

Observer-Based Secure Control of Vehicular Platooning Under DoS attacks

by

Sakineh Khodadadi

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

Master of Science
in
Control Systems

Department of Electrical and Computer Engineering

University of Alberta

© Sakineh Khodadadi, 2022

Abstract

This thesis investigates observer-based secure control problem for platooning of connected vehicles in the presence of Denial-of-Service (DoS) attacks. DoS attacks usually prevent the vehicle-to-vehicle data packets transmission which will lead to performance degradation of platooning system or vehicle collision. To deal with DoS attacks, we consider an observer-based mechanism to estimate the state of vehicles based on available sensor measurements which significantly improves the resilience and tolerance of platooning system during the attack interval. Then, we provide the optimization framework to maximize the duration of DoS attack such that the platooning system can tolerate safe operation without performance degradation. The simulation results verify the effectiveness of the proposed method.

Preface

Chapter 3 has been submitted for publication in the article: Sakineh Khodadadi, Tohid Kargar Tasooji, Horacio J. Marquez, "Observer-Based Secure Control for Vehicular Platooning Under DoS attacks", IEEE Transactions on Intelligent Transportation Systems. I was responsible for the main contribution and idea, mathematical derivations, design, analysis, simulation and the work drafting. Tohid Kargar Tasooji helped in the formulation of the LMI conditions. Dr. Marquez contributed in the main idea and had the supervision role throughout the work. He was involved with the paper drafting and composition.

To my father, in heaven

To my mother

To my husband

For their endless love and support

The way to succeed is to double your failure rate.

– Thomas J. Watson, pioneer in the development of computing equipment
for IBM.

Acknowledgements

First, I would like to express my sincere appreciation to my supervisor, Professor Horacio. J. Marquez, for his guidance, support, and patience during my graduate study.

My deepest gratitude to my father, in heaven, Your love for me is forever engraved in my heart, forever lingering in my mind, and forever mine to cherish. To my kind and lovely mother who is always there for me and taught me lessons that nobody else could have.

Last but not least, to my beloved husband, I simply could not have done this without him, Words can not express how grateful I am to him.

Contents

1	Introduction	1
I	Literature review	1
I.1	CVs platooning control	1
I.2	DoS attacks	6
I.3	CVs platooning control under cyber attacks	10
II	Statement of contribution	10
III	Thesis Outline	11
2	Preliminaries	13
I	Graph Theory	13
II	Lyapunov stability	14
III	Linear Matrix Inequality (LMI)	16
IV	Vehicle-to-vehicle (V2V), vehicle-to- infrastructure (V2I), and vehicle-to- vehicle/vehicle-to-infrastructure (V2V/V2I, or V2X) Communication	18
V	Connected vehicles (CVs), autonomous vehicles (AVs), and con- nected autonomous vehicles (or CAVs)	20
3	Stability Analysis of Vehicular Platooning Under DoS attacks	24
I	Introduction	24
I.1	Graph Theory	25
I.2	Problem Statement	25
I.3	Vehicle Dynamics	27
I.4	DoS Attack Model	27
II	Observer-based Secure Control Scheme Design For Platooning System	29
II.1	Closed-Loop System Model	29
II.2	Stability Analysis	31
III	Simulation Results	36
4	Summary and Conclusions	43
I	Directions for Future Work	44

List of Figures

1.1	CVs platoon	3
2.1	(a) Directed graph (b) Undirected graph [65]	14
2.2	V2X communication system [59]	20
2.3	Automated driving levels [63]	22
3.1	A platoon of connected vehicles under DoS attacks	26
3.2	Block diagram of observer-based secure control for a platoon of connected vehicles under DoS attacks	26
3.3	Illustration of DoS attack strategy	27
3.4	Communication topology of vehicles	38
3.5	Spacing errors of vehicles under DoS attacks [1].	39
3.6	Velocities of vehicles under DoS attacks [1].	39
3.7	Spacing errors of vehicles under DoS attacks.	40
3.8	Velocities of vehicles under DoS attacks.	40
3.9	Spacing errors of vehicles under DoS attacks [1].	41
3.10	Velocities of vehicles under DoS attacks [1].	41
3.11	Spacing errors of vehicles under DoS attacks.	42
3.12	Velocities of vehicles under DoS attacks.	42

List of Symbols

$\text{diag}(\cdot)$	Block diagonal matrix
\otimes	Kronecker product
A^T	Transpose of matrix A
A^{-1}	Inverse of matrix A
I_N	Identity matrix of appropriate dimensions
i and j	Identity of vehicle i and vehicle j
\mathcal{H}	Laplacian matrix
$\lambda_{\min}(A)$	The minimum eigenvalue of the matrix A
$\lambda_{\max}(A)$	The maximum eigenvalue of the matrix A
\mathcal{N}_i	Communication neighboring set of the vehicle i
$p_i(t)$	The position of vehicle i
$v_i(t)$	The speed of vehicle i
$a_i(t)$	The acceleration of vehicle i
$x_i(t)$	The state of vehicle i
$x_0(t)$	The state of the leader vehicle
$d_{i,i-1}$	The desired space between vehicle i and $i - 1$
$\hat{x}_i(t)$	The estimated state of vehicle i
$\tilde{x}_i(t)$	The estimation error of vehicle i
G_{ob}	The observer gain of vehicle i
K	The control gain of vehicle i

List of Acronyms

DoS Denial of Service

DSRC Dedicated Short Range Communication

VCPSs Vehicular Cyber Physical Systems

ITS Intelligent Transportation Systems

CVs Connected Vehicles

CAVs Connected Automated Vehicles

MPC Model Predictive Control

V2V Vehicle-to-Vehicle

V2I Vehicle-to-Infrastructure

V2V/V2I, or V2X Vehicle-to-Vehicle/Vehicle-to-Infrastructure

LMI Linear Matrix Inequality

FDI False Data Injection

CPSs Cyber-Physical Systems

RSU Remote Switching Unit

WNCS Wireless Networked Control System

MASs Multi Agent Systems

LFC load frequency control

DMFAC Distributed Model-Free Adaptive Control

NCSs Networked Control Systems

VRUs Vulnerable Road Users

AVTs Automated Vehicles Technologies

Chapter 1

Introduction

In this thesis, we study stability of platoons of connected vehicles (CVs) under denial-of-service (DoS) attacks.

The main purpose of this work is to compute the maximum duration and frequency of DoS attack that the platoons of CVs can tolerate such that the platooning system remains stable. This chapter provides an outline to the topic, literature review, contribution and motivation for our work, and thesis outline.

I Literature review

I.1 CVs platooning control

The rapid development of intelligent transportation systems (ITS) has paved the way to consider vehicular platoons in which vehicles move in a coordinated manner, maintaining a minimal intervehicular distance. Platooning system can be categorized into five main criteria: i) the type of platooned vehicles, ii) the platoon length, iii) the information flow topology, iv) the formation policies and v) the following policies [70]. The types of the platooned vehicles are as follows::

- Homogeneous: Vehicles have similar characteristics in terms of size and degree of automation.
- Heterogeneous: Vehicles have different sizes and/or degrees of automation.

In terms of vehicle number, finite and infinite number of vehicles are considered. Also regarding information flow topology, there is two types including:

- Nearest vehicles: Each vehicle receives/exchanges information from/with r vehicles ahead
- Nearest vehicles and leader: Each vehicle receives/exchanges information from/with r vehicles ahead, plus the leader.

In terms of formation policies, platooning types include opportunistic (on-the-fly), cooperative, online, dynamic or in real time, offline, static or scheduled, and merging policies has been investigated. We briefly define the features of these types of platooning system:

- Opportunistic (on-the-fly): Only CAVs that happen to drive consecutively in a lane form a platoon
- Cooperative: All CAVs within a certain range try to join in a platoon
- Online, dynamic or in real time: Vehicles announce their destination and/or routes just before or during the journey
- Offline, static or scheduled: Trips are announced in advance to facilitate coordination
- Merging policies: Catch-up, slow-down or hybrid strategies

Car-following policies are as follows:

- Constant space gap: Followers maintain a fixed distance with the preceding vehicle
- Constant time gap: Followers maintain a fixed time with the preceding vehicle
- Variable gap: Followers maintain a variable space or time gap depending i.a. on road features

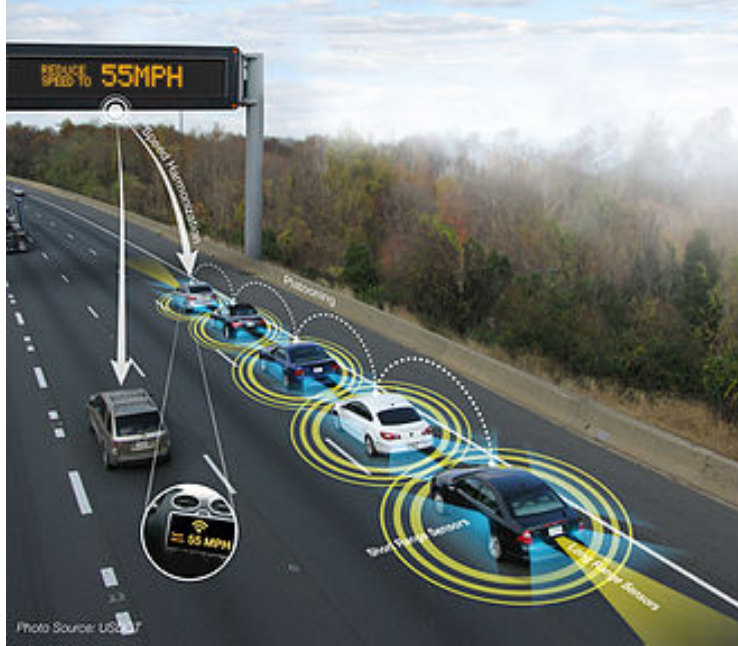


Figure 1.1: CVs platoon

Comparing with individual driving, platoon-based driving can significantly improve traffic efficiency and fuel economy while reducing traffic congestion and the risk of accidents because of vehicles maintaining small spacings, i.e., occupying less space while travelling at relatively high speeds, thus increasing capacity [1]. The magnitude of the improvement will depend on the scenario, e.g. the penetration rate of CAVs, the platoons' length, the car-following policies, the road features, etc. In fact, the main purpose of controlling a platoon is stabilizing the platoon of CVs such that all vehicles track the desired trajectory conditions, typically speed and acceleration, while ensuring that safety distances between vehicles are maintained. The safe operation of platoon systems can be guaranteed using cooperative control that employs measurements from onboard sensors and state packets of neighbouring vehicles through Dedicated Short Range Communication (DSRC) radios to control the speed of the platoon system as well as intervehicular distance [8] (See figure 1.1). Due to these potential benefits, cooperative platooning control has been extensively investigated over the past few years [2, 3, 4, 5, 6, 7, 12, 13, 14, 25, 26, 71].

An adaptive control system automatically compensates for variations in system dynamics by adjusting the controller characteristics so that the overall

system performance remains the same, or rather maintained at optimum level. This control system takes into account any degradation in plant performance with time. Zhang et al. [27] proposed a delay-adaptive switching-type control for platoons of CVs with unknown input delays. They use estimated unknown input delays to guarantee the stability of whole platoon. Hu et al. [37] investigate a two-layer cooperative control strategy to preserve string (also called platoon) stability of a heterogeneous platoon of vehicles. They apply feedback linearization and an adaptive control to deal with the nonlinearities, converting the problem into a linear heterogeneous control problem to ensure safety inter vehicle space while keeping the desired velocity of the platoon. Chen and Park [41] investigate the preceding vehicle identification system (PVIS) taking into consideration sensor/GPS errors in cooperative adaptive cruise control (CACC) of CVs and evaluate distance-based PVIS, location-based PVIS, and combining distance and location PVIS. Wei et al. [36] propose a control system adopting vehicle to vehicle (V2V) communication and radar information in order to achieve both longitudinal and lateral vehicle tracking. They use a path estimation and a linear feed-forward and feedback controllers to guarantee a safe distance between vehicles and determine the trajectory of the former vehicle. They use MPC to control the steering angle of the front wheel.

A distributed control system (DCS) is a computerised control system for a process or plant usually with many control loops, in which autonomous controllers are distributed throughout the system, but there is no central operator supervisory control. This is in contrast to systems that use centralized controllers; either discrete controllers located at a central control room or within a central computer. Du et al. [29] investigate the cooperative startup control for the platoon of CVs. First, they demonstrate a hierarchical finite-time control, second, they design the distributed finite-time observer based on observer and consensus errors, third, they design a distributed finite-time controller. They validate the proposed method using numerical simulation. Li et al. [31] study a distributed nonlinear consensus control for platoon of CVs. They design a nonlinear function based on the behaviour of the follower vehicle. The authors analyze the convergence of delay-dependent controllers using

the Lyapunov–Krasovskii methodology. They verify their proposed method with a simulation of the position, speed, and acceleration trajectories. Zhang et al. [32] study distributed secure control of a platoon of CVs under DoS attacks. In order to capture DoS attacks and time-varying sampling, they introduce a switched time-delay model. They obtain conditions for exponential performance of platoons of CVs based on the Jensen’s Inequality method, the Lyapunov method, and the topology matrix decoupling approach. They validate their approach using simulation and experiments using a platoon of four-vehicles. Zheng et al. [38] analyze robustness and propose a distributed H_∞ (H-infinity) controller synthesis for a CVs platoon with undirected topologies. They formulate the optimization of the undirected topologies for the CVs platoon, and analyze the upper and lower bounds of the control objectives and utilize the coordination of several CVs mini-platoon to control large scale CV platoon.

Optimal control is the process of determining control and state trajectories for a dynamic system over a period of time to minimise a performance index. Shao and Sun [35] study a real-time control for co-optimization of gear position and vehicle speed at the same time for CAVs in order to optimize fuel consumption. They find optimal solutions using model predictive control (MPC). Bian et al. [28] propose a fuel economy optimization strategy using distributed economic model predictive control (MPC) for a platoon of CVs. With its neighbors’ and its own assumed trajectories, each CV first solves an open-loop control optimization problem for platoon formation, and then solves an open-loop economic optimization problem for direct fuel economy enhancement. Asymptotic stability of the platoon system is proven using a Lyapunov analysis. Wang et al. [39] propose an optimal longitudinal control for connected cruise control (CCC) taking into consideration of V2V communication delays in order to minimize the deviations of vehicle’s velocity and headway. They utilize backward recursion technique in order to repetitively obtain the optimal control. Yang et al. [42] proposed a collision-free cooperative control system for a CAVs platoon with communication delays with the objective of minimizing fuel consumption and ensure performance tracking.

