8-2015

Attacker-Induced Traffic Flow Instability in a Stream of Automated Vehicles

Daniel D. Dunn
Utah State University

ATTACKER-INDUCED TRAFFIC FLOW INSTABILITY IN A STREAM OF AUTOMATED VEHICLES

by

Daniel D. Dunn

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

of

MASTER OF SCIENCE

in

Electrical Engineering

Approved:

Dr. Ryan M. Gerdes Major Professor	Dr. Donald Cripps Committee Member
Dr. Rajnikant Sharma Committee Member	Dr. Ming Li Committee Member

Dr. Mark R. McLellan
Vice President for Research and
Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2015

Abstract

Attacker-Induced Traffic Flow Instability in a Stream of Automated Vehicles

by

Daniel D. Dunn, Master of Science

Utah State University, 2015

Major Professor: Dr. Ryan M. Gerdes
Department: Electrical and Computer Engineering

Automated driving technologies such as Adaptive Cruise Control (ACC) are becoming a standard package on mid-grade vehicles. An ACC system utilizes local sensors to monitor the motion of surrounding vehicles. Feedback from these sensors is used to calculate automated braking and acceleration requirements to maintain a specified inter-vehicle spacing. Another near term technology, Cooperative Adaptive Cruise Control (CACC), will augment the data collected by the local sensors of ACC with inter-vehicle communication. This will allow vehicles to cooperatively change their state with respect to surrounding vehicles, such as increase their nominal velocity to adjust highway vehicle density to accommodate merging vehicles. As these technologies become mainstream the widely researched concept of Automated Highway Systems (AHS) is quickly becoming a reality.

Extensive research over the last several decades has proposed various ACC and CACC schemes as a solution to highway automation. The stability of these designs has been analyzed in great detail. However, the field of research largely assumes all the vehicles in a traffic system of automated vehicles are operating in a non-adversarial environment. This work highlights the error of such assumptions and considers attacks against the system where some members act in a malicious manner with the intent of destabilizing traffic flow. This type of attack could consist of active attackers who modify their control gains to affect neighboring vehicles, or passive attackers whose gains have been changed, perhaps without the knowledge of the vehicles driver, and could be remotely activated.

A variety of proposed control algorithms are surveyed as part of this work, several of which have been simulated under attack as an automated traffic system of n-vehicles is considered. The results demonstrate that an attacker can force surrounding vehicles into a never ending cycle of oscillatory braking and acceleration. By placing themselves strategically in a system of traffic colluding attackers can destabilize the entire system. The same can be accomplished by remotely activating the maliciously modified control laws of the unwitting passive attack participants.

(141 pages)

Public Abstract

Attacker-Induced Traffic Flow Instability in a Stream of Automated Vehicles

by

Daniel D. Dunn, Master of Science
Utah State University, 2015

Major Professor: Dr. Ryan M. Gerdes
Department: Electrical and Computer Engineering

Highway systems world wide continue to see an ever increased number of vehicles and subsequently a rise in congested traffic. This results in longer commute times, wasted energy as vehicles idle in stop and go traffic, and increases the risk of accidents. In short, increased congestion costs time and money. These issues have prompted much research into Automated Highway Systems (AHS). In AHS vehicles using computer algorithms can safely travel at much smaller inter-vehicle distances than human drivers are capable of. This increases the capacity of existing highway systems. Sensors aboard each vehicle make this possible by monitoring their surroundings. Vehicles equipped with Adaptive Cruise Control (ACC) are capable of this type of close proximity travel. ACC packages are becoming common as a standard package on many mid-priced vehicles.

Another form of automation, Cooperative Adaptive Cruise Control (CACC), which utilizes wireless communication between vehicles, has been proposed and will likely become available within the next couple decades. CACC allows each vehicle to communicate their intended speed or position changes to surrounding vehicles, further decreasing the possibility of collisions.

These automation methods are proposed to reduce driver stress, increase highway throughput, and decrease accident rates. However, the fact that vehicles are being automated creates new opportunities for malicious individuals to wreak havoc on society.

This research investigates the possibility that some vehicles on the highway might be under the control of malicious individuals who have modified their automated control systems to negatively affect vehicles around them. These malicious actors might also exploit the wireless communication of CACC vehicles and hack their control algorithms, causing them to become unstable. These hacked vehicles could become passive participants in the attack unbeknownst to the driver of the vehicle. The result of such attacks could be congested traffic, rapid changes in acceleration causing drivers discomfort, or multi-vehicle collisions. Such attacks could effectively negate the benefits of implementing AHS.

The goal of this work is to bring to light possible weaknesses in the proposed systems so they can be rectified before becoming an issue to the public at large.

To my amazing wife, Veronica, and our three wonderful children, Jacie, Paisley, and Kyler, who have never known a time when I was not in college ....

Acknowledgments

I would like to acknowledge and thank the many excellent individuals who have aided me and formed a support structure during my graduate studies at Utah State University.

Foremost, I would like to thank Dr. Ryan Gerdes for the opportunity to work with him as a graduate research assistant at the Safe and Automated Transportation Systems (SATS) lab. I appreciate the time he has dedicated to helping me to refine and focus my work, and for his insight and experience in the field of hardware security.

I would also like to thank Dr. Don Cripps, who has an amazing depth of knowledge and experience at his command. Many times he has provided me with advice and a suggested path of action that has stopped me from straying to the dark side. I would like to thank Dr. Rajnikant Sharma for his assistance and expertise in the area of modern control. He has been a patient and invaluable resource in helping me develop a deeper understanding of the field. I extend thanks to Dr. Ming Li from the Computer Science Department for serving as the outside member of my graduate committee. I greatly appreciate your help and support.

I would like to extend special thanks to my friend Thomas Amely for his support and help as we have labored through school as project and lab partners. You have had my back on more than one occasion, and I greatly appreciate the hard work, innovation, and knowledge you have applied to our projects.

I thank all the graduate students that I have worked with, Sam, Imran, Soudeh, Ali, Mehedi, Saptarshi, Bidisha, and Ruchir, to name a few, for their continual friendship and support. You have given me the wonderful opportunity of being part of your lives as we all experience the hard work and sacrifice that is required of graduate students. You have helped make my time as a student more enjoyable.

Most importantly of all I would like to thank my amazing wife, Veronica. Without her love and support I would never have been able to start college, let alone finish both my bachelor's and master's degree in five years. You have been an amazing companion through

all of my crazy ideas. Also I am grateful to our wonderful children Jacie, Paisley, and Kyler for being so understanding when I had to study and could not come and play. I promise to make up all of the lost play time now that I am finished with school.

I also extend immense thanks and gratitude to my main source of financial support while attending college, the SMART scholarship. I am grateful to Jared Abbey at Hill Air Force Base for choosing me as his final candidate for this scholarship. The funding I have received from the SMART scholarship has made it possible for me to attend college and has financially given me the ability to perform my graduate research and develop this thesis.

Daniel D. Dunn

Contents

List of Tables

List of Figures

Figure Page

Acronyms

ACC	adaptive cruise control
AHS	automated highway system
AICC	autonomous intelligent cruise control
CACC	cooperative adaptive cruise control
CPS	cyber physical system
CSP	constant spacing policy
CTG	constant time gap
HDV	heavy duty vehicle
IDM	intelligent driver model
IVC	inter-vehicle communication
PTJ	phantom traffic jamb
SAACC	semi-autonomous ACC
VANET	vehicular ad-hoc network
VTG	variable time gap

Chapter 1

Introduction

1.1 Background

In an era of high speed long distance travel, the ability to easily and safely commute from place to place is important to the economic well being and life style enjoyed by modern society. Current highway and freeways systems are seeing increasing congestion from personal commuter, and commercial shipping and transportation vehicles. Fifteen years ago Powers and Nicastri [1] predicted that by 2011 the number of registered vehicles worldwide would rise to 800 million units. A study by Sousanis [2] shows that by 2010 the actual number exceeded 1 billion units. The results of a 2007 urban mobility study, Schrank and Lomax [3], states the number of hours an urban America driver spent delayed in traffic rose from 14 hours per year in 1982 to 38 hours in 2005, an increase of over 270%. A total of 14.2 billion hours per year were wasted in congested traffic. In addition to lost time, traffic congestion resulted in wasted energy consumption of 2.5 billion gallons of fuel in 2005 alone. The sheer magnitude of these losses has prompted much research into alternate transportation solutions.

One family of solutions, Automated Highway Systems (AHS), has been extensively researched as part of the California PATH program since 1986 (Shladover [4]). In an AHS automated vehicles follow each other on a dedicated highway lane in closely nit groups called platoons. These systems require sensors arrays aboard each vehicle, along the roadway, or both. This allows each vehicle to monitor their environment, including surrounding vehicles. Distances between vehicles and relative velocities are controlled in this manner, allowing each vehicle to maintain a safe and efficient orientation in the platoon. However, to implement AHS roadways and vehicles must be upgraded and outfitted with the required hardware and software.

Implementation of a fully automated system such as AHS is projected between 2025–2030 according to the 2014 National Highway Traffic Safety Administration (NHTSA) report Trimble et al. [5]. This report also predicts wide spread use of adaptive cruise control (ACC) as a near term technology (2012–2017). The driver of a vehicle using this technology maintains control over the steering of the vehicle, while the ACC system uses local sensors to maintain relative inter-vehicle spacing and velocity according to a longitudinal control scheme. Rajamani and Zhu [6], Xiao and Gao [7], Marsden et al. [8], and Kesting et al. [9] have all proposed such control schemes.

Cooperative Adaptive Cruise Control (CACC) has been proposed as a method of partially automating the highway systems utilizing a control scheme such as that proposed by Naus et al. [10]. This technology is described as midterm in the NHTSA report with projected implementation between 2017–2025. In addition to the local sensors utilized by ACC, a CACC system incorporates communication between vehicles in a platooning configuration. A vehicle using CACC technology can communicating their intent to merge or change lanes to surrounding vehicles, thus increasing safety according to Schakel et al. [11]. Additionally a platoon of vehicles using CACC can receive desired velocity information from the leader of the platoon, allowing allowing each vehicle to predict acceleration requirements to maintain smaller safe inter-vehicle spacing than an ACC system.

Both ACC and CACC are proposed as methods to increase highway throughput and safety. While the designers of these systems have surely considered safety, it is important that any proposal affecting the public interest be vetted by the scrutiny of outside sources. These proposed technologies should be thoroughly investigated to discover possible vulnerabilities before they are implemented on a large scale. It is likely malicious actors will attempt to attack traffic system using these technologies. An attack against the stability of an automated vehicular system utilizing ACC or CACC could result in congested traffic and wasted energy consumption. Additionally attacks could cause catastrophic failure of the system resulting in multi-vehicle collisions and human fatalities.

1.2 Traffic Flow Stability, a Motivating Example

Consider a conventional stream of traffic on a highway system where the acceleration and braking of each vehicle is directly controlled by a human operator. As predicted by the Intelligent Driver Model (IDM) developed by Treiber et al. [12], stop-and-go waves will propagate through the stream of traffic as vehicle density increases. This phenomena occurs even in the absence of obstructions such as an accident or merging vehicles. The IDM suggests that human drivers are incapable of maintaining stable traffic flow patterns. Congested stop-and-go traffic caused by the human drivers increases driver and passenger stress as well as the possibility of accidents. Additionally, highway systems are underutilized due to large inter-vehicle following distances required as a result of slow human reaction times.

Now consider a stream of traffic where the vehicles are interacting in an automated manner. Acceleration and braking requirements are calculated by computer implemented control algorithms. These control laws are designed to allow vehicles to safely maintain much smaller inter-vehicle following distances than a human driver is capable of. The automated system maintains inter-vehicle distances without the human tendency to deviate from a constant velocity. This increases the comfort of travel even in high density traffic. Additionally the density of vehicles per mile of roadway will increase providing better utilization of the highway, fuel economy will increase due to smaller deviations in velocity, and accident rates will decrease.

But what if the act of automating vehicles creates new vulnerabilities? Suppose that malicious actors have modified the control algorithm on several vehicles and join the stream of automated vehicles. The algorithms could be modified to introduce an unstable behavior such as oscillatory acceleration. The effect on surrounding vehicles could be large velocity deviations and stop-and-go waves. The theoretical benefits of automation are effectively destroyed in such a scenario.

1.3 Related Work

As highway transportation networks move toward semi-automated or fully automated operation it becomes important to analyze the safety and security of such systems.

The relative stability of automated vehicles has been studied extensively in the context of string stability and string instability, or slinky effect as it is refereed to in some works. These concepts refers to the attenuation, or amplification, of relative spacing and velocity errors between consecutive vehicles that are interacting in an automated manner. Yanakiev and Kanellakopoulos [13, 14] have proposed a simplified method for analyzing stability in this context. They have proposed several control algorithms and outlined a method for selecting gains to guarantee system wide stability. This same concept has also been analyzed by Rajamani [6, 15], Swaroop [16], Swaroop and Hedrick [17], Chien and Ioannou [18], and Eyre et al. [19, 20]. According to Yanakiev and Kanellakopoulos [13, 14] string stability is one of the most important issues in the safety and performance of AHS. A common theme amongst all of these works is the assumption that all vehicles in the system are utilizing the same control algorithm.

It is more accurate to assume a heterogeneous system of vehicles utilizing different control algorithms. String stability for such a system is discussed by Shaw and Hedrick [21]. In another work by the same authors [22], controller designs are proposed to maintain string stability of the heterogeneous system. These are the only works the author is aware of that specifically discuss a heterogeneous mixture of automated vehicles.

All of the aforementioned works do not consider operation in a adversarial environment. In particularly, they assume all vehicles in the system are behaving strictly according to the given control law, and do not consider the possibility of malicious actors within the system of vehicles. Additionally these works assume that all information exchanged is authentic. These assumptions leave these proposed control algorithms open to the possibility of destabilizing attacks.

A non-destabilizing attack against automated vehicular transportation systems detailed by Gerdes et al. [23], focuses on degrading efficiency by causing surrounding vehicles to needlessly expend energy. This is accomplished by optimal sequences of braking and acceleration. A similar attack is analyzed by Sosa [24]. These attacks focus on traffic stability from the perspective of energy expenditure, but are not destabilizing in a strict sense.

Operation of automated vehicles in an adversarial environment is discussed by Dadras et al. [25], where a platooning environment is explicitly considered utilizing a bidirectional control algorithm. Two attacks are detailed demonstrating that given a system of vehicles utilizing the same control scheme (homogeneous case), an attack vehicle can judiciously modify their gains to affect the stability of the platoon. The attack outlined in this thesis is more general in that semi-automated systems such as ACC and CACC are not constrained to a platooning structure but are simply acting in a cooperative manner due to the proximity of neighboring vehicles, and need not be utilizing similar control schemes. In short a cooperative heterogeneous system of semi-automated vehicles is considered.

The literature does provide stability analysis from the broader scope of a cyber physical system (CPS), defined as a system of computational elements collaboratively controlling physical systems. Cardenas et al. [26] discuss threats against such systems and possible venerability to resonance as the result of an attack. This is the type of behavior a malicious actor is likely to target, and is closely related to the attacks proposed in this thesis. A related subject vehicular ad-hoc networks (VANET's) are considered by Rawat et al. [27]. They discuss the challenging question of securing inter-vehicle communication (IVC) in the presence of malicious drivers. This particular problem will be an issue for the implementation of CACC systems.

In spite of the extensive amount of research in the field of automated transportation systems relatively little work has been done to secure proposed automated vehicle technologies against malicious actors.

1.4 Outline of Thesis

To examine the effect of intentional malicious behavior, or an attack on an automated system, a software traffic simulation framework has been implemented in Matlab as part of this work. The simulation framework is scalable allowing the number of vehicles, their parameters, the simulation time, and control law to be varied. Using this framework groups of vehicles are simulated operating with specific control laws that have been proposed in the literature and are representative of ACC and CACC systems.

This work utilizes the simulation framework to explore different ways an attacking vehicle could introduce undesirable behavior such as oscillation and instability into a cooperative system of automated vehicles. The objective of such attacks is to cause a traffic system to become unstable.

In addition to the software simulation framework a hardware test platform has been developed. This platform consists of 10 four-wheeled robots representing scaled versions of a full size vehicle. The vehicles are outfitted with sensor arrays representing those of actual ACC and CACC systems, and capable of similar data collection and measurements. A kinematic model of the hardware platform similar to that described by Rajamani [15] is used to design a low level longitudinal control scheme. Various proposed attack scenarios will be carried out in real time using this hardware platform.

The purpose of this work is to investigate different methods of mounting an attack against a grouping of vehicles operating with ACC or CACC. If all of the vehicles on a stretch of highway are using such systems they will interact in a cooperative manner. Through analysis the author investigates what happens if a one or more vehicles in the cooperative system is purposefully being operated in a manner that is not compatible with neighboring vehicles automated control laws. In this manner undesirable behavior is introduced to investigate the possibility of causing system wide instability which could result in large scale collisions. This could cause higher vehicle operating costs as well as cost of injury or life. By identifying how attacks can be mounted, countermeasures can be designed and implemented before ACC, CACC, or AHS in general become widely used and actual damage occurs.

The remainder of this thesis is organized as follows. Chapter 2 discusses currently proposed control methods for ACC and CACC. Papers that were reviewed in preparation for this work are summarized and a table of various control laws is generated. Chapter 3 outlines a threat model against cooperative streams of automated vehicles. An attack scenario is proposed, and assumptions are given that allow the attack to be carried out in simulation. Chapter 4 contains an analysis regarding the stability of the various control laws selected in Chapter 2. A proof is given demonstrating that homogeneous and heterogeneous traffic systems utilizing automated unidirectional control schemes can be destabilized. Chapter 5 provides results for the simulated attacks and gives a comparison benchmark simulation for the IDM. Chapter 6 details the testing and demonstration platform that is being developed to physically demonstrate attack scenarios against a platoon of vehicles. Finally, Chapter 7 provides a brief conclusive summary of this work and details future work and considerations.

Chapter 2

A Survey of Automated Vehicle Control Algorithms

2.1 Overview

This work focuses on the exploitation and analysis of longitudinal control schemes, which are intended to allow an automated vehicle to maintain a desired separation/velocity from adjacent vehicles as they travel a straight path. Currently vehicles with such automation are available from the major manufacturers in the form of ACC. There are many affordable vehicles equipped with ACC that can be purchased today. Ten commonly available vehicles with ACC are shown in Table 2.1 (Haj-Assaad [28]).

Other systems like CACC are currently being researched and developed, and are not yet available commercially. This is partially due to the communication requirement between vehicles. Many of the vehicles traveling on the roadway will need to be outfitted with the required communication equipment before CACC is viable. However, ACC does not require inter-vehicle communication (IVC) and can be used regardless of the type and function of other vehicles on the roadway.

In the 2014 National Highway Traffic Safety Administration (NHTSA) report Trimble et al. [5] outline the state of current and projected vehicle automation technologies. The report details Ford Motor Company projections that ACC will be widely implemented near term (2012-2017), and CACC technology to be implemented midterm (2017-2025). The expectation is for fully automated self driving technology by 2025 to 2030.

There are many control models that have been proposed for ACC and CACC. This work focuses on the behavior of a transportation network consisting solely of these vehicles. The papers reviewed in preparation for this work, and the control algorithms selected for analysis are discussed in following sections.

Table 2.1: Ten commonly available vehicles that come standard with ACC, or have an optional package with ACC.

Make	**Model**	**Year Available**
Chrysler	200C FWD with Safety Package	2015
Ford	Fusion Titanium 2.0 FWD w/adaptive cruise control	2013
Honda	2015 CR-V Touring FWD	2015
Jeep	Cherokee Limited FWD With Technology Package	2011
Mazda	Mazda3 Grand Touring 2.5 with Technology Package	2014
Mazda	Mazda6 Grand Touring with Technology Package	2014
Subaru	Forester 2.5i Premium with Eyesight Package	2014
Subaru	Legacy 2.5i Premium with Eyesight package	2013
Subaru	Outback 2.5i premium with Eyesight package	2013
Toyota	2015 Camry XLE 2.5 with options	2015

2.2 Papers Reviewed

A variety of sources from existing literature were considered in preparation for this work. A high level overview of ACC has been studied by Xiao and Gao [7], Marsden et al. [8], and Kesting et al. [9]. They discuss ACC as an emerging technology, provide a background for the operational principles of ACC, and the history of design considerations to date. They also provide a good statistical background for the benefits automated vehicles could bring to congested highways, but do not provide detailed information on specific control laws. Specific control models for automated vehicle interaction are discussed in what follows.

There are several different linear control models proposed by Yanakiev and Kanellakopoulos [13], and further defined by Eyre et al. [19, 20]. For each model a bidirectional and unidirectional case are analyzed. In a unidirectional configuration a particular vehicles controller is only tracking the relative distance and velocity of the vehicle immediately preceding it. Hence these laws represent vehicles using an ACC system. The ACC models of Eyre et al. [13, 20] are referenced and discussed in further detail in additional works by the same authors (Eyre et al. [14, 19]). Of the three unidirectional control laws proposed by these authors two represent ACC systems. The first of these relies on speed dependent spacing between vehicles, commonly called a constant time-gap (CTG). This refers to the scalar multiplier of velocity that is used to determine inter-vehicle spacing. The second law uses a variable time gap (VTG) that is dependent upon changes in velocity. At steady state a VTG policy allows much smaller inter-vehicle spacing than the CTG policy. The third proposed unidirectional law, in addition to utilizing relative distance and velocity of the preceding vehicle, requires IVC from a leader vehicle. The leader vehicle is at the front of the platoon communicating a desired velocity, or their actual velocity. As discussed previously, this communication requirement is what distinguishes an ACC model from CACC. This law uses a constant spacing policy (CSP), relying on inter-vehicle communication to achieve a stable system.

The controller design proposed by Chien and Ioannou [18], is also unidirectional in nature and therefore representative of an ACC system. This control law is design with the nonlinear aspects of a vehicle in mind. It addresses mechanical and aerodynamic drag, in addition to time delays due to the vehicles engine time constant. The affect of the nonlinearities are then canceled out with a feedback linearization technique resulting in a third order control law which uses a VTG policy dependent upon relative changes in velocity and acceleration.

The control laws discussed next all require IVC, therefore describing CACC laws. A semi-automated ACC system is proposed by Rajamani and Zhu [6], vehicles are required to receive velocity and acceleration information from the imediate vehicle in front, and in turn transmit their acceleration and velocity to the vehicle behind. This work is discussed in more detail by Rajamani in his text book [15]. The research and analysis of Naus et al. [10] describes a CACC model that was implemented and tested on system of two vehicles. The controller designed by Jovanovic and Bamieh [29] requires that the desired cruising velocity of the platoon be provided to each vehicle. There is no specific mention of CACC in this paper but the only method of providing desired platoon cruise velocity is through some communication link. In their work, No and Chong [30], relax the requirement of direct communication from the platoon leader. However, a local link between a vehicle and its predecessor is still required. This model is therefore a hybrid type of CACC system similar to that of Rajamani and Zhu [6].

The CTG ACC control law, VTG ACC control law, and constant spacing CACC law, proposed by Eyre, Yanakiev. and Kanellakopoulos [13, 19, 20] will be included in this work for further analysis. The ACC law derived through nonlinear methods by Chien and Ioannou [18] will also used. The widely cited CACC law proposed by Rajamani and Zhu [6] will also be used for further analysis. These laws represent a broad range of proposed control designs and will provide generality in later chapters of this work, demonstrating that the effect of the attacks proposed in this thesis are not limit to a particular class of control laws, but apply in general to automated systems.

2.3 An Introduction to String Stability

Before detailing the various control algorithms chosen for analysis in this work the concept of string stability will be approached. Most of the control laws that will be discussed shortly refer to string stability and have been specifically designed with this concept in mind.

String stability is a property of an automated system of vehicles that act in an interconnected manner such as the models described in this chapter. This system of vehicles is commonly referred to as a platoon. In a string stable system the error in relative distance and velocity are guaranteed to decrease between consecutive vehicles toward the rear of the platoon. This is commonly called upstream the platoon, where the leader vehicle is considered the farthest downstream and the tail vehicle is the farthest upstream. In this work the 1^{st} vehicle is considered the farthest upstream and the n^{th} vehicle the farthest downstream as shown in Figure 2.1.

A formal definition for string stability is found in Section 4.1. The Laplace domain transfer function of a vehicles automated control law is commonly used to design string stable gains.

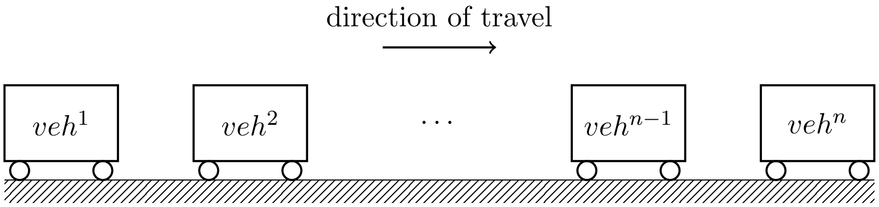


Fig. 2.1: A system of n-vehicles where vehicle 1 is at the rear of the system (upstream), and vehicle n is at the front of the system (downstream).

String stability is an important concept to consider when designing and analyzing automated control laws for vehicles and has been an area of extensive research in automated vehicle control. Rajamani [15] discusses the concept in detail, Swaroop [16,17] has published multiple works on the subject. Similarly, Yanakiev and Kanellakopoulos [13, 14, 31] have contributed extensively to this area of research and refer to string stability as one of the most important issues related to AHS safety and performance. Their model of string stability has been referred to in many other works, including Rajamani and Zhu's work [6] given in Control Algorithm 5. This concept is referred to the slinky effect in Chein and Ioannou's work [18].

2.4 Control Schemes

Several of the control algorithms described in the previous section have been chosen for analysis. These control laws display many characteristics desired by the highway automation community and are discussed in detail here.

2.4.1 Control Algorithm 1

This law is based off speed-dependent spacing commonly referred to as a constant time gap (CTG) policy. The advantage of using a CTG policy is that for some time headway h, the system will become string stable. It has been well established in the literature that string stability cannot be achieved with a simple constant spacing policy when using a unidirectional control scheme (Yanakiev and Kanellakopoulos [13], Chien and Ioannou [18]). However, it can be attained when using a CTG control law.

The first unidirectional scenario proposed byYanakiev and Kanellakopoulos [13] is represented by a one-way mass-spring-damper system as shown in Figure 2.2. The error in desired spacing for the i-th vehicle is given as $x_{i-1,1} - x_{i,1} - hx_{i,2}$, where h is the time headway, and $x_{i,1}$ and $x_{i,2}$ refer to the position and velocity respectively of the i^{th} vehicle. The model is given as:

$$
\begin{aligned}
\dot{x}_{1,1} &= x_{1,2} \\
\dot{x}_{1,2} &= -\frac{kh}{m}x_{1,2} + u \\
\dot{x}_{2,1} &= x_{2,2} \\
\dot{x}_{2,2} &= \frac{k}{m}x_{1,1} - \frac{k}{m}x_{2,1} + \frac{c}{m}x_{1,2} - \frac{c}{m}x_{2,2} - \frac{kh}{m}x_{2,2} \\
&\vdots \\
\dot{x}_{n-1,1} &= x_{n-1,2} \\
\dot{x}_{n-1,2} &= \frac{k}{m}x_{n-2,1} - \frac{k}{m}x_{n-1,1} + \frac{c}{m}x_{n-2,2} - \frac{c}{m}x_{n-1,2} - \frac{kh}{m}x_{n-1,2} \\
\dot{x}_{n,1} &= x_{n,2} \\
\dot{x}_{n,2} &= \frac{k}{m}x_{n-1,1} - \frac{k}{m}x_{n,1} + \frac{c}{m}x_{n-1,2} - \frac{c}{m}x_{n,2} - \frac{kh}{m}x_{n,2},
\end{aligned}
\tag{2.1}
$$

where,

$x_{i,1}$ = position of i^{th} mass in m,

$x_{i,2}$ = velocity of i^{th} mass in m/s,

u = input force applied to first mass,

k = spring constant,

b = damper constant,

m = mass in kg,

h = the time headway in s.

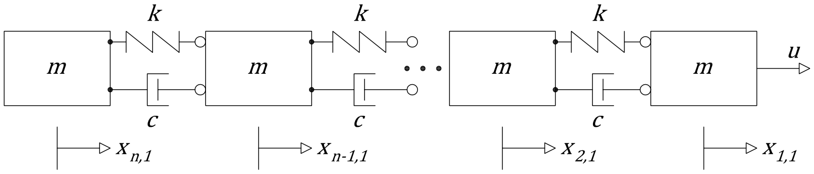


Fig. 2.2: Unidirectional mass-spring-damper system.

In order to study the string stability of this model Yanakiev and Kanellakopoulos [13] use error coordinates based off the relative position and velocity errors between masses:

$$\begin{aligned}
z_{1,1} &= x_{1,1} - x_{2,1} \\
z_{1,2} &= z_{\dot{1},1} = x_{1,2} - x_{2,2} \\
z_{2,1} &= x_{2,1} - x_{3,1} \\
z_{2,2} &= z_{\dot{2},1} = x_{2,2} - x_{3,2} \\
&\vdots \\
z_{n-1,1} &= x_{n-1,1} - x_{n,1} \\
z_{n-1,2} &= \dot{z}_{n-1,1} = x_{n-1,2} - x_{n,2}.
\end{aligned} \tag{2.2}$$

The error representation of the state-space model of Equation (2.1) is:

$$\begin{aligned}
\dot{z}_{1,1} &= z_{1,2} \\
\dot{z}_{1,2} &= -\frac{k}{m} z_{1,1} - \frac{c+kh}{m} z_{1,2} + u \\
\dot{z}_{2,1} &= z_{2,2} \\
\dot{z}_{2,2} &= \frac{k}{m}(z_{1,1} - z_{2,1}) + \frac{c}{m} z_{1,2} - \frac{c+kh}{m} z_{2,2} \\
&\vdots \\
\dot{z}_{n-2,1} &= z_{n-2,2} \\
\dot{z}_{n-2,2} &= \frac{k}{m}(z_{n-3,1} - z_{n-2,1}) + \frac{c}{m} z_{n-3,2} - \frac{c+kh}{m} z_{n-2,2} \\
\dot{z}_{n-1,1} &= z_{n-1,2} \\
\dot{z}_{n-1,2} &= \frac{k}{m}(z_{n-2,1} - z_{n-1,1}) + \frac{c}{m} z_{n-2,2} - \frac{c+kh}{m} z_{n-1,2}.
\end{aligned} \tag{2.3}$$

The effect of using a CTG policy is equivalent to providing additional damping with respect to the inertial frame of operation. The magnitude of the transfer function between any pair of vehicles is as follows:

$$\left|\frac{z_i(s)}{z_{i-1}(s)}\right| = \left|\frac{\frac{c}{m}s + \frac{k}{m}}{s^2 + \frac{c+kh}{m}s + \frac{k}{m}}\right| \begin{cases} = 1 \text{ if } \omega = 0 \\ < 1 \, \forall \omega > 0 \text{ if } c > \frac{2m - kh^2}{2h}, \end{cases} \tag{2.4}$$

therefore, when $h > 0$ system gains can be chosen to guarantee the attenuation of errors between vehicles for all frequencies.

The one-way mass-spring-damper system of this model does not represent a physical system in the conventional sense, but does provide an intuitive means of analyzing the unidirectional form of an ACC system.

2.4.2 Control Algorithm 2

Because the use of CTG policies can result in large inter-vehicle spacing variable time gap (VTG) policies have been proposed. In the second unidirectional law of Yanakiev and Kanellakopoulos [13], the time headway h is allowed to vary with the relative velocity. At steady state h becomes constant at a nominal value $h_0 > 0$: $h_i = h_0 - c_h(x_{i-1,2} - x_{i,2})$, where $c_h > 0$ is a constant. The intent of this approach is to make h_0 much smaller than the value of h conventionally required to achieve string stability. This model is given in the error coordinate system of Equation (2.2). Where again $x_{i,1}$ and $x_{i,2}$ refer to the position and velocity respectively. Additionally $z_{i,1}$ and $z_{i,2}$ refer to the relative distance and velocity errors respectively.

The state-space representation of the unidirectional model follows:

$$\begin{aligned}
\dot{z}_{1,1} =& z_{1,2}\\
\dot{z}_{1,2} =& -\frac{k}{m}z_{1,1} - \frac{c}{m}z_{1,2} - \frac{kh_0}{m}z_{1,2} - \frac{kc_h}{m}x_{1,2}z_{1,2} + \frac{kc_h}{m}z_{1,2}^2 + u\\
\dot{z}_{2,1} =& z_{2,2}\\
\dot{z}_{2,2} =& \frac{k}{m}(z_{1,1} - z_{2,1}) + \frac{c}{m}(z_{1,2} - z_{2,2}) - \frac{kh_0}{m}z_{2,2}\\
&+ \frac{kc_h}{m}(x_{1,2} - z_{1,2})(z_{1,2} - z_{2,2}) + \frac{kc_h}{m}z_{2,2}^2\\
&\vdots\\
\dot{z}_{n-2,1} =& z_{n-2,2}\\
\dot{z}_{n-2,2} =& \frac{k}{m}(z_{n-3,1} - z_{n-2,1}) + \frac{c}{m}(z_{n-3,2} - z_{n-2,2}) - \frac{kh_0}{m}z_{n-2,2}\\
&+ \frac{kc_h}{m}(x_{1,2} - z_{1,2} - \ldots - z_{n-3,2})(z_{n-3,2} - z_{n-2,2}) + \frac{kc_h}{m}z_{n-2,2}^2\\
\dot{z}_{n-1,1} =& z_{n-1,2}\\
\dot{z}_{n-1,2} =& \frac{k}{m}(z_{n-2,1} - z_{n-1,1}) + \frac{c}{m}(z_{n-2,2} - z_{n-1,2}) - \frac{kh_0}{m}z_{n-1,2}\\
&+ \frac{kc_h}{m}(x_{1,2} - z_{1,2} - \ldots - z_{n-2,2})(z_{n-2,2} - z_{n-1,2}) + \frac{kc_h}{m}z_{n-1,2}^2,
\end{aligned} \tag{2.5}$$

where,

u = input force applied to first mass,

k = spring constant,

b = damper constant,

m = mass in kg,

h = the time headway in s,

h_0 = nominal constant time headway in s.

