEEE Transactions on*, 57(1):90–104, Jan 2012.

[114] F. Pasqualetti, F. Dörfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[115] L. Peppard. String stability of relative-motion pid vehicle control systems. *IEEE Transactions on Automatic Control*, 19(5):579–581, 1974.

[116] I. Podlubny. *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*, volume 198. Elsevier, 1998.

[117] I. Polubny. Fractional-order systems and piλdμ controller. *IEEE Transactions on Automatic Control*, 44:208–214, 1999.

[118] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang. Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons. *IEEE Transactions on Control Systems Technology*, 8(4):695–708, 2000.

[119] M. Re. Most companies unprepared for emergence of autonomous vehicles, according to munich re survey, 19 July 2016.

[120] T. Robinson, E. Chan, and E. Coelingh. Operating platoons on public motorways: An introduction to the sartre platooning programme. In *17th world congress on intelligent transport systems*, volume 1, page 12, 2010.

[121] E. Sajad, D. Dun, R. Sharma, and R. Gardes. Attack mitigation in adversarial platooning using detection-based sliding mode control. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, pages 43–53. ACM, 2015.

[122] S. Santini, A. Salvi, A. Valente, A. Pescape, M. Segata, and R. L. Cigno. A consensus-based approach for platooning with inter-vehicular communications. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 1158–1166. IEEE, 2015.

[123] K. Scarfone and P. Mell. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007):94, 2007.

[124] E. Shaw and J. Hedrick. Controller design for string stable heterogeneous vehicle strings. In *Decision and Control, 2007 46th IEEE Conference on*, pages 2868–2875, Dec 2007.

[125] E. Shaw and J. Hedrick. String stability analysis for heterogeneous vehicle strings. In *American Control Conference, 2007. ACC '07*, pages 3118–3125, July 2007.

[126] S. Sheikholeslam and C. A. Desoer. Longitudinal control of a platoon of vehicles. In *American Control Conference, 1990*, pages 291–296. IEEE, 1990.

[127] S. Shladover. Path at 20—history and major milestones. *Intelligent Transportation Systems, IEEE Transactions on*, 8(4):584–592, Dec 2007.

[128] S. Shladover. Recent international activity in cooperative vehicle-highway automation systems. http://www.fhwa.dot.gov/advancedresearch/pubs/12033/index.cfm, 2012. [U.S. Department of Transportation Federal Highway Administration Report FHWA-HRT-12-033;Online; accessed 04-June-2014].

[129] S. E. Shladover, C. A. Desoer, J. K. Hedrick, M. Tomizuka, J. Walrand, W.-B. Zhang, D. H. McMahon, H. Peng, S. Sheikholeslam, and N. McKeown. Automated vehicle control developments in the path program. *IEEE Transactions on vehicular technology*, 40(1):114–130, 1991.

[130] Y. Shoukry, A. Puggelli, P. Nuzzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada. Sound and complete state estimation for linear dynamical systems under sensor attacks using satisfiability modulo theory solving. In *American Control Conference (ACC), 2015*, pages 3818–3823. IEEE, 2015.

[131] R. S. Smith. A decoupled feedback structure for covertly appropriating networked control systems. *IFAC Proceedings Volumes*, 44(1):90–95, 2011.

[132] D. Swaroop. String stability of interconnected systems: An application to platooning in automated highway systems. *California Partners for Advanced Transit and Highways (PATH)*, 1997.

[133] D. Swaroop, J. K. Hedrick, and S. Choi. Direct adaptive longitudinal control of vehicle platoons. *IEEE Transactions on Vehicular Technology*, 50(1):150–161, 2001.

[134] A. K. Tangirala. *Principles of system identification: Theory and practice*. Crc Press, 2014.

[135] S. Tsugawa, S. Kato, and K. Aoki. An automated truck platoon for energy saving. In *2011 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 4109–4114. IEEE, 2011.

[136] E. van Nunen, R. Kwakkernaat, J. Ploeg, and B. D. Netten. Cooperative competition for future mobility. *IEEE Transactions on Intelligent Transportation Systems*, 13(3):1018–1025, 2012.

[137] P. Van Overschee and B. De Moor. N4sid: Subspace algorithms for the identification of combined deterministic-stochastic systems. *Automatica*, 30(1):75–93, 1994.

[138] D. J. Verburg, A. C. M. van der Knaap, and J. Ploeg. Vehil: developing and testing intelligent vehicles. In *Intelligent Vehicle Symposium, 2002. IEEE*, volume 2, pages 537–544 vol.2, June 2002.

[139] J. Wang and R. Rajamani. Should adaptive cruise-control systems be designed to maintain a constant time gap between vehicles? *Vehicular Technology, IEEE Transactions on*, 53(5):1480–1490, Sept 2004.

[140] L. Y. Wang, A. Syed, G. G. Yin, A. Pandya, and H. Zhang. Control of vehicle platoons for highway safety and efficient utility: Consensus with communications and vehicle dynamics. *Journal of systems science and complexity*, 27(4):605–631, 2014.