They prove convergences using Barbalat’s lemma. Feng et al. [43] propose a robust control system for a platoon of CVs based upon tube MPC in mixed traffic flow. They use feedback and feed-forward control in order to obtain a tube for bounding CAVs’ real trajectories.

Li et al. [30] propose a longitudinal platoon controller for CVs using information communication between each CV and the multiple preceding CVs. They use Routh criterion to analyze stability. In order to verify the effectiveness of the proposed method, they use simulation based on the TransModeler software and the experimental platform. Chen et al. [33] propose a consensus control for a platoon of connected automated vehicles (CAVs) with variable time headway and input saturation. They derive global asymptotic stability conditions using the Lyapunov-Razumikhin and Lyapunov-Krasovskii techniques. Li et al. [34] propose an integral-sliding-mode control of a CVs platoon for cooperative braking control based on the car-following interaction. They analyze the convergence of the integral-sliding-mode controller using the Lyapunov theorem. Li et al. [40] study the CVs platoon control in a vehicle-to-vehicle/vehicle-to-infrastructure (V2V/V2I, or V2X) communication domain considering collision avoidance procedure. They use the perturbation technique to analyze stability of the vehicle follower model. The authors validate the proposed approach by conducting experiments with four CVs under the different scenarios of car merging, platoon forming, and car diverging. Li et al. [44] study consensus-based cooperative control for CAVs with V2V communication. They analyze consensus and stability of the proposed approach using the Lyapunov method and Routh–Hurwitz technique.

I.2 DoS attacks

In the future, it is expected that vehicles will receive basic safety information about roadway infrastructure warning the drivers about road crashes via vehicle to infrastructure (V2I) communication and exchange the information between vehicles via V2V communication. These communication systems can be implemented using dedicated short-range communication (DSRC) networks. Such complex systems, including communications, computing, and control de-

vices, can be viewed as vehicular cyber physical systems (VCPSs) where all vehicles are coordinated in a platoon pattern based on information exchange. One potential vulnerability of VCPSs is that since these systems rely on network communications, they are vulnerable to cyber-attacks.

Cyber-attacks represent a serious hazard. An adversary may launch an attack in the form of an attack signal that either blocks or compromises the transmission of data packets over the network, thus leading to performance degradation and possible vehicle collisions. As a result, cyber-attacks are considered one of the main threats in VCPSs [1]. In general, cyber-attacks can be categorized as denial-of-service (DoS) attacks, relay attacks, and false data injection (FDI) attacks.

DoS attacks are the easiest to implement by an adversary, and are therefore commonly encountered in communication networks. In DoS attacks an adversary aims to overload communication devices by propagating a random jamming signal that prevents the exchange the information with neighbouring vehicles. Consequently, DoS attacks can cause instability of the platoon system that can result in multiple collisions.

During an attack, “resiliency” helps maintain system performance close to normal (it i.e. at a reasonable level) during the interval between the start of attack and the detection and recovery mechanism. Resilience is defined as the property that enables the system to tolerate severe conditions resulting from natural faults or deliberate attacks. Resilience of a system against adverse conditions usually needs to be strengthened via proper design of the control system. Shao and Ye [46] propose a fuzzy adaptive event-triggered resilient control for stochastic nonlinear high order multi agent systems (MASs) under actuator faults and DoS attacks. They analyze stability and propose a recursive design procedure using adaptive back-stepping and the stochastic Lyapunov theorem. Du et al. [51] explore the resilient output synchronization issue of a class of linear heterogeneous multi agent systems under DoS attacks. They present event- and self-triggered control procedures in order to cut down redundant information transmission. Yang et al. [68] develop a distributed resilient consensus control with event triggering for linear leader-

following MASs in the presence of DoS attacks. Their design employs a dual-terminal event triggered approach, which schedules information transmission through two triggered functions for each follower: one on the measurement channel (sensor-to-controller) and the other on the control channel (controller-to-actuator). Theoretical analysis shows that the followers in MASs under DoS attacks are capable of tracking the leader and meanwhile Zeno behaviour is excluded. Chen et al. [48] study a resilient compensation control and co-estimation for multi area load frequency control (LFC) systems under DoS and FDI attacks. They derive exponential stability conditions for the output feedback of a multi area LFC subject to FDI and DoS attacks. Zhao et al. [49] study the problem of L_2 -gain control and exponential stability for networked cascade control systems with DoS attacks, actuator saturation, time delay, and external disturbances. They propose a resilient event-triggered communication approach based upon the adaptive threshold mechanism in order to tackle DoS attacks and decrease transmission frequency. They expand the event-driven cascade control procedure in order to enhance resistance towards DoS attacks and plan control updates. Kato et al. [50] investigate the stabilization issue of networked control systems subject to DoS attack. Especially, they study stabilization a nonlinear system with via linearization. They utilize a deterministic DoS model constrained in aspect of duration and attacks' frequency, with benefit of covering a large class of attacks. They propose the resilient dynamic quantizer to obtain asymptotic stabilization. Li et al. [56] develop a cyber-physical systems (CPSs) subject to DoS attacks, in the presence of DoS attacks for the controller-to-actuator (C-A) channel and the sensor-to-controller (S-C) channel. They use simulation and experiments in order to validate the efficiency of the active resilient control mechanism. Sun et al. [58] propose a resilient MPC framework to reduce the effects of DoS attacks for CPSs. They obtain multiple conditions that should be met to ensure exponential stability of the closed-loop system. They verify the efficiency of the suggested MPC method by simulation and comparisons. Kato et al. [47] propose a security analysis in order to linearize the networked nonlinear control system subject to DoS attack. They obtain a condition for local stability and

region of attraction, and then obtain a relationship between DoS parameters and the initial states to ensure convergence of trajectories. Zhao et al. [52] investigate the security problem of switched systems under asynchronous DoS attacks and disturbance. In order to tackle with asynchronous DoS attack, they propose an active control strategy.

Ma et al. [54] investigate distributed model-free adaptive control (DM-FAC) for learning nonlinear MASs under DoS attacks. They propose an enhancement of the dynamic linearization approach in order to achieve an equivalent linear system. Zhang and Feng [69] study the leader–follower robust H_∞ consensus of heterogeneous multi agent systems with DoS attack. They show that the consensus protocol design problem can be transformed into two static output feedback (SOF) control problems, also they show that the SOF controller gains can be determined by solving some linear matrix inequalities. Zhang et al. [45] study the optimal DoS attack with the goal of maximization of the Linear Quadratic Gaussian (LQG) cost function subject to energy constraint. They explore the optimal DoS attack schedule in a wireless networked control system (WNCS) with several subsystems. Wakaiki et al. [53] study the quantized output feedback for the problem of the stabilization of the networked control systems subject to DoS attack. They analyze stability of the closed-loop model by obtaining the required conditions on the boundaries of DoS frequency and duration using a Lyapunov function. Peng and sun [55] explore a switching-like event-triggered control for networked control systems (NCSs) subject to DoS attacks. Also, they obtain a trade-off between H_∞ control performance and communication efficiency. Chen et al. [57] propose a dynamic event-triggered strategy for the load frequency control under FDI attacks and DoS attacks through decentralized output-based control. Their proposed approach automatically changes the triggering parameters when detecting a DoS attack to maintain system stability while improving efficiency of transmission and decreasing network bandwidth usage.

I.3 CVs platooning control under cyber attacks

In this thesis we focus on addressing control issues in the presence of DoS attacks. To the best of our knowledge, there have been very few results on resilient platoon control of VCPSs in the presence of DoS attacks [1]. In particular, the problem of designing a resilient platoon control mechanism that achieves asymptotic stability in the presence of DoS attacks remains open. Up to date, there are few works in the literature addressing the impact of cyber-attacks on VCPSs. Zhao et al. [1] investigate the platoon control problem for VCPSs in the presence of DoS attacks with multiple disturbances. The authors propose a recovery mechanism to restrict the time duration rate and occurring frequency of the adverse impact of DoS attacks on VCPSs. Mousavinejad et al. [11] develop distributed attack detection and recovery mechanisms in a vehicle platooning control system. Biron et al. [10] propose a real-time scheme to detect the occurrence of DoS attacks and estimate the impact of the attack on the connected vehicle system. The scheme relies on a set of observers that can detect the attack and estimate its effect on the platoon. Petrillo et al. [9] propose a secure adaptive cooperative control approach to solve the problem of tracking the time-varying motion of the leading vehicle under different types of cyber attacks as well as network induced phenomena. The authors prove analytically the effectiveness of their approach using the Lyapunov–Krasovkii method under the assumption that the information provided by the leader vehicle cannot be falsified.

II Statement of contribution

In this thesis, we consider VCPSs and propose an observer-based control strategy that is resilient to DoS attacks. Our goal is to achieve asymptotic tracking of the leader while maintaining the desired inter-vehicular spacing despite the presence of DoS attacks. We cast our solution as an optimization problem that maximizes tolerance of the attack duration without degradation of performance.

Our main contribution can be summarized as follows:

1. Different from the existing work in resilient platoon control, [1], where the authors assume a recovery mechanism to deal with DoS attacks, we develop an observer-based secure control for the platooning system. The observer is employed to estimate the state of vehicles based on available measurements and the adverse impact caused by the DoS attacks can be weakened with the observer.
2. Unlike references [1, 10] which consider periodic DoS attacks and unknown but constant delay, we consider a more practical attack scenario where a DoS attacks occur aperiodically. Our goal is to obtain an upper bound for the duration and frequency of attacks such that the platooning system can achieve asymptotic tracking of the leader while maintain the desired inter-vehicular spacing.
3. We establish an optimization framework in order to maximize the duration of the attack such that the platooning system can tolerate safe operation without degradation of performance.

III Thesis Outline

The structure of this thesis is as follows:

Chapter 1 describes the research direction, including a literature review on platoon of CVs, cyber attacks, and platoon systems under cyber attacks. We introduce CVs platoon as an active research area, outline our research goals, and statement of contribution.

Chapter 2 provides the preliminary background and definitions needed in later chapters, including a brief summary of graph theory, Lyapunov stability, Linear matrix inequality (LMI), the definition of different types of communication connectivities between CVs like V2V, V2I, and V2X that play an important role in the formation of vehicular platooning systems. Also we describe different levels of automation and required devices for either connected, automated and connected automated vehicles (CVs, AVs and CAVs).

In Chapter 3, we design a secure controller that stabilizes the platooning

system in the presence of DoS attacks. We also present numerical simulations results to verify the efficiency of the theoretical results.

Chapter 4 contains summary and conclusions and final remarks with research direction for future works.

Chapter 2

Preliminaries

In this chapter, we summarize some concepts used throughout the rest of the thesis, including basic background on graph theory, Lyapunov stability, Linear Matrix Inequality (LMI), V2V communication, V2I communication, V2X communication, platoons of connected vehicles (CVs), and platoons of connected-automated vehicles (CAVs).

I Graph Theory

Graph theory is utilized in the multi-vehicle cooperative control for the information communication among connected vehicles, in order to analysis the stability of the platoon, and also to obtain consensus. The topology is modelled as a graph in which vehicles can be illustrated as nodes and links such as communication and sensing can be illustrated as edges [66].

Graph theory is mathematical structures utilized in order to model pairwise relations between objects. A graph consist of nodes which are connected by edges. There is different types of graphs including undirected graphs, in which edges link two nodes without orientation , and directed graphs, where edges link two nodes with orientation [65]. An illustration of these directed and undirected graphs is represented in the Figure 2.1 (a) and (b). An undirected graph is a graph in which edges do not have orientations, an undirected graph is an ordered pair $G = (V, E)$ comprising:

1. V , a set of nodes (also called points).

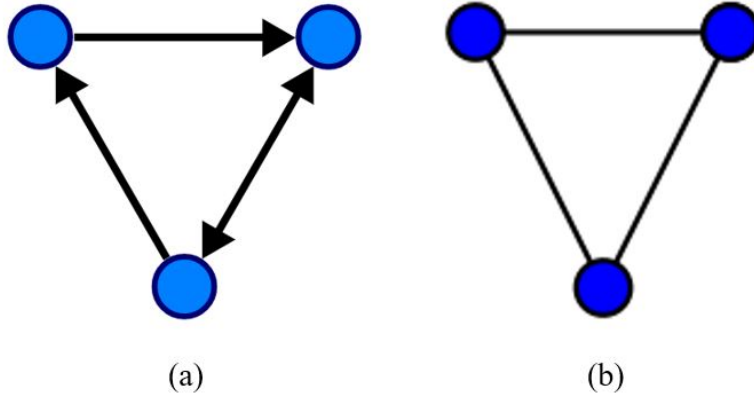


Figure 2.1: (a) Directed graph (b) Undirected graph [65]

2. $E \subseteq \{\{x, y\} \mid x, y \in V \text{ and } x \neq y\}$, a set of edges (also called links) which are unordered pairs of nodes.

A directed graph or digraph is a graph in which edges have orientations, a directed graph is an ordered pair $G = (V, E)$ comprising:

1. V , a set of nodes (also called points).
2. $E \subseteq \{(x, y) \mid (x, y) \in V^2 \text{ and } x \neq y\}$, a set of edges (also called directed links or directed edges) which are ordered pairs of nodes.

II Lyapunov stability

In this section we provide an outline of the Lyapunov stability theorem that will be needed in later sections. First, we introduce time-dependent positive definite functions. We consider a scalar function $W : D \times R^N \rightarrow R$ with variables $x \in D$ and time t . Assuming this function is continuous and has continuous partial derivatives with respect to its arguments, then the function $W(x, t)$ is said to be positive semi definite in D if it satisfies the following conditions [64]:

1. $0 \in D$
2. $W(0, t) = 0, \forall t \in R^+$
3. $W(x, t) \geq 0, \forall x \neq 0, x \in D$

$W(x, t)$ is said to be positive definite in D if conditions (1)-(3) above are satisfied, and there exists a time-invariant positive definite function $V_1(x)$ such that:

$$V_1(x) \leq W(x, t), \quad \forall x \in D$$

Similarly, $W(x, t)$ is said to be negative definite (semi definite) in D if $-W(x, t)$ is positive definite (semi definite).

$W(x, t)$ is said to be *decreasing* in D if there exists a positive definite function $V_2(x)$ such that: $|W(x, t)| \leq V_2(x), \quad x \in D, \quad \forall t$. $W(x, t)$ is said to be radially unbounded if $W(x, t) \rightarrow \infty$ as $x \rightarrow \infty$ uniformly on t .