This system is linearized about the nominal operation point $x_{1,2} = \ldots = x_{n,2} = v_d$, $x_{i,1} = x_{i-1,1} - h_0 v_d$, where all vehicles are moving at the desired steady state velocity v_d

and with the desired inter-vehicle spacing. The model simplifies to:

$$\begin{aligned}
\dot{z}_{1,1} =& z_{1,2} \\
\dot{z}_{1,2} =& -\frac{k}{m} z_{1,1} - \frac{c + kh_0 + kc_h v_d}{m} z_{1,2} + u \\
\dot{z}_{2,1} =& z_{2,2} \\
\dot{z}_{2,2} =& \frac{k}{m}(z_{1,1} - z_{2,1}) + \frac{c + kc_h v_d}{m} z_{1,2} - \frac{c + kh_0 + kc_h v_d}{m} z_{2,2} \\
\vdots& \\
\dot{z}_{n-2,1} =& z_{n-2,2} \\
\dot{z}_{n-2,2} =& \frac{k}{m}(z_{n-3,1} - z_{n-2,1}) - \frac{c + kc_h v_d}{m} z_{n-3,2} - \frac{c + kh_0 + kc_h v_d}{m} z_{n-2,2} \\
\dot{z}_{n-1,1} =& z_{n-1,2} \\
\dot{z}_{n-1,2} =& \frac{k}{m}(z_{n-2,1} - z_{n-1,1}) + \frac{c + kc_h v_d}{m} z_{n-2,2} - \frac{c + kh_0 + kc_h v_d}{m} z_{n-1,2}.
\end{aligned} \tag{2.6}$$

The magnitude of the transfer function between any pair of vehicles is as follows:

$$\left|\frac{z_i(s)}{z_{i-1}(s)}\right| = \left|\frac{\frac{c+kc_h v_d}{m} s + \frac{k}{m}}{s^2 + \frac{c+kh_0+kc_h v_d}{m} s + \frac{k}{m}}\right| \begin{cases} = 1 \text{ if } \omega = 0 \\ < 1 \; \forall \omega > 0 \text{ if } c > \frac{2m - kh_0^2 - 2kh_0 c_h v_d}{2h_0}, \end{cases} \tag{2.7}$$

for values of $h_0 < h$ and positive v_d string stability can be achieved.

if required for analysis purposes this system can be converted back into distance and velocity coordinates using the error coordinate relationships of Equation (2.2).

2.4.3 Control Algorithm 3

The third unidirectional law of Yanakiev and Kanellakopoulos [13] is a constant spacing policy (CSP) that uses inter-vehicle communication. String stability is said to be guaranteed if the lead vehicle communicates its velocity to the rest of the vehicles in the platoon. This algorithm requires less frequent communication updates than previous works. This law can be simulated using a mass-spring-damper system similar to Control Algorithms 1 and 2 by connecting each mass in the system to another mass in front of the leader by a unidirectional damper c_d as shown in Figure 2.3. The velocity of the additional mass is set to the desired velocity v_d of the platoon. The state-space equations of this system follow:

$$\begin{aligned}
\dot{v}_d &= u \\
\dot{x}_{1,1} &= x_{1,2} \\
\dot{x}_{1,2} &= \frac{c_d}{m}(v_d - x_{1,2}) \\
\dot{x}_{2,1} &= x_{2,2} \\
\dot{x}_{2,2} &= \frac{k}{m}(x_{1,1} - x_{2,1}) + \frac{c}{m}(x_{1,2} - x_{2,2}) + \frac{c_d}{m}(v_d - x_{2,2}) \\
&\vdots \\
\dot{x}_{n-1,1} &= x_{n-1,2} \\
\dot{x}_{n-1,2} &= \frac{k}{m}(x_{n-2,1} - x_{n-1,1}) + \frac{c}{m}(x_{n-2,2} - x_{n-1,2}) + \frac{c_d}{m}(v_d - x_{n-1,2}) \\
\dot{x}_{n,1} &= x_{n,2} \\
\dot{x}_{n,2} &= \frac{k}{m}(x_{n-1,1} - x_{n,1}) + \frac{c}{m}(x_{n-1,2} - x_{n,2}) + \frac{c_d}{m}(v_d - x_{n,2}),
\end{aligned} \tag{2.8}$$

where,

$x_{i,1}$ = position of i^{th} mass in m,

$x_{i,2}$ = velocity of i^{th} mass in m/s,

u = input force applied to first mass,

v_d = desired nominal platoon speed,

k = spring constant,

c = damper constant,

c_d = damper constant,

m = mass in kg,

h = the time headway in s.

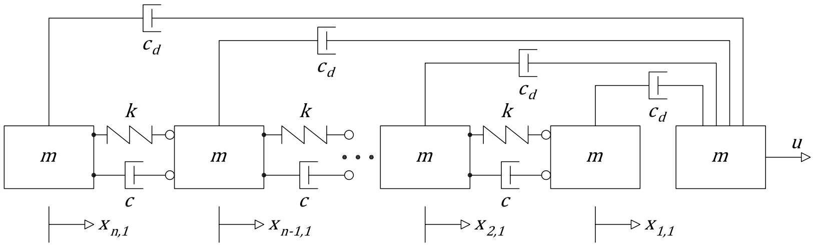


Fig. 2.3: Unidirectional mass-spring-damper system where leader is broadcasting its desired velocity.

Again using Equation (2.2), and the error coordinate $z_d = x_{1,2} - v_d$, the system can be transformed into error coordinate form:

$$\begin{aligned}
\dot{z}_{d,2} &= -\frac{c_d}{m} z_{d,2} + u \\
\dot{z}_{1,1} &= z_{1,2} \\
\dot{z}_{1,2} &= -\frac{k}{m} z_{1,1} - \frac{c + c_d}{m} z_{1,2} \\
\dot{z}_{2,1} &= z_{2,2} \\
\dot{z}_{2,2} &= \frac{k}{m}(z_{1,1} - z_{2,1}) + \frac{c}{m} z_{1,2} - \frac{c + c_d}{m} z_{2,2} \\
&\vdots \\
\dot{z}_{n-2,1} &= z_{n-2,2} \\
\dot{z}_{n-2,2} &= \frac{k}{m}(z_{n-3,1} - z_{n-2,1}) + \frac{c}{m} z_{n-3,2} - \frac{c + c_d}{m} z_{n-2,2} \\
\dot{z}_{n-1,1} &= z_{n-1,2} \\
\dot{z}_{n-1,2} &= \frac{k}{m}(z_{n-2,1} - z_{n-1,1}) + \frac{c}{m} z_{n-2,2} - \frac{c + c_d}{m} z_{n-1,2}.
\end{aligned} \tag{2.9}$$

For this law utilizing inter-vehicle communication provides the effect of introducing additional damping to the system similar to the CTG policy of Control Algorithm 1. The conditions for string stability can be found via the transfer function between any pair of vehicles:

$$\left|\frac{z_i(s)}{z_{i-1}(s)}\right| = \left|\frac{\frac{c}{m}s + \frac{k}{m}}{s^2 + \frac{c+c_d}{m}s + \frac{k}{m}}\right| \begin{cases} = 1 \text{ if } \omega = 0 \\ < 1 \, \forall \omega > 0 \text{ if } c > \frac{2m - c_d^2}{2h}. \end{cases} \tag{2.10}$$

2.4.4 Control Algorithm 4

This model is a description of a semi-automated ACC (SAACC) system. There is a requirement for communication from only the preceding vehicle on the highway. The assumption is that each vehicle in the system will be equipped with a radio receiver on its front bumper and a radio transmitter on the back bumper. Theoretically this configuration will allow inter-vehicle communication without using a specialized addressing system. Each vehicle could transmit any of its state information to the vehicle behind, and receive state information from the vehicle in front. The structure of this controller is given as:

$$u_{syn} = -k_1\ddot{x}_{i-1} - k_2\ddot{x}_i - k_3\dot{\varepsilon}_i - k_4\varepsilon_i - k_5\dot{x}_i. \tag{2.11}$$

where,

x_i = the position of the i^{th} vehicle in m,

$\dot{x}_i$ = the velocity of the i^{th} vehicle in m/s,

L = the desired minimum inter-vehicle separation in m,

h = the time headway in s.

For this control system the variables k_1, k_2, k_3, k_4, and k_5 are system gains. This control structure is to be used in conjunction with a constant time-gap (CTG) policy. The spacing error for the CTG policy is given as:

$$\varepsilon_i = x_i - x_{i-1} + L, \tag{2.12}$$

$$\delta_i = \varepsilon_i + h\dot{x}_i. \tag{2.13}$$

The inter-vehicle communication is said to insure a string stable system if:

$$\left|\left|\hat{H}(s)\right|\right|_\infty = \left|\left|\frac{\delta_i}{\delta_{i-1}}\right|\right|_\infty \leq 1. \tag{2.14}$$

This control model accounts for the presence of unknown actuator dynamics by using the mathematical representation of a first-order lag. Where τ is an estimate of the time lag due to the low level controller and vehicle dynamics:

$$\tau \dddot{x}_i + \ddot{x}_i = u_{syn}. \tag{2.15}$$

After accounting for the lag in actuator dynamics the final form of the coordinated control algorithm is given by:

$$u_{syn} = -k_1\ddot{x}_{i-1} - (k_1 + hk_1k_5)\ddot{x}_i - \frac{1}{h}(1 - k_1k_5h)\dot{\varepsilon}_i - \frac{k_5}{h}\varepsilon_i - k_5\dot{x}_i. \tag{2.16}$$

The gains k_1 and k_5 become the only design parameters that need to be choosed by placing the following restrictions are on the remaining system gains:

$$\begin{align} -k_1h &= \tau, \tag{2.17}\\ k_2 &= -k_1 - k_1k_5h, \tag{2.18}\\ k_3 &= \frac{1}{h}(1 - k_1k_5h), \tag{2.19}\\ k_4h &= k5, \tag{2.20}\\ -k_1 - k_2 + k_3h &= 1. \tag{2.21}\end{align}$$

Finally to insure the control effort will result in a string stable system the error coordinate transfer function is considered:

$$\left|\frac{\delta_i}{\delta_{i-1}}\right| = \left|\frac{1}{1 + h\left[\frac{\tau s^2 + s - k_1k_5hs + k_5}{-k_1hs^2 + s - k_1k_5hs + k_5}\right]s}\right| < 1\,\forall\omega > 0 \text{ if } -k_1h > \tau. \tag{2.22}$$

The major benefit of this controller is, that theoretically, string stability can be maintained in a platoon of vehicles for very small time headway values h. This controller also accounts for the presence of lag (τ_{lag}) due to the low level controller and vehicle dynamics time delay.

2.4.5 Control Algorithm 5

This algorithm is based on an Autonomous Intelligent Cruise Control (AICC) law, as described by Chein and Ioannou [18]. Each vehicle is assumed to be able to measure the relative distance, and velocity between itself and its predecessor. In addition each vehicle must estimate the relative acceleration between itself and its predecessor. Each vehicle must also be able to measure its own velocity and acceleration. Using these measurements and a safety distance rule $S_{d_i} = \lambda_2 v_i + S_{0_i}$ based on the results obtained by Sheikholeslam [32]. The vehicle model adopted for this implementation is as follows:

$$\frac{d}{dt}x_i(t) = \dot{x}_i(t) = v_i(t), \tag{2.23}$$

$$\frac{d}{dt}\dot{x}_i(t) = \ddot{x}_i(t) = a_i(t), \tag{2.24}$$

$$\frac{d}{dt}\ddot{x}_i(t) = b(\dot{x}_i\ddot{x}_i) + a(\dot{x}_i)u_i(t), \tag{2.25}$$

where,

$$\begin{aligned}
a(\dot{x}_i) &= \tfrac{1}{m_i\tau_i(\dot{x}_i)}, \\
b(\dot{x}_i, \ddot{x}_i) &= -2\tfrac{k_{d_i}}{m_i}\dot{x}_i\ddot{x}_i - \tfrac{1}{\tau(\dot{x}_i))}\left[\ddot{x}_i + \tfrac{k_{d_i}}{m_i}\dot{x}_i^2 + \tfrac{d_{m_i}(\dot{x}_i)}{m_i}\right],
\end{aligned}$$

x_i = the position of the i_{th} vehicle in m,

v_i = the velocity of the i_{th} vehicle in m/s,

a_i = the acceleration of the i_{th} vehicle in m/s^2,

m_i = the mass of the i_{th} vehicle in kg,

τ_i = the i_{th} vehicle's engine time constant in s,

$u_i(t)$ = the i_{th} vehicle's engine input,

k_{d_i} = the aerodynamic drag coefficient of the i_{th} vehicle in kg/m.

$d_{m_i}(\dot{x}_i)$ = the mechanical drag of the i_{th} vehicle in $kg \cdot m/s^2$, which is a nonzero-constant but zero for zero velocity.

Such a platoon of vehicles is depicted in Figure 2.4, where L_i denotes the length of the i_{th} vehicle in m, $S_{d_i}(t)$ is the desired safety spacing in m, $S_{0_i} = S_{d_i}(t_0)$ is the spacing at initial time $t = t_0$, and $\delta_i(t)$ is the deviation from the desired safe spacing (positive or negative values).

Based off this vehicle model the following control law has been proposed:

$$u_i(t) = \frac{1}{a(\dot{x}_i)} \left[c_i(t) - b(\dot{x}_i, \ddot{x}_i)\right] \quad (for \quad i = 2, 3, 4, \ldots, n), \tag{2.26}$$

where,

$$c_i(t) = \frac{1}{1 + \lambda_2 C_a} \left[C_p \delta_i(t) + C_v \dot{\delta}_i(t) + C_a \left(a_{i-1}(t) - a_i(t)\right) + K_v v_i(t) + K_a a_i(t)\right], \tag{2.27}$$

$$\delta_i(t) = x_{i-1}(t) - x_i(t) - \left(L_i + S_{0_i} + \lambda_2 v_i(t)\right), \tag{2.28}$$

$$\dot{\delta}_i(t) = v_{i-1}(t) - v_i(t) - \lambda_2 a_i(t), \tag{2.29}$$

$$(for \quad i = 2, 3, 4, \ldots, n).$$

The values of C_p, C_v, C_a, K_v, and K_a are design constants. By substituting Equation (2.26) into Equations (2.23), (2.24), and (2.25), the closed-loop dynamics of the vehicle following system can be described. With initial conditions $v_i(0) = v_0$, and $\delta_i(t) = \dot{\delta}_i(t) = 0$, for $i = 2, 3, 4, \ldots, n$.

2.5 Summary of Control Algorithms

The five control laws that have been selected for analysis have been assembled for reference in Table 2.2. These laws use various policies to insure proper inter-vehicle spacing (CSP, VTG, and CTG) and represent both ACC and CACC system. For future reference and brevity these laws are restated in the form that will be used for the remainder of this

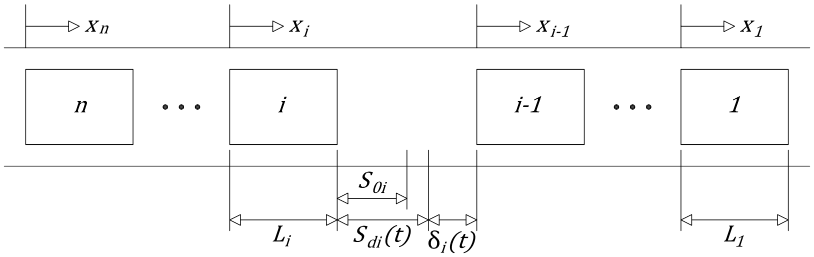


Fig. 2.4: A platoon of n vehicles with vehicle number 1 being the leader.

work:

$$1)\ \ddot{x}_i = \ k_p(x_{i+1} - x_i - h\dot{x}_i) + k_d(\dot{x}_{i+1} - \dot{x}_i), \tag{2.30}$$

$$2)\ \ddot{x}_i = \ k_p(x_{i+1} - x_i) + (k_d + k_p k_h v_d)\dot{x}_{i+1} - (k_d + k_p h_0 + k_p k_h v_d)\dot{x}_i, \tag{2.31}$$

$$3)\ \ddot{x}_i = \ k_p(x_{i+1} - x_i) + k_d(\dot{x}_{i+1} - \dot{x}_i) + k_h(v_d - \dot{x}_i), \tag{2.32}$$

$$4)\ \dddot{x}_i = \ \frac{1}{\tau}[-k_1\ddot{x}_{i-1} + (k_1 - 1 + k_1 k_5 h)\ddot{x}_i - \frac{1}{h}(1 - k_1 k_5 h)\dot{\delta}_i(t) - \frac{k_5}{h}\delta_i(t) - k_5\dot{x}_i], \tag{2.33}$$

$$5)\ \dddot{x}_i = \ \frac{1}{1 + hC_a}[C_p\delta_i(t) + C_v\dot{\delta}_i(t) + C_a\left(\ddot{x}_{i-1} - \ddot{x}_i\right) + K_v\dot{x}_i + K_a\ddot{x}_i], \tag{2.34}$$

where x_i, $\dot{x}_i = v_i$, $\ddot{x}_i = \alpha_i$, $\dddot{x}_i = j_i$, represent the position, velocity, acceleration requirement, and jerk requirement, of the i^{th} vehicle, respectively. For Control Algorithms 1–3 k_p, k_d, and k_h represent system gains, h_0 and h are the desired steady state time headway and time headway constants, respectively. The value v_d denotes the desired nominal velocity. Referring to control laws 4 and 5, $\delta_i(t)$, $\dot{\delta}_i(t)$, and τ are the relative distance and velocity errors and time constant for the i^{th} vehicle, h is the time headway in seconds, and k_1, k_5, C_p, C_v, C_a, K_v, and K_a are system gains.

Table 2.2: Various semi-automated vehicle control laws and their sources.

Control Algorithm	Inter-Veh. Comm.	Type		Reference
1	NO	CTG	ACC	Yanakiev, Kanellakopoulos, Eyre [13,19,20]
2	NO	VTG	ACC	Yanakiev, Kanellakopoulos, Eyre [13,19,20]
3	YES	CSP	CACC	Yanakiev, Kanellakopoulos, Eyre [13,19,20]
4	YES	CTG	CACC	Rajamani and Zhu [6]
5	NO	CTG	ACC	Chein and Ioannou [18]

2.6 Discussion

It has been established by Eyre, Yanakiev, and Kanellakopoulos [13, 14, 19, 20] that string stability cannot be achieved when utilizing a CSP in a unidirectional control scheme in the absence of inter-vehicle communication. In the same works several control laws (Control Algorithms 1, 2, and 3) are proposed that demonstrate string stable behavior. Control Algorithms 1, and 2 are linear autonomous laws derived by treating a platoon of vehicles as a mass-spring-damper system. Control Algorithm 1 provides a control structure similar to that given by Ioannou and Xu [33]. Control Algorithm 3 describes a non-autonomous control system where the leader vehicle velocity must be know by all other vehicles in the system.

An autonomous system is described by Eyre et al. [20], as a system that uses only local sensors to determine the relative distance and velocity of surrounding vehicles, which is also the description of an ACC system. This is in contrast to an non-autonomous system that requires IVC in addition to the local sensing. The non-autonomous model describes a CACC system. Therefore, Control Algorithm 3 is a non-autonomous or CACC system, whereas Control Algorithms 1, and 2 are ACC systems.

The system of Control Algorithm 4 comes from work by Rajamani and Zhu [6], which has been cited extensively, including in Rajamani's automated vehicle text book [15]. Their work describes a linear SAACC system which requires communication between a each vehicle and its predecessor. The proposed communication link is local to each pair of vehicles and does not require unique addresses for each vehicle. Because of the requirement for communication the resulting control law will be categorized with the CACC algorithms for analysis in this thesis. Additionally this model accounts for the fact that there will be a time delay between a control effort request from the platooning controller to the actual response from the vehicle. An analysis is provided that guarantees string stability for time-headway values as small as $h = 0.1s$. With a platoon velocity of 31.29 m/s (70 mph) this would result in an inter-vehicle spacing of just over 3 meters.

A highly non-linear model for automatic vehicle following is proposed by Chein and

Ioannou [18] (Control Algorithm 5). This model describes an AICC law where it is assumed that each vehicle is able to measure the relative distance and velocity of the preceding vehicle. In addition each vehicle must be able to estimate the relative acceleration between itself and the preceding vehicle. Because this model only requires local sensing it is a description of an ACC control law. This work is cited by multiple sources, including Ioannou's own work in conjunction with Xu [33], as well as Yanakiev and Kanellakopoulos [13,14,31]. The advantage of this model is that it accounts for non-linear properties of a vehicle such as time delay caused by the engine, in addition to aerodynamic, and mechanical drag.

String stability is considered a very important concept in automated transportation networks, and is discussed in detail in most of the references cited to this point. If error is proven to decrease between consecutive vehicles upstream a theory for stability in AHS can be established. The goal of this work is to demonstrate flaws in the current theoretical work due to adversarial operating environments. This will deepen the current understanding of stability in AHS, helping provide more well rounded solutions in the future.

Chapter 3

Threat Model Against a Cooperative Stream of Automated Vehicles

Automated vehicles operating on a highway system will form a cooperative traffic stream as density increases. If vehicles are within sensor range of each other their control laws will begin making decisions based off input that is directly affected by surrounding vehicles. At this point the vehicles become a coupled cooperative system. As long as vehicles are within sensor range, and the automated system remains turned on and is functioning properly, the cooperative behavior will persist.

3.1 Threat Model

A multi actor attack scenario is examined where one active attacker directly controls a vehicle within a stream of automated vehicles traveling at a steady velocity. Additionally one or multiple passive attackers, following a modified control law, are present in the stream of vehicles and are located upstream relative to the active attacker as shown in Figure 3.1. Passive attackers have gains intentionally designed to cause oscillation in their desired acceleration or jerk requirement.

The passive attacker vehicles could be colluding with the active attacker, or might be participants as the result of a local or remote exploitation of their control law, in which case the operator would unknowingly be an actor in the attack scenario. All other vehicles in the traffic system are considered victim vehicles.

Actively colluding passive attackers will place themselves advantageously in the traffic system prior to beginning an attack. In this manner a desired density of passive attackers versus victims can be achieved. The attackers will communicate amongst themselves to coordinate attack initiation. In the case of unintentional participants the malicious control

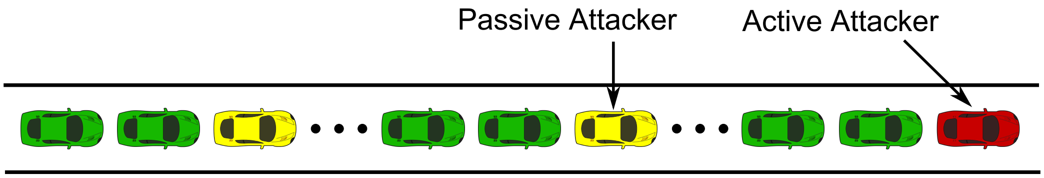


Fig. 3.1: System of automated vehicles in the presence of attackers.

law will be remotely activated, density however, cannot be directly controlled for this case.

This work assumes that traffic system has been manipulated by the active attacker to obtain a desirable vehicle density, or critical density. This density will be different for each type of control algorithm and refers to a scenario where each vehicle in the traffic system is approximately following at the minimum steady state inter-vehicle distance allowed by its control law. All vehicles are assumed to be operating at the same steady state nominal velocity.

3.2 System/Attack Assumptions

To analyze the impact of the malicious attacker, or attackers, on surrounding vehicles the following assumptions are made:

1. All vehicles, attackers and victims alike, have similar dimensions, and share the same velocity constraints:

   Length $5m$.

   Nominal steady state velocity 31.2928 m/s (70 mph).

   Maximum velocity of any vehicle 44.704 m/s (100 mph).

2. Victim vehicles and attacker vehicles alike are assumed to have the following performance characteristics:

   Maximum acceleration $2m/s^2$.

   Maximum deceleration $-4m/s^2$.

3. All vehicles are operating on a straight section of highway.

4. A single lane of traffic is considered where no vehicles are entering or leaving the lane, in other words no lane changes are allowed.

5. One or several attackers have manipulated the system to force surrounding vehicles into a stream of cooperative vehicles and achieve a desired critical density, and the system velocity is constant.

6. Attacker vehicles may locate themselves at any position in the platoon.

To facilitate comparison between the different control laws the attacker vehicles will be simulated using Control Algorithm 1 for all cases. This will accurately describe a real world scenario where there is a heterogeneous mix of vehicles in the traffic system. This will demonstrate the proposed attack is resilient to variations in victim control schemes.

Formally stated the goals of the attackers are: 1) to introduce instability by a simple modification of control law gains, so as to produce an unstable system, and then perturb the system to ensure it is forced out of steady state equilibrium, and 2) to induce global string instability by introducing passive attacker into the system at a density that will ensure the magnification of errors.

Both marginally stable, and unstable gains will cause continual oscillation in victim acceleration, velocity, and inter-vehicle spacing. Global string instability will increase the amplitude of error upstream the system of vehicles. The typical definition of marginally stable behavior refers to oscillations with bounded amplitude. Comparatively unstable behavior will result in oscillations with ever growing amplitude. Practically however this will be limited by acceleration and velocity saturations of the physical vehicles.

The attackers will accomplish their goal by first modifying the control law of the passive attacker vehicles, allowing the law to be switched from a factory provided algorithm to a modified control law. This could be accomplished by inserting a hardware or software Trojan at some point in the manufacturing process, or could be accomplished at a later time. The modified controller may be activated by the driver if actively participating in the attack, or remotely in the case of vehicles that are unintentional participants. The modified control law will have gains intentionally designed to cause marginally stable, or unstable oscillation in desired acceleration requirement and velocity.

Chapter 4

Traffic Flow Stability

The focus of this work is to present and analyze weaknesses in cooperative systems of vehicles using Adaptive Cruise Control (ACC) and Cooperative Adaptive Cruise Control (CACC). These weakness will be discussed in the context of attacks against the ACC or CACC control system by single or multiple actors. The effect of a successful attack against a stream of these automated vehicles could be to negate some or all of the desired benefits of implementing such a system. These laws govern how a vehicle should behave with respect to the movements of the preceding vehicle, thus forming a cooperative system. Due to this interaction the system of cooperative vehicles can be described mathematically using coupled differential equations. A stream of n vehicles (Figure 2.1) using Control Algorithm 1, for example, can be described by the following state equations:

$$\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= k_p(x_2 - x_1 - h\dot{x}_1) + k_d(\dot{x}_2 - \dot{x}_1) \\
&\vdots \\
\dot{x}_{n-1} &= v_{n-1} \\
\dot{v}_{n-1} &= k_p(x_n - x_{n-1} - h\dot{x}_{n-1}) + k_d(\dot{x}_n - \dot{x}_{n-1}) \\
\dot{x}_n &= v_n \\
\dot{v}_n &= u.
\end{aligned} \tag{4.1}$$

The equivalent state-space representation of a linear-time-invariant (LTI) system is:

$$\begin{aligned}
\dot{\mathbf{x}} &= A\mathbf{x} + B\mathbf{u} \\
\mathbf{y} &= C\mathbf{x},
\end{aligned} \tag{4.2}$$

where $x = [x_1,\ v_1,\ x_2,\ v_2, ...,\ x_{n-1},\ v_{n-1},\ x_n,\ v_n]^\top \in \mathbb{R}^{2n}$ are the vehicle states, $A \in \mathbb{R}^{2n\times 2n}$, $B \in \mathbb{R}^{2n}$, $C \in \mathbb{R}^{2n\times 2n}$, and $\mathbf{u}$ is a scalar input. Assuming all vehicle states are measurable C is defined as an identity matrix, and B may have non-zero entry corresponding to attacker inputs.

To begin a discussion regarding the stability of the LTI system of (4.2) several definitions will be drawn from traditional linear systems theory as detailed by Chen [34].

Definition 1 (Marginal and Asymptotic Stability)**.** *The homogeneous LTI system* $\dot{\mathbf{x}} = A\mathbf{x}$ *is said to be marginally asymptotically stable if, for every initial condition* $\mathbf{x}(t_0) = \mathbf{x}_0$*, the homogeneous state-space response* $\mathbf{x}(t) = \Phi(t, t_0)\mathbf{x}_0,\ \ \forall t \geq 0$*, where* $\Phi(t, t_0)$ *is the state transition matrix, and is uniformly bounded. The system is asymptotically stable if* $\mathbf{x}(t) \Rightarrow 0$ *as* $t \Rightarrow \infty$*.*

The homogeneous LTI system is both marginally and asymptotically stable if all the eigenvalues of A have negative real part (Chen [34]).

Definition 2 (Marginal Stability)**.** *The equation* $\dot{\mathbf{x}} = A\mathbf{x}$ *is said to be marginally stable if all the eigenvalues of* A *have zero or negative real parts and those with zero real parts are simple roots of the minimal polynomial of* A*.*

if A has multiple complex pairs of eigenvalues with zero real part these eigenvalues will not be simple roots of the system. Therefore the system is not marginally stable but unstable (Chen [34]).

Definition 3 (String Stability)**.** *A stream, or string, of implicitly cooperative vehicles is said to be string stable when any non-zero position, speed, and acceleration errors of any individual vehicle are not amplified as they propagate upstream (toward the rear of the system).*

A system of cooperative automated vehicles must be string stable to ensure errors do not amplify causing oscillation, traffic jambs, and collisions.

In the analysis that follows it is shown that by a modification of gains attackers can introduce both instability and global string instability into the stream of vehicles. Similar

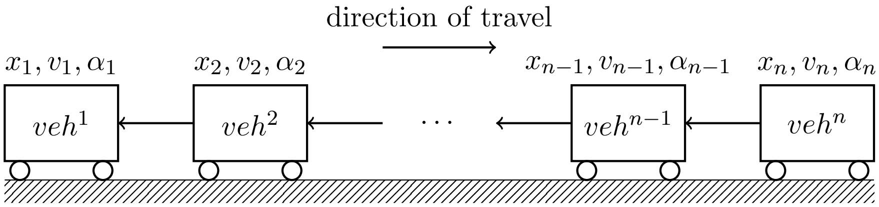


Fig. 4.1: A stream of n-vehicles employing a unidirectional control law. x_i, v_i, and α_i are the position, velocity, and acceleration of the i^{th} vehicle respectively. Arrows represent the flow of information.

to Yanakiev and Kanellakopoulos [13], and Dadras et al. [25], the time headway h, and gain k_p are assumed to be similar for all vehicles, attackers and victims alike. First a general case is define where all vehicles in the system may be utilizing different control algorithms. The analysis is then extended to the special case where all attackers use one control law (Control Algorighm 1) and all victims are utilizing the various control laws from Table 2.2.

4.1 String Stability Criterion

The string stability condition (Definition 3) states that spacing and velocity errors between vehicles should attenuate as they move upstream. To analyze error propagation and stability it is useful to represent error between the i^{th} and i^{th}+1 explicitly utilizing error coordinates as described by Yanakiev and Kanellakopoulos [13].

$$\begin{aligned} z_i &= x_{i+1} - x_i \\ y_i &= \dot{x}_{i+1} - \dot{x}_i = v_{i+1} - v_i \end{aligned} \tag{4.3}$$

The string stability criterion may now be stated as:

$$|G_i(s)| = \left| \frac{z_i}{z_{i+1}} \right| < 1 \text{ for } i = 1, 2, \ldots, n \tag{4.4}$$

where $s = j\omega$ and ω is the angular frequency, and $|G_i(s)|$ is a transfer function representing the magnitude of error between the i^{th} and i^{th}+1 vehicles.

Transfer Function Derivation

Using error coordinates the system of Equation (4.1) (unidirectional CTG model from Control Algorithm 1), is transformed in terms of relative positions and velocities:

$$\begin{aligned}
\dot{z}_1 &= y_1 \\
\dot{y}_1 &= k_p(z_2 - z_1 - h\dot{z}_1) + k_d(\dot{z}_2 - \dot{z}_1) \\
&\vdots \\
\dot{z}_{n-2} &= y_{n-2} \\
\dot{y}_{n-2} &= k_p(z_{n-3} - z_{n-2} - h\dot{z}_{n-2}) + k_d(\dot{z}_{n-3} - \dot{z}_{n-2}) \\
\dot{z}_{n-1} &= y_{n-1} \\
\dot{y}_{n-1} &= -k_p(z_{n-1} - h\dot{x}_{n-1}) - k_d\dot{z}_{n-1} + u.
\end{aligned} \tag{4.5}$$

Now using the transformed system of Equation (4.5) and the Laplace transform a transfer function can be derived that models the error propagation between a particular vehicle in the system versus the preceding vehicle:

$$\begin{aligned}
\dot{y}_i = \ddot{z}_i &= k_p(z_{i+1} - z_i - h\dot{z}_i) + k_d(\dot{z}_{i+1} - \dot{z}_i) \\
s^2 Z_i(s) &= -[(k_p h + k_d)s + k_p]Z_i(s) + (k_d s + k_p)Z_{i+1}(s) \\
(s^2 + (k_p h + k_d)s + k_p)Z_i(s) &= (k_d s + k_p)Z_{i+1}(s),
\end{aligned}$$

$$G_i(s) = \frac{Z_i(s)}{Z_{i+1}(s)} = \frac{k_d s + k_p}{s^2 + (k_p h + k_d)s + k_p}, \quad \text{for } i = 1, 2, \ldots, n. \tag{4.6}$$

The results of (4.6) can be used to select a k_d that will guarantee string stability, this result is same as that given by Yanakiev and Kanellakopoulos [13]:

$$|G_i(s)| \begin{cases} = 1 \text{ if } \omega = 0 \\ < 1\, \forall \omega > 0 \text{ if } k_d > \frac{2 - k_p h^2}{2h} > 0 \end{cases} \tag{4.7}$$

4.2 Instability

In the following a prove is given that demonstrates an attacker can affect stability by changing their gains and subsequently the eigenvalues of A.

A System of Implicitly Cooperative Vehicles

Consider the following state-space equations, which represent a heterogeneous system of cooperative automated vehicles, where the highest order derivatives are simply a function of other states and can represent any LTI unidirectional control law:

$$
\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= f(x_2, x_1, \dot{x}_1, \dot{x}_2) \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= f(x_3, x_2, \dot{x}_2, \dot{x}_3) \\
&\vdots \\
\dot{x}_{n-1} &= v_{n-1} \\
\dot{v}_{n-1} &= f(x_n, x_{n-1}, \dot{x}_{n-1}, \dot{x}_n) \\
\dot{x}_n &= v_n \\
\dot{v}_n &= u.
\end{aligned}
\tag{4.8}
$$

The system of (4.8) can be represented by a cascaded system of transfers functions. The output from one transfer function being the input to the next, each transfer function contributing to the eigenvalues of the larger system.