[141] S. Weerakkody and B. Sinopoli. Detecting integrity attacks on control systems using a moving target approach. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5820–5826. IEEE, 2015.

[142] D. Yanakiev and I. Kanellakopoulos. A simplified framework for string stability analysis in ahs. In *In the Proceedings of the 13th IFAC World Congress*, pages 177–182, 1996.

[143] S. Z. Yong, M. Zhu, and E. Frazzoli. Resilient state estimation against switching attacks on stochastic cyber-physical systems. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages 5162–5169. IEEE, 2015.

[144] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

[145] Y. Zhou and J. S. Baras. Reachable set approach to collision avoidance for uavs. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 5947–5952, Dec 2015.

APPENDICES

APPENDIX A

Transfer functions for string instability

A.1 Calculation of the Transfer functions

Following the procedure set forth in Section 2.3.1 for an attacker in the second position gives the error transfer functions

$$\begin{aligned} &|G_1(s)| = |g_1|, |G_2(s)| = \left|\frac{g_2}{1-G_1g_1}\right|, \\ &|G_3(s)| = \left|\frac{g_3}{1-G_2g_3}\right|, \cdots, |G_i(s))| = \left|\frac{g_3}{1-G_{i-1}g_3}\right|, \cdots, \\ &|G_{n-2}(s)| = \left|\frac{g_3}{1-G_{n-3}g_3}\right| \end{aligned} \tag{A.1}$$

while for the third position

$$\begin{aligned} &|G_1(s)| = |g_3|, |G_2(s)| = \left|\frac{g_1}{1-G_1g_2}\right|, \\ &|G_3(s)| = \left|\frac{g_2}{1-G_2g_1}\right|, |G_4(s)| = \left|\frac{g_3}{1-G_3g_3}\right|, \cdots, \\ &|G_i(s)| = \left|\frac{g_3}{1-G_{i-1}g_3}\right|, \cdots, |G_{n-2}(s)| = \left|\frac{g_3}{1-G_{n-3}g_3}\right| \end{aligned} \tag{A.2}$$

For an attacker in the j^{th} position where $j = [4, n-2]$ we have

$$|G_{n-j}(s)| = \left|\frac{g_1}{1-G_{n-4}g_2}\right|, |G_{n+1-j}(s)| = \left|\frac{g_2}{1-G_{n-3}g_1}\right|$$

otherwise $|G_i(s)| = \left|\frac{g_3}{1-G_{i-1}g_3}\right|$ and $|G_1(s)| = |g_3|$.

Finally, for an attacker at the n^{th}-1 position, the system transfer functions are

$$\begin{aligned} &|G_1(s)| = |g_3|, |G_2(s)| = \left|\frac{g_3}{1-G_1g_3}\right|, \cdots, \\ &|G_i(s)| = \left|\frac{g_3}{1-G_{i-1}g_3}\right|, \cdots, |G_{n-2}(s)| = \left|\frac{g_3}{1-G_{n-3}g_2}\right| \end{aligned} \tag{A.3}$$

CURRICULUM VITAE

Soodeh Dadras

Published Conference Papers on Ph.D. Project

- **Vehicular platooning in an adversarial environment**, **Soodeh Dadras**, Ryan M Gerdes, and Rajnikant Sharma, in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015.
- **Visual distance estimation for pure pursuit based platooning with a monocular camera**, Samuel Mitchell, Imran Sajjad, Ali Al-Hashimi, **Soodeh Dadras**, Ryan M Gerdes, and Rajnikant Sharma, in *Proc. American Control Conference (ACC)*, 2017.
- **Reachable Set Analysis of Vehicular Platooning in Adversarial Environment**, **Soodeh Dadras**, Sara Dadras, and Chris Winstead, *Proc. American Control Conference (ACC)*, 2018.
- **Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment**, **Soodeh Dadras**, Sara Dadras, and Chris Winstead, *Proc. American Control Conference (ACC)*, 2018.
- **Collaborative Attacks on Autonomous Vehicle Platooning**, **Soodeh Dadras**, Sara Dadras, and Chris Winstead, *Proc. IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2018.
- **Resilient Control Design for Vehicular Platooning in an Adversarial Environment**, **Soodeh Dadras**, Sara Dadras, and Chris Winstead, *Proc. American Control Conference (ACC)*, 2019.

Presentations on Ph.D. Project

- **Cybersecurity of Autonomous Vehicle Platooning**, **Soodeh Dadras**, and Chris Winstead, in *Student Research Symposium, Utah State University*, 2017.
- **Insider Vs. Outsider Threats to Autonomous Vehicle Platooning**, **Soodeh Dadras**, and Chris Winstead, in *Student Research Symposium, Utah State University*, 2018.

- **Collaborative attacks on vehicular platooning**, **Soodeh Dadras**, and Chris Winstead, in *Student Research Symposium, Utah State University*, 2018.

Invited Talks on Ph.D. Project

- **Security of Control Systems in Autonomous Vehicle Platooning**, **Soodeh Dadras**, and Chris Winstead, in *Institute of Advanced Mathematics, Princeton*, 2018.