Now, consider the system $\dot{x} = f(x, t)$, $f : D \times R^+ \rightarrow R^n$ and assume that the origin is an equilibrium state: $f(0, t) = 0, \quad \forall t \in R$. Then if in a neighborhood D of the equilibrium state $x = 0$ there exist a differentiable function $W(., .) : D \times [0, \infty) \times R$ such that:

1. $W(x, t)$ is positive definite.
2. The derivative of $W(., .)$ along any solution of $\dot{x} = f(x, t)$ is negative semi definite in D .

then, the equilibrium state is stable. Moreover, if $W(x, t)$ is also *decreasing* then the origin is uniformly stable. The equilibrium state is uniformly asymptotically stable if

1. $W(x, t)$ is positive definite and decreasing.
2. The derivative of $\dot{W}(x, t)$ is negative definite in D

If there exists a differentiable function $W(., .) : R^n \times [0, \infty) \rightarrow R$ such that:

1. $W(x, t)$ is positive definite, decreasing, and radially unbounded $\forall x \in R^n$ and that
2. The derivative of $\dot{W}(x, t)$ is negative definite in $\forall x \in R^n$, then

the equilibrium state at $x = 0$ is globally uniformly asymptotically stable. Suppose that the equilibrium state $x = 0$ is uniformly asymptotically stable, and in addition assume that there exist positive constants K_1, K_2 and K_3 such that:

1. $K_1\|x\|^p \leq W(x, t) \leq K_2\|x\|^p$.
2. $\dot{W}(x, t) \leq -K_3\|x\|^p$

Then the origin is exponentially stable. When the above conditions hold globally, then the equilibrium state $x = 0$ is globally exponentially stable.

III Linear Matrix Inequality (LMI)

The history of LMIs in the analysis of dynamical systems goes back more than 100 years, when Lyapunov published his seminal work introducing what we now call Lyapunov theory. He showed that the differential equation

$$\frac{d}{dt}x(t) = Ax(t) \tag{2.1}$$

is stable (i.e., all trajectories converge to zero) if and only if there exists a positive-definite matrix P such that

$$A^T P + P A < 0 \tag{2.2}$$

The requirement $P > 0$, $A^T P + P A < 0$ is what we now call a Lyapunov inequality on P , which is a special form of an LMI. Lyapunov also showed that this first LMI could be explicitly solved. Indeed, we can pick any $Q(x) = Q^T(x)$ and then solve the linear equation $A^T P + P A = -Q(x)$ for the matrix P , which is guaranteed to be positive-definite if the system (2.1) is stable. In summary, the first LMI used to analyze stability of a dynamical system was the Lyapunov inequality (2.2), which can be solved analytically (by solving a set of linear equations) [67].

A linear matrix inequality (LMI) has the form

$$F(x) = F_0 + \sum_{i=1}^m x_i F_i > 0 \tag{2.3}$$

where $x \in R^m$ is the variable and the symmetric matrices $F_i = F_i^T \in R^{n \times n}$, $i = 0, \dots, m$, are given. The inequality symbol in (2.3) means that $F(x)$ is positive-definite, i.e., $u^T F(x) u > 0$ for all nonzero $u \in R^n$. Of course, the LMI

(2.3) is equivalent to a set of n polynomial inequalities in x , i.e., the leading principal minors of $F(x)$ must be positive.

We will also encounter nonstrict LMIs, which have the form

$$F(x) \geq 0 \tag{2.4}$$

The strict LMI (2.3) and the nonstrict LMI (2.4) are closely related, but here we consider strict LMIs.

The LMI (2.3) is a convex constraint on x , i.e., the set $\{x|F(x) > 0\}$ is convex. Although the LMI (2.3) may seem to have a specialized form, it can represent a wide variety of convex constraints on x . In particular, linear inequalities, (convex) quadratic inequalities, matrix norm inequalities, and constraints that arise in control theory, such as Lyapunov and convex quadratic matrix inequalities, can all be cast in the form of an LMI.

Multiple LMIs $F^{(1)}(x) > 0, \dots, F^{(p)}(x) > 0$ can be expressed as the single LMI $\mathbf{diag}(F^{(1)}(x), \dots, F^{(p)}(x)) > 0$. Therefore we will make no distinction between a set of LMIs and a single LMI, i.e., "the LMI $F^{(1)}(x) > 0, \dots, F^{(p)}(x) > 0$ " will mean "the LMI $\mathbf{diag}(F^{(1)}(x), \dots, F^{(p)}(x)) > 0$ ".

When the matrices F_i are diagonal, the LMI $F(x) > 0$ is just a set of linear inequalities. Nonlinear (convex) inequalities are converted to LMI form using Schur complements [67]. The basic idea is as follows: the LMI

$$\begin{bmatrix} Q(x) & S(x) \\ S^T(x) & R(x) \end{bmatrix} > 0 \tag{2.5}$$

where $Q(x) = Q^T(x)$, $R(x) = R^T(x)$, and $S(x)$ depend on x , is equivalent to

$$R(x) > 0, \quad Q(x) - S(x)R(x)^{-1}S(x)^T > 0 \tag{2.6}$$

In other words, the set of nonlinear inequalities (2.6) can be represented as the LMI (2.5).

IV Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle/vehicle-to-infrastructure (V2V/V2I, or V2X) Communication

The increasing number of vehicles in urban areas leads to traffic congestion and delays, as well as air pollution and traffic accidents [60]. One approach to improve traffic flow is through the use of intelligent traffic management. Intelligent traffic management refers to the sharing of traffic data among CVs in real time with the purpose of improving safety. Intelligent management requires modern vehicles to be equipped with communication capabilities as well as road infrastructure, including vehicle-to-vehicle/vehicle-to-infrastructure (V2V/V2I, or V2X) communications, as shown in Figure 1.

Vehicles exchange information with other vehicles using vehicle-to-vehicle (V2V) communications, and share data with the road infrastructure through the vehicle-to-infrastructure (V2I) network. Both networks comprise multiple nodes, including the communication devices of cyclist, pedestrians, and charging stations. These modes can be utilized simultaneously for safety and vehicle control improvement, by employing data from neighbours sensors and accident avoidance [61]. Each communication mode can be describes as follows:

- Vehicle-to-Vehicle (V2V): V2V permits nearby vehicles to form a communications network capable of sharing data among nodes. This can be done by subscribing to the network and obtaining authorization. V2V networks can be used to share data such as vehicle position, traffic dynamics and vehicle attributes. To improve transmission, message payload is maintained flexible and one-to-many communication of data is done with minimum delay [62].
- Vehicle-to-Infrastructure (V2I): V2I application information is communicated via a Remote Switching Unit (RSU) or locally accessible server. RSUs are roadside and infrastructure stationary units. Accessible application servers or RSUs collect the message and broadcast the message

to one or more V2I application units. V2I can provide information such as traffic congestion, accessible parking space and road circumstances. Because of long deployment time and high cost, its installation and use are more difficult and challenging [62].

- Vehicle-to-Pedestrian (V2P): V2P communication happens between a vehicle and Vulnerable Road Users (VRUs) such as cyclists pedestrians, and etc. The user equipment carried by pedestrians and the drivers will be capable of receiving and sending warnings, alerts and messages. Vehicles can have transmission with VRUs even under low perceptibility and visibility situations like heavy rain, dark night, foggy weather. The sensitivity and vulnerability of pedestrian user equipment is much lower than vehicular user equipment due to the battery capacity and antenna difference. As a result V2P application user equipment cannot communicate continuous messages similar to V2V user equipment.
- Vehicle-to-Network (V2N): V2N communication is between a vehicle-to-vehicle/ vehicle-to-infrastructure (V2V/V2I, or V2X) application and a vehicle. A user equipment supporting V2N application server can transmit with the application supporting V2N applications, while the parties transmit the messages with one another employing Evolved Packet Switching (EPS). V2X servers are needed for different operation scenarios and applications like assisting mobile operators to transmit the tasks of the RSU in its network, removing the complexity of designing, decreasing time spent to market, cost and running a purpose-made network for V2I in order to include transmission between the server through 4G or 5G network and vehicles.

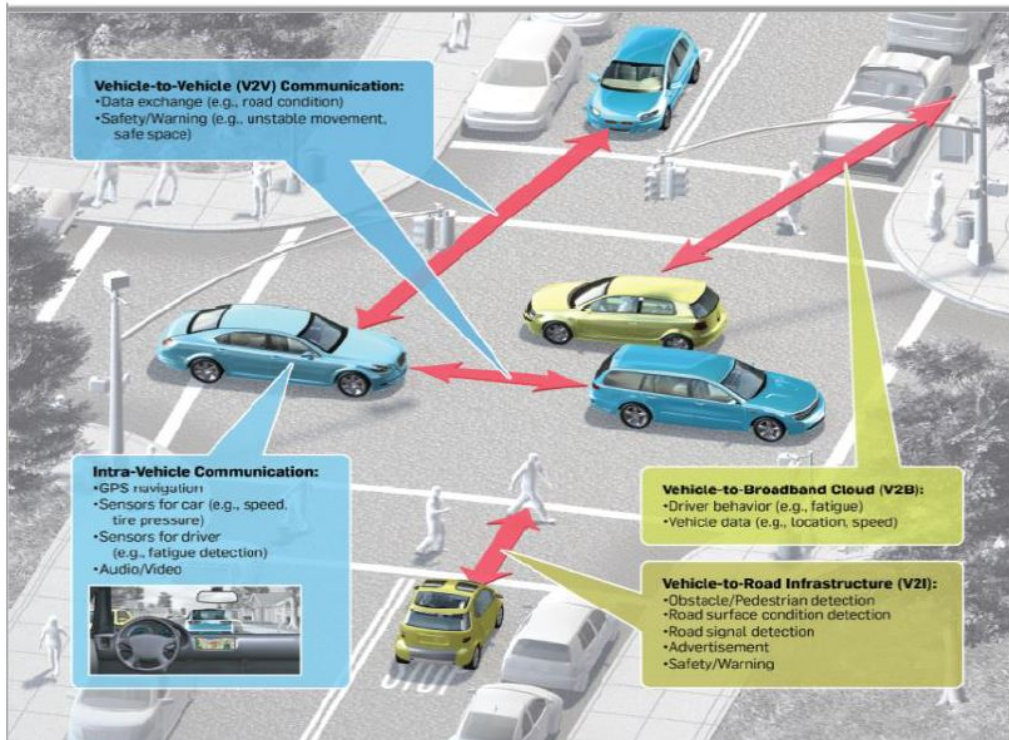


Figure 2.2: V2X communication system [59]

V Connected vehicles (CVs), autonomous vehicles (AVs), and connected autonomous vehicles (or CAVs)

Current technological developments in V2V and V2I communications have led to advancement within the industry of Connected vehicles (CVs), autonomous vehicles (AVs), and connected autonomous vehicles (or CAVs). CVs present vehicles utilize any of a diversity of different transmission and communication technologies to allow the communication with other vehicles on the road, the driver, roadside infrastructure. This technology can be employed to enhance vehicle efficiency, vehicle safety, and transmission times. The cutting-edge area of Automated Vehicles Technologies (AVTs) explain how CVs technology complements and cooperates automation. AVT falls roughly into the categories of: perception, planning and execution (exerted through actuators) using devices like LiDAR, Radar, DSRC, GPS, camera, mapping, sensors, which brief description of them is provided as follows [61]:

- LiDAR (light detection and ranging): LiDAR functions likewise to sonar in that it releases and measures the laser signals that rebound to compute the distance of objects in the neighbourhood of the vehicle.
- Radar: vehicles equipped with Radar release radio waves that rebound off objects and go back to a receiver to compute the distance of objects in the neighbourhood of the vehicle.
- Dedicated short-range communications (DSRC): DSRC is a wireless transmission protocol IEEE 802.11p utilized to communicate with infrastructure/or roadside units (V2I) as well as other vehicles (V2V).
- Global positioning system (GPS): GPS is a radio navigation system that empowers users to determine their actual position, time, and speed.
- Camera: cameras enable vehicles to recognize objects like vehicles, pedestrians, trucks, emergency lights, motorcycles, etc.
- Mapping: Route planning and navigation algorithms utilized in V2V to choose the shortest path to the destination, even in situations of blocked or heavy traffic and rerouting faster possible paths by using GPS. These algorithms serve on-ramps, intersections, and exits as decision nodes and those roads that connect them together as links that inform the vehicle's position on the road in V2V.
- Sensors: the combination of sensors and data plays a crucial role for AVTs. The data provided from specified sensors (OBU, fog sensor, and ultrasonic) can be combined to realize the roadway circumstances and environment.

Each modern vehicle has some level of automation, like cruise control, parking assist, lane centring systems, braking systems, automated windshield wipers and automated headlights [61]. As vehicles become more automated, it is common to identify distinct levels of the automation. In accordance with the National Highway Traffic Safety Administration (NHTSA) and the Society

of Automotive Engineers (SAE), published descriptions and definitions of the levels of automation for the vehicle which had the 5 levels of autonomy for the vehicles. These levels vary from level 0 which means no automation to levels 4 or 5, which mean full automation (may no need to driver at all) as you see in Figure 2 based upon functional terms of technology.







Automation Level	Modes	Terminals
 0 None	All driving functions assumed by user.	All functions assumed by manually operated equipment.
 1 Basic	Driving assistance (e.g. cruise control), but user responsible for core driving functions.	Operation assistance (location of drop-off, storage and pick up), but manually operated equipment.
 2 Partial	Some driving tasks (e.g. steering, acceleration, deceleration). User monitors environment and ready to take control.	Planning and managing the use of equipment and storage space (Warehouse and yard management systems).
 3 Conditional	Perform most driving tasks and monitors driving environment. User must be ready to take control at request.	Semi-automatic equipment (cranes, gantries, storage stacks). Automated access to facilities (automated gates).
 4 High	Performs all driving tasks and monitors controlled driving environment. User does not need to take control.	Integration between automated handling and storage systems (Fully automated terminal or warehouse). Automated pick-up and deliveries.
 5 Full	Autonomous vehicle; Performs all driving functions under all environments. User provides destination, but does not control vehicle.	Autonomous terminal; responds to demand (modal, intermodal, flows).

Figure 2.3: Automated driving levels [63]

- Level 0 (no automation): cars and equipment operated manually, which represents ordinary mechanical operations.
- Level 1 (basic): A number of driving helps and assistance is given to vehicles, providing them capability to change speed subject to adaptive cruise control and the operator required to be in control constantly.
- Level 2 (partial control): under this level of automation the vehicle is capable of undertaking partial management and control like steering under well-defined situations and acceleration/or deceleration.
- Level 3 (conditional control): This level of automation is achieving nearby actually autonomous vehicles because the majority of the driving is automated and so the operator is capable to take control based on request and much more complex situations. The vehicle can adequately

precept and monitor the environment with utilizing different kinds of sensors.