Lemma 1. *The heterogeneous cooperative automated vehicle system represented by Equation* (4.8) *cannot be stable if the real part of a single eigenvalue of A is greater that zero. An attacker can judiciously select gains corresponding with their control law that will cause A to have at least one eigenvalue with a zero or positive real part, and therefore make the cooperative system unstable.*

Proof. Without loss of generality the system of (4.8) can be expressed as a cascaded system of transfer functions

$G_1(s),\ G_2(s), \ldots,\ G_{n-1}(s),\ G_n(s)$, where:

$$G_i(s) = \frac{Z_i(s)}{Z_{i+1}(s)},\ \text{for } i = 1, 2, \ldots, n, \tag{4.9}$$

is the error coordinate transfer function of the i^{th} vehicle in the system. Assuming an n vehicle system the input to the i^{th} vehicles transfer function $G_i(s)$, is the error state $Z_{i+1}(s)$, representing measured position and velocity error relative to the $(i+1)^{\text{th}}$ vehicle and its predecessor the $(i+2)^{\text{th}}$ vehicle. The output of $G_i(s)$ is $Z_i(s)$, the measured position and velocity error relative to the current vehicle and its predecessor the $(i+1)^{\text{th}}$ vehicle. More generally the error measurements could include any measurable states required by a particular vehicles control law.

The transfer function $G_i(s)$ of the i^{th} vehicle can be expressed in terms of the poles and zeros which it contributes the system of Equation (4.8):

$$G_i(s) = \frac{Z_i(s)}{Z_{i+1}(s)} = \frac{N_i(s)}{D_i(s)},\ \text{for } i = 1, 2, \ldots, n, \tag{4.10}$$

and if $G_i(s)$ is a strictly proper transfer function the roots of $D_i(s)$ determine the stability of the impulse response (Chen [34]). If a single real root, or real and complex conjugate pair of roots, have positive real parts (unstable) then $\mathbf{x}(t) \Rightarrow \infty$ as $t \Rightarrow \infty$, and the system of (4.8) will be unstable.

Assuming an attacker is using the system of Control Algorithm 1 and Equation (4.1), which is expressed as an error coordinate transfer function in Equation (4.6), by choosing $k_d = -k_p h$:

$$D_{i_{atk}}(s) = s^2 + (k_p h + k_d)s + kp = s^2 + k_p \implies s = 0 \pm j\sqrt{k_p}, \tag{4.11}$$

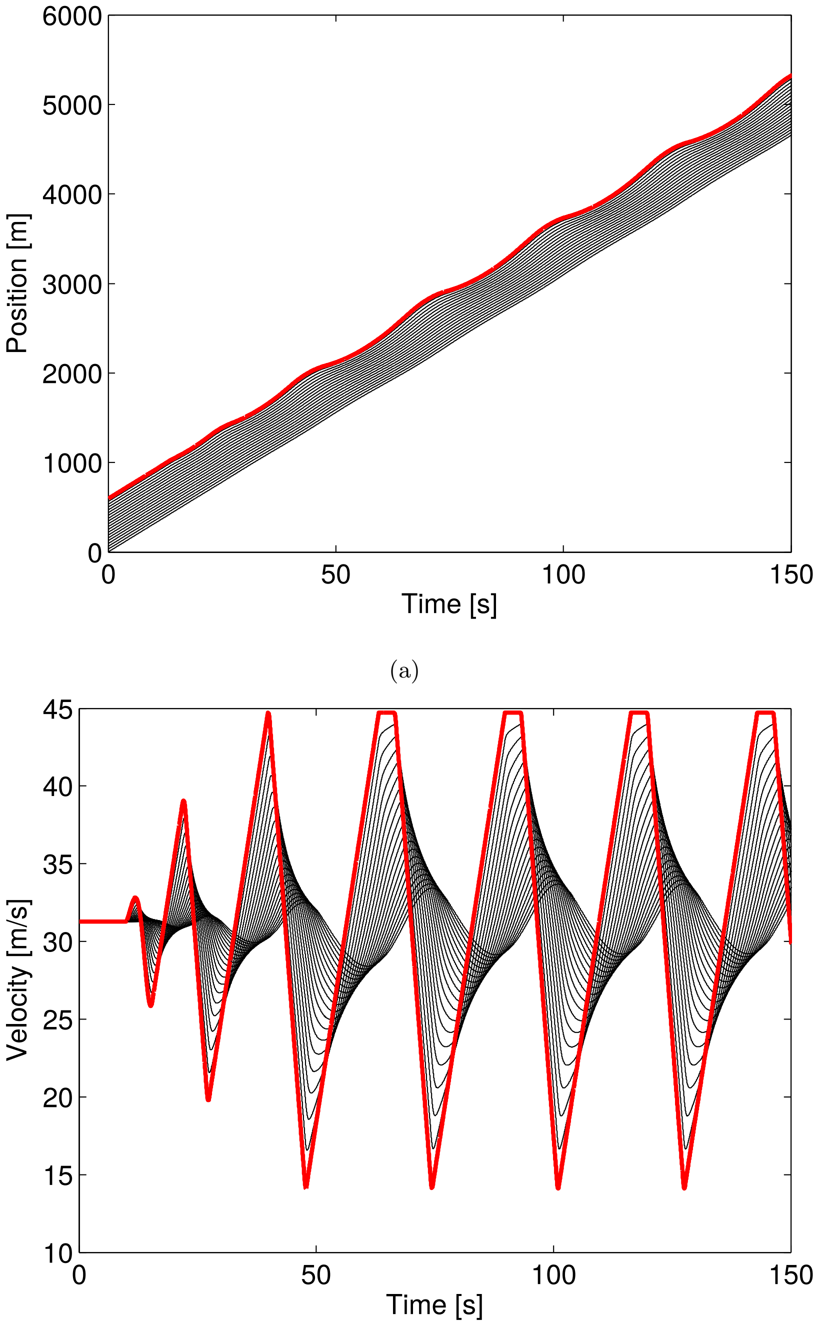
a marginally stable complex pair of eigenvalues have been added to the system. By choosing $k_d < -k_p h$, a complex pair of unstable eigenvalues will be added to the system. Because the roots of $D_{i_{atk}}(s)$ are independent of surrounding vehicles a heterogeneous mixture of vehicles can be destabilized by the judicious selection of gains.

Referring to Definition 2, if more than one attacker with marginally stable eigenvalues is present in the system these eigenvalues will not be simple roots of the system. Therefore the system is not marginally stable but unstable. $\square$

This ensures that $\mathbf{x}(t) \Rightarrow \infty$ as $t \Rightarrow \infty$, $\therefore \forall k_{d_{atk}} < -k_d h$ the system of Equation (4.1) will be unstable. Less negative values of $k_{d_{atk}}$ might cause the system to diverge more slowly, while more negative values will likely cause the system to diverge more quickly. However, in practical application physical acceleration and velocity saturations will not allow unbounded instability in the traffic system. This will be apparent in the simulations results provided in later sections. Additionally while this is a necessary condition to insure instability in general it is not sufficient to ensure system wide instability for a unidirectional control scheme. By definition a unidirectional control law ensures that a particular vehicle in the system will only influence vehicles behind it but not in front.

4.3 Global Instability and String Instability

In a real system the attacker cannot incite unbounded oscillations due to physical acceleration and velocity saturation limits. Also to guarantee that spacing and velocity errors will decrease, control gains for the victims have been chosen to insure $|G_i(s)| \leq 1$ as previously discussed. In short even if an attacker chooses unstable gains the resulting oscillation will reach an upper bound, and given a sufficiently large traffic system the victim vehicles will attenuate error toward the rear of the system which as a whole will remain string stable as shown in Figure 4.2. Clearly deviation from the nominal velocity decreases the further upstream a vehicle is from the attacker. Multiple attackers however, can amplify the attack as it progresses toward the rear of the traffic system ensuring the entire system deviates from the desired nominal velocity.



(a)

(b)

Fig. 4.2: Position (a) and velocity (b) of a system of 20 vehicles under attack. An attacker (shown in red) introduces instability, due to physical acceleration and velocity saturations there is an upper bound on the attack. Deviation from the nominal velocity decreases the farther upstream from the attacker a vehicle is located.

Density of Attackers

Drawing from the proof for Lemma (1) the cumulative system response can be considered as the product of cascaded transfer functions of each individual vehicle. Let $|G_a(s)|$ be the transfer function magnitude of an attacker, and $|G_v(s)|$ be the magnitude of a victim with respect to frequency. If all the victims in a group are using different control laws (heterogeneous case) the cumulative gain of this group can be expressed as:

$$|G_{v_1}(s)| \times |G_{v_2}(s)| \times \ldots \times |G_{v_n}(s)| = \prod_{j=1}^{n} \left|G_{v_j}(s)\right| . \tag{4.12}$$

A subsystem with n unique victims following an attacker can be expressed as:

$$|G_a(s)| \prod_{j=1}^{n} \left|G_{v_j}(s)\right| , \tag{4.13}$$

if the magnitude of this expression is > 1 global string instability can be achieved, this is a function of n, the number of victim vehicles in the subsystem. In other words by judicious placement within a traffic system and proper gain selection, a density of attackers can insure errors are magnified toward the rear of the system despite the fact victim gains have been designed to ensure attenuation of errors.

The larger traffic system can be expressed as a multiplicity of the subsystem of (4.13). As a general case each victim and each attacker utilize different control laws and gains resulting in a unique transfer function for each vehicle:

$$|G_{sys}(s)| = \left(|G_{a_1}(s)| \prod_{j_1=1}^{n_1} \left|G_{v_{j_1}}(s)\right| \right) \times$$
$$\left(|G_{a_2}(s)| \prod_{j_2=1}^{n_2} \left|G_{v_{j_2}}(s)\right| \right) \times \ldots \times \left(|G_{a_i}(s)| \prod_{j_i=1}^{n_i} \left|G_{v_{j_i}}(s)\right| \right) ,$$

and the cumulative gain of the system can be expressed as:

$$|G_{sys}(s)| = \prod_{i=1}^{N} \left(|G_{a_i}(s)| \prod_{j_i=1}^{n_i} \left|G_{v_{j_i}}(s)\right| \right) , \tag{4.14}$$

if the attackers are using stable, but not string stable gains, and $|G_{sys}(s)| > 1$ the system is globally string unstable. The attackers could also choose unstable gains (for example if Control Algorithm 1 is being used, $k_d \leq -k_p h$) and as detailed in the proof for Lemma (1) the system will be globally unstable. For analysis a special case will be considered where attackers use the same control law, all victims use the same control law which is not necessarily the same as the attackers, and attackers are distributed uniformly within the traffic system. The cumulative gain of this system can be expressed as:

$$|G_{sys}(s)| = \left(|G_a(s)|\,|G_v(s)|^n\right)^N, \tag{4.15}$$

to ensure global string instability it is sufficient however to ensure $|G_a(s)|\,|G_v(s)|^n > 1$. The required attacker density can be easily calculated where n is the number of victims between attackers:

$$\begin{aligned}
&|G_a(s)|\,|G_v(s)|^n > 1,\\
&|G_v(s)|^n > \frac{1}{|G_a(s)|},\\
&n\ln\left(|G_v(s)|\right) > \ln\left(\frac{1}{|G_a(s)|}\right),\\
&n > \frac{\ln\left(\frac{1}{|G_a(s)|}\right)}{\ln|G_v(s)|},
\end{aligned}$$

$$\rho_{atk} > \frac{1}{n} \implies \rho_{atk} > \frac{\ln|G_v(s)|}{\ln\left(\frac{1}{|G_a(s)|}\right)}. \tag{4.16}$$

The density of attackers required to incite global instability, or string instability depends on the magnitude of attenuation a victim vehicle can achieve, and amplification an attacker can provide. The attenuation $(1 - |G_v(s)|)$ of a victim using Control Algorithm 1 with $k_p = 1,\ h = 1$ is shown in Figure 4.3 for different values of k_d with respect to frequency. Clearly an upper bound on the attenuation can be establish over a range of attacker frequencies. For example, the upper bound on victim attenuation for frequencies below 0.7 rad/s is calculated as $1 - 0.8051 = 0.1949$ for the data of Figure 4.3, where 0.8051 is the minimum victim gain for this range. The frequency response of a string stable victim transfer function is illustrated in Figure 4.4.

If an attacker using Control Algorithm 1 chooses gains $h = 1,\ k_p = 0.5,\ k_d = -0.45$ which are stable but string unstable, they produce a gain of 16.76 (24.89dB) at a frequency of 0.7 rad/s as shown in Figure 4.5. Now using Equation (4.16), an attacker density $\rho_{atk} > \frac{\ln|0.8051|}{\ln\left(\frac{1}{|16.76|}\right)} > 0.077$, or 7.7% is required to achieve global string instability. A system of 100 vehicles is shown in Figure 4.6 with attacker densities of 6% and 8%. In the first case (Figure 4.6(a)) the system remains string stable, the second case (Figure 4.6(b)) illustrates global string instability. As each victim vehicles control law is trying to attenuate error the passive attackers are amplifying error. This demonstrates that the traditional concept of string stability is a necessary but not sufficient condition to ensure error attenuation.

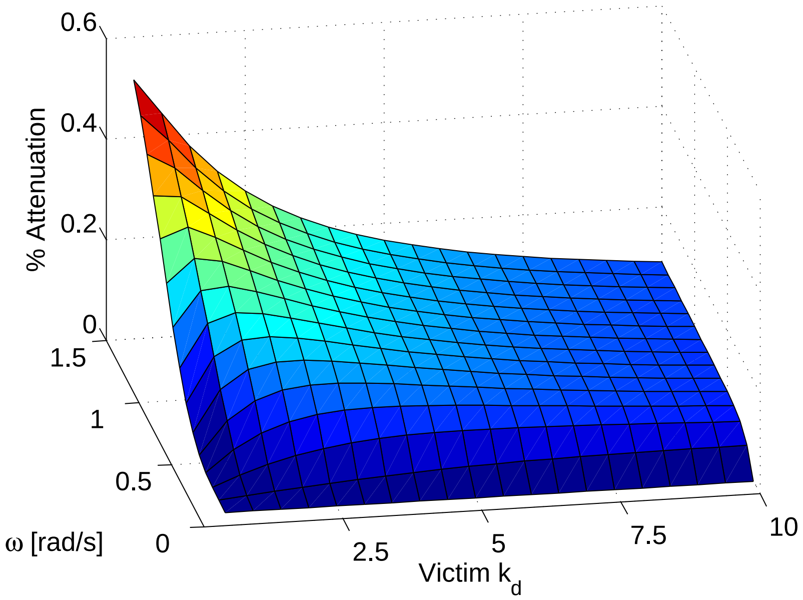


Fig. 4.3: Percentage of attenuation for a victim vehicle, with respect to victim gain and frequency.

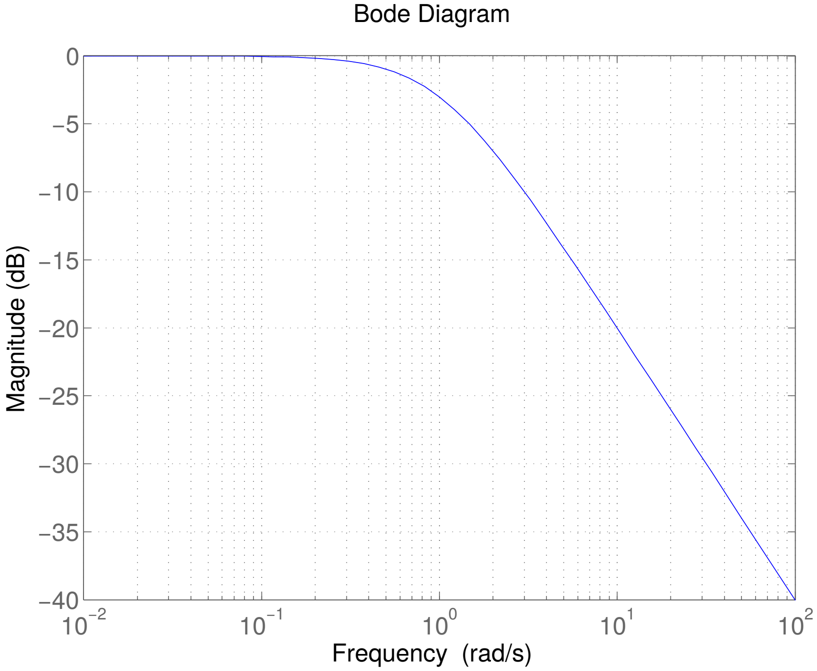


Fig. 4.4: Magnitude plot of the error representation transfer function of a victim vehicle using Control Algorithm 1. In this case gains have been chosen to create a string stable system.

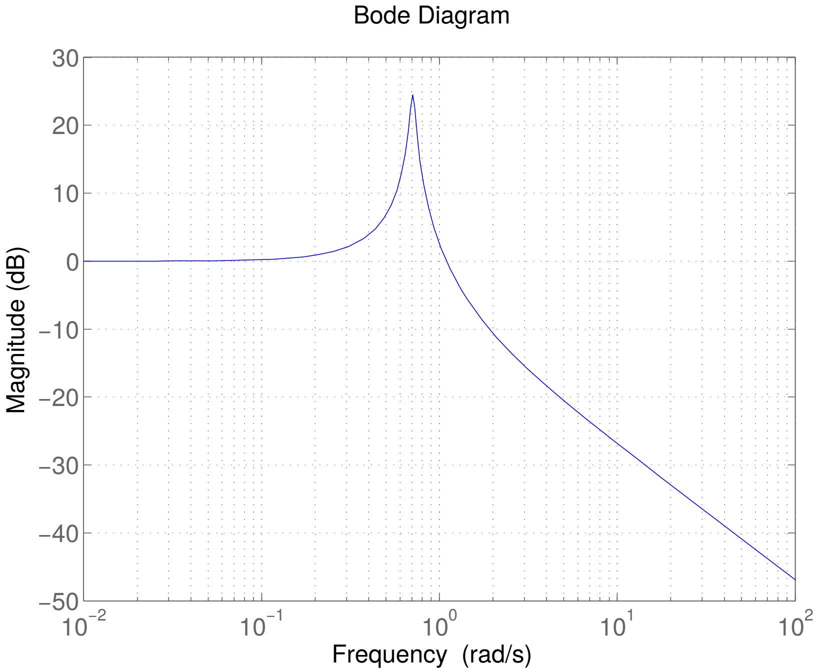
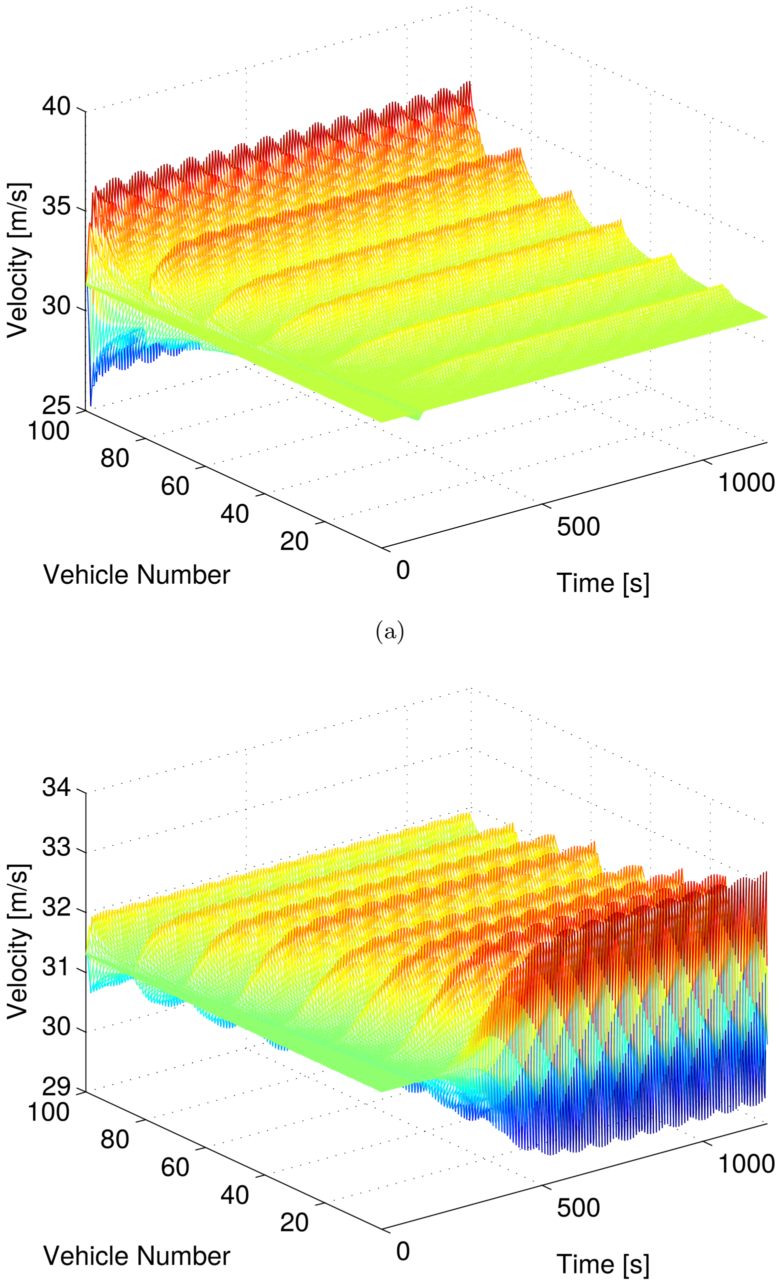


Fig. 4.5: Magnitude plot of the error representation transfer function of an attacker. In this case gains have been chosen to ensure magnification of error.



(a)

(b)

Fig. 4.6: A system of 100 vehicles under attack. (a) The attacker density is too low (6%), the system is global string stable. (b) A higher attacker density (8%) produces global string instability.

Chapter 5

A Destabilizing Attack Against an Automated Stream of Vehicles

The security and safety implications of the findings detailed in Chapter 4 are discussed here. Two main attacks scenarios are considered: 1) the attackers have stable but string unstable gains, i.e. the poles of each resulting transfer function have strictly negative eigenvalues, and the criterion of Equation (4.4) has been violated, and 2) the attackers have strictly unstable gains, i.e. the eigenvalues corresponding to each transfer function have zero real parts or are strictly positive.

As discussed previously, barring collisions, a single attacker will have limited effect on a large traffic system due to physical saturations in acceleration and velocity. However a density of attackers can propagate an attack through a large system.

5.1 Attack Against Control Algorithm 1

The attack scenarios discussed above are simulated against a system of automated vehicles using Control Algorithm 1. A traffic system of 100 vehicles is considered with the victims using the following gains to ensure string stable operation: $h = 1$, $k_p = 1$, $k_d = 1$ (Equation (2.4) and Equation (4.6)). A passive attacker density of 8% and 1 active attacker are simulated. Because of the unidirectional control law used the active attacker does not influence the vehicles preceding it. Therefore, the active attacker is placed at the front of the simulated system, with the understanding that this group of vehicles could be part of a larger traffic system. Acceleration and velocity saturation constraints have been implemented in the simulated.

5.1.1 Attack Scenario 1

Attackers using scenario 1 can ensure string instability but maximum error amplitude will be limited by the frequency of oscillation. For example an oscillation at 1 rad/s or 0.15 Hz will have a period of 6.3 seconds. If the average vehicle in the system accelerates at $2m/s^2$, for example, a maximum velocity error of approximately $1.6m/s$ can be achieved due to the frequency of oscillation. Lower attack frequencies will achieve higher amplitudes and can be attained by judicious gain selection. Because the attacker gains are stable they will settle to a steady nominal state in the absence of disturbance. The active attacker will provide input to the system, by operating at the resonate frequency of the attacker transfer functions maximum gain can be achieved.

For attack Scenario 1 attacker control gains of $h = 1$, $k_p = .5$, $k_d = -.48$ are used, producing an error amplification of 42.7 at 0.707 rad/s. For the simulation results shown in the figures below the active attacker perturbs the system by varying their velocity $\pm 5m/s$ at a frequency of 0.112Hz (0.707 rad/s). This is simulated by adding a sinusoidal component $5\sin(0.707 * t)$, to the active attackers control requirement. The attack is initiated at 10 seconds, the system response to this disturbance has been simulated for a period of 20 minutes. Referring to Figure 5.1 vehicle 1 is at the rear of the traffic system and vehicle 100, the active attacker, is at the front. The magnitude of vehicle velocity is growing toward the rear of the system demonstrating global string unstable behavior as predicted in Chapter 4.

The beginning of the attack can be seen in Figure 5.2. By approximately 150 seconds all of the passive attackers are oscillating and amplifying the disturbance, again demonstrating global string instability. The end of the simulated attack is shown in Figure 5.3 and has reached the maximum error magnitude for this frequency. The amplitude of the attack could of course be increased by choosing strictly unstable passive attacker gains. However, the larger deviations might alert victims that an attack is underway. Additionally there is a high probability of collisions which will bring the attack to a halt. Attack Scenario 1 while having a lower probability of collisions will endure, causing vehicles to continually deviate from the desired nominal system velocity. This will not only result in driver discomfort but will cause excessive energy expenditure over an extended period.

The velocities of victim vehicles following the attacker furthest downstream are shown in Figure 5.4. The velocities of victim vehicles following the passive attacker farthest upstream are shown in Figure 5.5. Examining both plots it is clear that the velocity error for a particular victim decreases the further from an attacker it is located. This is due to the local string stability property of the system. However, the magnitude of oscillation for the group of victims located farthest upstream is significantly greater. This is because the passive attackers are amplifying error causing the traffic system as a whole to become globally string unstable.

Similarly the accelerations of the same groups of victim vehicles are given in Figure 5.6 and Figure 5.7. Again the magnitude variation is greater for the group of victims located furthest upstream. The higher amplitude oscillations cause the accelerations to saturate. By inspecting the velocity and acceleration figures it is clear that the frequency of oscillation decreases for the group of victims furthest upstream. The period of oscillation for the group of victims behind the first attacker is approximately 9 seconds where the oscillation for the group of victims behind the rearmost attacker is approximately 17 seconds. This is caused by saturation in vehicle acceleration which can be seen in Figure 5.7.

Examining Figure 5.8 the standard deviation of the victim vehicle velocities approximately $3m/s$. This value will be used as one indicator of how disruptive, i.e. how successful, the attack is. Another good indicator is the percentage of victims deviating from the nominal velocity. This metric is shown in Figure 5.9. Approximately 10% of the victims are deviating by at least 15% of the nominal velocity, and approximately 2% of vehicles are deviating by as much as 40% of the nominal velocity.

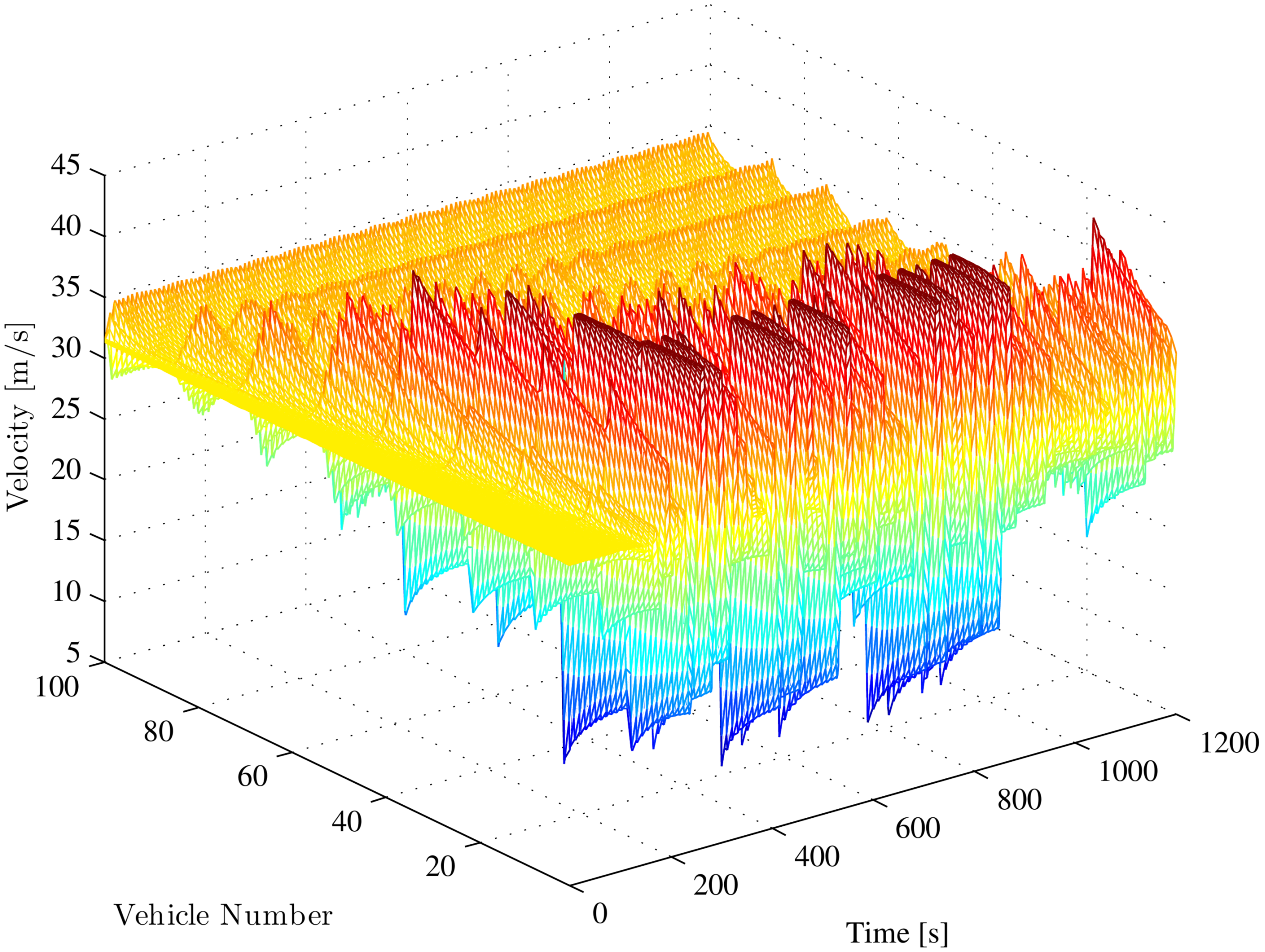


Fig. 5.1: Velocity landscape of Control Algorithm 1 during a simulated attack.

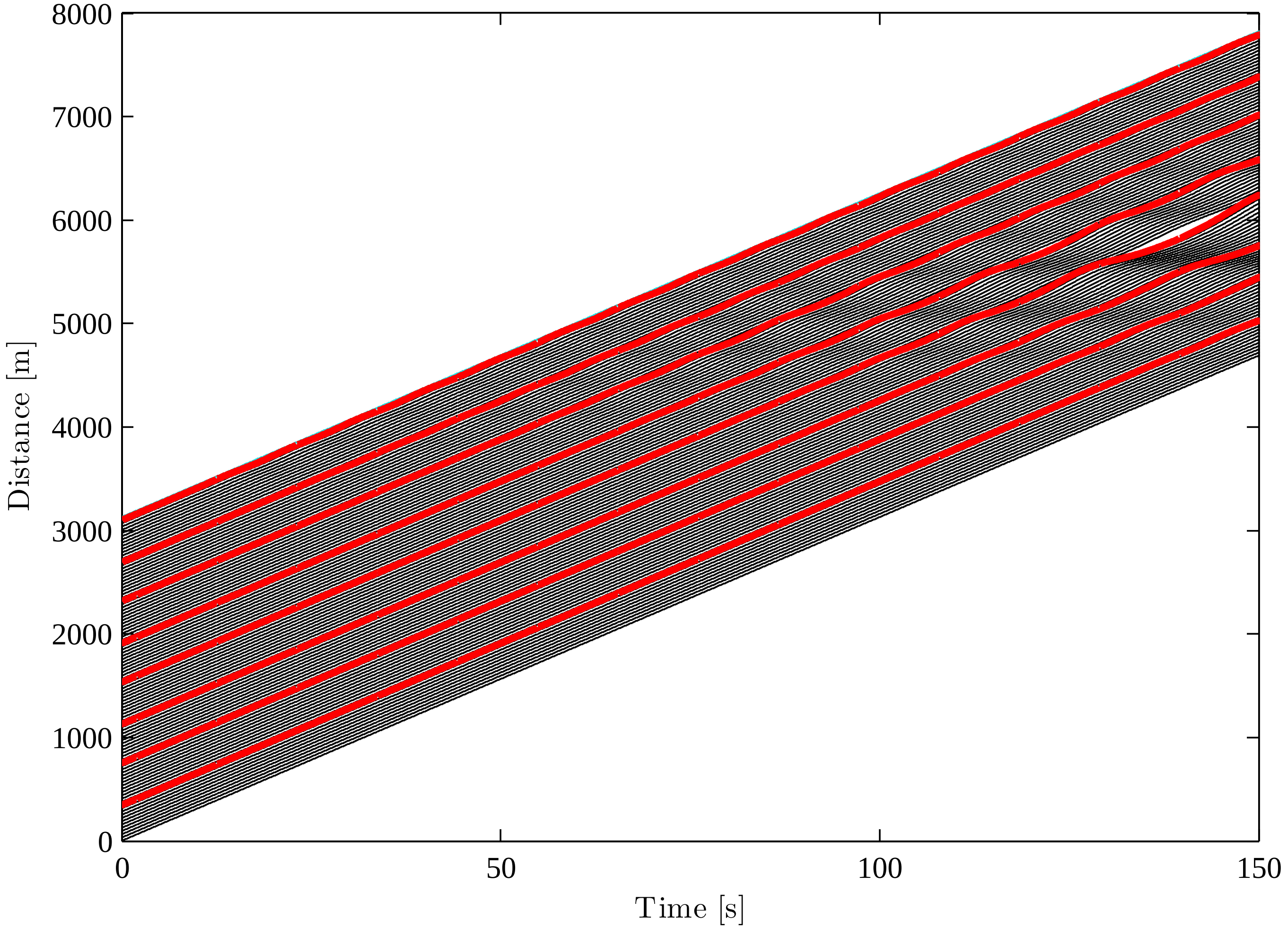


Fig. 5.2: Vehicle positions at the beginning of the simulated attack against Control Algorithm 1, attacker vehicles are shown in red.

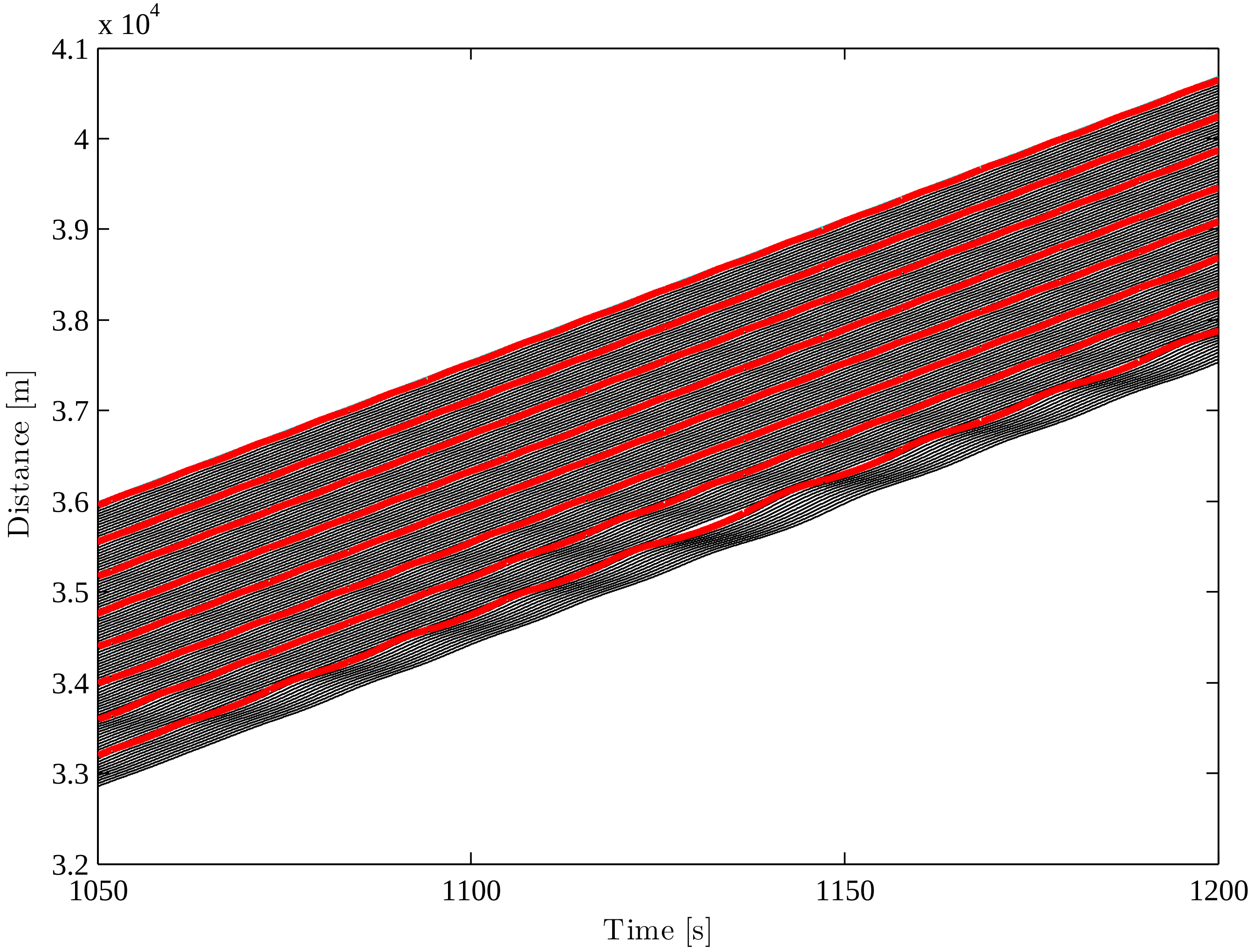


Fig. 5.3: Vehicle positions at the end of the simulated attack against Control Algorithm 1, attacker vehicles are shown in red.

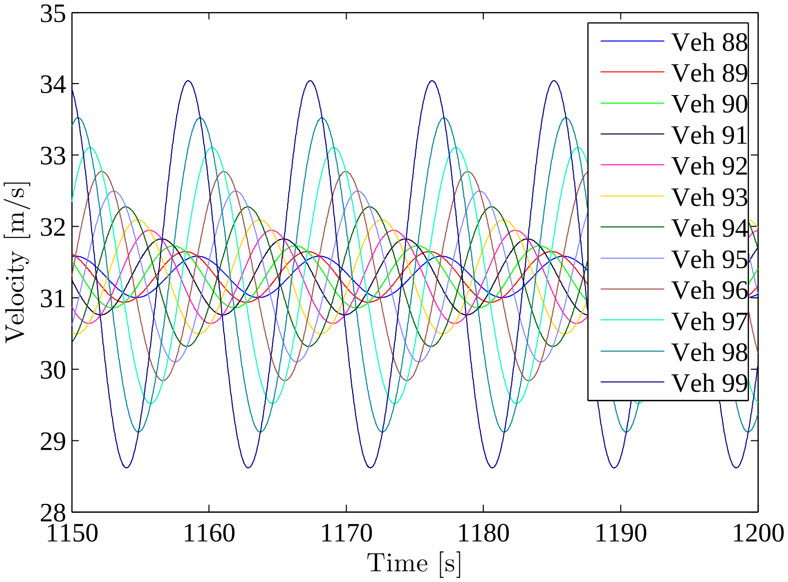


Fig. 5.4: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 1).

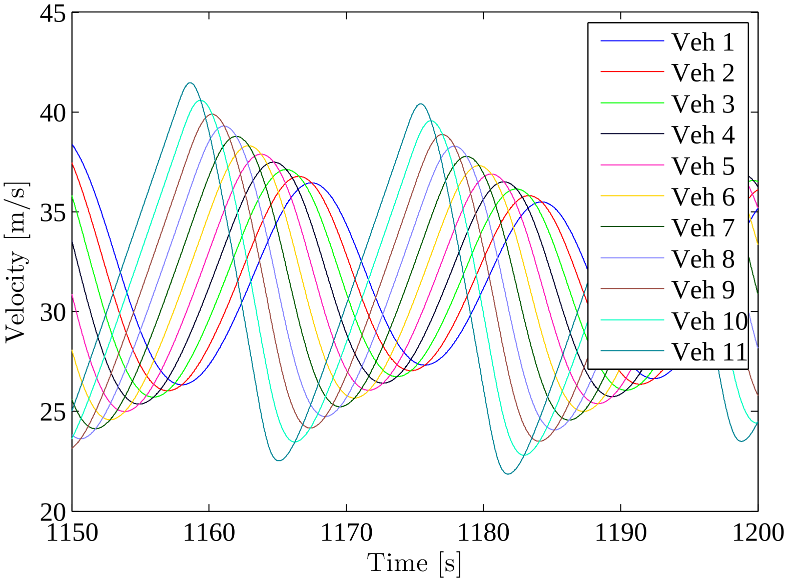


Fig. 5.5: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 1).

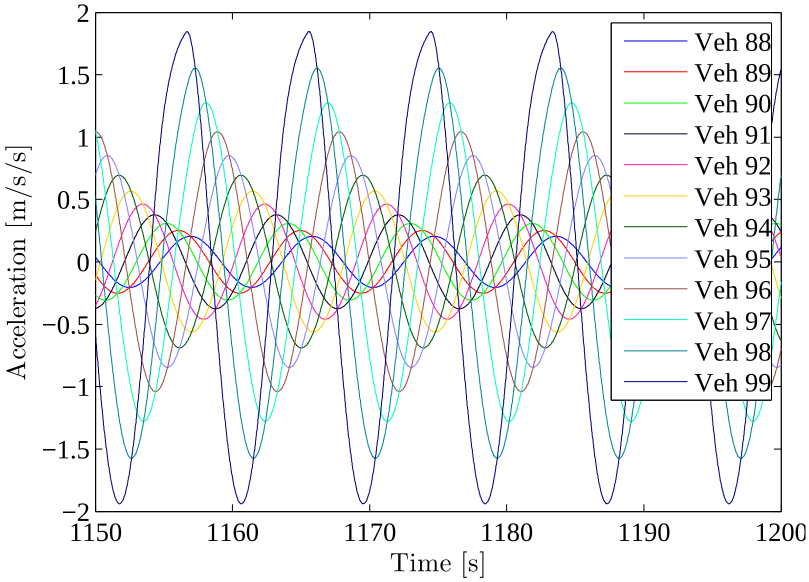


Fig. 5.6: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 1).

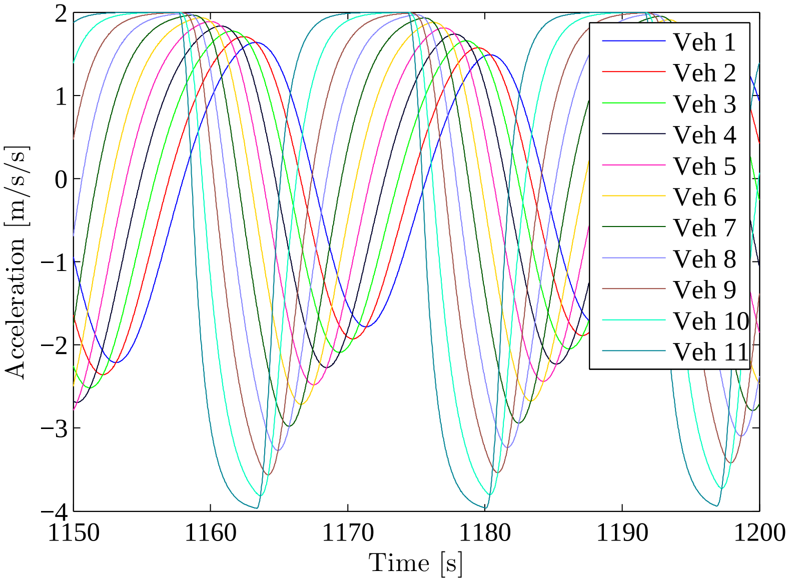


Fig. 5.7: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 1).

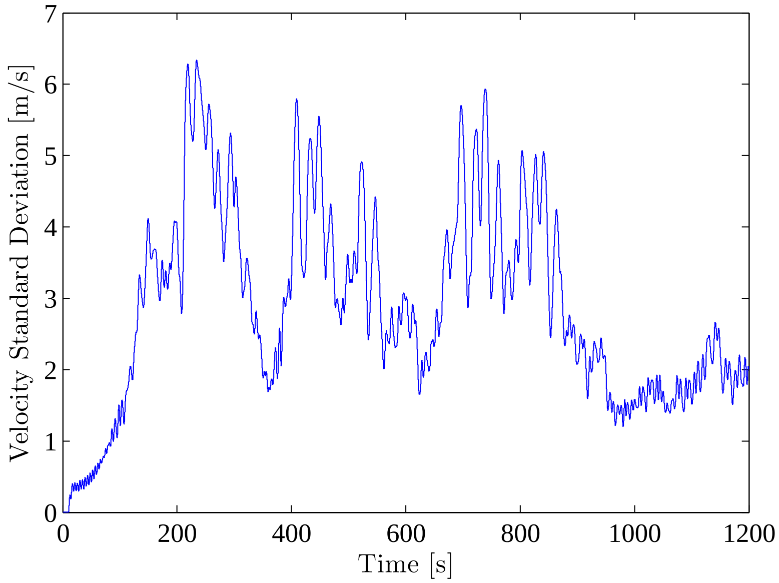


Fig. 5.8: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against Control Algorithm 1.

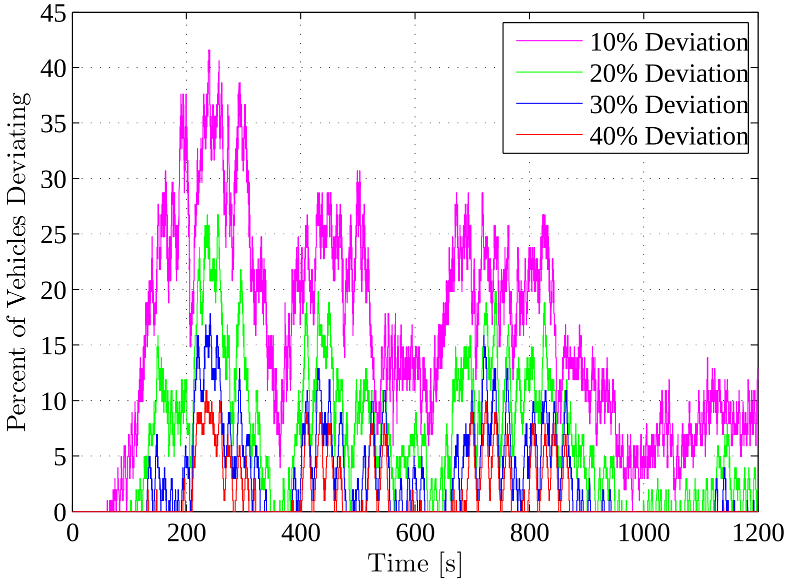


Fig. 5.9: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack against Control Algorithm 1.

5.1.2 Attack Scenario 2

By using strictly unstable gains attack Scenario 2 has greater potential to cause acceleration and velocity saturation. As a sub system of vehicles begin to saturate in acceleration and velocity the frequency of oscillation will drop until the attacker is saturated. The longer the acceleration of the passive attackers is saturated the lower the frequency of oscillation will become. As the frequency decreases the magnitude of the oscillations in velocity will increase, thus increasing the magnitude of oscillation in vehicle positions.

For attack Scenario 2 attacker gains of $h = 1$, $k_p = .5$, $k_d = -.6$ are used to produce an unstable system as given in the proof for Lemma (1). For the unstable case it is not necessary for the active attacker to provide continual input to the system. To get the attack moving the attacker performs a 10 second braking maneuver, the passive attackers begin to oscillate as seen in Figure 5.11. The system is unstable as can be seen in Figure 5.12.

The entire system is saturated in velocity as shown in Figure 5.10. Once this condition is reached vehicles will accelerate and decelerate rapidly from zero to maximum velocity. This stop and go traffic will drastically increase the possibility of large scale collisions. Attack Scenario 1 on the other hand will still generate error but with a much lower likelihood of collisions, resulting in persistent oscillation.

Referring to Figures 5.13 – 5.16 the change in frequency from the front to the rear of the system can be seen.

Figures 5.17 and 5.18 again show how widely the velocity is varying in the system. Collisions will most likely occur for this attack scenario.

The devastating extent of these attacks should be considered. The attack is generated due to instability in the automated control algorithm, once an attack has been initiated the traffic system will be unstable for all time. Barring collisions the only chance of recovery is for victim vehicles to drop out of automated mode or leave the traffic system altogether, if that is even an option. In other words it would be for safer for the drivers to take their chances with manual operation versus suffer from the unbearably abrupt changes in acceleration and velocity caused by the unstable automated system.

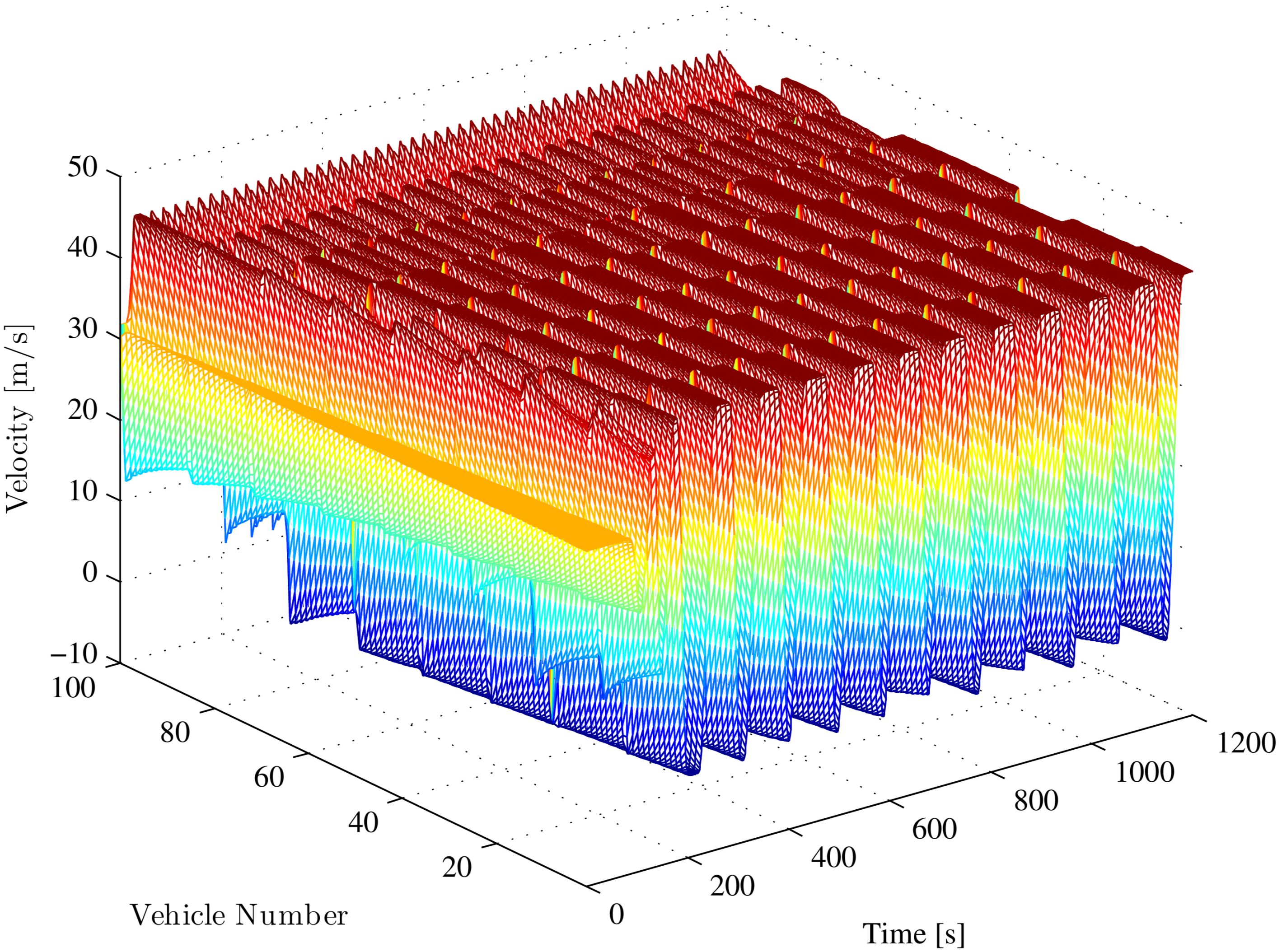


Fig. 5.10: Velocity landscape of Control Algorithm 1 during attack Scenario 2.

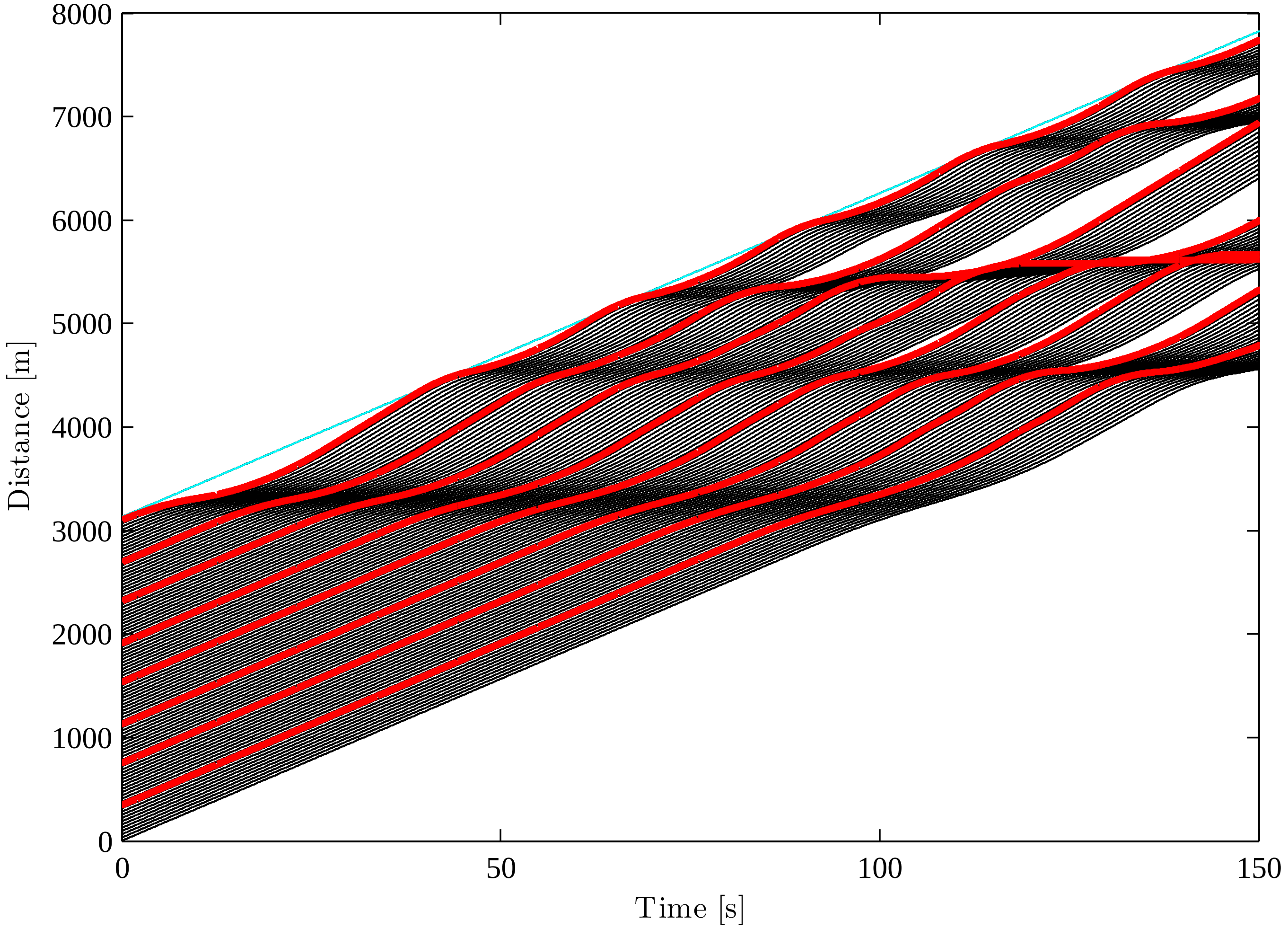


Fig. 5.11: Vehicle positions at the beginning of the simulated attack against Control Algorithm 1 (attack Scenario 2), attacker vehicles are shown in red.

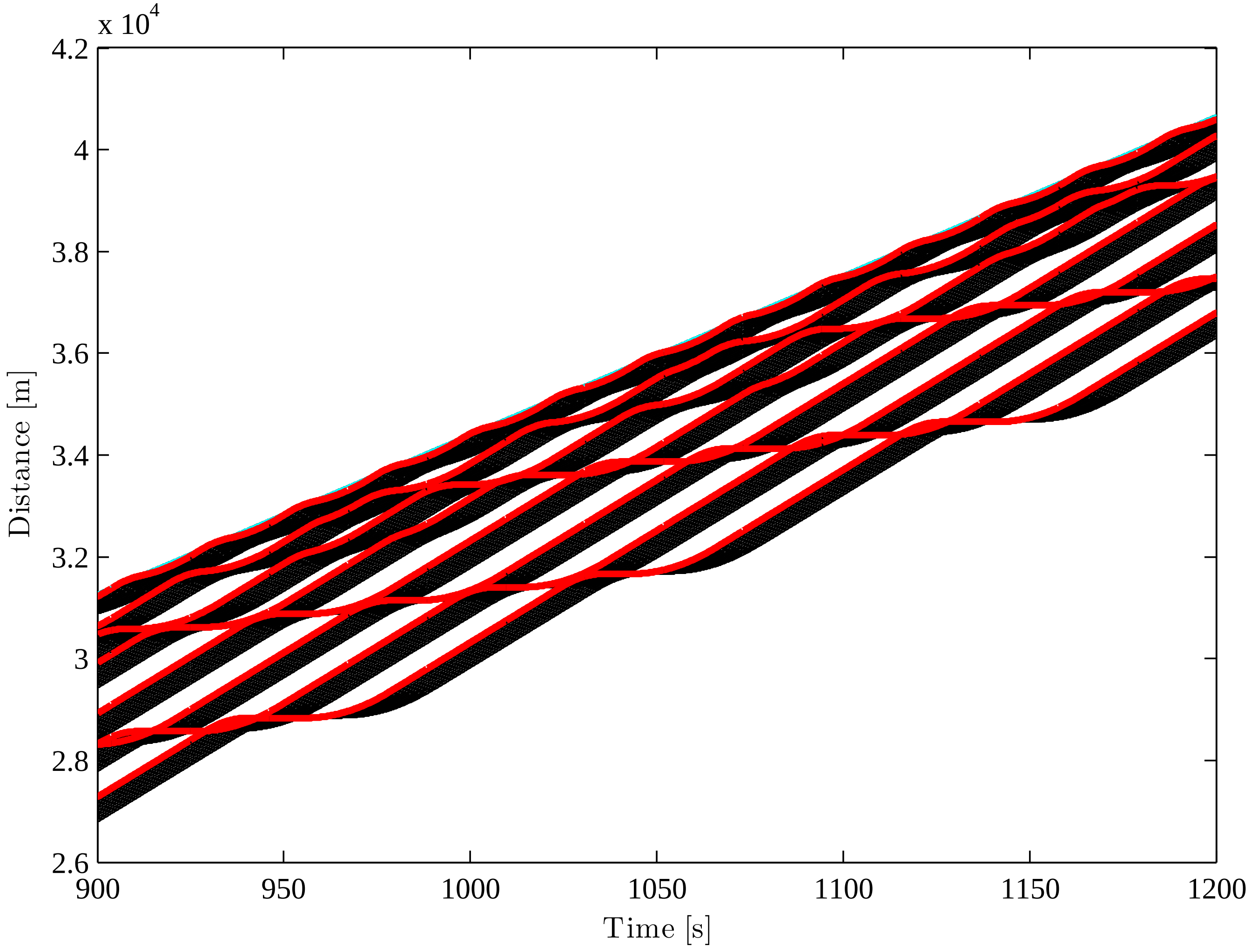


Fig. 5.12: Vehicle positions at the end of the simulated attack against Control Algorithm 1 (attack Scenario 2), attacker vehicles are shown in red.

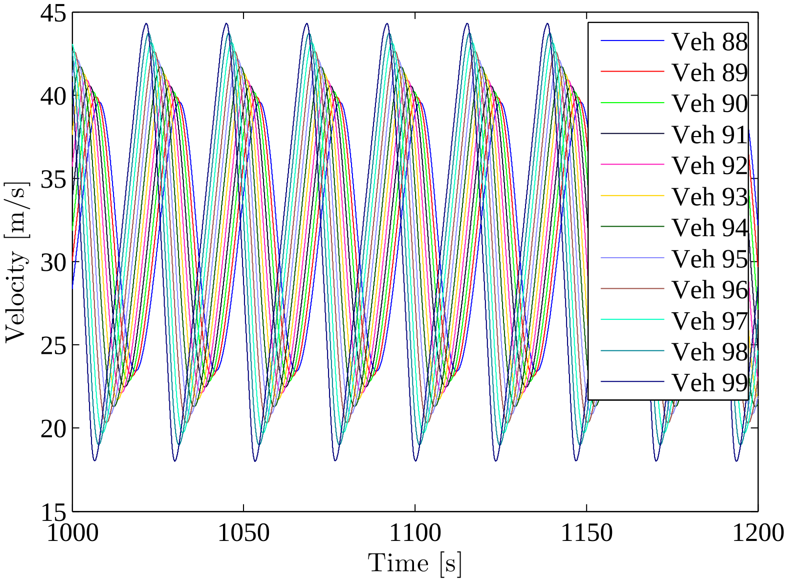


Fig. 5.13: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack Scenario 2 against Control Algorithm 1).

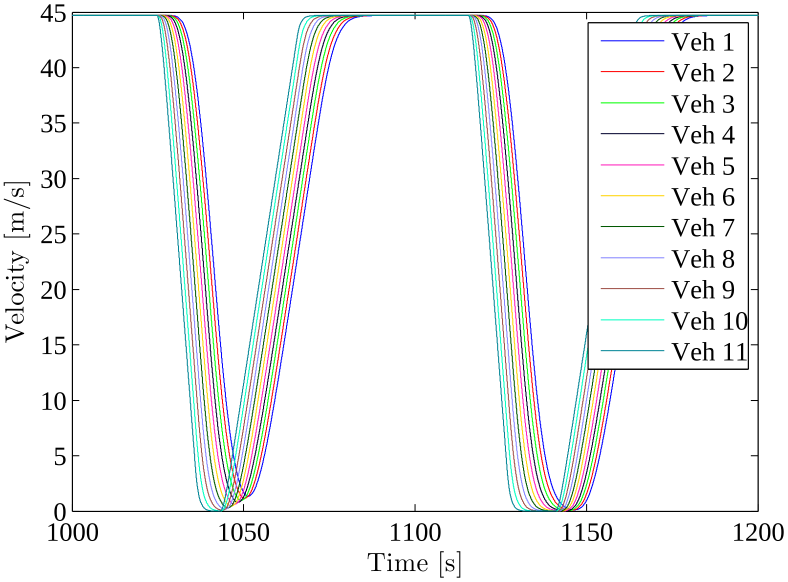


Fig. 5.14: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack Scenario 2 against Control Algorithm 1).

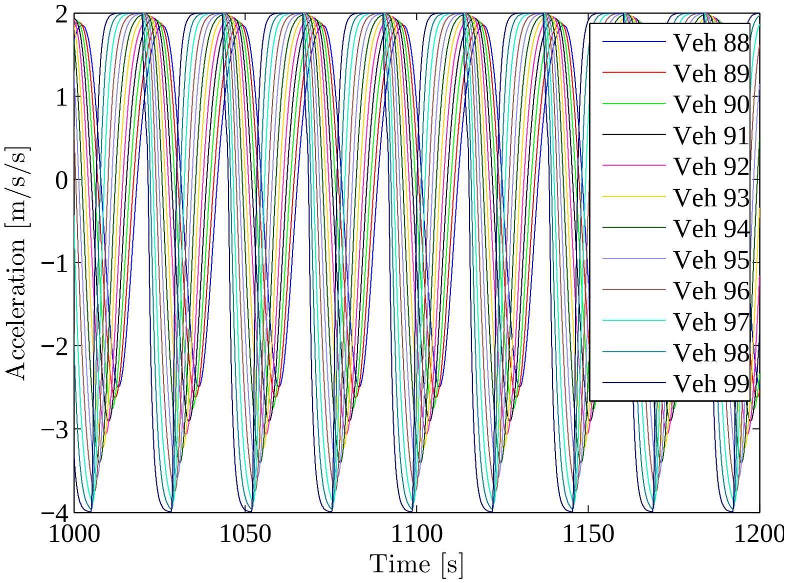


Fig. 5.15: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack Scenario 2 against Control Algorithm 1).

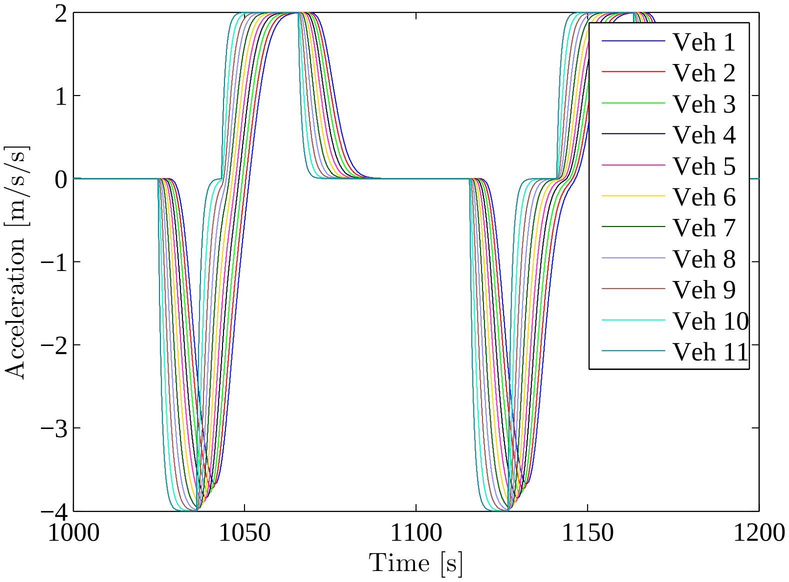


Fig. 5.16: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack Scenario 2 against Control Algorithm 1).

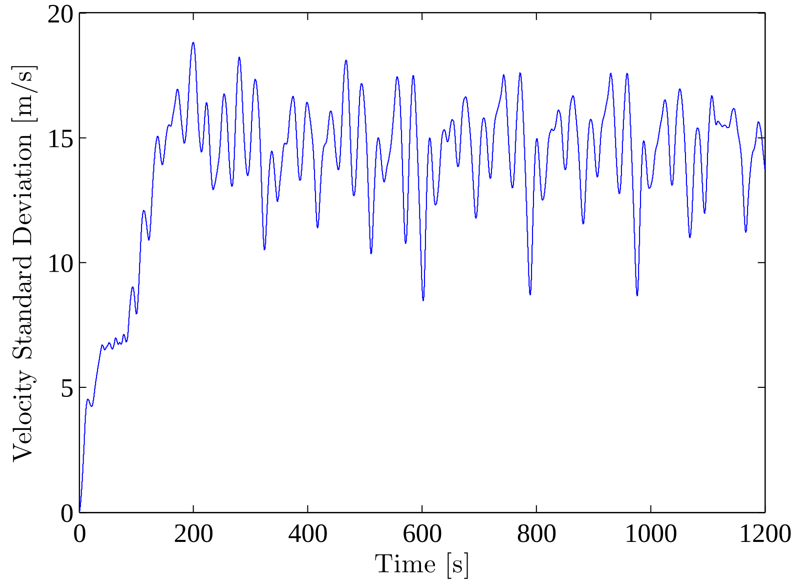


Fig. 5.17: Standard deviation of the victim vehicle velocities for the duration of the simulated attack Scenario 2 against Control Algorithm 1.