- Level 4 (high level control): present actual self-driving or automated vehicles ready to accomplish all the identified navigation with no intervention. This would need an active and constant monitoring of the environment and the ability to adapt. There is an alternative option to operate the vehicle manually.
- Level 5 (fully controlled): A fully autonomous vehicle prepared to operate in any environment with no intervention, and also can be employed remotely controlled Users simply require to input information about origin and destination [63].

Chapter 3

Stability Analysis of Vehicular Platooning Under DoS attacks

I Introduction

In this chapter, we present a complete theory of the observer-based control mechanism for platooning system in the presence of DoS attacks. More specifically, we study platoons of interconnected vehicles in which the local state of each vehicle is transmitted to the neighbouring vehicles through a V2V communications network. We introduce an observer to estimate the states of vehicles during the period of DoS attacks. We explore the practical problem where DoS attacks occur aperiodically and obtain an upper bound for the duration and frequency of attacks such that the vehicles in the platoon system asymptotically track the leader and maintain a safe inter-vehicular distance. Finally we present an optimization framework to maximize the duration of DoS attacks without performance degradation.

The rest of this chapter is organized as follows. In Section I.1 and I.2, the graph theory and the problem statement of platooning system are defined. In Section I.3 and I.4, the dynamic model of vehicles and the DoS attack model are presented. In Section II, the theory of the observer-based secure control approach for the vehicular platooning system is studied. Finally, simulation results are presented in Section III to show the efficiency of the proposed approach.

I.1 Graph Theory

We consider a platoon-based vehicular system with $N + 1$ vehicles including a leader vehicle and N following vehicles. An directed communication graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ is used to describe the interaction among vehicles. Here $\mathcal{V} = \{v_1, \dots, v_N\}$ is the set of follower vehicles in the graph, \mathcal{E} is a set of edges and $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$ represents the adjacency matrix. The identifier “ i ” denotes the i th follower vehicle in the platoon. If $(i, j) \in \mathcal{E}$, then the two follower vehicles i and j are adjacent with $a_{ij} = 1$. In this case, vehicles i and j can exchange information with each other or are in the measurement range of each other, otherwise $a_{ij} = 0$. \mathcal{N}_i represents the communications neighbouring set of vehicle i . The matrix $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{n_i \times n_i}$ represents the Laplacian matrix of the graph with $l_{ij} = \sum_{i \neq j, j \in \mathcal{N}_i} a_{ij}$ and $l_{ij} = -a_{ij}$ where $i \neq j$.

We also consider a graph $\bar{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}}, \bar{\mathcal{A}})$ to describe a communication graph between a leader and the followers where $\bar{\mathcal{V}} = \mathcal{V} \cup \{0\}$. Note that node 0 denotes a leader vehicle and $\mathcal{V} = \{1, 2, \dots, N\}$ denote the index of all other follower vehicles. If a follower vehicle i receives information from the leader, then $a_{i0} > 0$, otherwise $a_{i0} = 0$. Also, the leader does not receive information from the follower vehicles. Therefore, the communication interaction between a leader and followers is directed. We define $\mathcal{H} = \mathcal{L} + \Delta$ where $\Delta = \text{diag}(a_{10}, \dots, a_{N0})$.

I.2 Problem Statement

Consider a platoon-based vehicular system with a group of autonomous vehicles including a leader vehicle and N following vehicles (see Fig. 1). Specifically, we use an observer for each vehicle i equipped with on-board sensors to reconstruct the state based on available measurements. Then, each vehicle exchange the estimated states with other vehicles through a Dedicated Short Range Communication (DSRC) network. As Fig. 2 shows, each vehicle i can transmit the estimated position $\hat{p}_i(t)$, estimated velocity $\hat{v}_i(t)$ and estimated acceleration $\hat{a}_i(t)$ with neighbouring vehicles through an unreliable commu-

nication network susceptible to DoS attacks. In this thesis, we consider a scenario in which the attacker can launch a DoS attacks to the communication channels between vehicles for a period of time so that the transmission of information among vehicles is not possible. Our goal is to design a resilient controller for each vehicle i with observer scheme and investigate under what sufficient conditions the platooning system achieves asymptotic tracking of the leader and maintains a safe intervehicular distance.

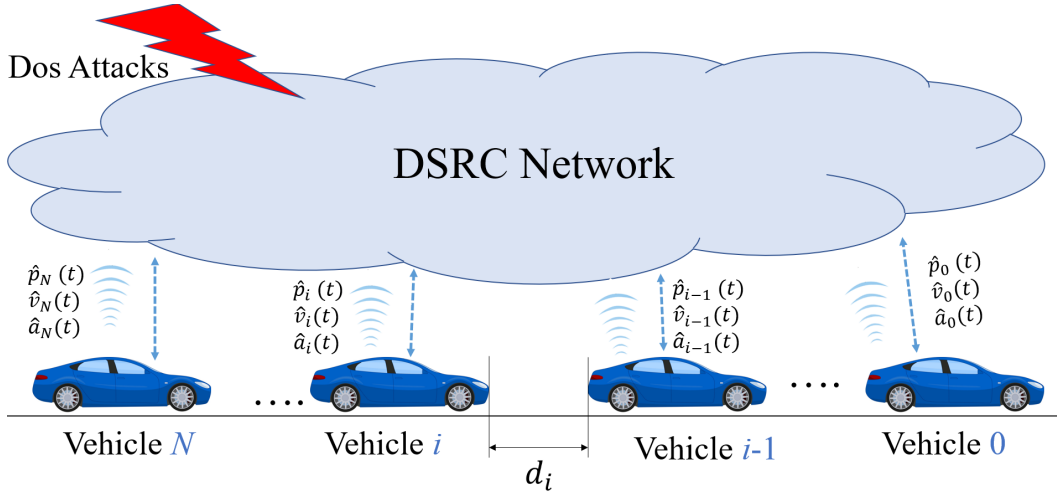


Figure 3.1: A platoon of connected vehicles under DoS attacks

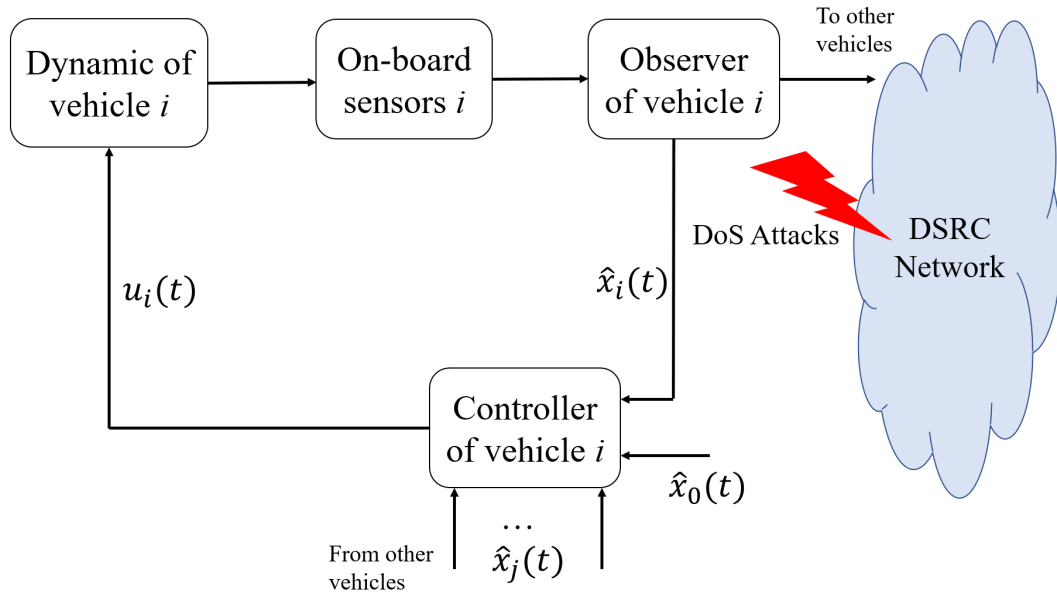


Figure 3.2: Block diagram of observer-based secure control for a platoon of connected vehicles under DoS attacks

I.3 Vehicle Dynamics

The longitudinal dynamic of each vehicle $i \in \mathcal{V}$ can be represented as follows [1]:

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = -\frac{1}{\tau}a_i(t) + \frac{1}{\tau}u_i(t) \end{cases} \quad (3.1)$$

where τ denotes the inertial time constant of a vehicle and $u_i(t)$ is the control signal of each vehicle i . Note that we assume that the external disturbance caused by wind gusts, ground frictions and rolling resistance is negligible. Inspired by [1], the work here can be extended in the case of disturbances. The main goal of the platoon control is to ensure that each follower vehicle tracks the velocity $v_0(t)$ of the leader while maintaining a desired intervehicular distance $d_{i,i-1}$ with its predecessor vehicle $i - 1$. In other words, each follower vehicle i is expected to achieve the following:

$$\begin{cases} p_i(t) - p_{i-1}(t) \rightarrow d_{i,i-1} \\ v_i(t) \rightarrow v_0(t) \end{cases} \quad (3.2)$$

I.4 DoS Attack Model

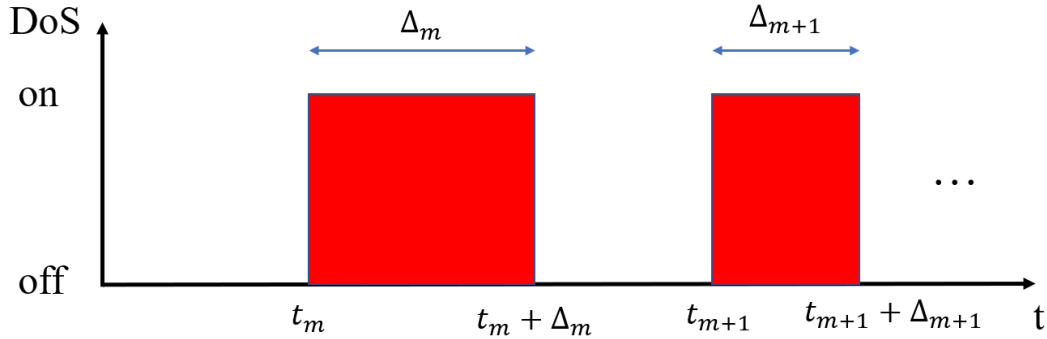


Figure 3.3: Illustration of DoS attack strategy

DoS attacks are one of the most commonly encountered cyber attacks in communication networks. DoS attacks in VCPSs impose illegitimate requests in order to change the average service time in the communication network. Therefore, DoS attacks induce extra service time which leads to interruptions of the transmission of information over the network. An attacker uses an attack signal to flood the communication channels, jamming the network nodes so

that information packets transmitted by legitimate users have to queue up for the duration of the attack. There are several ways of mathematically representing DoS attacks, including (i) treating the attack as packet losses [17, 18], or (ii) as a time-delay [19, 20, 13]. In the first case, the model assumes that the attack causes network congestion ultimately leading to the loss of useful communication packets between vehicles.

In the second, the network congestion produces a delay such that vehicles in the platoon cannot access to the DSRC on time and receive information from other vehicles with a time delay.

In this thesis, we consider the first type of DoS attack model. Fig. 3 represents the DoS attack strategy. The attacker launches an attack signal of variable duration. We assume that the attacker signal consists of variable on and off periods. This situation is typical in DoS attacks, primarily to avoid detection, and also due to limited energy resources by a non-sophisticated attacker. Accordingly, we assume that the total time-sequence is divided in two parts: (i) normal period without DoS attacks (ii) intervals where a DoS attack blocks the transmission of information between vehicles. The m th attack period is denoted as $D_m = [t_m, t_m + \Delta_m)$ where t_m is the time instant that the DoS attack starts and Δ_m is the duration of attack. For given $t \geq \tau$, the set of intervals such that the communication between vehicles is denied is defined as $\Xi_a(\tau, t) = \bigcup D_m \cap [\tau, t]$, the set of time intervals where communication between vehicles is allowed is $\Xi_s(\tau, t) = \Xi_a(\tau, t) \setminus [\tau, t]$. We also make the following assumptions with respect to the duration and frequency of the DoS attacks (see reference ([15]):

Assumption 1. For any $T_2 > T_1 \geq t_0$, $N_a(T_1, T_2)$ represents the total number of Dos attacks over the interval $[T_1, T_2)$. The frequency of DoS attacks over the interval $T_a(T_1, T_2)$ is defined as follows ([15]):

$$F_a(T_1, T_2) = \frac{N_a(T_1, T_2)}{T_2 - T_1} \quad (3.3)$$

Assumption 2. For any $T_2 > T_1 \geq t_0$, let $T_a(T_1, T_2)$ represent the total time interval of DoS attacks over the interval $[T_1, T_2)$. The attack duration

over $[T_1, T_2]$ is described as follows: there exists scalars $T_0 \geq 0$ and $\tau_a > 1$ satisfying ([15])

$$T_a(T_1, T_2) \leq T_0 + \frac{T_2 - T_1}{\tau_a} \quad (3.4)$$

II Observer-based Secure Control Scheme Design For Platooning System

II.1 Closed-Loop System Model

The dynamical equations of vehicle (3.1), can be written in the following form:

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad i = 1, 2, \dots, N, \quad (3.5)$$

where $x_i(t) = [p_i(t), v_i(t), a_i(t)]^T$, represents the state vector of vehicle i , and the matrices A and B are given by:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ -\frac{1}{\tau} \end{bmatrix}.$$

where we assume a homogeneous platoon of vehicles. The observer for each vehicle i is designed to estimate the state of vehicle i based on available sensor measurements (exteroceptive sensors when there is an attack) with the following structure:

$$\dot{\hat{x}}_i(t) = A\hat{x}_i(t) + Bu_i(t) + G_{ob}\left(y_i(t) - \hat{y}_i(t)\right), \quad i = 1, \dots, N. \quad (3.6)$$

In this equation $\hat{x}_i(t)$ represents the estimated state of vehicle i , G_{ob} is the observer gain and $y_i(t)$ is measured via onboard sensors in vehicle i .