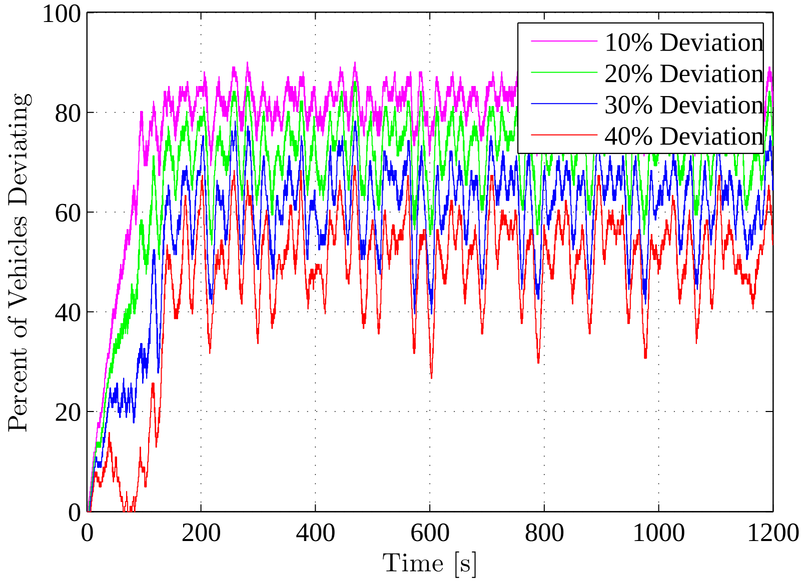


Fig. 5.18: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack Scenario 2 against Control Algorithm 1.

5.2 Intelligent Driver Model Benchmark Simulation

The IDM described by by Treiber et al. [12] is used in this work as a benchmark for evaluating the effect of attack scenarios on traffic systems. The IDM is a follow-the-leader model that predicts human driving behavior and has been used extensively to analyze traffic flow patterns. The simplified IDM is described by the following system of equations:

$$\begin{aligned} \dot{x_i} &= v_i \\ \dot{v_i} &= a\left[1 - \left(\frac{v_i}{v_0}\right)^{\delta} - \left(\frac{s^*(v_i, \Delta v_i)}{s}\right)^2\right], \end{aligned} \tag{5.1}$$

where,

$$\begin{aligned} s^*(v_i, \Delta v_i) &= s_0 + T v_i + \tfrac{v_i \Delta v_i}{2\sqrt{ab}}, \\ s &= x_{i-1} - x_i - L_{i-1}, \\ \Delta v_i &= v_i - v_{i-1}, \\ x_i &= \text{position of } i^{th} \text{ vehicle } m, \\ v_i &= \text{velocity of } i^{th} \text{ vehicle } m/s, \\ v_0 &= \text{nominal velocity the vehicle would drive in free traffic } m/s, \\ s_0 &= \text{minimum desired inter-vehicle spacing at zero velocity } m, \\ T &= \text{the time headway in } s, \\ L_i &= \text{vehicle length } m, \\ a &= \text{acceleration } m/s^2, \\ d &= \text{deceleration } m/s^2, \\ \delta &= \text{a design parameter.} \end{aligned}$$

It should be noted that the $i - 1^{th}$ vehicle is defined as the vehicle directly preceding the i^{th} vehicle. The IDM model parameters used in work are shown in table Table 5.1.

As discussed in the threat model (Chapter 3) the stream of vehicles is assumed to be operating at critical density. The benchmark simulation must therefore start at critical density. To achieve this the inter-vehicle separation Δx at steady state must be found. At

Table 5.1: Model parameters of the IDM used throughout this work.

Parameter	Description	typical value
v_0	desired velocity	31.2928 m/s
T	safe time headway	1.6 s
a	maximum acceleration	2 m/s^2
b	maximum deceleration	4 m/s^2
δ	acceleration exponent	4
s_0	jamb distance	2 m
L	vehicle length	5 m

steady state all vehicle accelerations will be zero:

$$\dot{v_i} = a\left[1 - \left(\frac{v_i}{v_0}\right)^{\delta} - \left(\frac{s^*(v_i, \Delta v_i)}{s}\right)^2\right] = 0 \implies$$
$$1 - \left(\frac{v_i}{v_0}\right)^{\delta} - \left(\frac{s^*(v_i, \Delta v_i)}{s}\right)^2 = 0.$$

Now substituting in the expressions for s and s^* from above:

$$1 - \left(\frac{v_i}{v_0}\right)^{\delta} - \left(\frac{s_0 + Tv_i + \frac{v_i \Delta v_i}{2\sqrt{ab}}}{\Delta x - L_{i-1}}\right)^2 = 0$$
$$\frac{s_0 + Tv_i + \frac{v_i \Delta v_i}{2\sqrt{ab}}}{\Delta x - L_{i-1}} = \sqrt{1 - \left(\frac{v_i}{v_0}\right)^{\delta}},$$

$$\Delta x = L_{i-1} + \frac{s_0 + Tv_i + \frac{v_i \Delta v_i}{2\sqrt{ab}}}{\sqrt{1 - \left(\frac{v_i}{v_0}\right)^{\delta}}}. \tag{5.2}$$

At steady state $\Delta v_i = 0$ and Equation (5.2) will further reduce to:

$$\Delta x = L_{i-1} + \frac{s_0 + Tv_i}{\sqrt{1 - \left(\frac{v_i}{v_0}\right)^{\delta}}}. \tag{5.3}$$

By examining Equation (5.3) the IDM model predicts that inter-vehicle separations will increase as $v_i \to v_0$. To simulate steady state critical density a dummy lead vehicle will be used that maintains a constant velocity v_l, this will create an upper bound on the steady state velocity $v_{i_{ss}} \leq v_l$ for all other vehicles. Additionally a value $v_0 > v_l$ will be chosen to avoid division by zero.

Again a system of 100 vehicles has been simulated, with 1 active attacker preceding a passive attacker density of 8%. The system response to the attack was simulated for a total time of 20 minutes. Both attack Scenario 1 and 2 have been simulated against the IDM. The active attacker at position 100 is providing oscillatory input of $5\sin(0.707 * t)$ as before for Scenario 1.

In Figure 5.19 the velocity landscape of attack scenario 1 is shown, the active attackers disturbance is damped out very quickly. Additional figures are not necessary for this scenario as the attack is essentially non existent and fails miserably. The IDM predicts inter-vehicle separation will increase as inter-vehicle velocity increases. Intuitively this makes sense, a human driver would tend to distance their vehicle from wildly oscillating vehicles preceding them.

Figure 5.20 shows a velocity landscape of the system as attack Scenario 2 is being carried out. The regions of high velocity variation correspond with the attacker vehicles. The attacker vehicles are all oscillating at the end of the simulation as can bee seen in Figure 5.22. The victim vehicles however, are relatively unaffected by the attack.

The standard deviation of the victim vehicles can be seen in Figure 5.27. The vehicles are deviating from the desired nominal velocity by approximately $3m/s$, again showing a minimal response the the attack. Additionally Figure 5.28 shows that after 300 seconds an average of 22% of the victim vehicles are deviating from 10% of the nominal velocity. And only 5% of victims are deviating by as much 20% of the nominal velocity.

The magnitude of velocity variation for the groups of victims furthest downstream and upstream are shown in Figure 5.23 and Figure 5.24. While the vehicles toward the rear of this system are operating at higher velocities no saturation has occurred.

Similar results are seen for victim accelerations shown in Figure 5.25 and Figure 5.26. The passive attacker only exerts significant influence upon the first few victims in each group.

This simulation demonstrates that the IDM is resilient in the face of a stability attack. For large velocity differences Equation (5.1) reduces to $-a\left(\frac{v_i \Delta v_i}{2s\sqrt{ab}}\right)^2$ which predicts driving behavior that compensates for velocity differences. Clearly the IDM predicts that a human driver would tend to distance their vehicle from a predecessor that is continually changing their velocity.

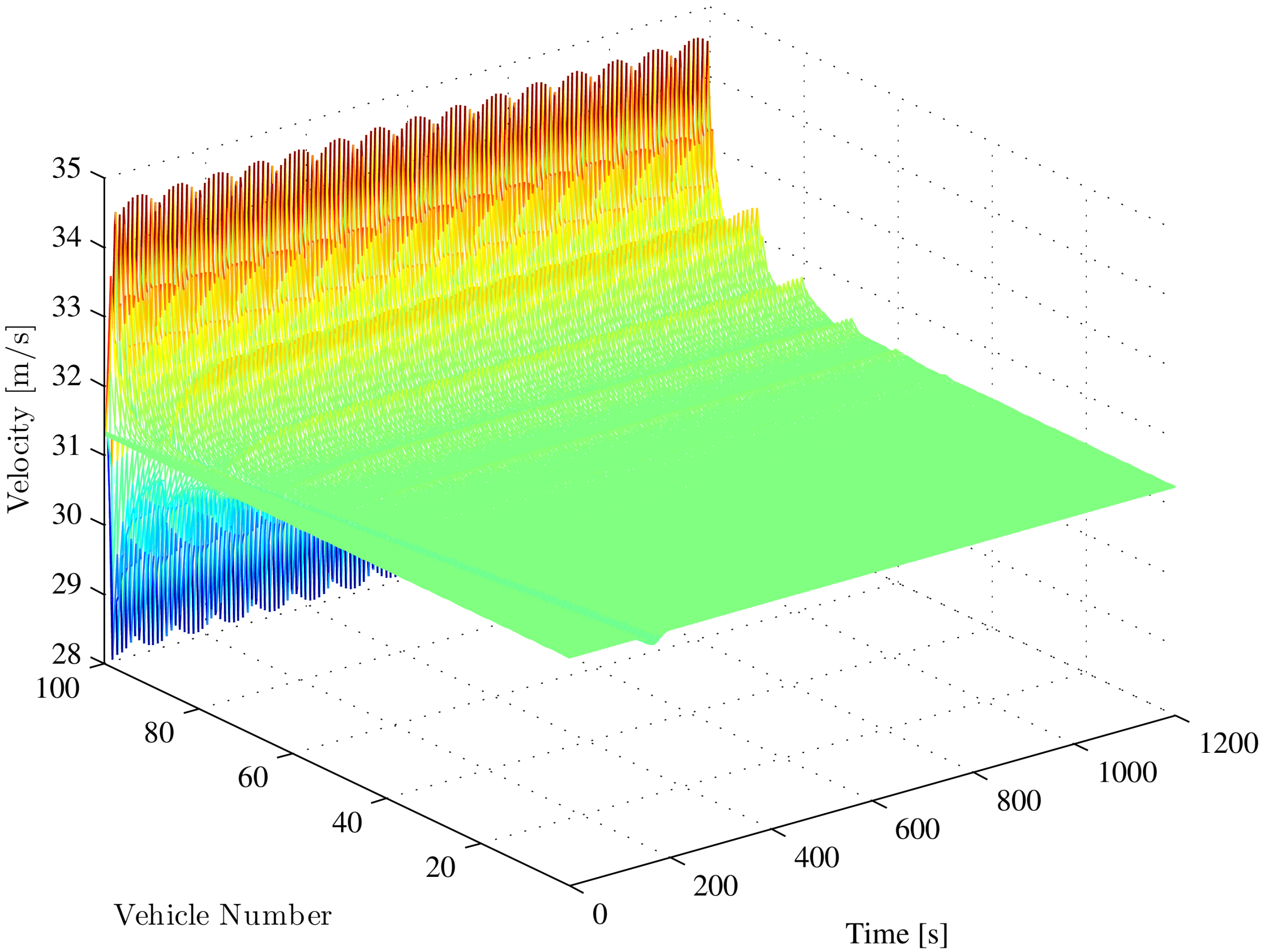


Fig. 5.19: Velocity landscape of the IDM during a simulated attack (attack Scenario 1).

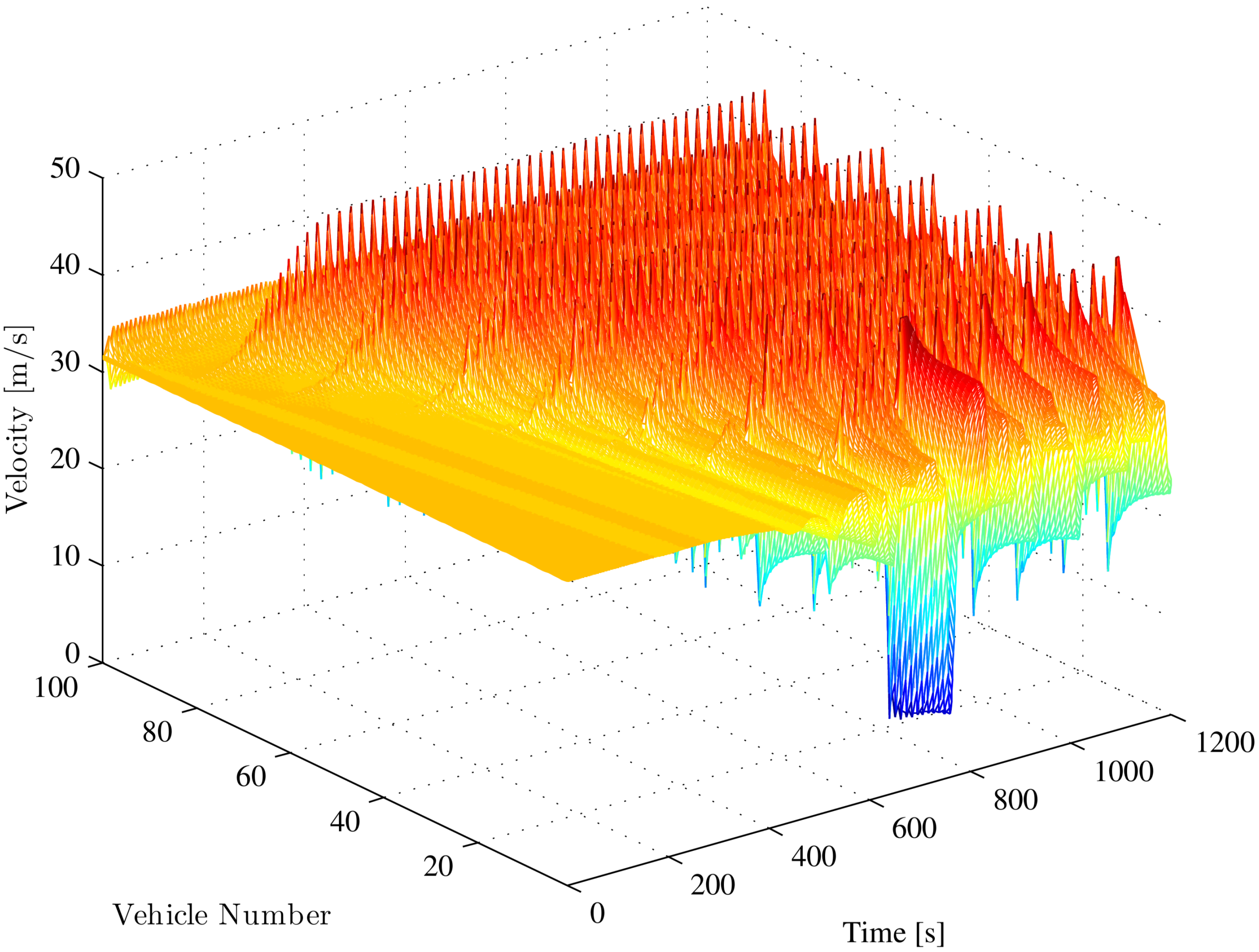


Fig. 5.20: Velocity landscape of the IDM during a simulated attack (attack Scenario 2).

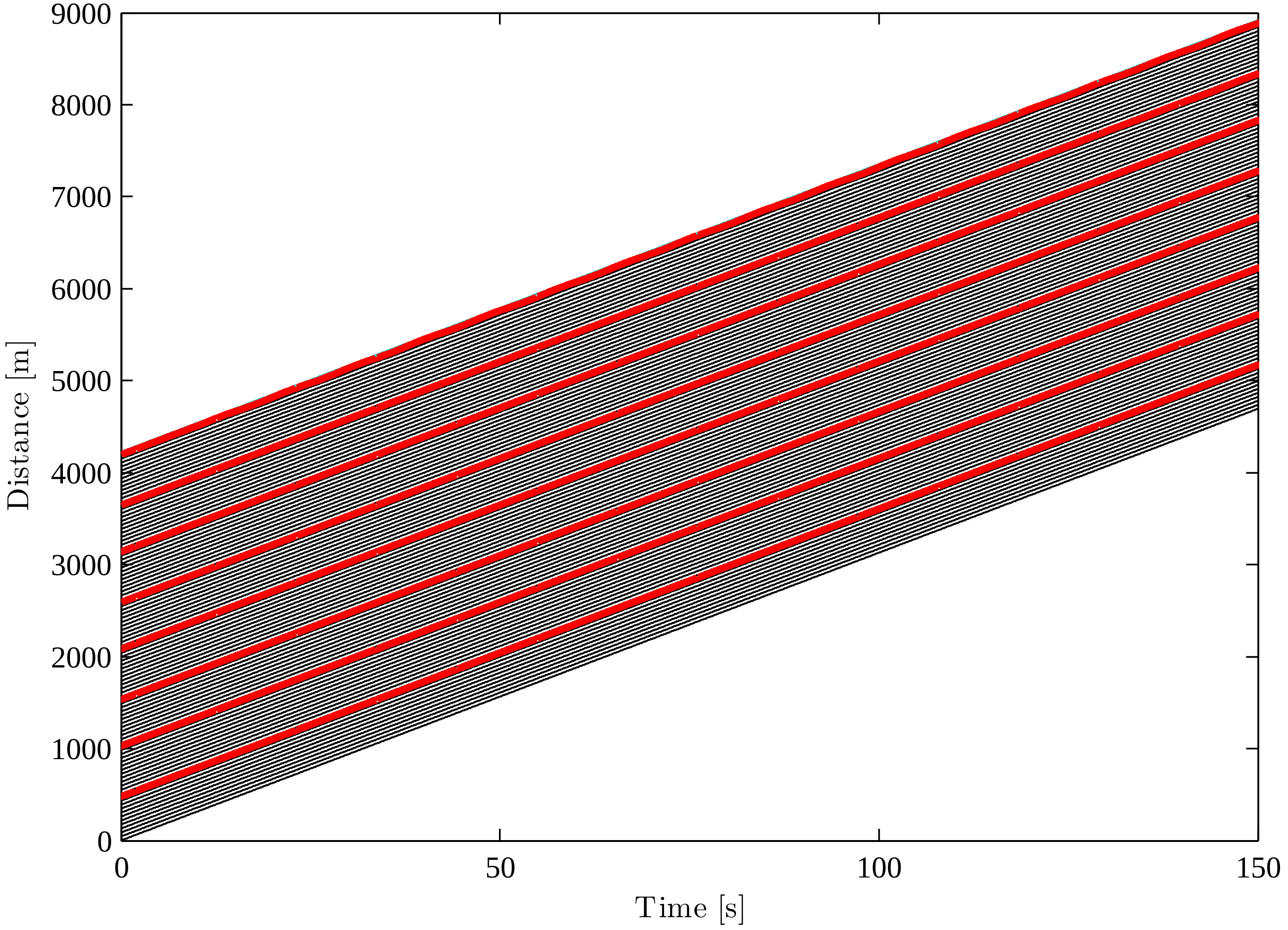


Fig. 5.21: Snapshot of vehicles positions at the beginning of a simulated attack against the IDM (attack Scenario 2).

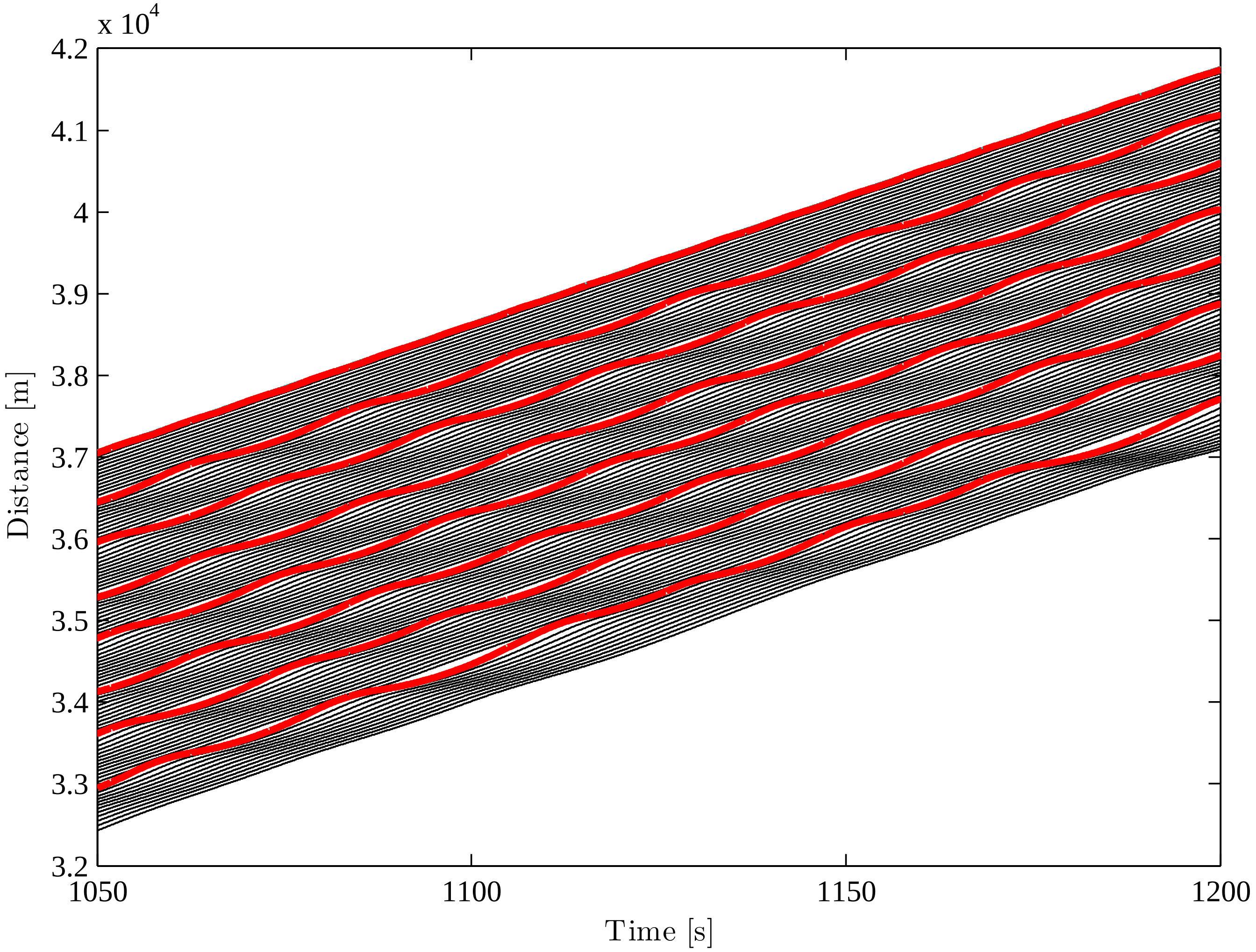


Fig. 5.22: Snapshot of vehicles positions at the end of a simulated attack against the IDM (attack Scenario 2)

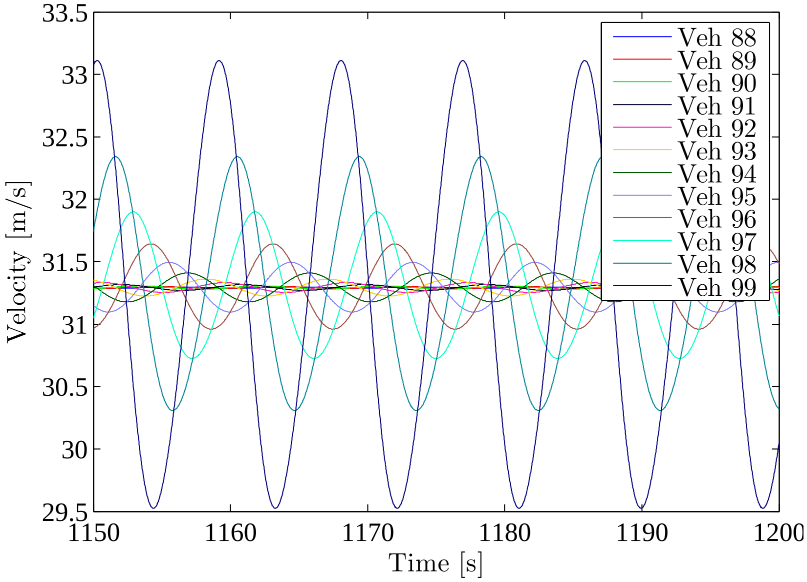


Fig. 5.23: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against IDM, Scenario 2).

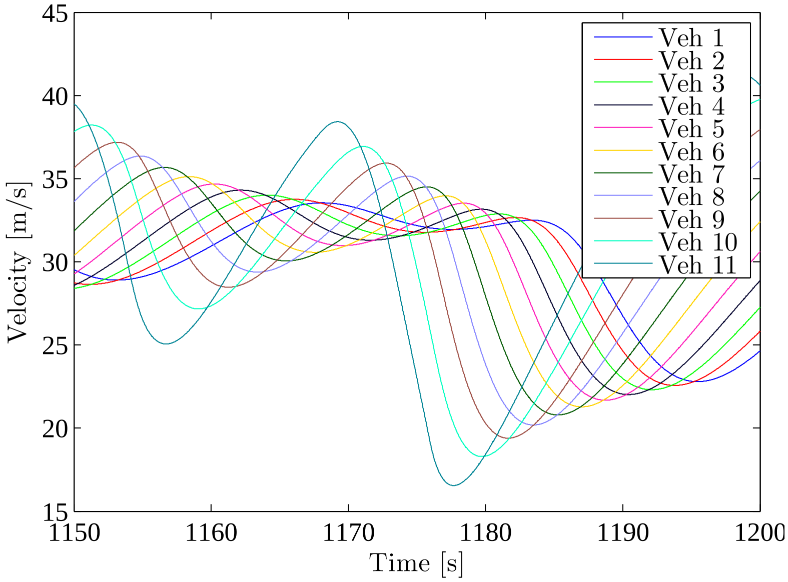


Fig. 5.24: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against IDM, Scenario 2).

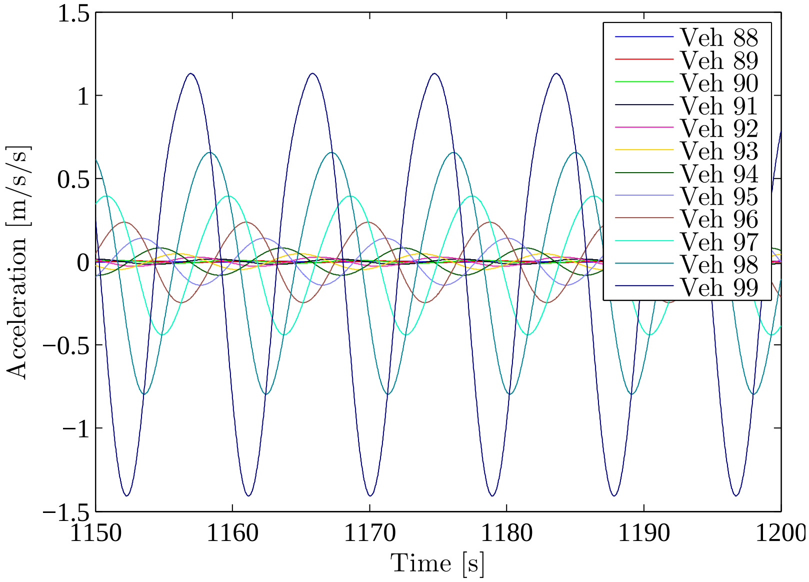


Fig. 5.25: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against IDM, Scenario 2).

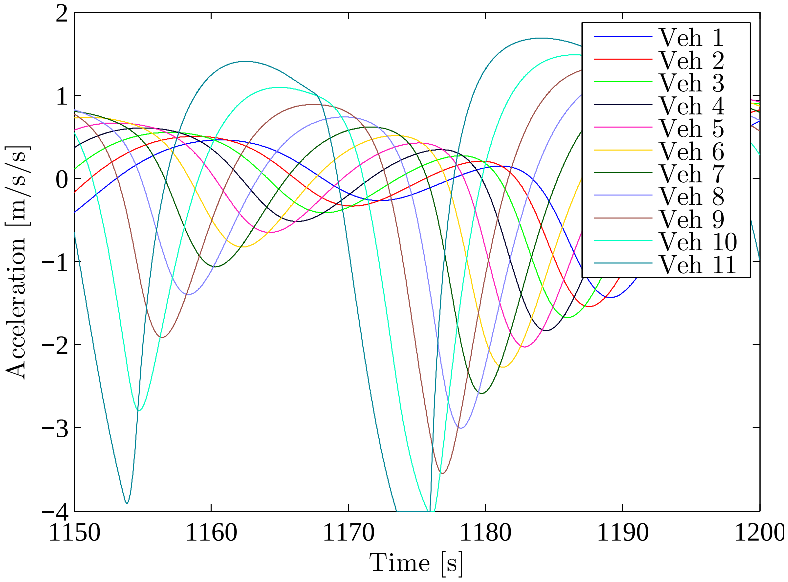


Fig. 5.26: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against IDM, Scenario 2).

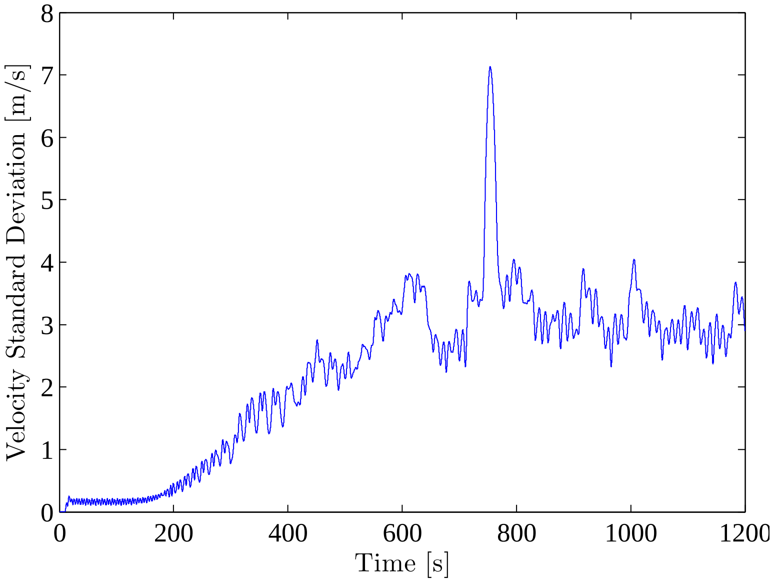


Fig. 5.27: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against the IDM (attack Scenario 2).

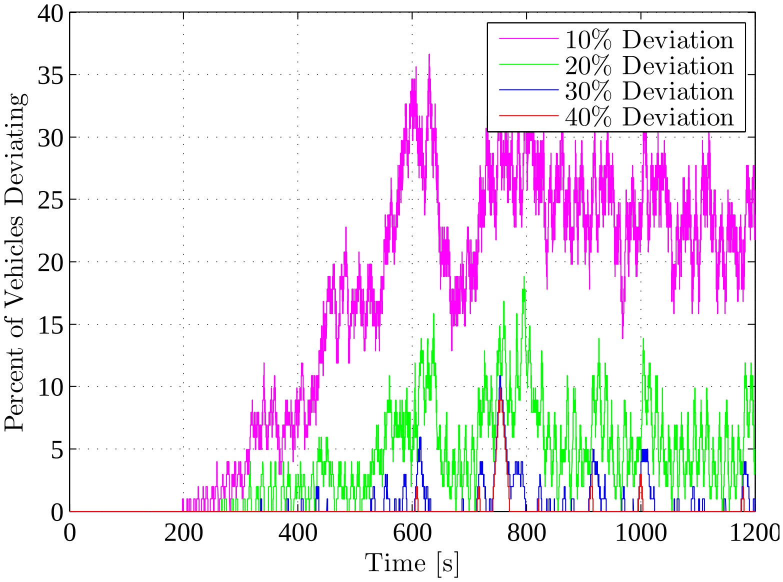


Fig. 5.28: Percentage of victim vehicles deviating from the desired nominal velocity for the duration of the simulated attack against the IDM (attack Scenario 2).

5.3 Simulation Results

The attacks described above have been simulated against Control Algorithms 1-5. All results are for a system of 100 vehicles with an 8% attacker density, the attack is simulated for 20 minutes. Additionally the attacks have been simulated against the IDM to present a benchmark for human driver behavior versus the automated system. For each case Control Algorithm 1 was used for the attacker vehicles. Acceleration and velocity saturation constraints have been implemented in all simulated results.

To begin the attack, all attackers gains are switched to either attack Scenario 1 or 2. The system is then perturbed by the active attacker who either provides a continual sinusoidal input for attack Scenario 1, where stable but string unstable gains are used, or performs an aggressive braking maneuver decelerating at $-4m/s$ for a period of 10 seconds for attack Scenario 2 where unstable gains are chosen.

A comparison of the simulation results for attack Scenario 1 is given in Table 5.2. The initial steady state inter-vehicle spacing is shown for each Control Algorithm for both attacker and victim vehicles. For each automated case the initial spacing is much smaller than the safe recommended following distance for a human driver. Two initial spacing scenarios are given for the IDM, the first is a larger safe following distance, the second is much smaller distance similar to the automated systems to provide a better comparison of results.

The highway utilization in vehicles per kilometer is also given. For Control Algorithms 1 and 2 this metric remains essentially the same from the beginning to end of the simulated attack. However, the standard deviation and percentage of vehicles deviating from the desired nominal velocity provides additional understanding of how the system reacts to an attack. Greater deviations indicate the attack will be more devastating against Control Algorithm 2 than 1, for instance. The combination of initial-inter vehicle spacing, highway utilization, standard deviation, and vehicle deviation from desired nominal velocity, provides a good overall picture of the effectiveness of the attack.

Referring to Appendix A, Appendix B, Appendix C, and Appendix D. Figures for the simulated attacks against Control Algorithm 2, Control Algorithm 3, Control Algorithm 4, and Control Algorithm 5, respectively, can be found. Referencing these figures it appears that some of the control laws begin to recover toward the end of the simulation period. This is misleading however. By examining the position plots it is apparent that collisions have occurred near the beginning of the attack as the instability is building. For the purposes of this work collisions have been ignored, instead the intent is to demonstrate the magnitude of chaos that can be achieved. In a physical system the traffic flow would come to a standstill in the event even a single collision has occurred.

Clearly the automated systems do not perform well under the proposed attacks. Overall the most resilient automated law is Control Algorithm 1. Only 8% of the vehicles are deviating significantly from the nominal velocity, and vehicle density is essentially the same from the beginning to end of the simulation. But if strictly negative gains are chosen for the attackers this system will become unstable as demonstrated in Section 5.1.2. The other control laws fail miserably under attack. It is clear that even attack Scenario 1 is devastating for Control Algorithms 2 - 5, forcing the victims into a never ending cycle of aggressive braking and acceleration. If attack Scenario 2 is employed the results will only be more devastating, with a high likelihood of collisions as shown in Section 5.1.2.