The control law to achieve the platoon control objective (3.2) is defined as follows:

$$u_i(t) = K \left[\sum_{j=1}^N a_{ij} \left(\hat{x}_i(t) - \hat{x}_j(t) - D_{ij} \right) + a_{i0} \left(\hat{x}_i(t) - \hat{x}_0(t) - D_{i0} \right) \right] \quad (3.7)$$

where $D_{ij} = [d_{ij}, 0, 0]^T$ with $d_{ij} = \sum_{l=j}^{i-1} d_{l,l+1}$ being the desired space between the vehicle i and vehicle j ; $K = [k^p, k^v, k^a]$ is the controller gain to be designed

and a_{ij} is the element of adjacency matrix and indicate the interaction between vehicle i and vehicle j . The parameter a_{i0} indicates the communication interaction between the leader and follower. Note that each vehicle i needs to know its interaction with other vehicles which can be detected by roadside infrastructures and transmit to all vehicles through Vehicle to Infrastructure (V2I) communication [1].

Assumption 3. *Each vehicle needs to know the interaction topology of platooning system, which can be detected by roadway infrastructures and transmit to each vehicle via V2I communications which is free of DoS attacks.*

Remark 1. *Assumption 3 reflects the fact that current approaches in cyber-attack detection and network recovery mechanisms [21, 22, 23, 24] all rely on dedicated trustworthy roadside units (RSUs) to ensure high quality V2I communications, which can be guaranteed by large-scale deployment of roadside units (RSUs) or by employing visible light as communication links [21]. Therefore, in this work we consider secured V2I communications to broadcast the interaction topology of platooning system while designing an observer-based secure control for each vehicle to handle DoS attacks on V2V network.*

Consider now vehicle i in (3.5) and the objective of the platooning system (3.2). The tracking error between the leader and vehicle i can be defined as follows:

$$e_i(t) = x_i(t) - x_0(t) - D_{i0}, \quad (3.8)$$

where $x_0(t) = [p_0(t), v_0(t), 0]$. Using Eqs. (3.5)-(3.8) and considering the observer error $\tilde{x}_i(t) = x_i(t) - \hat{x}_i(t)$, we obtain the following expression for the tracking error:

$$\begin{aligned} \dot{e}_i(t) = & Ae_i(t) + BK \left[\sum_{j=1}^N a_{ij} \left(e_i(t) - e_j(t) - \tilde{x}_i(t) + \tilde{x}_j(t) \right) \right. \\ & \left. + a_{i0} \left(e_i(t) - \tilde{x}_i(t) \right) \right] \end{aligned} \quad (3.9)$$

Let the extended vectors $e(t)$ and $\hat{x}(t)$ be defined as follows: $e(t) = [e_1^T(t), e_2^T(t), \dots, e_N^T(t)]^T$ and $\hat{x}(t) = [\hat{x}_1^T(t), \hat{x}_2^T(t), \dots, \hat{x}_N^T(t)]^T$. We can write:

$$\dot{e}(t) = \left(I_N \otimes A + \mathcal{H} \otimes BK \right) e(t) - \left(\mathcal{H} \otimes BK \right) \hat{x}(t) \quad (3.10)$$

$$\dot{\tilde{x}}(t) = \left[I_N \otimes A - I_N \otimes G_{ob}C \right] \tilde{x}(t) \quad (3.11)$$

where $\mathcal{H} = \mathcal{L} + \Delta$. Then, we say that the platooning system is stable provided that:

$$\lim_{t \rightarrow \infty} e_i(t) = 0. \quad (3.12)$$

Therefore, our objective is to design the feedback controller gain K and observer gain G_{ob} for each follower vehicle i and derive sufficient conditions for the duration $T_a(T_1, T_2)$ and frequency $F_a(T_1, T_2)$ of the DoS attacks such that stability of all follower vehicles in the platooning system is guaranteed.

Remark 2. *In this thesis, the observer plays an important role during the DoS attack interval. We consider a scenario in which each vehicle i in the platooning system is equipped with onboard sensors to measure, directly or indirectly, relative distance, velocity, and acceleration, with respect to the preceding and follower vehicles. This task can be accomplished by fusing LiDAR data and image based object detection, and estimating the state of vehicle j in order to design the controller of vehicle i during the attack interval. Therefore, the observer is used to mitigate the adverse effects caused by Dos attacks and to improve the resilience and tolerance of the platooning system against DoS attacks. We emphasize the difference of this approach with previous work. Indeed, some references (see for example [15, 16]) set the control input to be either zero or constant during the attacked period.*

II.2 Stability Analysis

In this section we develop sufficient conditions for the duration and frequency of the DoS attacks for the platooning system to achieve asymptotic tracking of the leader and maintain the desired intervehicular spacing. We then propose an optimization framework to improve the resiliency and tolerance of the platooning system against DoS attacks by simultaneously designing the controller gain and observer gain.

Theorem II.1. *Consider the system dynamics described in (3.5) with the observer structure (3.6). If Assumptions 1-3 are satisfied, then stability of the platooning system is guaranteed if the following conditions are satisfied:*

1. There exist a constant ξ^* such that the frequency of DoS attacks $F_a(t_0, t)$ satisfies the following inequality:

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \leq \frac{\xi^*}{\ln(\mu) + (\gamma_s + \gamma_a)\Delta^*} \quad (3.13)$$

2. There exists a positive constant τ_a in the duration of DoS attack with an arbitrary constant $T_0 \geq 0$ such that

$$\tau_a > \frac{\gamma_s + \gamma_a}{\gamma_s + \xi^*} \quad (3.14)$$

the parameters γ_s and γ_a can be obtained from the following linear matrix inequality (LMI) conditions:

$$\begin{bmatrix} QA + A^T Q + \gamma_1 I & QC & \mathcal{H} \otimes BK \\ C^T Q & R & 0 \\ (\mathcal{H} \otimes BK)^T & 0 & P \end{bmatrix} < 0 \quad (3.15)$$

$$\begin{bmatrix} A^T P^{-1} + P^{-1} A + \gamma_2 I + \epsilon^{-1} P^{-1} & P^{-1} B \\ B^T P^{-1} & -T \end{bmatrix} < 0 \quad (3.16)$$

$$\begin{bmatrix} QA + A^T Q - \gamma_3 I & QC & \mathcal{H}^{\delta(t)} \otimes BK \\ C^T Q & R & 0 \\ (\mathcal{H}^{\delta(t)} \otimes BK)^T & 0 & S \end{bmatrix} < 0 \quad (3.17)$$

$$\begin{bmatrix} A^T S^{-1} + S^{-1} A - \gamma_4 I + \epsilon^{-1} S^{-1} & S^{-1} B \\ B^T S^{-1} & -T \end{bmatrix} < 0 \quad (3.18)$$

where $\mathcal{H}^{\delta(t)}$ is the Laplacian matrix in the case of attack and convergence rate γ_s during the normal period and convergence rate γ_a during the attacked interval are given as

$$\begin{aligned} \gamma_s &= \max\{\gamma_1, \gamma_2\} \\ \gamma_a &= \min\{\gamma_3, \gamma_4\} \end{aligned}$$

Proof. Step 1 (Two Intervals Classification):

We define the interval of time where the communications are free of DoS attack and also the interval of time with DoS attack. The m th time interval of DoS attack is as follows:

$$\Upsilon_m = [t_m, t_m + \Delta_m + \Delta^*)$$

where t_m is the time instant that the DoS attack starts, Δ_m is the duration of attack and Δ^* represent the uncertainty in the m th time interval of DoS

attack. Therefore the time interval $[\tau, t)$ consists of the following union of subintervals: $[\tau, t) = \bar{\Xi}_s(\tau, t) \cup \bar{\Xi}_a(\tau, t)$ with

$$\bar{\Xi}_a(\tau, t) = \cup \Upsilon_m \cap [\tau, t], \quad \bar{\Xi}_s(\tau, t) = [\tau, t] \setminus \bar{\Xi}_a(\tau, t)$$

Step 2 (Lyapunov Stability Analysis):

1) We consider the time interval $\bar{\Xi}_s(\tau, t)$ where vehicles communicate with each other without DoS attack and choose the following Lyapunov function:

$$V_1(t) = \tilde{x}^T(t)(\Phi \otimes Q)\tilde{x}(t) + e^T(t)(\Phi \otimes P^{-1})e(t) \quad (3.19)$$

Using Eqs. (3.10)-(3.11), the time derivative of (3.19) is given by:

$$\begin{aligned} \dot{V}_1(t) = & \tilde{x}^T(t) \left[\Phi \otimes (QA + A^T Q) \right] \tilde{x}(t) \\ & - \tilde{x}^T(t) \left(\Phi \otimes QCR^{-1}C^T Q \right) \tilde{x}(t) \\ & + e^T(t) \left[\Phi \otimes (A^T P^{-1} + P^{-1} A) \right. \\ & \left. + (\mathcal{H}^T \Phi + \mathcal{H} \Phi) \otimes P^{-1} B T^{-1} B^T P^{-1} \right] e(t) + M \end{aligned} \quad (3.20)$$

where

$$M = \tilde{x}^T(t) (\Phi \mathcal{H} \otimes BK)^T P^{-1} e(t) + e^T(t) (\Phi \mathcal{H} \otimes P^{-1} BK) \tilde{x}(t) \quad (3.21)$$

Using Young's inequality $2a^T b \leq \varepsilon a^T a + \varepsilon^{-1} b^T b$ for any ε and $a, b \in \mathbb{R}^n$ we can write:

$$\begin{aligned} \dot{V}_1(t) \leq & \tilde{x}^T(t) \left[\Phi \otimes (QA + A^T Q) - (\Phi \otimes QCR^{-1}C^T Q) \right. \\ & \left. - \varepsilon (\Phi \mathcal{H} \otimes BK)^T P^{-1} (\Phi \mathcal{H} \otimes BK) \right] \tilde{x}(t) \\ & + e^T(t) \left[\Phi \otimes (A^T P^{-1} + P^{-1} A) + (\mathcal{H}^T \Phi + \mathcal{H} \Phi) \right. \\ & \left. \otimes P^{-1} B T^{-1} B^T P^{-1} - \varepsilon^{-1} P^{-1} \right] e(t) = \\ & \begin{bmatrix} \tilde{x}(t) \\ e(t) \end{bmatrix}^T \begin{bmatrix} \Pi_1 & 0 \\ 0 & \Pi_2 \end{bmatrix} \begin{bmatrix} \tilde{x}(t) \\ e(t) \end{bmatrix}. \end{aligned} \quad (3.22)$$

Therefore, the condition for stability of the platooning system in a period of normal operation without attack is:

$$\begin{aligned} \Pi_1 = & \Phi \otimes (QA + A^T Q) - (\Phi \otimes QCR^{-1}C^T Q) \\ & - \varepsilon (\Phi \mathcal{H} \otimes BK)^T P^{-1} (\Phi \mathcal{H} \otimes BK) + \gamma_1 I < 0 \end{aligned} \quad (3.23)$$

$$\begin{aligned} \Pi_2 &= \Phi \otimes (A^T P^{-1} + P^{-1} A) + (\mathcal{H}^T \Phi + \mathcal{H} \Phi) \\ &\otimes P^{-1} B T^{-1} B^T P^{-1} - \varepsilon^{-1} P^{-1} + \gamma_2 I < 0. \end{aligned} \quad (3.24)$$

Using the Schur complement lemma, inequalities (3.23)-(3.24) can be transformed into the following LMI conditions:

$$\begin{bmatrix} QA + A^T Q + \gamma_1 I & QC & \mathcal{H} \otimes BK \\ C^T Q & R & 0 \\ (\mathcal{H} \otimes BK)^T & 0 & P \end{bmatrix} < 0, \quad (3.25)$$

$$\begin{bmatrix} A^T P^{-1} + P^{-1} A + \gamma_2 I + \varepsilon^{-1} P^{-1} & P^{-1} B \\ B^T P^{-1} & -T \end{bmatrix} < 0. \quad (3.26)$$

2) We now consider the DoS attack periods. During attack intervals, malicious attacks affect the communication channels between vehicles and the interaction topology becomes $\mathcal{H}^{\delta(t)}$. We consider the Lyapunov function V_2 for observer error dynamic and tracking error dynamics:

$$V_2(t) = \tilde{x}^T(t) (\Phi \otimes Q) \tilde{x}(t) + e^T(t) (\Phi \otimes S^{-1}) e(t) \quad (3.27)$$

Taking the derivative of $V_2(t)$ along the trajectories (3.10)-(3.11) we have:

$$\begin{aligned} \dot{V}_2(t) &\leq \tilde{x}^T(t) \left[\Phi \otimes (QA + A^T Q) - (\Phi \otimes QCR^{-1}C^T Q) \right. \\ &\quad \left. - \varepsilon (\Phi \mathcal{H}^{\delta(t)} \otimes BK)^T S^{-1} (\Phi \mathcal{H}^{\delta(t)} \otimes BK) \right] \tilde{x}(t) \\ &\quad + e^T(t) \left[\Phi \otimes (A^T S^{-1} + S^{-1} A) + (\mathcal{H}^{\delta(t)T} \Phi + \mathcal{H}^{\delta(t)} \Phi) \right. \\ &\quad \left. \otimes S^{-1} B T^{-1} B^T S^{-1} - \varepsilon^{-1} S^{-1} \right] e(t) = \\ &\quad \begin{bmatrix} \tilde{x}(t) \\ e(t) \end{bmatrix}^T \begin{bmatrix} \Pi_3 & 0 \\ 0 & \Pi_4 \end{bmatrix} \begin{bmatrix} \tilde{x}(t) \\ e(t) \end{bmatrix}. \end{aligned} \quad (3.28)$$

Therefore, the condition for stability of the platooning system during attack intervals is:

$$\begin{aligned} \Pi_3 &= \Phi \otimes (QA + A^T Q) - (\Phi \otimes QCR^{-1}C^T Q) \\ &\quad - \varepsilon (\Phi \mathcal{H} \otimes BK)^T P^{-1} (\Phi \mathcal{H} \otimes BK) - \gamma_3 I < 0 \end{aligned} \quad (3.29)$$

$$\begin{aligned} \Pi_4 &= \Phi \otimes (A^T P^{-1} + P^{-1} A) + (\mathcal{H}^T \Phi + \mathcal{H} \Phi) \\ &\quad \otimes P^{-1} B T^{-1} B^T P^{-1} - \varepsilon^{-1} P^{-1} - \gamma_4 I < 0. \end{aligned} \quad (3.30)$$

Then, we obtain the following LMI conditions:

$$\begin{bmatrix} QA + A^T Q - \gamma_3 I & QC & \mathcal{H}^{\delta(t)} \otimes BK \\ C^T Q & R & 0 \\ (\mathcal{H}^{\delta(t)} \otimes BK)^T & 0 & S \end{bmatrix} < 0 \quad (3.31)$$

$$\begin{bmatrix} A^T S^{-1} + S^{-1} A - \gamma_s I + \epsilon^{-1} S^{-1} & S^{-1} B \\ B^T S^{-1} & -T \end{bmatrix} < 0. \quad (3.32)$$

Based on above analysis, we can combine both scenarios for the platooning system with/without DoS attacks to obtain the following relationship:

$$V(t) = \begin{cases} e^{-\gamma_s(t-t_m-\Delta_m)} V(t_m + \Delta_m), & t \in \Xi_s(\tau, t) \\ e^{\gamma_a(t-t_m)} V(t_m), & t \in \Xi_a(\tau, t), \end{cases} \quad (3.33)$$

where $V(t) = V_1(t) + V_2(t)$. Our goal is to find an upper bound on the DoS attacks frequency and duration. The solution of Lyapunov function can be written as follows:

$$V(t) \leq \mu^{N_a(t_0, t)} e^{-\gamma_s |\bar{\Xi}_s(t_0, t)|} e^{\gamma_a |\bar{\Xi}_a(t_0, t)|} V(0), \quad (3.34)$$

where $N_a(t_0, t)$ is the number of activation of attack. Note that $|\bar{\Xi}_s(t_0, t)| = t - t_0 - |\bar{\Xi}_a(t_0, t)|$ and due to uncertainty of duration attack $|\bar{\Xi}_s(t_0, t)| \leq |\bar{\Xi}_s(t_0, t)| + (1 + N_a(t_0, t)) \Delta^*$. Then,

$$\begin{aligned} & -\gamma_s \left(t - t_0 - |\bar{\Xi}_a(t_0, t)| \right) + \gamma_a |\bar{\Xi}_s(t_0, t)| = \\ & -\gamma_s (t - t_0) + (\gamma_s + \gamma_a) |\bar{\Xi}_s(t_0, t)| \leq \\ & -\gamma_s (t - t_0) + (\gamma_s + \gamma_a) \left[T_0 + \frac{t - t_0}{\tau_a} + (1 + N_a(t_0, t)) \Delta^* \right] \end{aligned} \quad (3.35)$$

We can write:

$$V(t) \leq e^{(\gamma_s + \gamma_a)(T_0 + \Delta^*)} e^{-\gamma_s(t-t_0)} e^{\frac{(\gamma_s + \gamma_a)}{\tau_a}(t-t_0)} \times e^{[\ln(\mu) + (\gamma_s + \gamma_a)\Delta^*]N_a(t_0, t)} V(t_0). \quad (3.36)$$

Considering Eqs. (3.13)-(3.14) and $\xi = \gamma_s + \frac{(\gamma_s + \gamma_a)}{\tau_a} - \xi^* > 0$ we obtain:

$$V(t) \leq e^{(\gamma_s + \gamma_a)(T_0 + \Delta^*)} e^{-\xi(t-t_0)} V(t_0) \quad (3.37)$$

which completes the proof. \square

Remark 3. According to the result of Theorem II.1, stability of the platooning system can be guaranteed provided that conditions (3.13) and (3.14) are satisfied. Notice that, according to the assumptions and practical considerations, DoS attacks have limited duration and frequency. The system tolerance to DoS attacks, however, is proportional to the maximum convergence rate γ_s during

the normal period and minimum convergence rate γ_a during attacked intervals. Therefore, by maximizing the γ_s and minimizing the γ_a , the our solution can improve the tolerance of platooning system against DoS attacks. Theorem II.1 provides conditions for the upper bound of the attack duration to achieve the platooning objectives (3.2). Therefore, asymptotic tracking of the leader and maintaining the desired safety distance of platooning system can achieved provided that the attack duration is smaller than a certain value. This is accomplished provided that $\tau_a > \frac{\gamma_s + \gamma_a}{\gamma_s + \xi^*}$. Notice also that the uncertainty term Δ^* in (3.35) relaxes the assumption of periodic attack duration with respect to previous references. Our goal is to design the control gain and observer gain such that tolerance to the duration of DoS attacks is maximized as much as possible to ensure the robustness of the platooning system against DoS attacks. To this end, we establish the following optimization problem:

$$\begin{aligned} & \min_{K, G_{ob}, \gamma_s, \gamma_a} && \frac{\gamma_s + \gamma_a}{\gamma_s + \xi^*} \\ & s.t. && \text{LMI conditions (15) – (18)} \end{aligned} \quad (3.38)$$

III Simulation Results

In this section, we provide simulation results to illustrate the effectiveness of proposed method. We consider a team of seven vehicles, consistent of one leader and six follower vehicles. The vehicle state is defined as follows:

$$x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix}$$

where x_1 represents position, x_2 velocity, and x_3 acceleration of the respective vehicle. The communication topology of vehicles is shown in Fig. 4. The inertial time constant of each vehicle is assumed as $\tau_a = 0.54$. We consider the system (3.5) with

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1.8519 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ -1.8519 \end{bmatrix}$$

$$C = [1 \quad 1 \quad 0].$$

Considering the directed communication topology of the six follower vehicles, the associated adjacency matrix can be selected as follows:

$$\mathcal{L} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}$$

$$\Delta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We consider the optimization framework (38) to design the controller and observer gains that maximize the duration of attack. Using the MATLAB software and selecting $T = 0.5$, $R = 0.1$, we obtain the set of feasible solutions for the Lyapunov matrices P , and S , as well as the control gain K and observer gain G :

$$\begin{aligned} K &= [-2.7386 \quad -5.3068 \quad -2.7725] \\ G &= [-1.2247 \quad -2.6814 \quad -1.3229]^T \\ P &= \begin{bmatrix} 1.4533 & 1.0331 & 0.1479 \\ 1.0331 & 1.8541 & 0.2866 \\ 0.1479 & 0.2866 & 0.1497 \end{bmatrix} \\ Q &= \begin{bmatrix} 1.6420 & 1.4225 & 0.3307 \\ 1.4225 & 2.7837 & 0.7240 \\ 0.3307 & 0.7240 & 0.3572 \end{bmatrix} \end{aligned}$$

In our simulation we assume that the initial state of the leader vehicle is $x_0(0) = [0, 15, 0]^T$. The initial state of the followers is as follows: $x_1(0) = [-7, 15, 0]^T$, $x_2(0) = [-15, 15, 0]^T$, $x_3(0) = [-35, 15, 0]^T$, $x_4(0) = [-44, 15, 0]^T$, $x_5(0) = [-57, 15, 0]^T$, $x_6(0) = [-68, 15, 0]^T$. Also, the desire trajectory of the leader vehicle is as follows:

$$v_0(t) = \begin{cases} 15, & 0 \leq t < 10 \\ 15 + 2t, & 10 \leq t < 15 \\ 25, & 15 \leq t < 35 \\ 25 - t, & 35 \leq t < 40 \\ 20, & 40 \leq t < 65 \end{cases} \quad (3.39)$$

The simulation results in Fig. 5-8 show a comparison between the approach proposed in this article and the traditional method in [1] considering the effect of DoS attacks. As can be seen from Fig. 7 and Fig. 8 that using the proposed approach (observer-based resilient controller) the platooning system can tolerate safety distance and velocity tracking longer than using a traditional approach proposed in [1] (Fig. 5 and Fig.6). In other words, using a traditional control scheme where the control signal is maintained zero or constant during the DoS attack interval, the time to tolerate safety distance and velocity tracking is shorter than using our proposed method. Therefore, using our proposed approach (see Fig. 7-8) the follower vehicles can tolerate the DoS attacks at $[0s, 10s]$ and $[16s, 35s]$ and continue to track both velocity and trajectory of the leader while maintaining the desired safety distance with slight performance degradation.

Figures 9-12 expand the previous case by extending the duration of the DoS attack. Considering the same system, we now simulate DoS attacks over the intervals $[0s, 10s]$ and $[16s, 45s]$, with the same initial conditions. Figures 11 and Fig 12 show the system performance using our controller whereas figures 9 and 10 show the same system response using the controller of reference [1]. As can be seen from the figures, our proposed controller show significantly improved tracking, thus illustrating the advantage of the proposed approach.

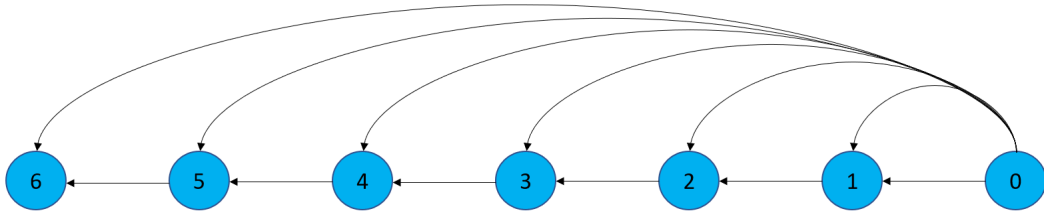


Figure 3.4: Communication topology of vehicles

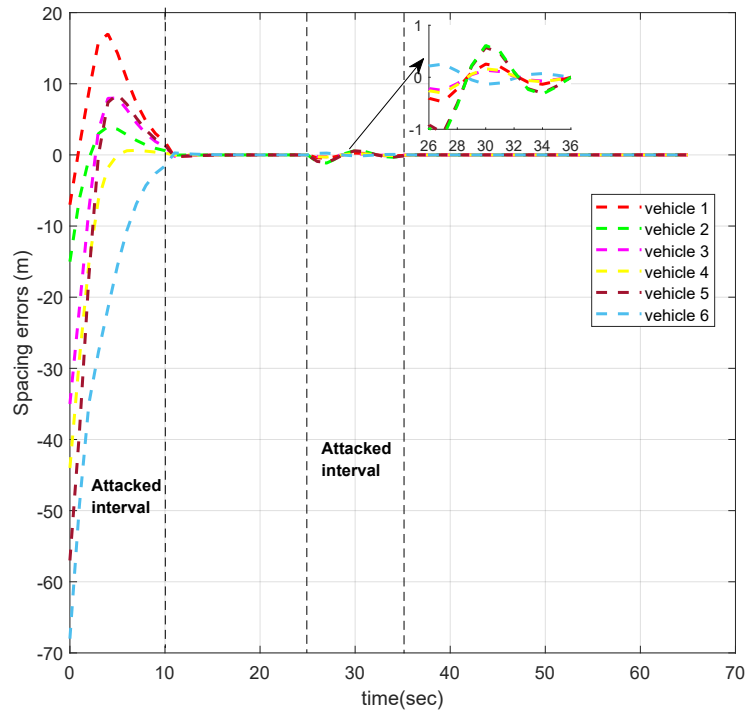


Figure 3.5: Spacing errors of vehicles under DoS attacks [1].

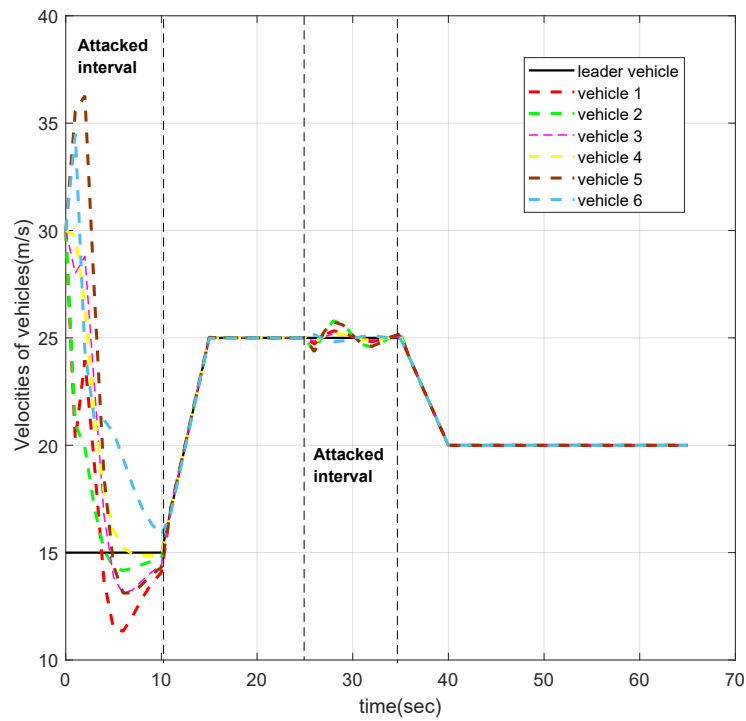


Figure 3.6: Velocities of vehicles under DoS attacks [1].

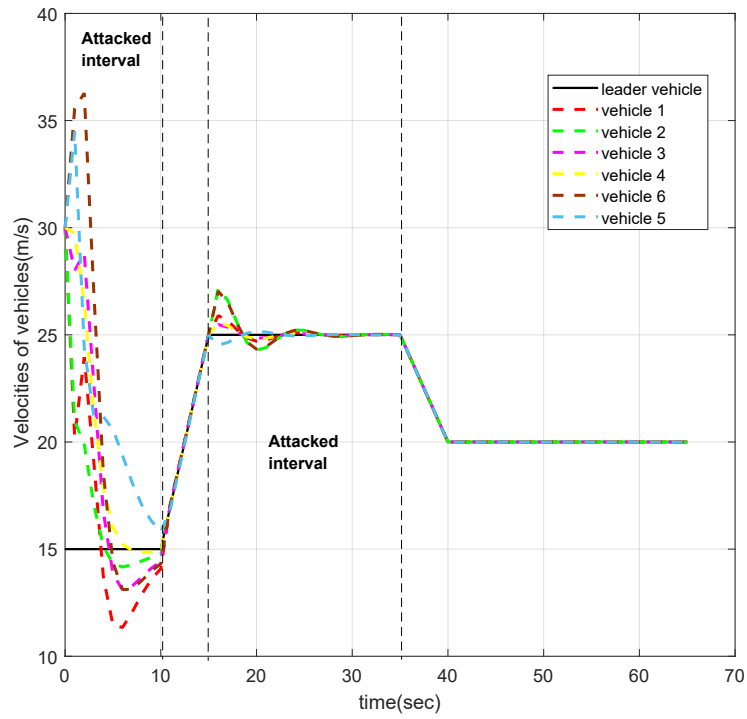


Figure 3.7: Spacing errors of vehicles under DoS attacks.