As illustrated in Section 5.2, and further demonstrated in Table 5.2, the IDM is resilient to the proposed attacks. Not only does the highway utilization remain the same during the simulated attack, but the victim vehicles do not deviate significantly from the desired nominal velocity. The IDM predicts these two attacks will not be affective against a human driver, whereas it is clear that the attacks have devastating results against the automated system. In short the act of automating vehicles introduces new venerabilities.

Table 5.2: Results of attack Scenario 1 against Control Algorithms 1-5 and the IDM.

Control Algorithm	Initial Inter-Vehicle Spacing [m]		Highway Utilization [Vehicles per km]		Victim STD [m/s] @>400 sec	Percentage of Vehicles Deviating From Nominal Velocity @>400 sec			
	Attacker	Victim	Start of Sim	End of Sim		10% Dev.	20% Dev.	30% Dev.	40 Dev.
1	31.29	31.29	32.27	31.58	1.1	7.9%	3.96%	.9%	0%
2	31.29	17.21	55.01	53.55	3.4	26.7%	10.9%	2%	0%
3	31.29	15	61.95	52.26	5.9	43.6%	25.7%	18.8%	13.9%
4	31.29	25.34	39.12	22.81	9.8	45.5%	39.6%	34.7%	29.7%
5	31.29	22.65	43.27	31.84	11.67	62.4%	52.4%	42.6%	35.6%
IDM 1.6 s Hdwy	31.29	64.73	16.27	16.27	0.09	0%	0%	0%	0%
IDM 0.8 s Hdwy	31.29	36.01	28.49	28.42	0.19	0%	0%	0%	0%

Chapter 6
Experimental Validation

The following sections detail the design and implementation of a physical system on which to test theoretical automated vehicle control laws. This testing and development platform consists of automated vehicles that are approximately $1/10^{th}$ full scale. The test platform will be used to validate the attack scenarios discussed in this work. The objective of this implementation is to bring attention to the potential flaws in AHS proposed by industry and academia by physically demonstrating conditions that will cause instability in a platoon.

High level platoon operation will not be discussed in detail here, instead the low level controller necessary to maintain longitudinal vehicle stability will be designed. Additionally the hardware and software design considerations for this project are documented here.

6.1 Vehicle Hardware Platform

The vehicles chosen for this project (Figure 6.1) are differential steer with two 4 inch diameter wheels on each side. Each vehicle has two DC motors, each motor drives two wheels on one side of the vehicle. The motors are driven by a two channel motor controller that accepts PWM input signals. The duty cycle of this signal will be the output from the low level longitudinal controller which is implemented discretely in the C coding language.

There are two vehicle configurations. The standard configuration corresponding to a victim vehicle, has lower acceleration and velocity capabilities (Table 6.1). The enhanced configuration has greater acceleration and velocity capabilities (Table 6.2), and will be used as attackers in the system. Eight standard configurations vehicle will be assembled, and two enhanced vehicles.

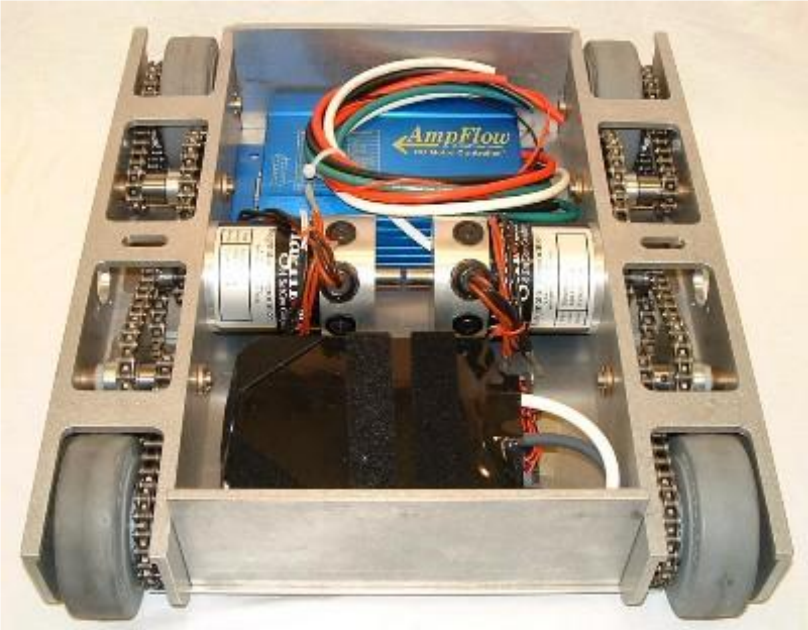


Fig. 6.1: Light Weight Battle Kit [35].

Table 6.1: Specifications of standard vehicle.

Standard Vehicle Configuration [35]
Light weight kit Length: 45 cm Width: 39.6 cm Weight: 22.7 kg (including motors, controller, and 3 batteries)
Gear ratio 3.4 (high speed ratio) Wheel diameter 10.13 cm (4in) (measured circumference 31.8 cm)
System voltage 36V (3 – 12V sealed lead acid (SLA) batteries in series)
2 – E30-150 AmpFlow motors AmpFlow 160 motor controller
Differential steer
Average acceleration 7.8 m/s^2 Theoretical top speed 13.32 m/s (29.8 mph)

Table 6.2: Specifications of enhanced vehicle.

Enhanced Vehicle Configuration [35]
Light weight kit Dimensions and weight same as standard configuration
Gear ratio 3.4 (high speed ratio) Wheel diameter 12.7 cm (5in)
System voltage 36V (3 – 12V sealed lead acid (SLA) batteries in series)
2 – F30-150 AmpFlow motors AmpFlow 160 motor controller
Differential steer
Average acceleration 10.0 m/s^2 Theoretical top speed 20.21 m/s (45.2 mph)

6.2 High Level System Architecture

A high level view of the system architecture is shown in Figure 6.2. The different subsystems that have been implemented are shown, in addition to the flow of data between functional blocks.

The longitudinal control laws are implemented on a Texas Instruments EK-TM4C123GXL ARM Cortex M4F micro-controller. There is one micro-controller aboard each vehicle running with a clock frequency of 20MHz. The following resources of the micro-controller have been used to implement this project:

- Pulse Width Modulation (PWM) modules 0 and 1
- I2C module 0
- Quadrature Encoder Input (QEI) modules 0 and 1
- UART modules 0 and 1
- GPIO ports for TTL input and output

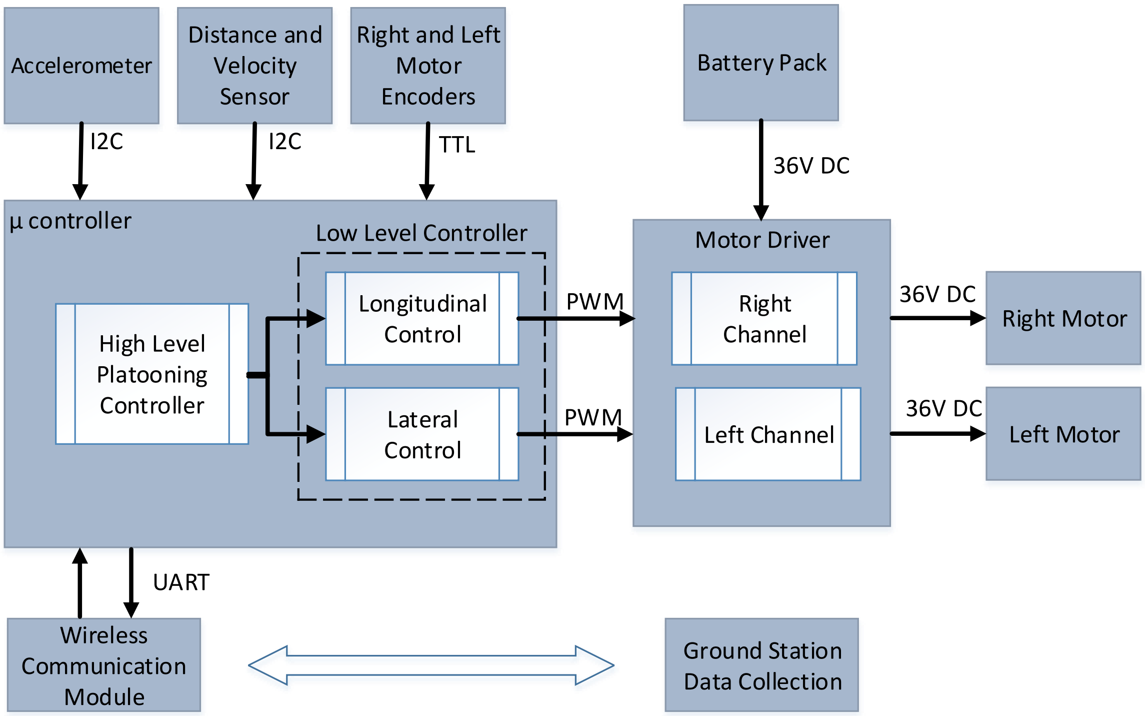


Fig. 6.2: Top level view of vehicle system architecture. The interaction between individual subsystems is shown, in addition to data flow between subsystems.

The lead vehicle can be commanded by an operator via 2.4GHz radio transmitted command signals, or operated using pre-simulated acceleration requirements that are remotely uploaded. Each vehicle after the lead vehicle (follower vehicles) will run in a completely automated mode similar to a vehicle equipped with ACC or CACC. Each follower vehicle will track the vehicle directly in front of it. The follower vehicles will maintain an inter-vehicle separation from the preceding vehicle according to its high level control law. The vehicle platoon must be able to travel in excess of 20 mph while maintaining the proper inter-vehicle spacing as well as maintain stability as the platoon accelerates and decelerates.

Sensors

A variety of sensors are used for this project. These sensors provide the feedback necessary to implement control schemes to maintain desired inter-vehicle separations and velocities.

Range sensors are used to measure the relative distances and velocities between vehicles. Additionally the actual velocity of individual each vehicle will be measured utilizing quadrature encoders. These state variables are the main feedback to the high and low level control schemes. Real-time data is collected from each vehicle using wireless communication and is used to create plots of the real time performance of the controllers aboard each vehicle as well as the interaction between vehicles.

- Lidar range finder provides inter-vehicle separation distance and relative velocity between vehicles.
- Encoders, provide velocity of left and right wheel pairs, and an estimate of cumulative distance traveled.
- Ultrasonic (optional), provides inter-vehicle separation distance. The difference between subsequent sensor readings can be used to estimate relative velocity between vehicles.
- Radar (optional), Doppler shift is used to calculate the relative velocity between vehicles.
- Accelerometer, provides acceleration in X, Y, Z directions. The acceleration can be integrated to give estimates of velocity for short time durations.
- XBee, provides wireless communication based on the IEEE 802.15.4 protocol.

Table 6.3: Sensors used for experimental vehicle platform.

Sensor	Manufacturer	Part No.
Lidar	Pulsed Light	LL-905PIN-01
Encoders	US Digital	E2-500-375-IE-D-G-B
Ultrasonic	PARALLAX INC.	PING #28015
Accelerometer	DFROBOT	SEN0032
XBee	Digi International	XBP24BZ7SIT-004

6.3 Low Level Longitudinal Control Scheme

This work is focused on examining the longitudinal characteristics of AHS and inter-vehicle stability. Therefore, the lateral dynamics are neglected. For this work, this is accomplished by running the vehicles on a cable system, thus restraining them to longitudinal motion only.

In order for a particular vehicle to track the preceding vehicle it must accelerate and decelerate to achieve the desired inter-vehicle separation and velocity. The automated control schemes discussed in previous chapters are designed to calculate this acceleration requirement. They are commonly referred to as high level controllers. The high level controllers job is to maintain a safe orientation with respect to surrounding vehicles.

To achieve the desired acceleration response a low level controller must be implemented aboard each vehicle. The low level controller interacts with a particular vehicles mechanics to produce acceleration. The relationship between these two levels of control is shown in Figure 6.3. The input to the high level control is a safe time headway in addition to: inter-vehicle distance Δd and velocity Δv measured with respect to the preceding vehicle, and the vehicles own velocity v. A desired acceleration requirement is calculated based on these states and fed as the input to the low level controller. The low level controller also uses velocity feedback to then calculate an actuator requirement. For the physical vehicles presented here this is a PWM reference to the DC motor controller.

6.3.1 Vehicle Model

To design the low level longitudinal controller a mathematical model and transfer function of the longitudinal vehicle dynamics is required.

As mentioned above the vehicles implemented for this project are driven by electric motors. Each vehicle has a pair of DC motors that drive the right and left set of wheels respectively. By uniformly varying the angular velocity of the motors the vehicle can be made to drive a straight trajectory. The vehicles can be rotated by non-uniformly varying the motor velocities with respect to each other. A kinematic model such as that given by

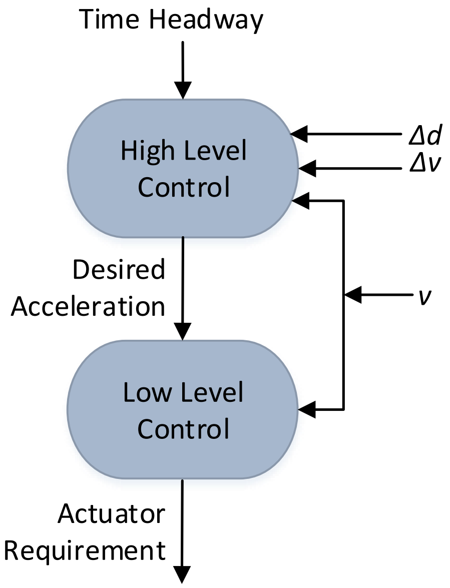


Fig. 6.3: Structure of longitudinal control schemes.

Rajamani [15] can be utilized to represent the motion of the vehicle:

$$\begin{aligned} \dot{x} &= vcos(\psi) \\ \dot{y} &= vsin(\psi) \\ \dot{\psi} &= \frac{v}{r}. \end{aligned} \tag{6.1}$$

Referring to Figure 6.4, the angle ψ is the heading angle in the inertial frame, the velocity v of the vehicle is considered an input to the system. The rate of change in the x and y directions is trigonometrically related to ψ and linearly related to v. The rate of change of ψ is linearly related to v and inversely proportional to the turn radius r which is defined from the center of the vehicle wheel base to the center of the turn, reference point O.

For this work the vehicles are assumed to be operating on a straight section of highway with no lane changes. The longitudinal motion of the vehicle will be examined by neglecting lateral motion and dynamics. The model of Equation (6.1) can therefore be simplified by setting the heading angle $\psi = 0$. Consequently the heading rate of change $\dot{\psi} = 0$ as well.

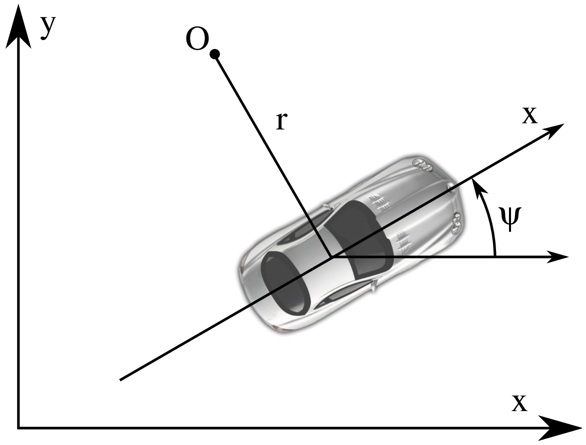


Fig. 6.4: Kinematic relationship of vehicle dynamics in inertial coordinate frame.

The longitudinal model of the reduced system is:

$$\dot{x} = v. \tag{6.2}$$

The velocity v will now be considered a state of the system. The rate of change in velocity $\dot{v}$ will be driven by an unknown input u which is scaled by parameter α minus system damping represented by parameter β multiplied by the vehicle velocity:

$$\begin{aligned} \dot{x} &= v \\ \dot{v} &= \alpha u - \beta v. \end{aligned} \tag{6.3}$$

As discussed previously the vehicle velocity is a consequence of the two DC electric motors. The velocity of the vehicle can be by determined by modeling these motors. Equations of motion for a motor can be obtained using a method similar to that described by Özgüner [36]. Using simple circuit analysis on the model of Figure 6.5 and Newtonian physics:

$$\begin{aligned} V_{eq} &= R_a I_a + L\dot{I}_a + V_a \\ T_a &= J_a \dot{\omega}_a + N J_L \dot{\omega}_L, \end{aligned} \tag{6.4}$$

where,

V_{eq} = voltage input to motor,

T_a = torque at motor shaft,

I_a = motor armature current,

R_a = motor armature resistance,

L_a = motor armature inductance,

J_a = motor armature inertia,

N = gear reduction to vehicle wheels,

J_L = inertia of load,

ω_a = angular velocity of motor shaft,

ω_L = angular velocity at vehicle wheels.

The following relationships are utilized to couple the differential equations of motion:

$$\begin{aligned} V_a &= K_T \omega_a \\ T_a &= K_T I \\ \omega_a &= N \omega_L, \end{aligned} \tag{6.5}$$

where K_T is the back EMF constant of the motor which in SI units is also equivalent to the motor torque constant.

For this work the armature inductance and inertia will be neglected. These parameters contribute to the electrical time constant of the model which is typically much quicker than the mechanical time constant which will dominate the system response. Additionally the

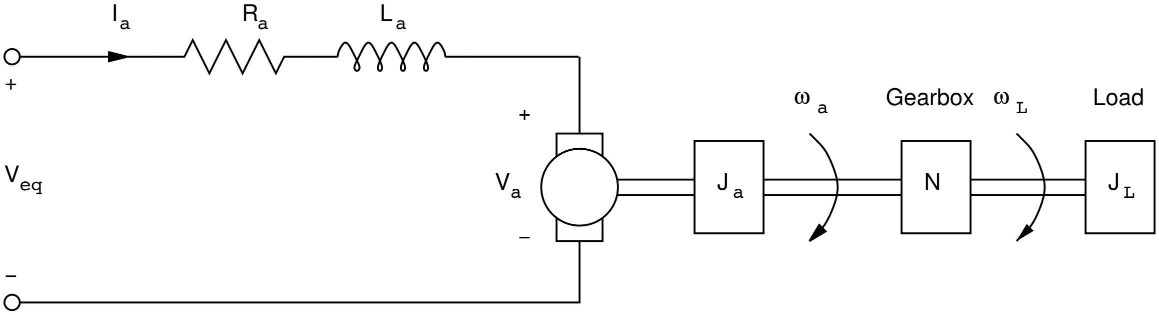


Fig. 6.5: Model of DC electric motor driving a load [36].

equivalent input voltage to the system is defined as the input u of Equation (6.3):

$$\begin{aligned} V_{eq} &= \frac{R_a J_L}{K_T}\dot{\omega}_a + K_T \omega_a \\ u &= V_{eq}. \end{aligned} \tag{6.6}$$

The coupled differential equation can equivalently be represented as a Laplace domain transfer function with input $u(s)$ and output $\omega_a(s)$:

$$\frac{\omega_a(s)}{u(s)} = \frac{\frac{1}{K_T}}{\frac{R_a J_L}{K_T^2}s + 1}. \tag{6.7}$$

The linear velocity at the vehicle wheels is related to the angular velocity of the motor shaft by the following equation, where r_{wheel} is the radius of the vehicle wheels:

$$v(s) = \frac{\omega_a(s)}{N r_{wheel}}.$$

6.3.2 Experimentally Determined Parameters

The input output transfer function of the vehicle takes on the form of a generic first order system:

$$\frac{v(s)}{u(s)} = \frac{K_0}{\tau s + 1}, \tag{6.8}$$

where the gain K_0 and time constant τ can be determined experimentally based off techniques from classical control theory. This system is of the same form as the model predicted by Equation (6.3). By transforming Equation (6.3) into Laplace domain the relationship between parameters becomes apparent:

$$\begin{aligned} \frac{v(s)}{u(s)} &= \frac{\frac{\alpha}{\beta}}{\frac{1}{\beta}s + 1} \\ \alpha &= \beta K_0 \\ \beta &= \frac{1}{\tau}. \end{aligned} \tag{6.9}$$

Velocity data was collected from a vehicle in response to various voltage step inputs and is shown in Figure 6.6. The steady state velocity corresponding to each voltage input and the time corresponding to 63.2% of the steady state values have been compiled in Table 6.4.

The input and output have a linear relationship as can be seen in Figure 6.7. The gain K_0 is estimated by dividing the steady state velocity by the corresponding voltage input. The time constant τ is found by subtracting the time corresponding to the commanded step input from the time value of the system response at 63.2% of the steady state velocity. The parameters α and β of the physical system can now be estimated:

$$\begin{aligned} \frac{v(s)}{u(s)} &\approx \frac{0.317}{0.37s+1} \\ \alpha &\approx 0.857 \\ \beta &\approx 2.7 \end{aligned} \tag{6.10}$$

These parameters provide a reasonable estimate of the system response as shown in Figure 6.8.

Table 6.4: Velocity output response to voltage step input

$u(s)$ [Volts]	$v(s)$ Steady State [m/s]	Input Start Time [s]	63.2% Rise Time [s]
2.4	0.702	2.25	2.61
4.9	1.51	2.25	2.58
7.9	2.51	2.25	2.61
11.4	3.62	2.25	2.62

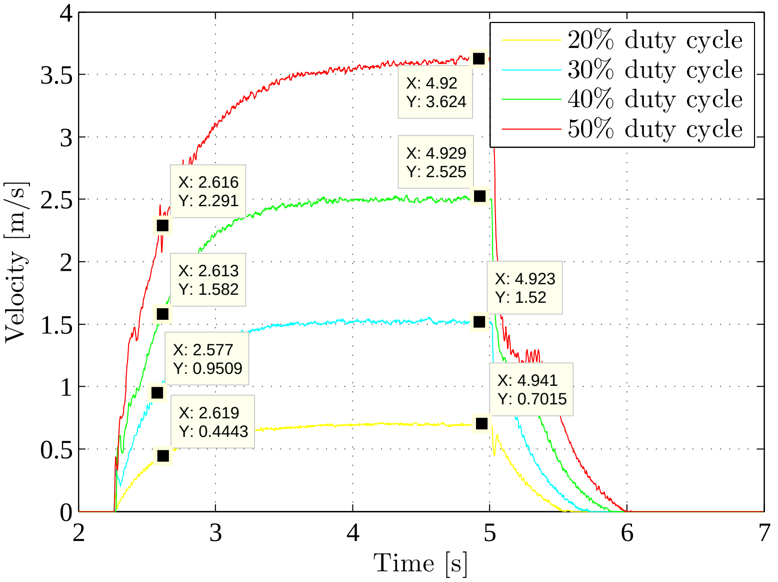


Fig. 6.6: Vehicle response to voltage step input.

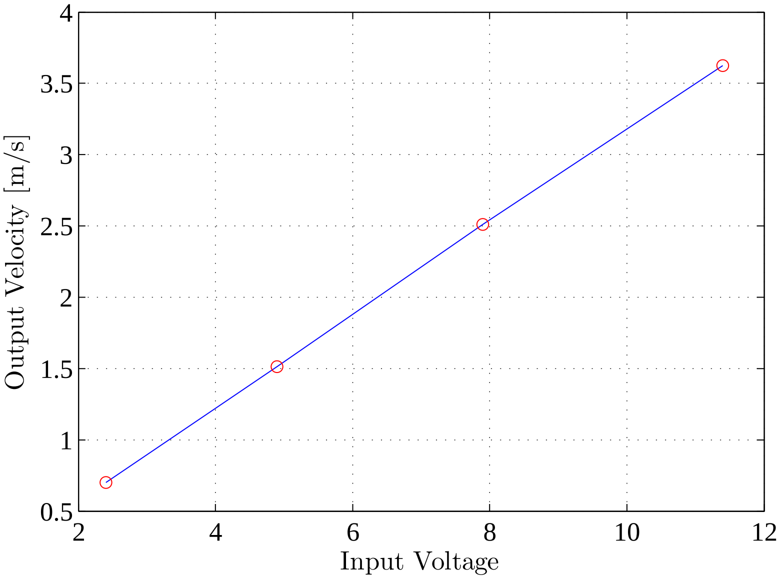


Fig. 6.7: Linear relationship between input and output.

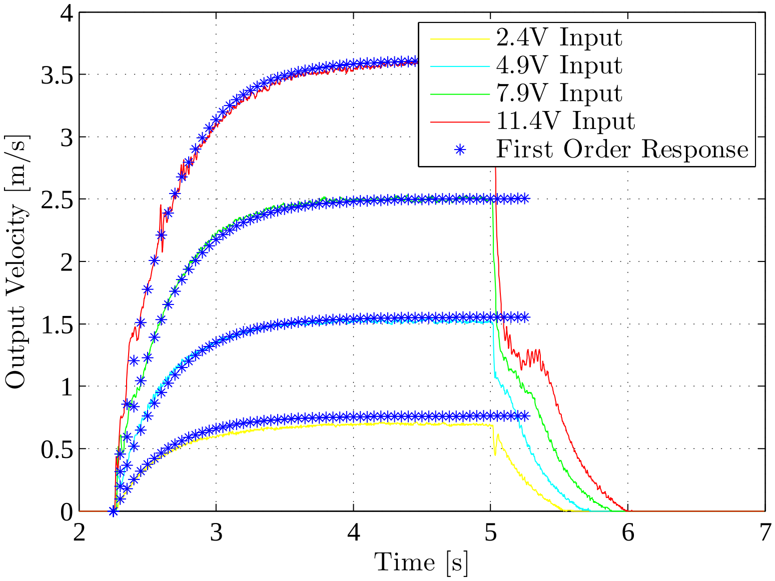


Fig. 6.8: Estimated first order response versus actual response.

6.3.3 Low Level Control

The desired low level control effort can now be formulated. By rearranging Equation (6.3) and using the experimentally determined values for α and β the control effort is as follows:

$$u = V_{eq} = \frac{\dot{v} + \beta v}{\alpha}, \tag{6.11}$$

where the acceleration requirement $\dot{v}$ is the output of the high level controller. The low level controller relies on velocity feedback due to the v term in the numerator of the expression. As previously discussed $u = V_{eq}$ which is the average of the PWM output of the AmpFlow 160 motor controller. To implement the low level controller in code the relationship between the supply voltage of the battery and V_{eq} may be expressed by the following linear expression:

$$V_s T_{on} = V_{eq} T_{sw}, \tag{6.12}$$

where,

V_s = the supply voltage (+36V nominal),

T_{on} = pulse duration,

V_{eq} = the average (equivalent) voltage seen by the motor,

T_{sw} = the switching period of the PWM signal (300Hz).

The duty cycle (DC) of the PWM signal is expressed as $DC = \frac{T_{on}}{T_{sw}}$. Rearranging Equation (6.12) the duty cycle required to achieve the desired acceleration requirement is:

$$DC = \frac{V_{eq}}{V_s}. \tag{6.13}$$

The desired voltage at the motor will first be calculated using Equation (6.11) and then realized by setting the duty cycle of the motor controller PWM output reference via the micro-controller.

6.4 Results of Experimental Validation

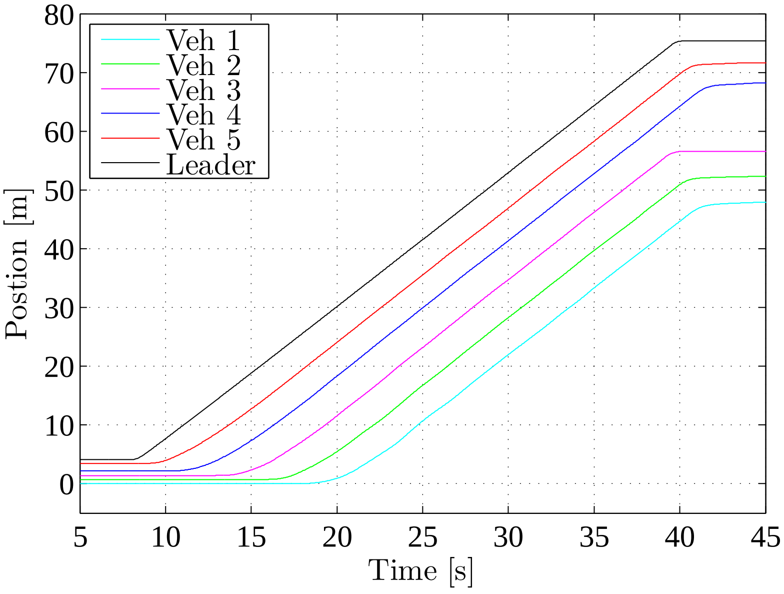
Referring to Figure 6.9 a physical implementation of Control Algorithm 1 utilizing stable gains, $h = 0.5,\ k_p = 1,\ k_d = 2$ is demonstrated. The leader accelerates to a constant velocity and the vehicles which were at a random initial spacing settle into steady state while maintaining inter-vehicle spacing requirements. The system is string stable, the variations in velocity (Figure 6.9(b)) are due to sensor and environmental noise.

Experimental data has been collected for a system under attack as shown in Figure 6.10. The attacker located at position 5 has string unstable gains $h = 0.5,\ k_p = 1.5, k_p = -0.6$, the victim vehicles gains remain the same as the first case. The system is allowed to reach steady state before the attack is initiated. The system overall remains string stable due to the damping of victim vehicles. The attack dies out by vehicle 3, and referring to Figure 6.10(b) vehicle 4's velocity error is decreasing toward the end of the data set.

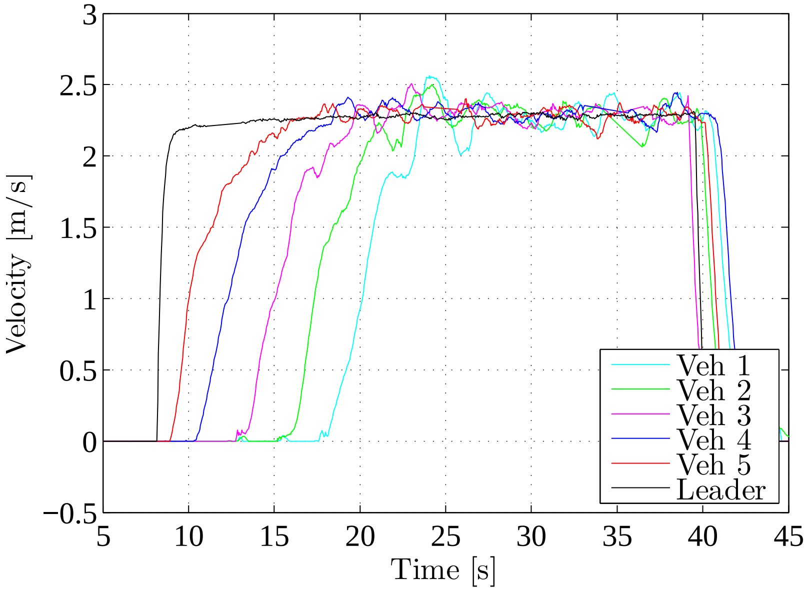
The physical system demonstrates the same characteristics as predicted in the theoretical work. This platform provides a relatively low cost method of testing control schemes compared to a full scale vehicle implementation, allowing a variety of control methods to be easily verified.

Large traffic systems have been simulated in this work. To perform an experimental validation of the proposed attacks a piecewise validation can be used. An initial experiment will be performed on a subsystem where the first attacker and victim vehicles are interacting. Real time data will be collected from the vehicle states, such as actual velocity and acceleration, relative velocity and position, and actual position. The data points from the rearmost vehicle can then be used as an input to the leader in a new experimental run. By repeating this procedure iteratively the interaction of large systems can be simulated with the 10 vehicle platoon.

Figure 6.11 shows the assembled vehicles used to perform the physical validation.

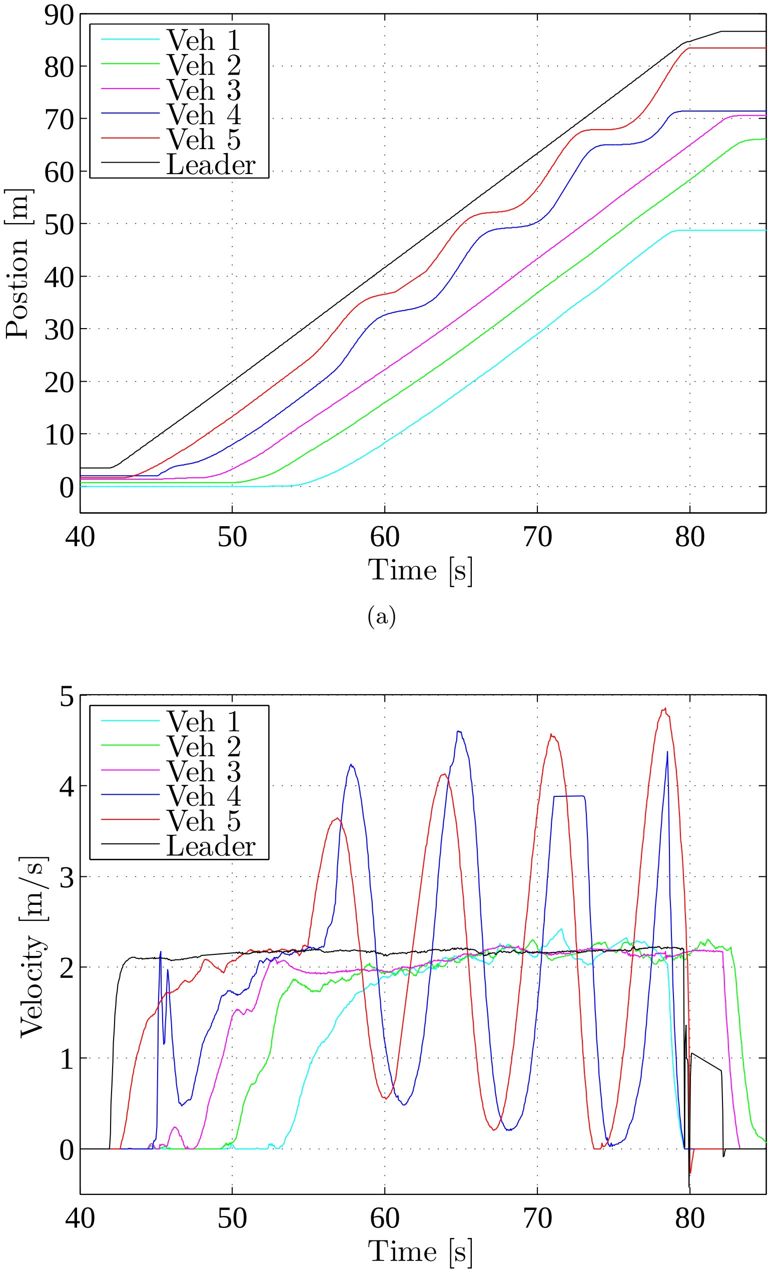


(a)



(b)

Fig. 6.9: A physical system of 6 vehicles using Control Algorithm 1 and stable gains. (a) Positions. (b) Velocities.



(a)

(b)

Fig. 6.10: A physical system of 6 vehicles using Control Algorithm 1 with active attacker at location 5. (a) Positions. (b) Velocities.

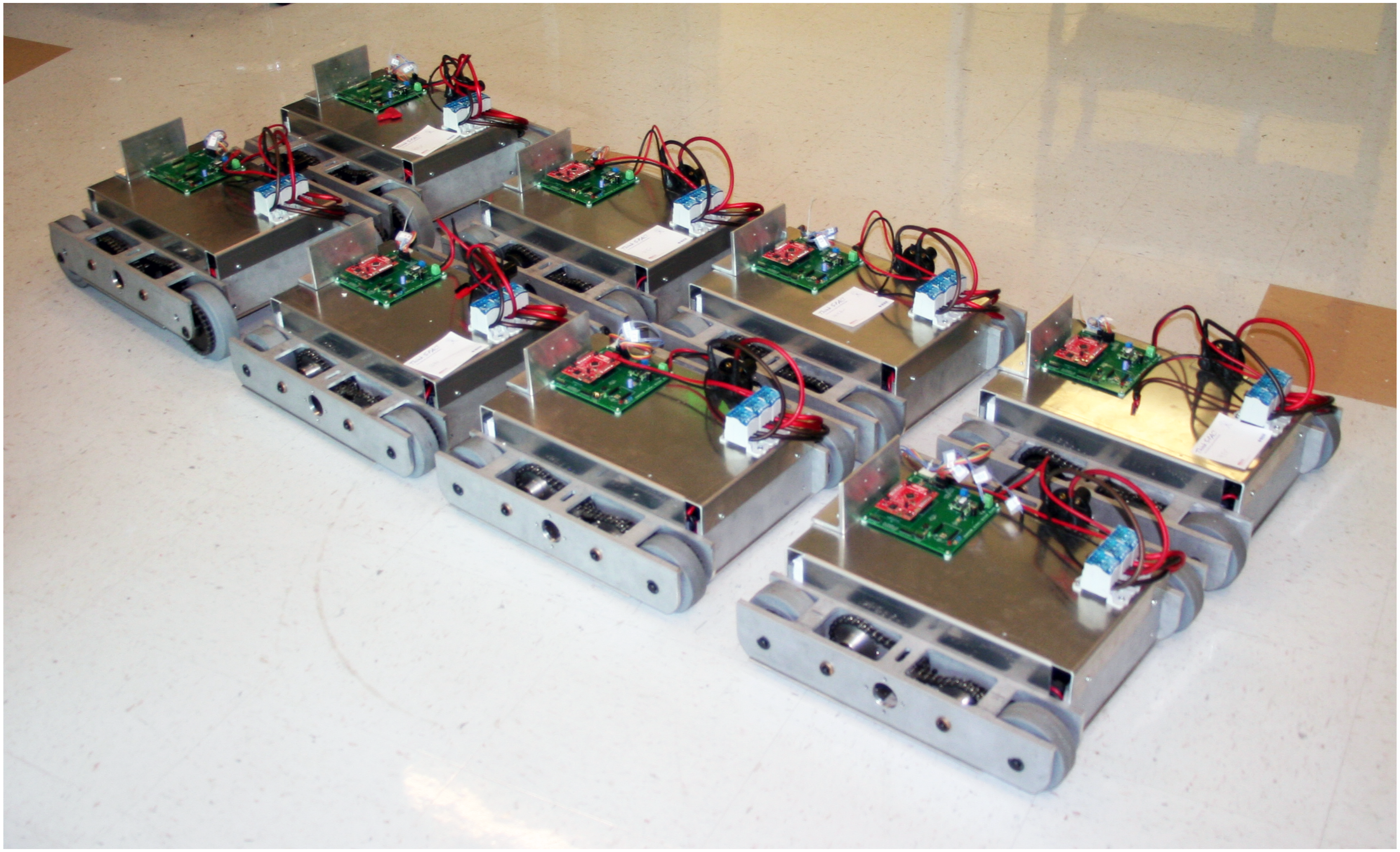


Fig. 6.11: Experimental vehicle platform developed for physical testing and validation.

Chapter 7

Conclusion and Future Work

In this work a variety of proposed control laws have been drawn from the existing literature. These laws were selected to cover a broad spectrum of proposed control methods that display traits desirable to the vehicle automation community.

Using these various control laws it has been shown that a density of attackers with modified gains can destabilize large traffic systems of automated vehicles using ACC or CACC control schemes. A proof was developed demonstrating a heterogeneous traffic system consisting of automated vehicles utilizing a mixture of control laws can be destabilized in an adversarial environment. An attack was proposed using an active attacker and a density of passive attackers, whom might be unknowingly participating in a malicious scheme to destabilize the traffic system. The attack was then successfully carried out in simulation against heterogeneous traffic systems.

The concept of local versus global string instability was developed to analyze the results of this attack which was demonstrated not only in simulation but against a system of physical vehicles. Additionally it has been shown that simply increasing the victim gains is not sufficient to mitigate the proposed attack, but in fact makes the victim vehicles venerable to oscillation over a greater range of frequencies. This work demonstrates the necessity of considering the presence of adversarial vehicles when designing future automated solutions.

Future work will focus on designing countermeasures to mitigate the effects of stability attacks. Denial of service attacks will be investigated and their effectiveness against proposed solutions such as CACC that rely on wireless communication to maintain stability. Furthermore, the authors desire is to endeavor to advance the current field of knowledge to the point that controllers may be designed that actively detect an attack and adjust dynamically to maintain stability or at a minimum reduce collateral damage to the system.

References

[1] W. F. Powers and P. R. Nicastri, “Automotive vehicle control challenges in the 21st century,” *Control Engineering Practice*, vol. 8, no. 6, pp. 605–618, 2000.

[2] J. Sousanis, “World Vehicle Population Tops 1 Billion Units,” 2011.

[3] D. L. Schrank and T. J. Lomax, *The 2007 urban mobility report.* Texas Transportation Institute, Texas A & M University, 2007.

[4] S. E. Shladover, “The California PATH Program of IVHS research and its approach to vehicle-highway automation,” in *Intelligent Vehicles' 92 Symposium., Proceedings of the.* IEEE, 1992, pp. 347–352.

[5] T. Trimble, R. Bishop, J. Morgan, and M. Blanco, “Human factors evaluation of level 2 and level 3 automated driving concepts: Past research, state of automation technology, and emerging system concepts,” National Highway Traffic Safety Administration, Washington, DC, Tech. Rep. DOT HS 812 043, jul 20014.

[6] R. Rajamani and C. Zhu, “Semi-autonomous adaptive cruise control systems,” *Vehicular Technology, IEEE Transactions on*, vol. 51, no. 5, pp. 1186–1192, 2002.

[7] L. Xiao and F. Gao, “A comprehensive review of the development of adaptive cruise control systems,” *Vehicle System Dynamics*, vol. 48, no. 10, pp. 1167–1192, 2010.

[8] G. Marsden, M. McDonald, and M. Brackstone, “Towards an understanding of adaptive cruise control,” *Transportation Research Part C: Emerging Technologies*, vol. 9, no. 1, pp. 33–51, 2001.

[9] A. Kesting, M. Treiber, M. Schönhof, and D. Helbing, “Adaptive cruise control design for active congestion avoidance,” *Transportation Research Part C: Emerging Technologies*, vol. 16, no. 6, pp. 668–683, 2008.

[10] G. Naus, R. Vugts, J. Ploeg, R. van de Molengraft, and M. Steinbuch, “Cooperative adaptive cruise control, design and experiments,” in *American Control Conference (ACC), 2010.* IEEE, 2010, pp. 6145–6150.

[11] W. J. Schakel, B. van Arem, and B. D. Netten, “Effects of cooperative adaptive cruise control on traffic flow stability,” in *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on.* IEEE, 2010, pp. 759–764.

[12] M. Treiber, A. Hennecke, and D. Helbing, “Congested traffic states in empirical observations and microscopic simulations,” *Physical Review E*, vol. 62, no. 2, p. 1805, 2000.

[13] D. Yanakiev and I. Kanellakopoulos, “A simplified framework for string stability analysis in AHS,” in *Proceedings of the 13th IFAC World Congress.* Citeseer, 1996, pp. 177–182.

[14] D. Yanakiev and I. Kanellakopoulos, "Variable time headway for string stability of automated heavy-duty vehicles," in *Proceedings of the 34th IEEE Conference on Decision and Control*, vol. 4. IEEE, 1995, pp. 4077–4081.

[15] R. Rajamani, *Vehicle Dynamics and Control.* Springer, 2011.

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

[17] D. Swaroop and J. Hedrick, "String stability of interconnected systems," *IEEE Transactions on Automatic Control*, vol. 41, no. 3, pp. 349–357, 1996.

[18] C. Chien and P. Ioannou, "Automatic vehicle-following," in *American Control Conference, 1992.* IEEE, 1992, pp. 1748–1752.

[19] J. Eyre, D. Yanakiev, and I. Kanellakopoulos, "String stability properties of AHS longitudinal vehicle controllers," UCLA Electrical Engineering, Tech. Rep., 1997.

[20] J. Eyre, D. Yanakiev, and I. Kanellakopoulos, "A simplified framework for string stability analysis of automated vehicles," *Vehicle System Dynamics*, vol. 30, no. 5, pp. 375–405, 1998.

[21] E. Shaw and J. K. Hedrick, "String stability analysis for heterogeneous vehicle strings," in *American Control Conference, 2007. ACC'07.* IEEE, 2007, pp. 3118–3125.

[22] E. Shaw and J. K. Hedrick, "Controller design for string stable heterogeneous vehicle strings," in *2007 46th IEEE Conference on Decision and Control.* IEEE, 2007, pp. 2868–2875.

[23] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: an efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference.* ACM, 2013, pp. 99–108.

[24] D. A. C. Sosa, "An efficiency-motivated attack against vehicles in a platoon: Local vehicle control, platoon control strategies, and drive train technologies considerations," Master's thesis, Utah State University, Logan, UT, 2013.

[25] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security.* ACM, 2015, pp. 167–178.

[26] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on Future Directions in Cyber-Physical Systems Security*, 2009.

[27] D. B. Rawat, B. B. Bista, G. Yan, and M. C. Weigle, "Securing vehicular ad-hoc networks against malicious drivers: a probabilistic approach," in *2011 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS).* IEEE, 2011, pp. 146–151.

[28] S. Haj-Assaad. (2014) Top 10 affordable cars with adaptive cruise control. [Online]. Available: http://www.autoguide.com/auto-news/2014/09/top-10-affordable-cars-adaptive-cruise-control.html

[29] M. R. Jovanovic and B. Bamieh, "On the ill-posedness of certain vehicular platoon control problems," *IEEE Transactions on Automatic Control*, vol. 50, no. 9, pp. 1307–1321, 2005.

[30] T. S. No and K. T. Chong, "Longitudinal spacing control of vehicles in a platoon," *Transaction on Control, Automation and Systems Engineering (ICASE)*, vol. 2, no. 2, pp. 92–97, 2001.

[31] D. Yanakiev and I. Kanellakopoulos, "Nonlinear spacing policies for automated heavy-duty vehicles," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 4, pp. 1365–1377, 1998.

[32] S. Sheikholeslam, *Control of a Class of Interconnected Nonlinear Dynamical Systems: The Platoon Problem*, ser. Memorandum (University of California, Berkeley, Electronics Research Laboratory). University of California, Berkeley, 1991. [Online]. Available: http://books.google.com/books?id=VfGJKQEACAAJ

[33] P. Ioannou and Z. Xu, "Throttle and brake control systems for automatic vehicle following," *Journal of Intelligent Transportation Systems*, vol. 1, no. 4, pp. 345–377, 1994.

[34] C.-T. Chen, *Linear System Theory and Design.* Oxford University Press, 1995.

[35] BattleKits, robot kits. [Online]. Available: http://battlekits.com/

[36] U. Özgüner. (2000) EE757 Control Systems Laboratory. [Online]. Available: http://www2.ece.ohio-state.edu/~umit/ee757.htm

Appendices

Appendix A

Figures for Attack Against Control Algorithm 2

The attackers are using Control Algorithm 1, all victim vehicles are using Control Algorithm 2. The gains used for this simulation are given in Table A.1.

A velocity landscape of the traffic system is shown in Figure A.1. Vehicle 1 is at the rear of the traffic system, vehicle 100 is at the front of the system.

The absolute vehicle positions at the beginning of the attack can be seen in Figure A.2. The vehicle positions at the end of the simulated attack are shown in Figure A.3.

The velocities of victim vehicles following the attacker furthest downstream are shown in Figure A.4. The velocities of victim vehicles following the passive attacker farthest upstream are shown in Figure A.5. Similarly the accelerations of the same groups of victim vehicles are given in Figure A.6 and Figure A.7.

Standard deviation of the victim vehicles is shown in Figure A.8, the percentage of victims deviating from the nominal velocity is shown in Figure A.9.

Table A.1: Simulation parameters for attack against Control Algorithm 2.

Gain	Attacker	Victim
k_p	0.5	1
k_d	-0.48	1
k_h	N/A	0.1
h	1	N/A
h_0	N/A	0.55

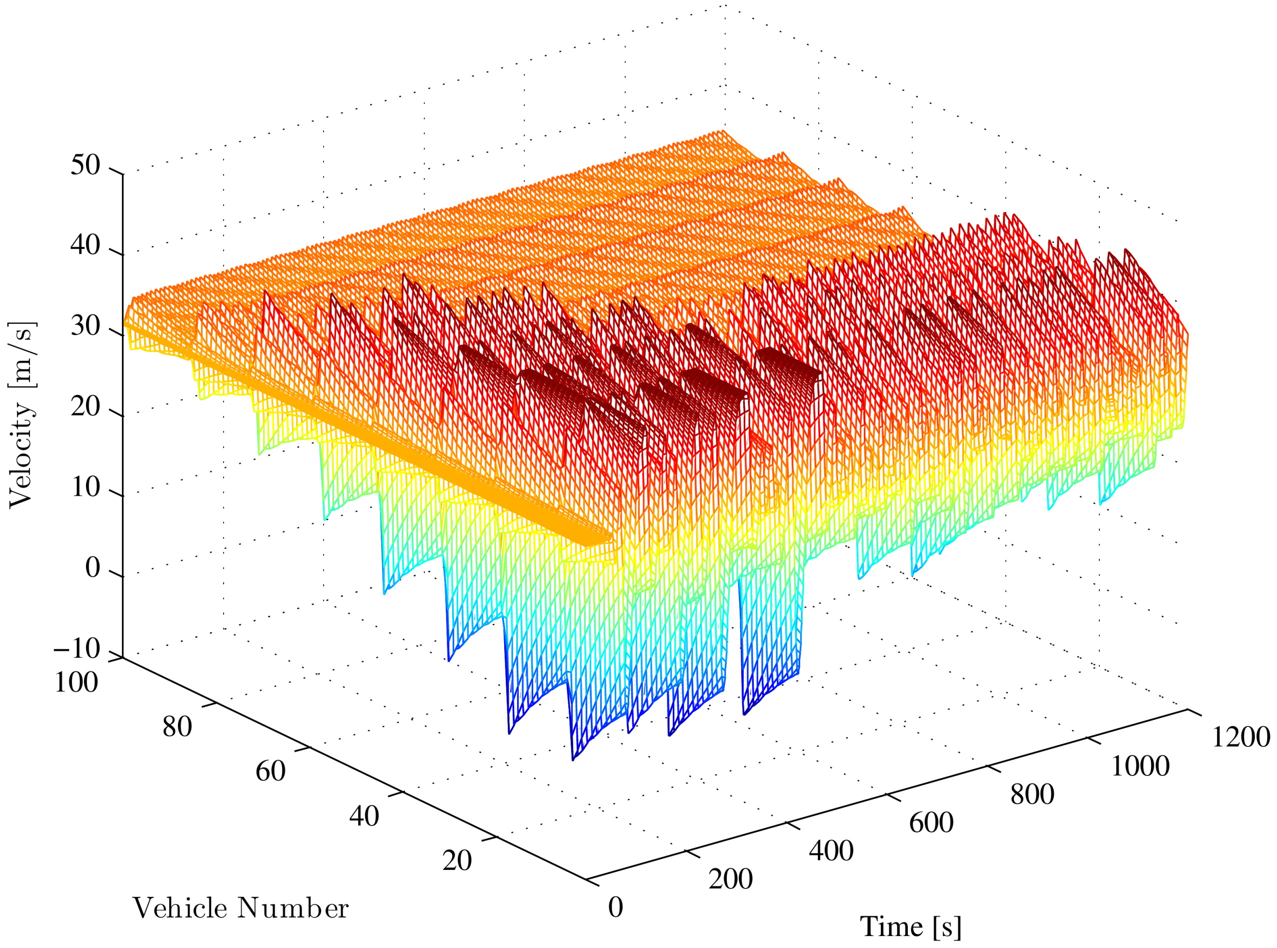


Fig. A.1: Velocity landscape of Control Algorithm 2 during a simulated attack.

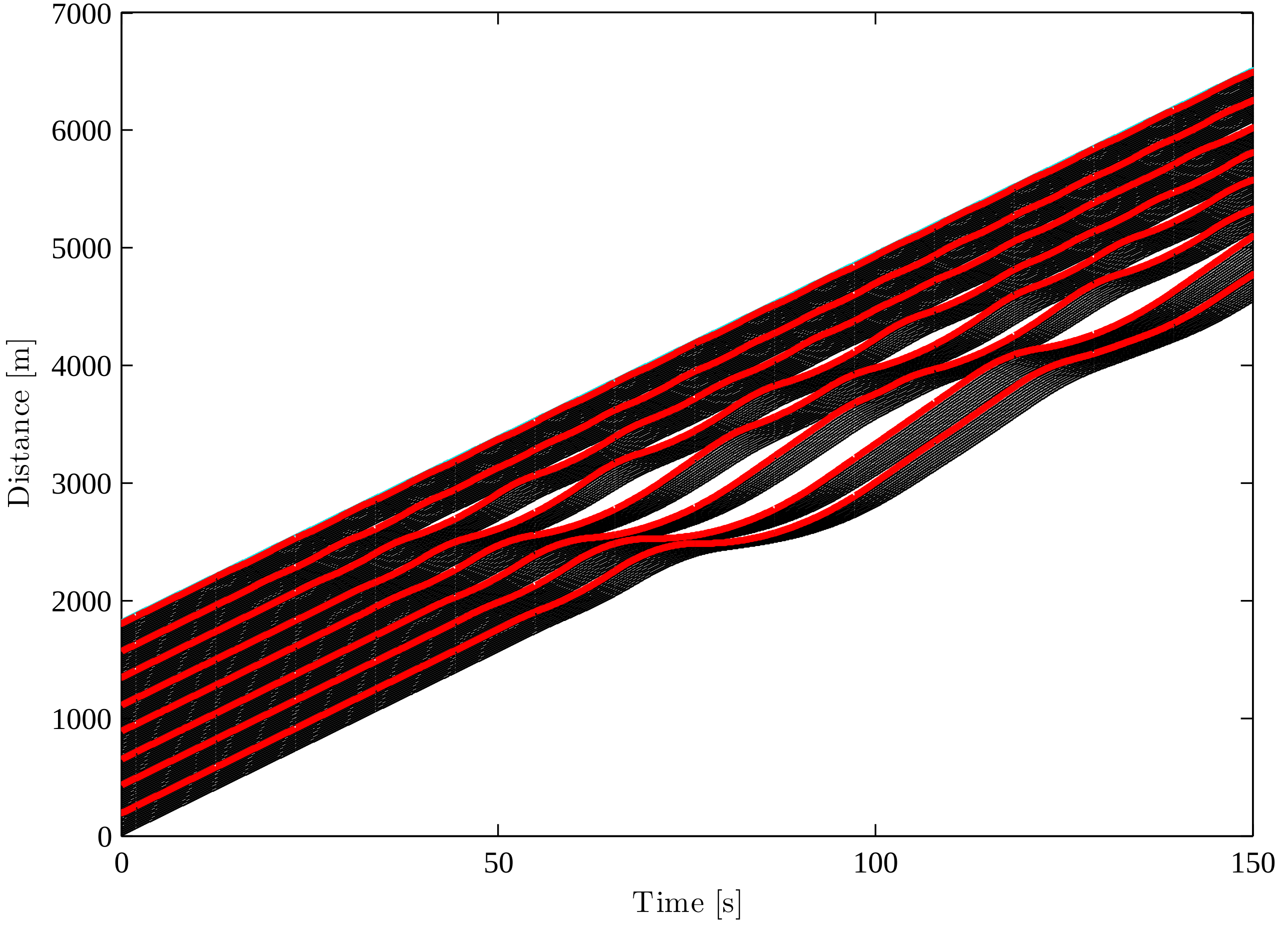


Fig. A.2: Initial perturbation of the simulated attack against Control Algorithm 2. Attacker vehicles are shown in red.

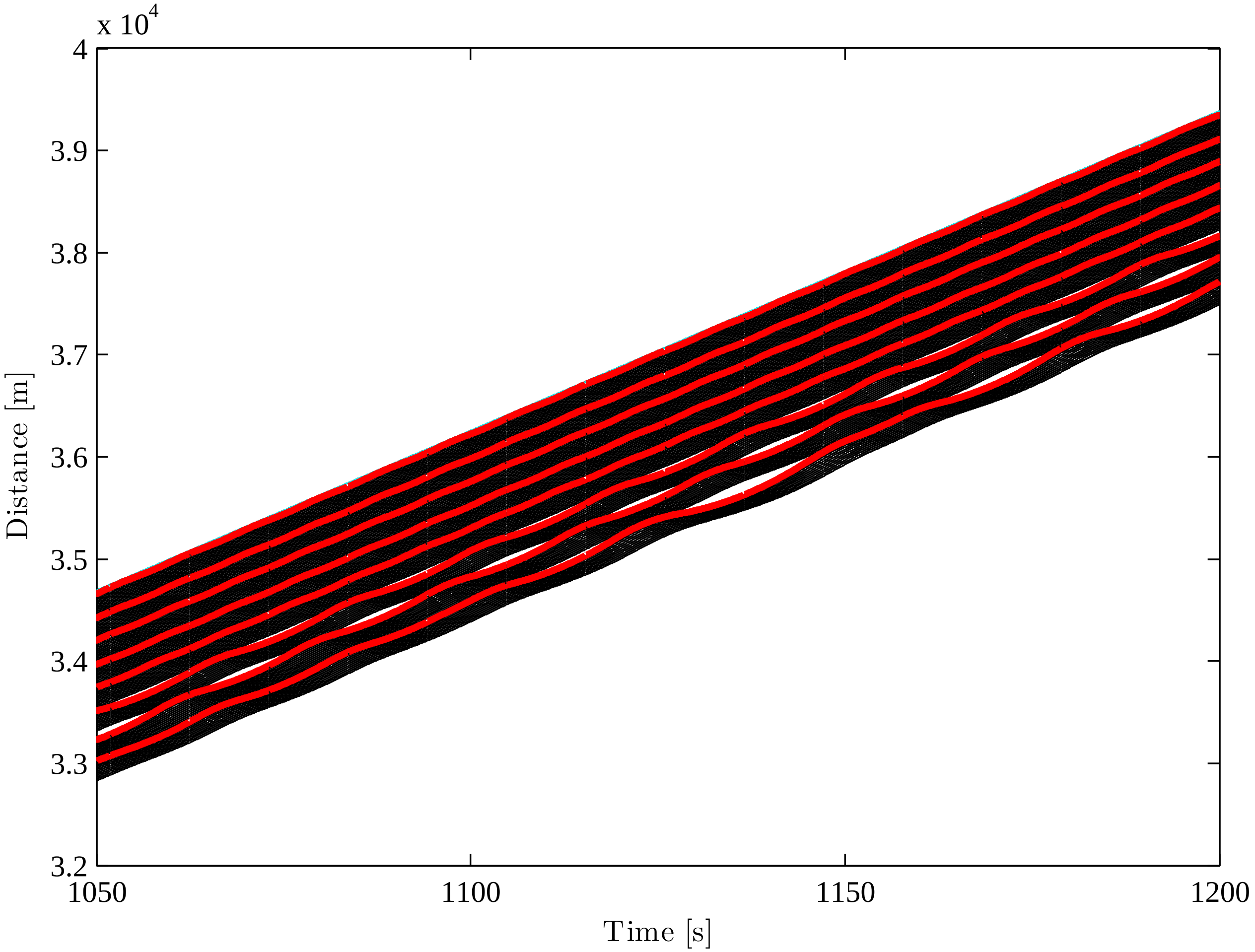


Fig. A.3: Vehicle positions at the end of the simulated attack against Control Algorithm 2.

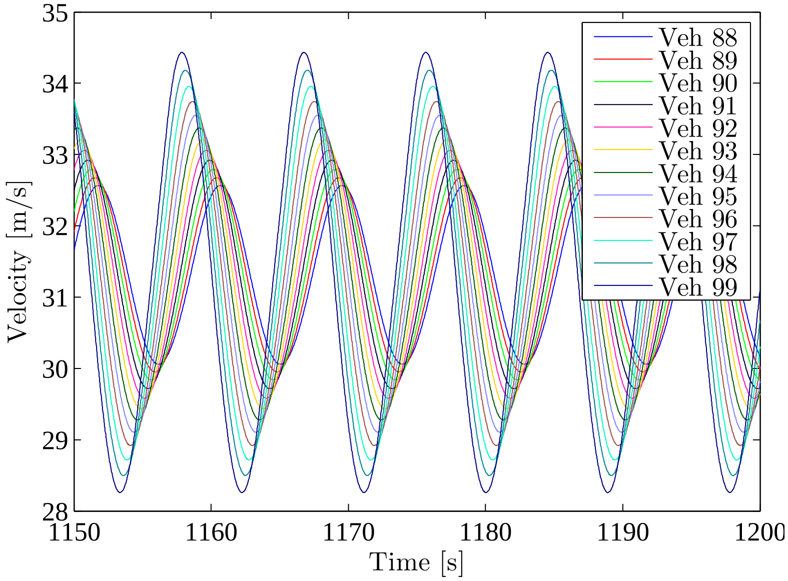


Fig. A.4: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 2).

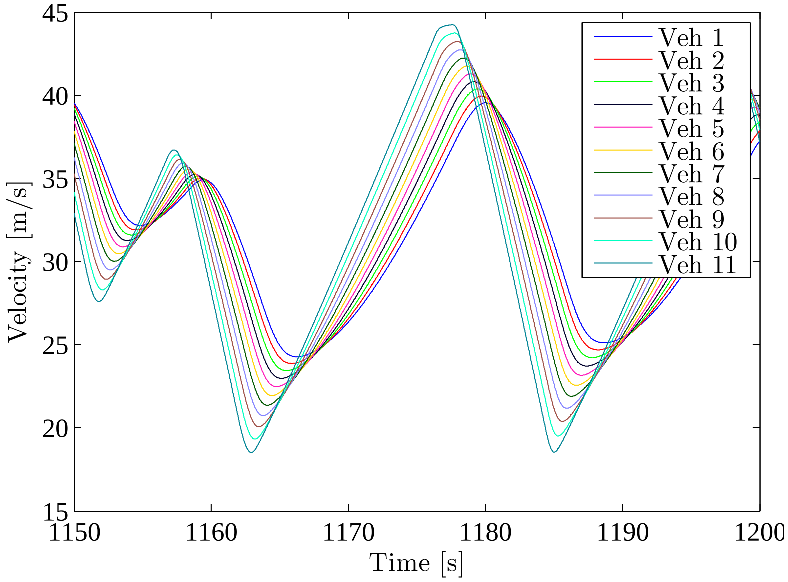


Fig. A.5: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 2).

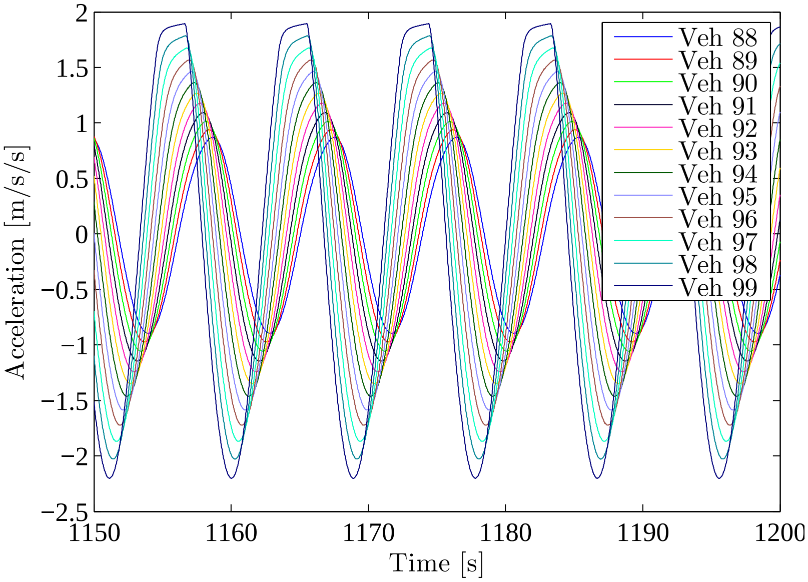


Fig. A.6: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 2).

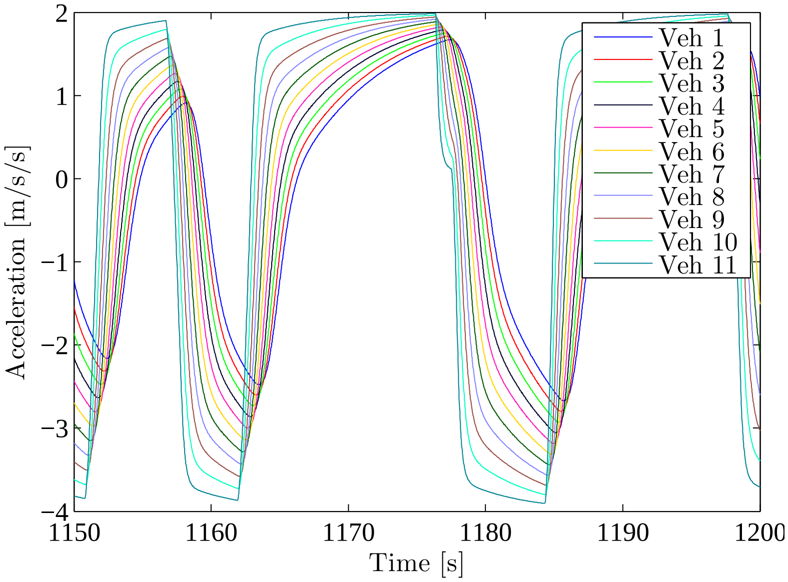


Fig. A.7: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 2).

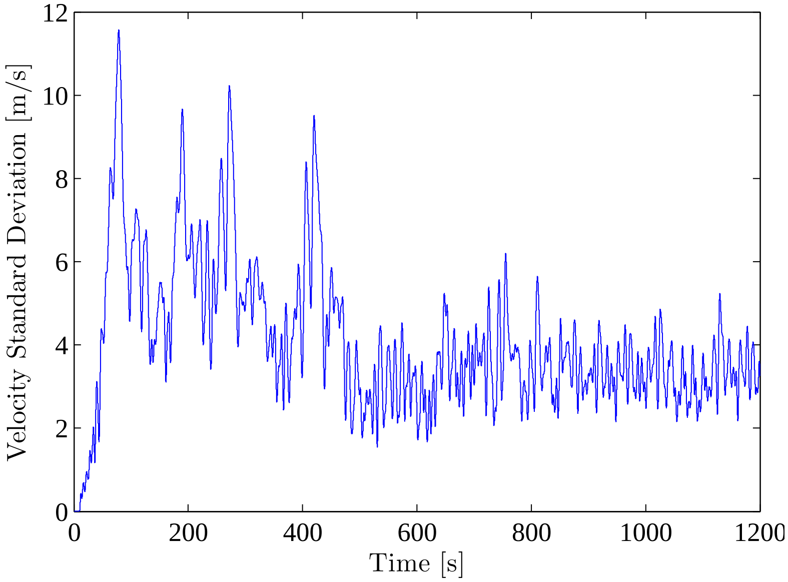


Fig. A.8: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against Control Algorithm 2.

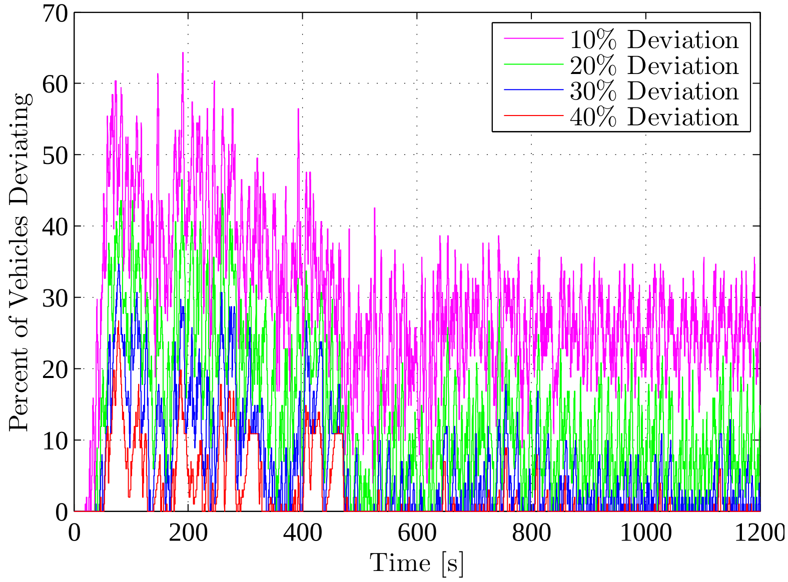


Fig. A.9: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack against Control Algorithm 2.

Appendix B

Figures for Attack Against Control Algorithm 3

The attackers are using Control Algorithm 1, all victim vehicles are using Control Algorithm 3. The gains used for this simulation are given in Table B.1.

A velocity landscape of the traffic system is shown in Figure B.1. Vehicle 1 is at the rear of the traffic system, vehicle 100 is at the front of the system.

The absolute vehicle positions at the beginning of the attack can be seen in Figure B.2. The vehicle positions at the end of the simulated attack are shown in Figure B.3.