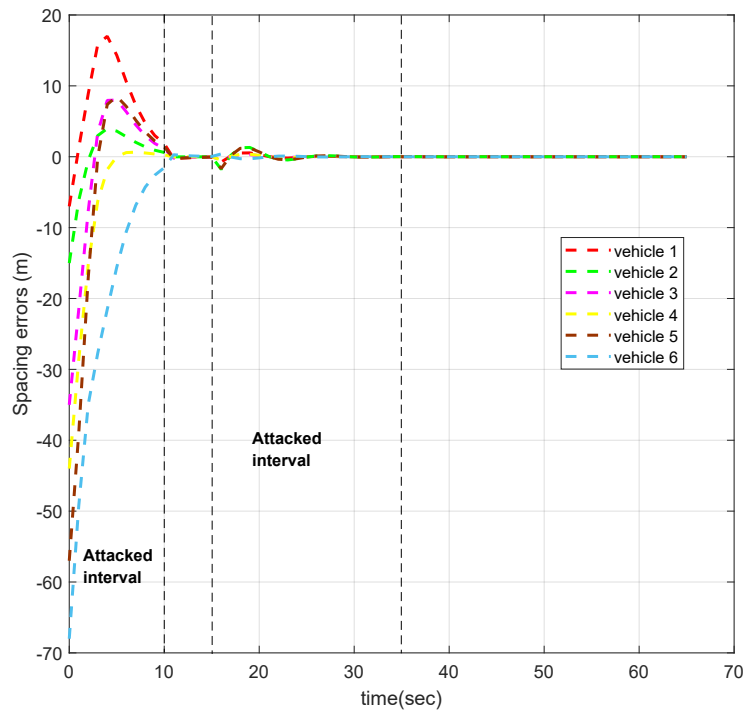
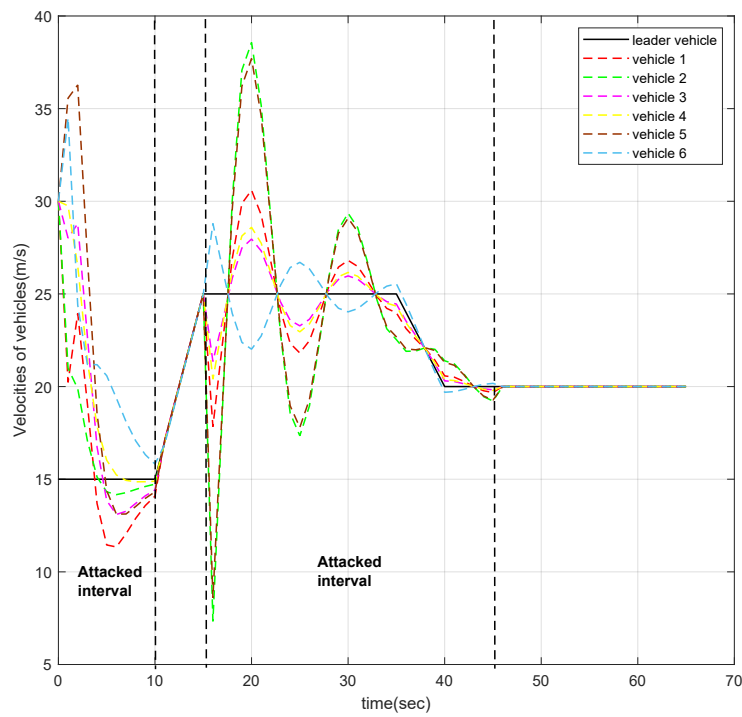
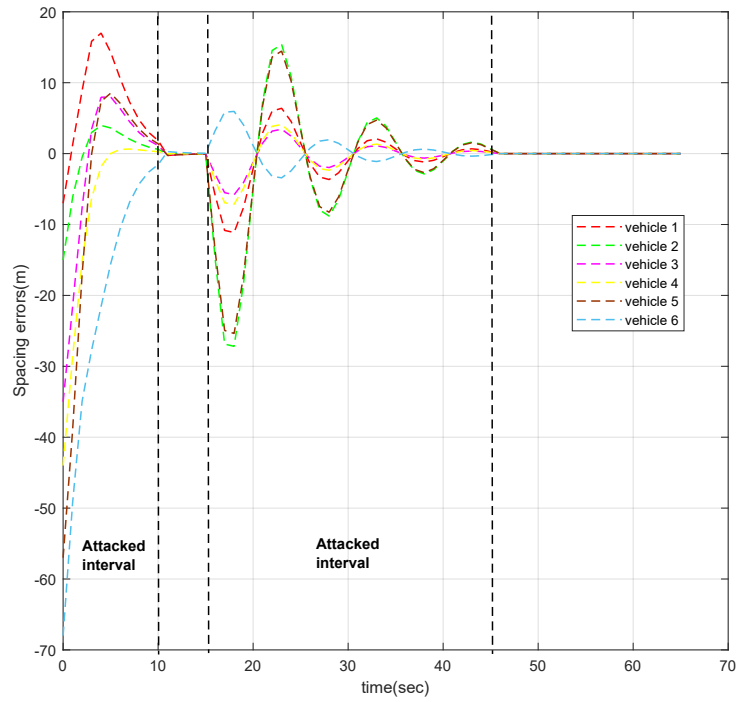


Figure 3.8: Velocities of vehicles under DoS attacks.



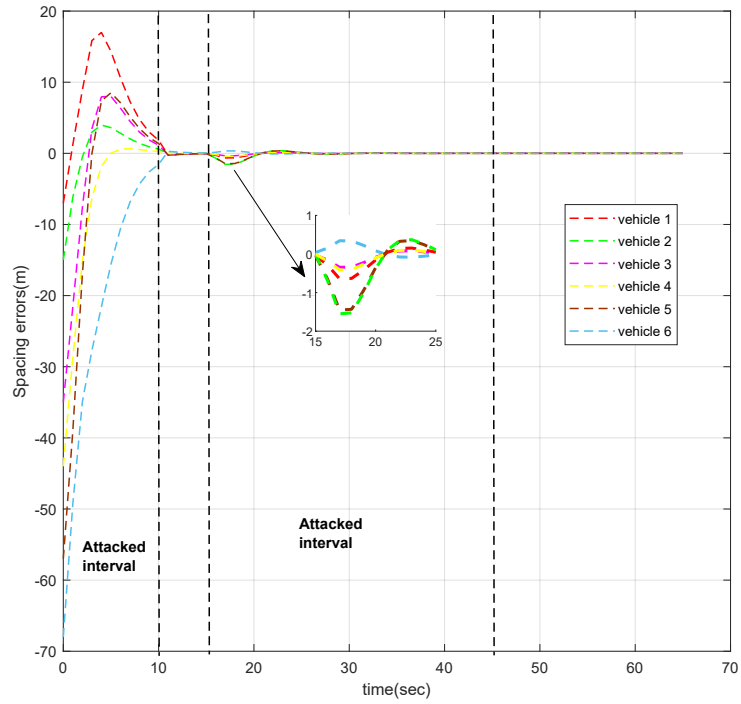


Figure 3.11: Spacing errors of vehicles under DoS attacks.

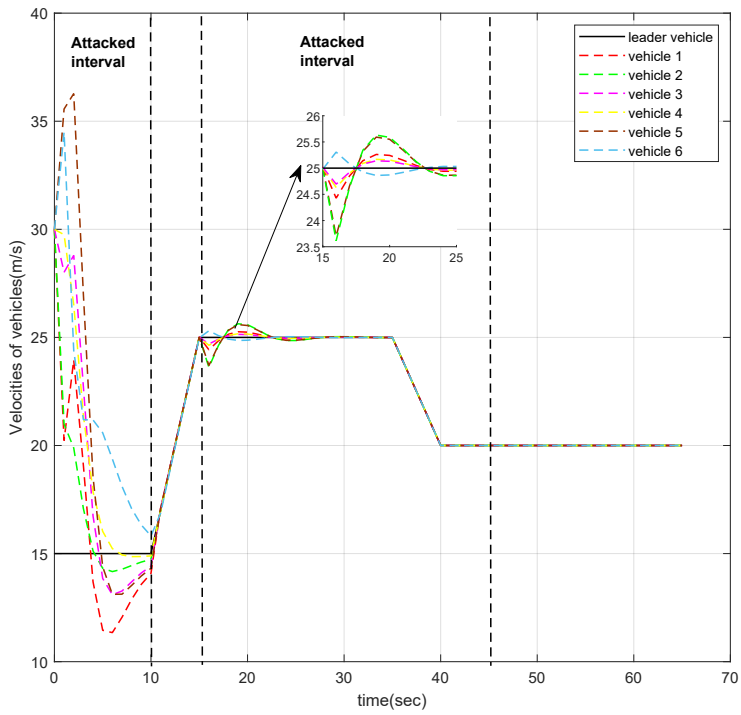


Figure 3.12: Velocities of vehicles under DoS attacks.

Chapter 4

Summary and Conclusions

In this thesis, we investigated the problem of observer-based secure control for platooning system suffering from aperiodic DoS attacks. We designed both controller and observer that ensure the platoon can tolerate maximum duration of DoS attack and remain stable. We represented briefly in chapter 2, some technical preliminaries. This includes Lyapunov stability theorem which is used to study the stability of our platoon of connected vehicles (CVs). Also, we briefly describe the vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-vehicle /or vehicle-to-infrastructure (V2V /or V2I, V2X) communication and also describe the connected vehicles (CVs), automated vehicles (AVs) and connected and automated vehicles (CAVs) and the devices for connected vehicles as well as explaining the different level of automation.

In chapter 3, we consider a platoon-based vehicular system with a group of autonomous vehicles including a leader vehicle and N following vehicles. Assuming a homogeneous platoon of vehicles, we model the longitudinal dynamic of each vehicle and also model the DoS attack. Afterwards, we design an observer for each vehicle to estimate the state of each vehicle based on available sensor measurements. Considering that each vehicle know the interaction topology of platooning system while designing an observer-based secure control for each vehicle to handle DoS attacks on V2V network. Then in stability analysis section, we develop sufficient conditions for the duration and frequency of the DoS attacks for the platooning system to achieve asymptotic tracking of the leader and maintain the desired intervehicular spacing. We

then propose an optimization framework to improve the resiliency and tolerance of the platooning system against DoS attacks by simultaneously designing the controller gain and observer gain. Finally, we provide simulation results to illustrate the effectiveness of proposed method. We consider a team of seven vehicles, consistent of one leader and six follower vehicles. We provide a comparison between the approach proposed in this thesis and the traditional method in [1] considering the effect of DoS attacks and show using our proposed approach (observer-based resilient controller) the platooning system can tolerate safety distance and velocity tracking longer than using a traditional approach proposed in [1]. In other words, using a traditional control scheme where the control signal is maintained zero or constant during the DoS attack interval, the time to tolerate safety distance and velocity tracking is shorter than using our proposed method. Moreover, we show that our proposed controller significantly improved tracking.

In conclusion, we consider the design of resilient control such that the stability of platooning system is guaranteed. We obtain sufficient conditions on duration and frequency of DoS attacks such that platooning system achieves asymptotic tracking of the leader and maintain the desired safety distance. We also provide an optimization approach to maximize the duration of DoS attacks such that a platooning system can tolerate without performance degradation.

I Directions for Future Work

There some other ideas which can be pursued in the future works as follows:

1. One aspect that is critical to the proper operation of a vehicular platooning system is the reliable localization of each vehicle in the platoon. Measuring the position of each vehicle is, however, difficult and often affected by measuring error. One way to improve this measure is to employ cooperative localization (CL). In CL, a team of vehicles can improve localization precision using relative observations with respect to other vehicles and then exchanging this information with other vehicles in the platoon, [71, 72]. As a further path in this research, CL of connected

vehicles in the platooning system can be explored.

2. Also, in order to alleviate limited bandwidth of the communication channel in the platooning system, event-triggered consensus control can be investigated. The idea behind the event-triggered formalism is to update the control signal based on the occurrence of some event, rather than periodically. In this scenario, the controller signal remains unchanged between updates of the control input. It would be valuable to explore the stability of the platooning system under denial-of-service attack using this scheme.

References

- [1] Y. Zhao, Z. Liu, and W. S. Wong, “Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–12, 2021.
- [2] P. Liu, A. Kurt, and U. Ozguner, “Distributed model predictive control for cooperative and flexible vehicle platooning,” *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 3, pp. 1115–1128, 2019.
- [3] J. Zhan, Z.-P. Jiang, Y. Wang, and X. Li, “Distributed model predictive consensus with self-triggered mechanism in general linear multiagent systems,” *IEEE Trans. Industr. Inform.*, vol. 15, no. 7, pp. 3987–3997, 2019.
- [4] Y. Feng, B. Hu, H. Hao, Y. Gao, Z. Li, and J. Tan, “Design of distributed cyber–physical systems for connected and automated vehicles with implementing methodologies,” *IEEE Trans. Industr. Inform.*, vol. 14, no. 9, pp. 4200–4211, 2018.
- [5] Y. Lu, R. Su, C. Zhang, and L. Qiao, “Event-triggered adaptive formation keeping and interception scheme for autonomous surface vehicles under malicious attacks,” *IEEE Trans. Industr. Inform.*, pp. 1–1, 2021.
- [6] Z. Feng and G. Hu, “Secure cooperative event-triggered control of linear multiagent systems under DoS attacks,” *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, 2020.
- [7] Y. Lu, R. Su, C. Zhang and L. Qiao, ”Event-Triggered Adaptive Formation Keeping and Interception Scheme for Autonomous Surface Vehicles

- Under Malicious Attacks,” *IEEE Trans. Industr. Inform.*, vol. 18, no. 6, pp. 3947-3957, June 2022, doi: 10.1109/TII.2021.3111219.
- [8] W. He, W. Xu, X. Ge, Q. -L. Han, W. Du and F. Qian, ”Secure Control of Multiagent Systems Against Malicious Attacks: A Brief Survey,” *IEEE Trans. Industr. Inform.*, vol. 18, no. 6, pp. 3595-3608, June 2022, doi: 10.1109/TII.2021.3126644.
- [9] Z. Huang, D. Chu, C. Wu, and Y. He, “Path planning and cooperative control for automated vehicle platoon using hybrid automata,” *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 3, pp. 959–974, 2019.
- [10] V. S. Dolk, J. Ploeg, and W. P. M. H. Heemels, “Event-triggered control for string-stable vehicle platooning,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 12, pp. 3486–3500, 2017.
- [11] P. Wang, H. Deng, J. Zhang, L. Wang, M. Zhang, and Y. Li, “Model predictive control for connected vehicle platoon under switching communication topology,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–14, 2021.
- [12] F. Ma et al., “Distributed control of cooperative vehicular platoon with nonideal communication condition,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8207–8220, 2020.
- [13] Y. Li, C. Tang, K. Li, X. He, S. Peeta, and Y. Wang, “Consensus-based cooperative control for multi-platoon under the connected vehicles environment,” *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 6, pp. 2220–2229, 2019.
- [14] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, and Y. Jin, “Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–12, 2020.
- [15] A. Petrillo, A. Pescape, and S. Santini, “A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of

- heterogeneous communication delays and cyberattacks,” *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134–1149, 2021.
- [16] Z. Abdollahi Biron, S. Dey, and P. Pisu, “Real-time detection and estimation of denial of service attack in connected vehicle systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, 2018.
- [17] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, “Distributed cyber attacks detection and recovery mechanism for vehicle platooning,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, 2020.
- [18] C. De Persis and P. Tesi, “Input-to-state stabilizing control under denial of-service,” *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.
- [19] B. Niemoczynski, S. Biswas, and J. Kollmer, “Stability of discrete-time networked control systems under denial of service attacks,” in *Proc. Resilience Week (RWS)*, Aug. 2016, pp. 119–124.
- [20] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal dos attack policy against remote state estimation,” in *Proc. IEEE 52nd Annu. Conf. Decision Control (CDC)*, Dec. 2013, pp. 5444–5449.
- [21] Z.-H. Pang, G. P. Liu, and Z. Dong, “Secure networked control systems under denial of service attacks,” *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 8908–8913, 2011.
- [22] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, “Resilient control of cyber-physical systems against denial-of-service attacks,” in *Proc. 6th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2013, pp. 54–59.
- [23] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.
- [24] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, “T-VNets: A novel trust architecture for vehicular networks using the

- standardized messaging services of ETSI ITS,” *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.
- [25] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: Detecting sybil attacks in urban vehicular networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012
- [26] K. Varma, H. Hasbullah, and A. Kumar, “Prevention dos attacks in vanet,” *Wireless Pers. Commun., Int. J.*, vol. 73, no. 1, pp. 95–126, 2013.
- [27] H. Zhang, J. Liu, Z. Wang, C. Huang and H. Yan, ”Adaptive Switched Control for Connected Vehicle Platoon With Unknown Input Delays,” in *IEEE Transactions on Cybernetics*, doi: 10.1109/TCYB.2021.3104622.
- [28] Y. Bian, C. Du, M. Hu, S. E. Li, H. Liu and C. Li, ”Fuel Economy Optimization for Platooning Vehicle Swarms via Distributed Economic Model Predictive Control,” in *IEEE Transactions on Automation Science and Engineering*, doi: 10.1109/TASE.2021.3128920.
- [29] C. Du, Y. Bian, H. Liu, W. Ren, P. Lu and X. Liu, ”Cooperative Startup Control for Heterogeneous Vehicle Platoons: A Finite-Time Output Tracking-Based Approach,” in *IEEE Transactions on Control of Network Systems*, vol. 8, no. 4, pp. 1767-1777, Dec. 2021, doi: 10.1109/TCNS.2021.3084463.
- [30] Y. Li et al., ”Longitudinal Platoon Control of Connected Vehicles: Analysis and Verification,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 5, pp. 4225-4235, May 2022, doi: 10.1109/TITS.2020.3042973.
- [31] Y. Li, C. Tang, S. Peeta and Y. Wang, ”Nonlinear Consensus-Based Connected Vehicle Platoon Control Incorporating Car-Following Interactions and Heterogeneous Time Delays,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 6, pp. 2209-2219, June 2019, doi: 10.1109/TITS.2018.2865546.

- [32] D. Zhang, Y. -P. Shen, S. -Q. Zhou, X. -W. Dong and L. Yu, "Distributed Secure Platoon Control of Connected Vehicles Subject to DoS Attack: Theory and Application," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 11, pp. 7269-7278, Nov. 2021, doi: 10.1109/TSMC.2020.2968606.
- [33] J. Chen, H. Liang, J. Li and Z. Lv, "Connected Automated Vehicle Platoon Control With Input Saturation and Variable Time Headway Strategy," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 4929-4940, Aug. 2021, doi: 10.1109/TITS.2020.2983468.
- [34] Y. Li, C. Tang, S. Peeta and Y. Wang, "Integral-Sliding-Mode Braking Control for a Connected Vehicle Platoon: Theory and Application," in *IEEE Transactions on Industrial Electronics*, vol. 66, no. 6, pp. 4618-4628, June 2019, doi: 10.1109/TIE.2018.2864708.
- [35] Y. Shao and Z. Sun, "Vehicle Speed and Gear Position Co-Optimization for Energy-Efficient Connected and Autonomous Vehicles," in *IEEE Transactions on Control Systems Technology*, vol. 29, no. 4, pp. 1721-1732, July 2021, doi: 10.1109/TCST.2020.3019808.
- [36] S. Wei, Y. Zou, X. Zhang, T. Zhang and X. Li, "An Integrated Longitudinal and Lateral Vehicle Following Control System With Radar and Vehicle-to-Vehicle Communication," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1116-1127, Feb. 2019, doi: 10.1109/TVT.2018.2890418.
- [37] J. Hu, P. Bhowmick, F. Arvin, A. Lanzon and B. Lennox, "Cooperative Control of Heterogeneous Connected Vehicle Platoons: An Adaptive Leader-Following Approach," in *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 977-984, April 2020, doi: 10.1109/LRA.2020.2966412.
- [38] Y. Zheng, S. E. Li, K. Li and W. Ren, "Platooning of Connected Vehicles With Undirected Topologies: Robustness Analysis and Distributed H-infinity Controller Synthesis," in *IEEE Transactions on Intelligent*

- Transportation Systems, vol. 19, no. 5, pp. 1353-1364, May 2018, doi: 10.1109/TITS.2017.2726038.
- [39] Z. Wang, Y. Gao, C. Fang, L. Liu, S. Guo and P. Li, "Optimal Connected Cruise Control With Arbitrary Communication Delays," in IEEE Systems Journal, vol. 14, no. 2, pp. 2913-2924, June 2020, doi: 10.1109/JSYST.2019.2933001.
- [40] Y. Li, W. Chen, S. Peeta and Y. Wang, "Platoon Control of Connected Multi-Vehicle Systems Under V2X Communications: Design and Experiments," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 5, pp. 1891-1902, May 2020, doi: 10.1109/TITS.2019.2905039.
- [41] Z. Chen and B. B. Park, "Preceding Vehicle Identification for Cooperative Adaptive Cruise Control Platoon Forming," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 1, pp. 308-320, Jan. 2020, doi: 10.1109/TITS.2019.2891353.
- [42] Z. Yang, J. Huang, D. Yang and Z. Zhong, "Collision-Free Ecological Cooperative Robust Control for Uncertain Vehicular Platoons With Communication Delay," in IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2153-2166, March 2021, doi: 10.1109/TVT.2021.3060808.
- [43] S. Feng, Z. Song, Z. Li, Y. Zhang and L. Li, "Robust Platoon Control in Mixed Traffic Flow Based on Tube Model Predictive Control," in IEEE Transactions on Intelligent Vehicles, vol. 6, no. 4, pp. 711-722, Dec. 2021, doi: 10.1109/TIV.2021.3060626.
- [44] Y. Li, C. Tang, K. Li, X. He, S. Peeta and Y. Wang, "Consensus-Based Cooperative Control for Multi-Platoon Under the Connected Vehicles Environment," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 6, pp. 2220-2229, June 2019, doi: 10.1109/TITS.2018.2865575.
- [45] H. Zhang, P. Cheng, L. Shi and J. Chen, "Optimal DoS Attack Scheduling in Wireless Networked Control System," in IEEE Transactions on

- Control Systems Technology, vol. 24, no. 3, pp. 843-852, May 2016, doi: 10.1109/TCST.2015.2462741.
- [46] X. Shao and D. Ye, "Fuzzy Adaptive Event-Triggered Secure Control for Stochastic Nonlinear High-Order MASs Subject to DoS Attacks and Actuator Faults," in IEEE Transactions on Fuzzy Systems, vol. 29, no. 12, pp. 3812-3821, Dec. 2021, doi: 10.1109/TFUZZ.2020.3028657.
- [47] R. Kato, A. Cetinkaya and H. Ishii, "Security Analysis of Linearization for Nonlinear Networked Control Systems Under DoS," in IEEE Transactions on Control of Network Systems, vol. 8, no. 4, pp. 1692-1704, Dec. 2021, doi: 10.1109/TCNS.2021.3078130.
- [48] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou and L. Ding, "Co-Estimation of State and FDI Attacks and Attack Compensation Control for Multi-Area Load Frequency Control Systems Under FDI and DoS Attacks," in IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 2357-2368, May 2022, doi: 10.1109/TSG.2022.3147693.
- [49] N. Zhao, P. Shi, W. Xing and R. K. Agarwal, "Resilient Event-Triggered Control for Networked Cascade Control Systems Under Denial-of-Service Attacks and Actuator Saturation," in IEEE Systems Journal, vol. 16, no. 1, pp. 1114-1122, March 2022, doi: 10.1109/JSYST.2021.3066540.
- [50] R. Kato, A. Cetinkaya and H. Ishii, "Linearization-Based Quantized Stabilization of Nonlinear Systems Under DoS Attacks," in IEEE Transactions on Automatic Control, doi: 10.1109/TAC.2021.3133180.
- [51] S. Du, W. Xu, J. Qiao and D. W. C. Ho, "Resilient Output Synchronization of Heterogeneous Multiagent Systems With DoS Attacks Under Distributed Event-/Self-Triggered Control," in IEEE Transactions on Neural Networks and Learning Systems, doi: 10.1109/TNNLS.2021.3105006.
- [52] R. Zhao, Z. Zuo, Y. Wang and W. Zhang, "Active Control Strategy for Disturbed Switched Systems Under Asynchronous DoS Attacks," in IEEE

Control Systems Letters, vol. 6, pp. 2701-2706, 2022, doi: 10.1109/LC-SYS.2022.3175982.

- [53] M. Wakaiki, A. Cetinkaya and H. Ishii, "Stabilization of Networked Control Systems Under DoS Attacks and Output Quantization," in IEEE Transactions on Automatic Control, vol. 65, no. 8, pp. 3560-3575, Aug. 2020, doi: 10.1109/TAC.2019.2949096.
- [54] Y. -S. Ma, W. -W. Che, C. Deng and Z. -G. Wu, "Distributed Model-Free Adaptive Control for Learning Nonlinear MASs Under DoS Attacks," in IEEE Transactions on Neural Networks and Learning Systems, doi: 10.1109/TNNLS.2021.3104978.
- [55] C. Peng and H. Sun, "Switching-Like Event-Triggered Control for Networked Control Systems Under Malicious Denial of Service Attacks," in IEEE Transactions on Automatic Control, vol. 65, no. 9, pp. 3943-3949, Sept. 2020, doi: 10.1109/TAC.2020.2989773.
- [56] T. Li, B. Chen, L. Yu and W. -A. Zhang, "Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems," in IEEE Transactions on Automatic Control, vol. 66, no. 9, pp. 4303-4310, Sept. 2021, doi: 10.1109/TAC.2020.3032598.
- [57] P. Chen, D. Zhang, L. Yu and H. Yan, "Dynamic Event-Triggered Output Feedback Control for Load Frequency Control in Power Systems With Multiple Cyber Attacks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, doi: 10.1109/TSMC.2022.3143903.
- [58] Q. Sun, K. Zhang and Y. Shi, "Resilient Model Predictive Control of Cyber-Physical Systems Under DoS Attacks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 7, pp. 4920-4927, July 2020, doi: 10.1109/TII.2019.2963294.
- [59] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," Communications of the ACM, vol. 55, no. 2, p. 90, 2012.

- [60] Samuel, A. J., & Sebastian, S. (2019). An algorithm for IoT based vehicle verification system using RFID. *International Journal of Electrical & Computer Engineering* (2088-8708), 9(5).
- [61] Ameen, H. A., Mahamad, A. K., Saon, S., Nor, D. M., & Ghazi, K. (2020). A review on vehicle to vehicle communication system applications. *Indonesian Journal of Electrical Engineering and Computer Science*, 18(1), 188-198.
- [62] “Radio Interface Standards of Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications for Intelligent Transport System Applications”, Recommendation ITU-R M.2084-0, September 2015.
- [63] J.-P. Rodrigue, C. Comtois, and B. Slack, ”The geography of transport systems 4th edition”. Jean-Paul Rodrigue (2017), New York: Routledge, 2016.
- [64] H. J. Marquez, *Nonlinear Control Systems: Analysis and Design*. New Jersey: John Wiley & Sons, Inc., 2003.
- [65] WIKIPEDIA. “Graph theory” [Online]. Available: https://en.wikipedia.org/wiki/Graph_theory/ (visited on 8/9/2022).
- [66] Soni A, Hu H. Formation control for a fleet of autonomous ground vehicles: A survey. *Robotics*. 2018 Nov 1;7(4):67.
- [67] Boyd, S., El Ghaoui, L., Feron, E. and Balakrishnan, V., 1994. *Linear matrix inequalities in system and control theory*. Society for industrial and applied mathematics.
- [68] Y. Yang, Y. Li, D. Yue, Y. -C. Tian and X. Ding, ”Distributed Secure Consensus Control With Event-Triggering for Multiagent Systems Under DoS Attacks,” in *IEEE Transactions on Cybernetics*, vol. 51, no. 6, pp. 2916-2928, June 2021, doi: 10.1109/TCYB.2020.2979342.

- [69] D. Zhang and G. Feng, "A New Switched System Approach to Leader-Follower Consensus of Heterogeneous Linear Multiagent Systems With DoS Attack," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 1258-1266, Feb. 2021, doi: 10.1109/TSMC.2019.2895097.
- [70] Martínez-Díaz, M., Al-Haddad, C., Soriguera, F. and Antoniou, C., 2021. Platooning of connected automated vehicles on freeways: a bird's eye view. *Transportation research procedia*, 58, pp.479-486.
- [71] T. K. Tasooji and H. J. Marquez, "Event-Triggered Consensus Control for Multi-Robot Systems with Cooperative Localization," in *IEEE Transactions on Industrial Electronics*, 2022, doi: 10.1109/TIE.2022.3192673.
- [72] T. K. Tasooji and H. J. Marquez, "Cooperative Localization in Mobile Robots Using Event-Triggered Mechanism: Theory and Experiments," in *IEEE Transactions on Automation Science and Engineering*, doi: 10.1109/TASE.2021.3115770.