The velocities of victim vehicles following the attacker furthest downstream are shown in Figure B.4. The velocities of victim vehicles following the passive attacker farthest upstream are shown in Figure B.5. Similarly the accelerations of the same groups of victim vehicles are given in Figure B.6 and Figure B.7.

Standard deviation of the victim vehicles is shown in Figure B.8, the percentage of victims deviating from the nominal velocity is shown in Figure B.9.

Table B.1: Simulation parameters for attack against Control Algorithm 3.

Gain	Attacker	Victim
k_p	0.5	1
k_d	-0.48	1
k_h	N/A	1.75
h	1	1

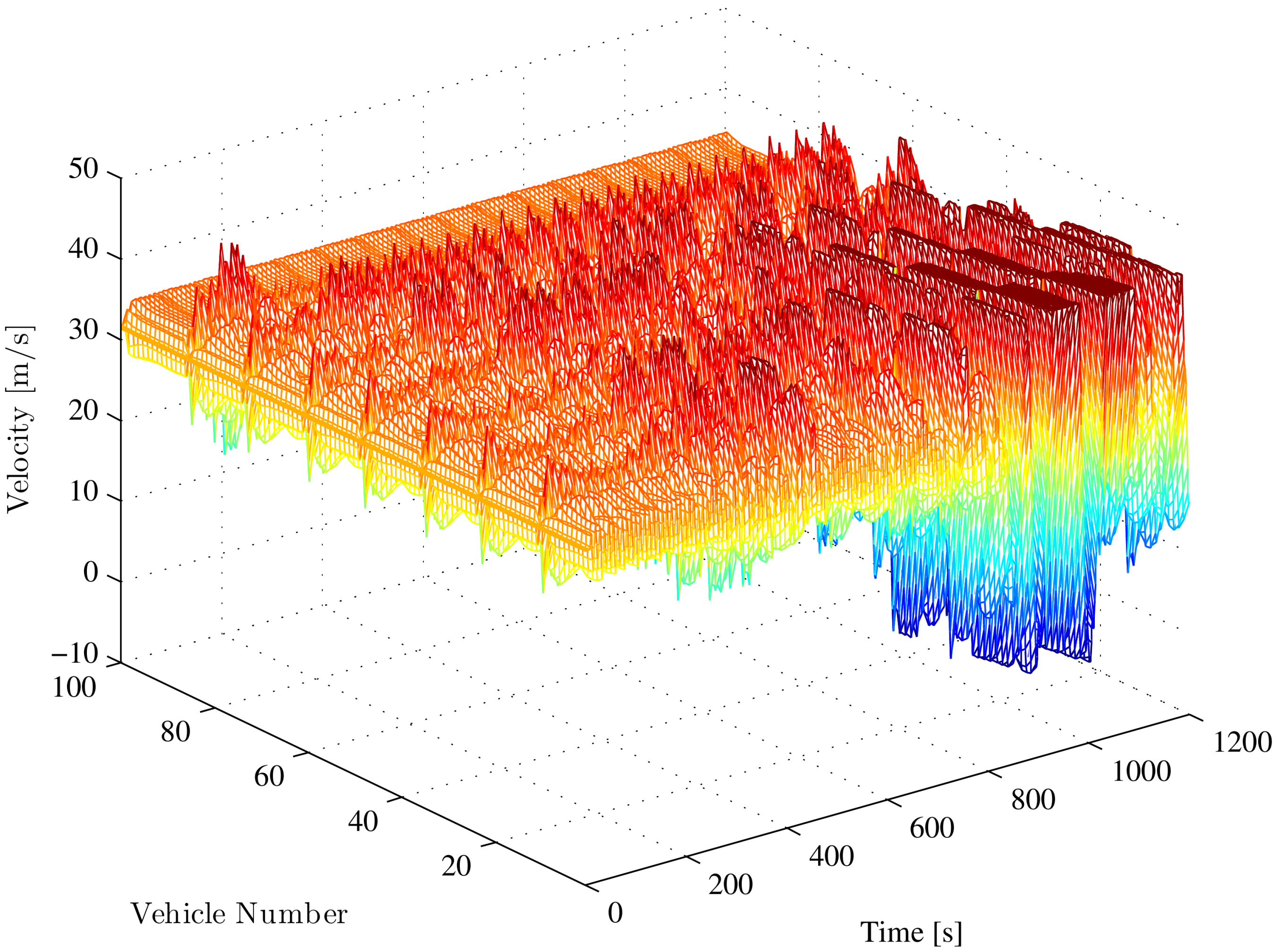


Fig. B.1: Velocity landscape of Control Algorithm 3 during a simulated attack.

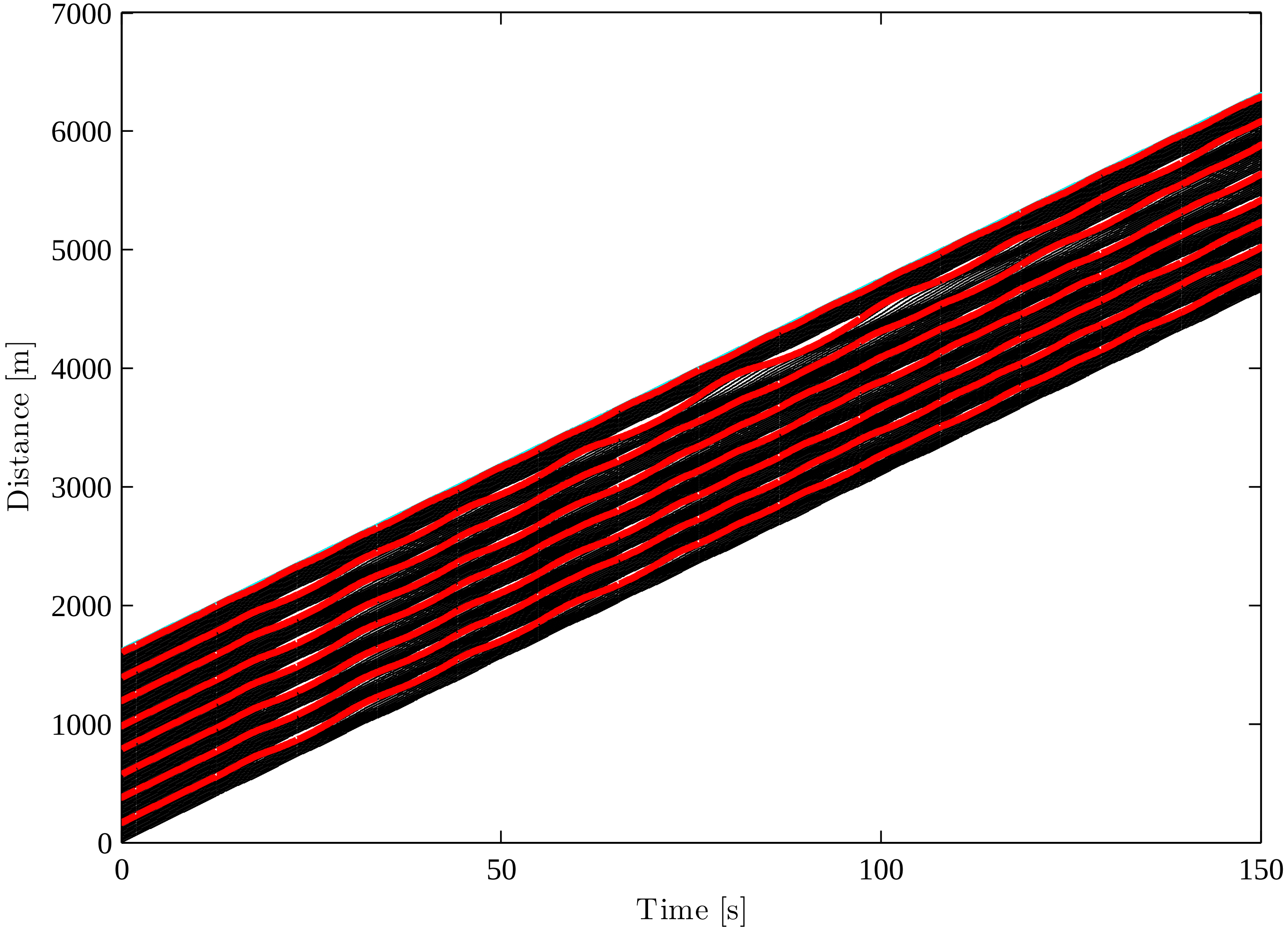


Fig. B.2: Initial perturbation of the simulated attack against Control Algorithm 3. Attacker vehicles are shown in red.

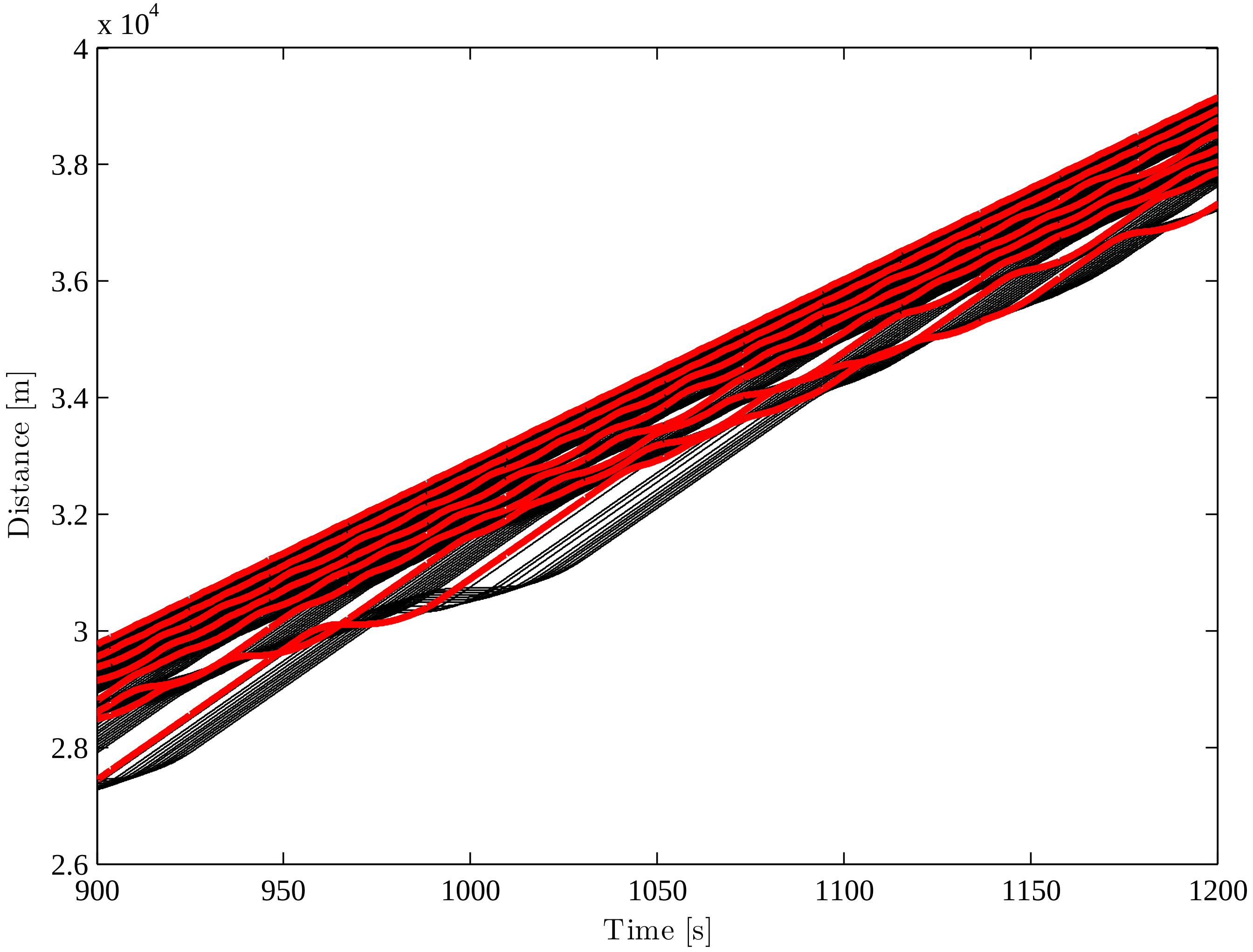


Fig. B.3: Vehicle positions at the end of the simulated attack against Control Algorithm 3.

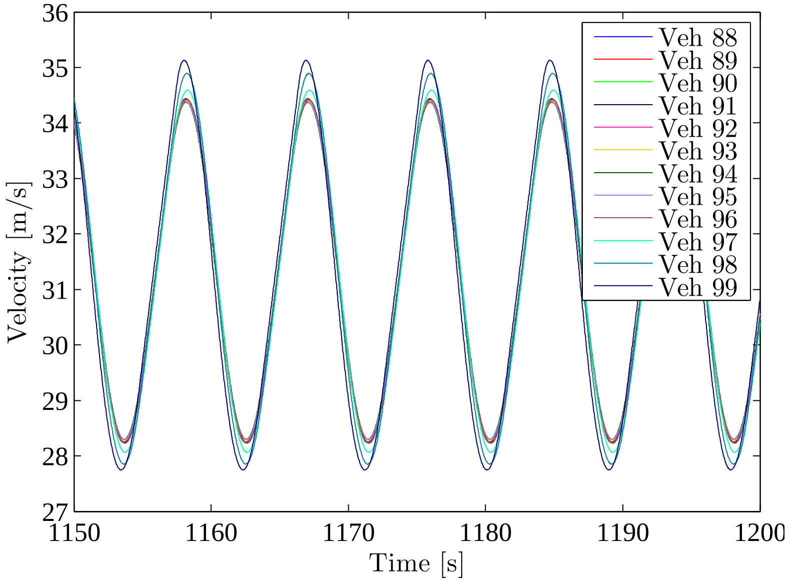


Fig. B.4: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 3).

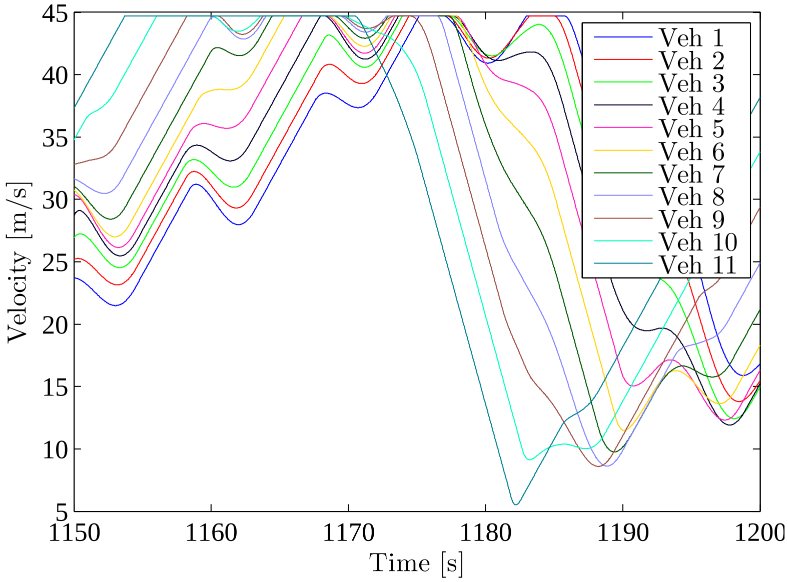


Fig. B.5: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 3).

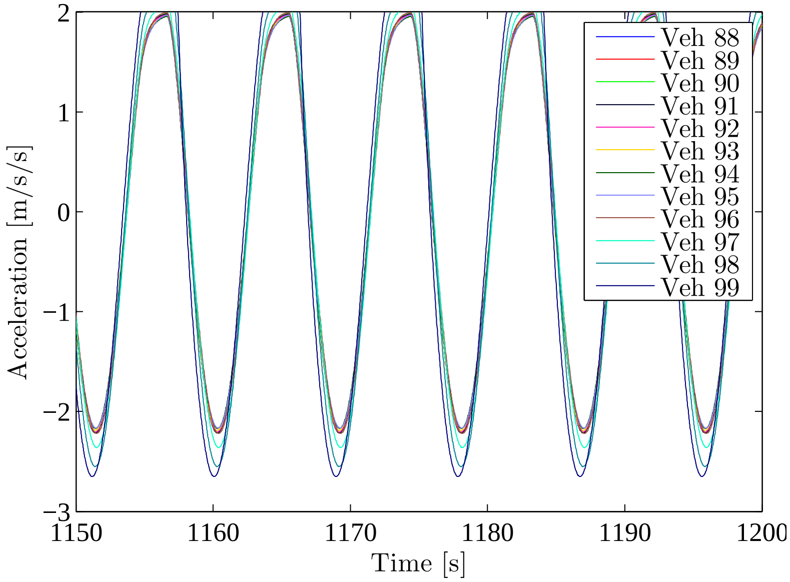


Fig. B.6: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 3).

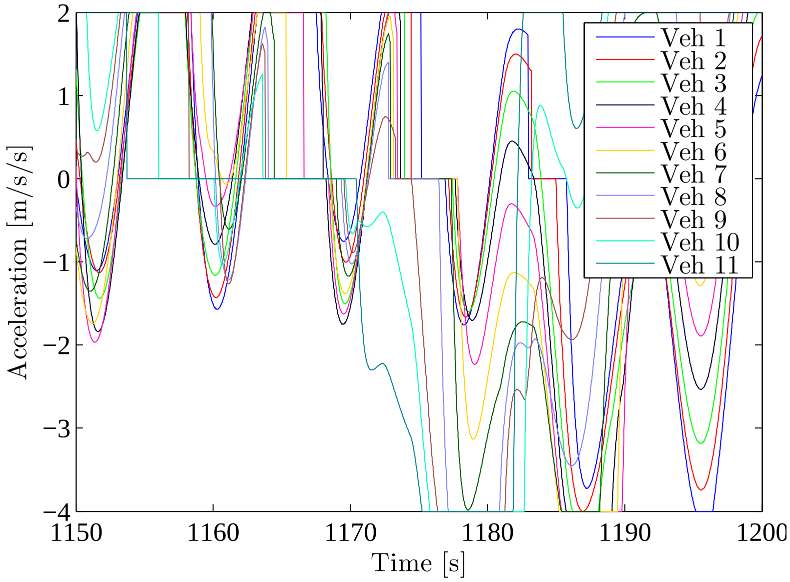


Fig. B.7: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 3).

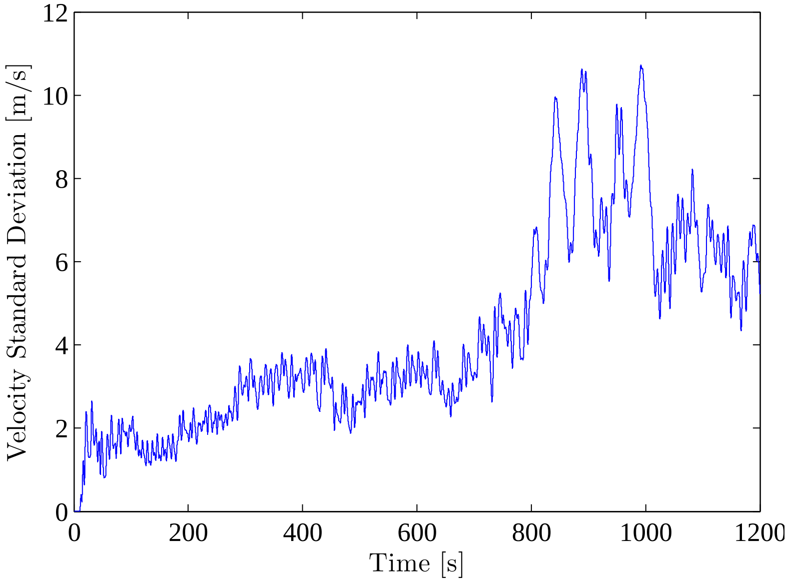


Fig. B.8: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against Control Algorithm 3.

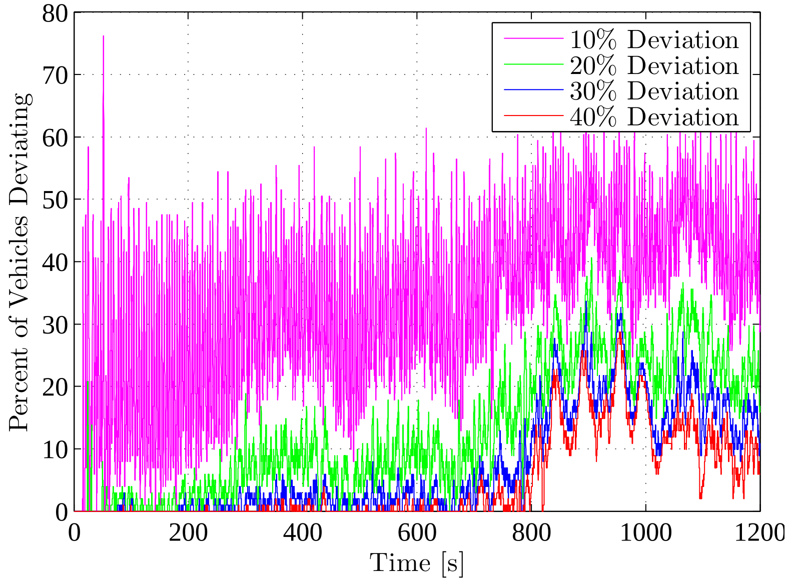


Fig. B.9: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack against Control Algorithm 3.

Appendix C

Figures for Attack Against Control Algorithm 4

The attackers are using Control Algorithm 1, all victim vehicles are using Control Algorithm 4. The gains used for this simulation are given in Table C.1.

A velocity landscape of the traffic system is shown in Figure C.1. Vehicle 1 is at the rear of the traffic system, vehicle 100 is at the front of the system.

The absolute vehicle positions for the duration of the simulated attack can be seen in Figure C.2.

The velocities of victim vehicles following the attacker furthest downstream are shown in Figure C.3. The velocities of victim vehicles following the passive attacker farthest upstream are shown in Figure C.4. Similarly the accelerations of the same groups of victim vehicles are given in Figure C.5 and Figure C.6.

Standard deviation of the victim vehicles is shown in Figure C.7, the percentage of victims deviating from the nominal velocity is shown in Figure C.8.

Table C.1: Simulation parameters for attack against Control Algorithm 4.

Gain	Attacker	Victim
k_p	0.5	N/A
k_d	-0.48	N/A
h	1	0.65
k_1	N/A	-1
k_2	N/A	1
τ	N/A	0.2

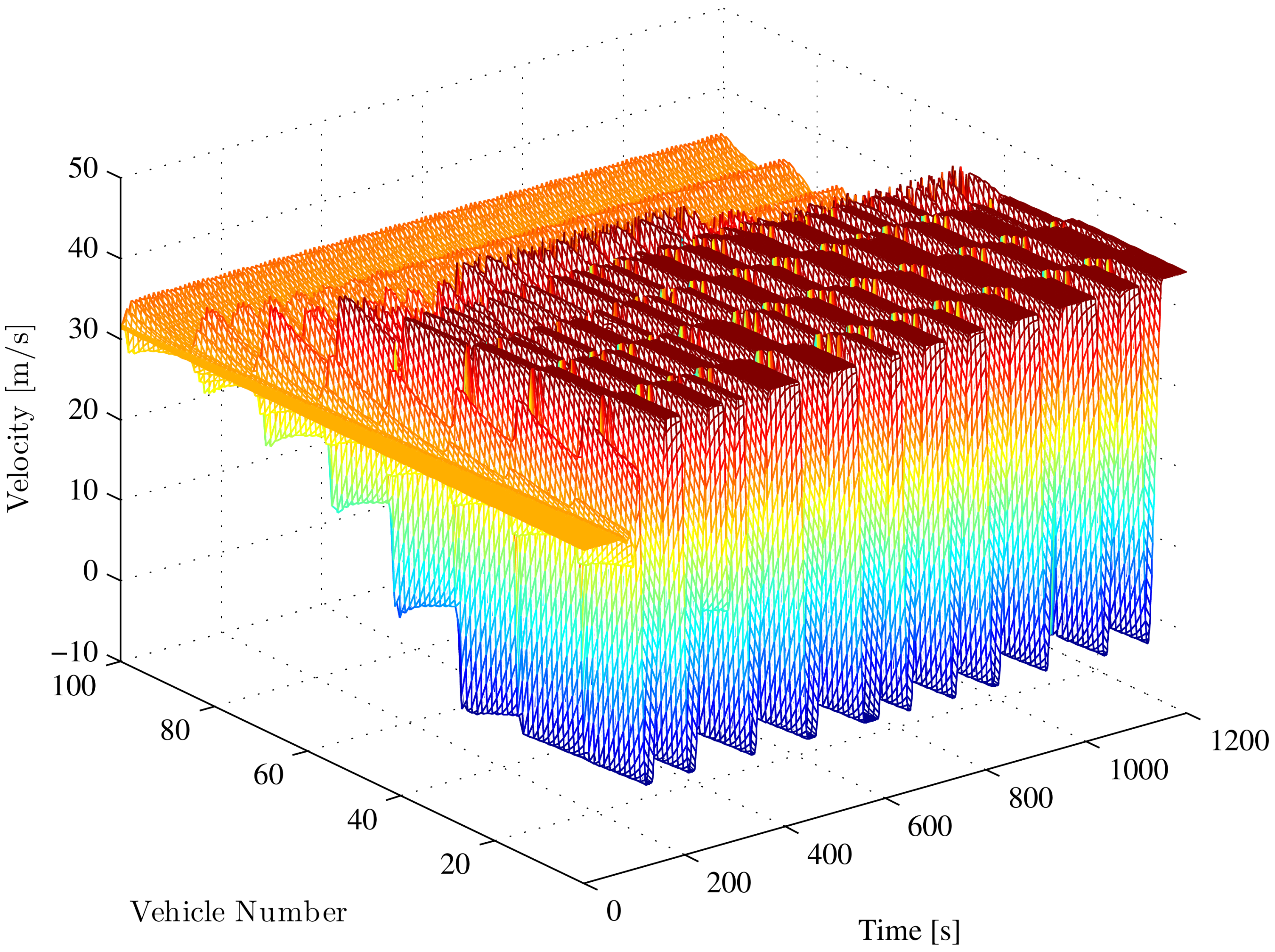


Fig. C.1: Velocity landscape of Control Algorithm 4 during a simulated attack.

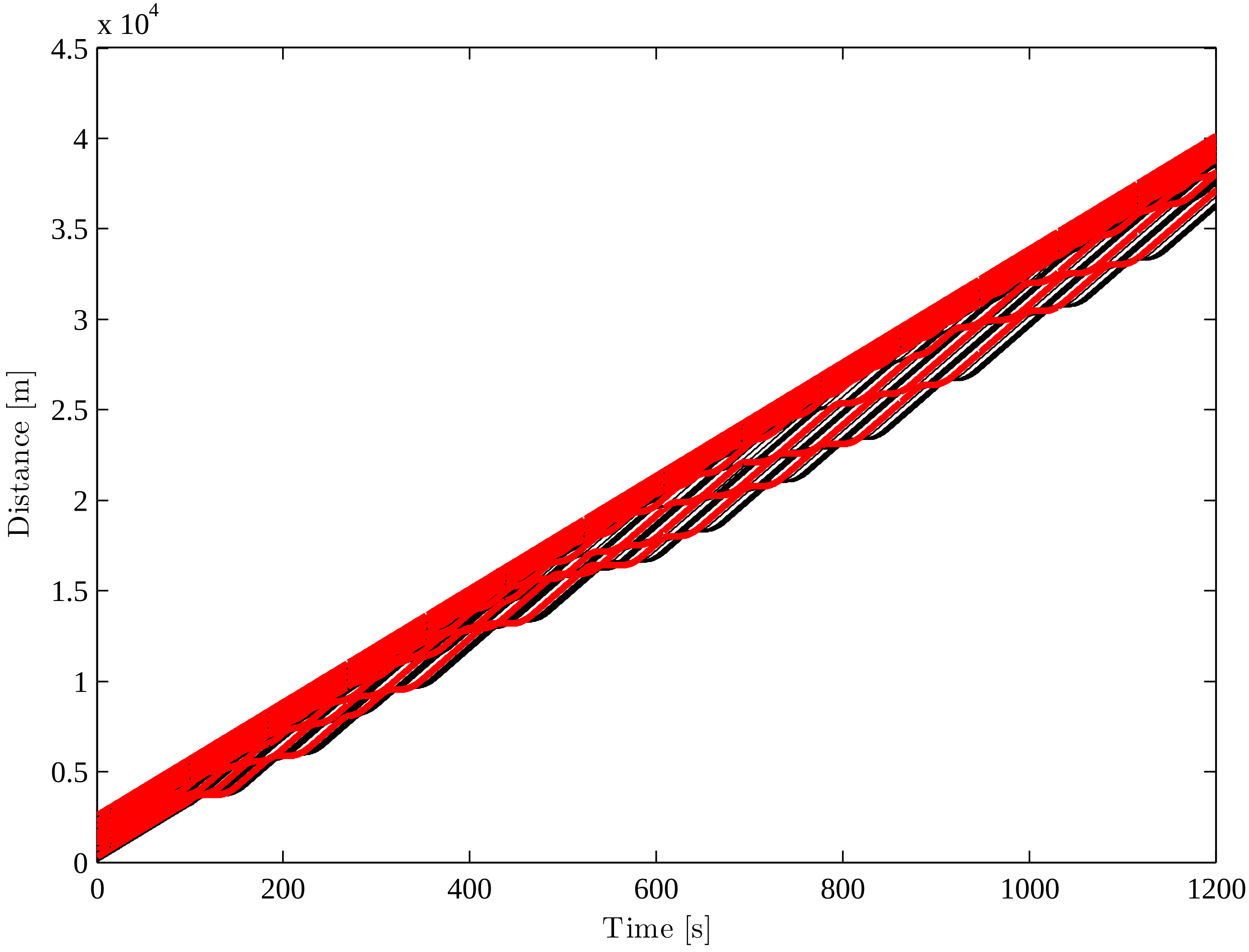


Fig. C.2: Attack against Control Algorithm 4 results in instability.

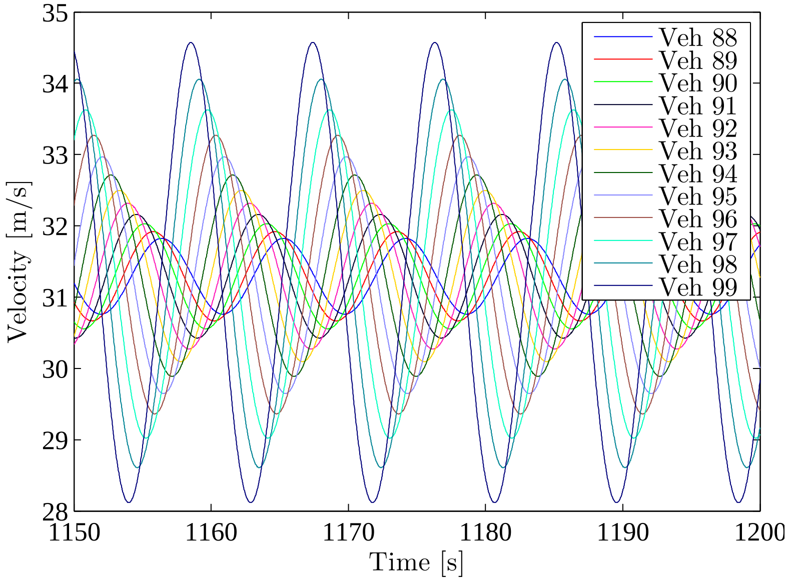


Fig. C.3: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 4).

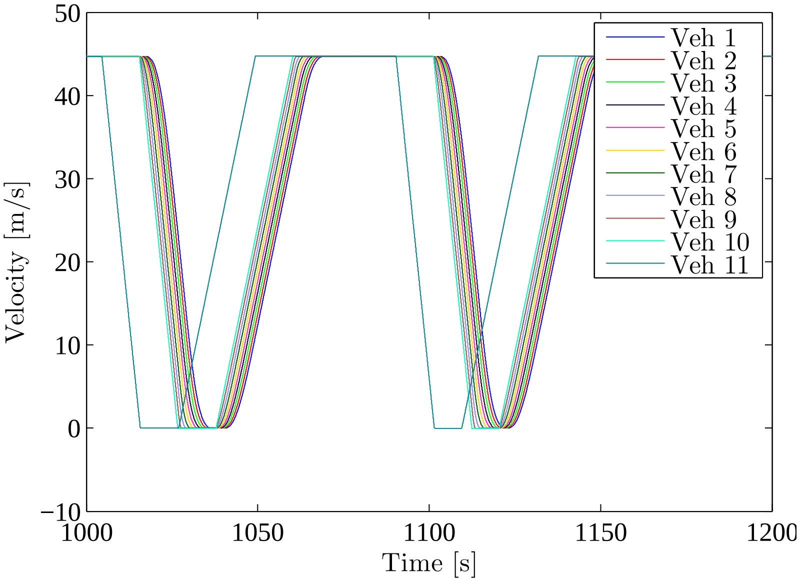


Fig. C.4: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 4).

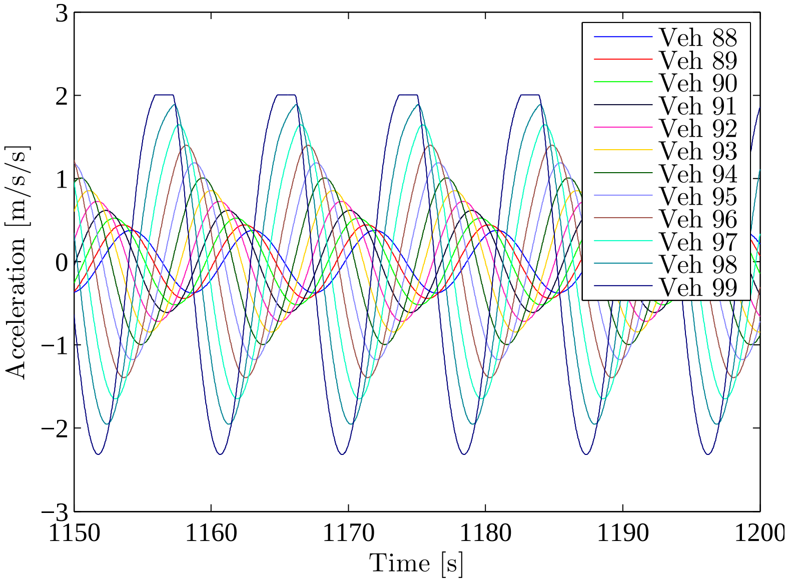


Fig. C.5: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 4).

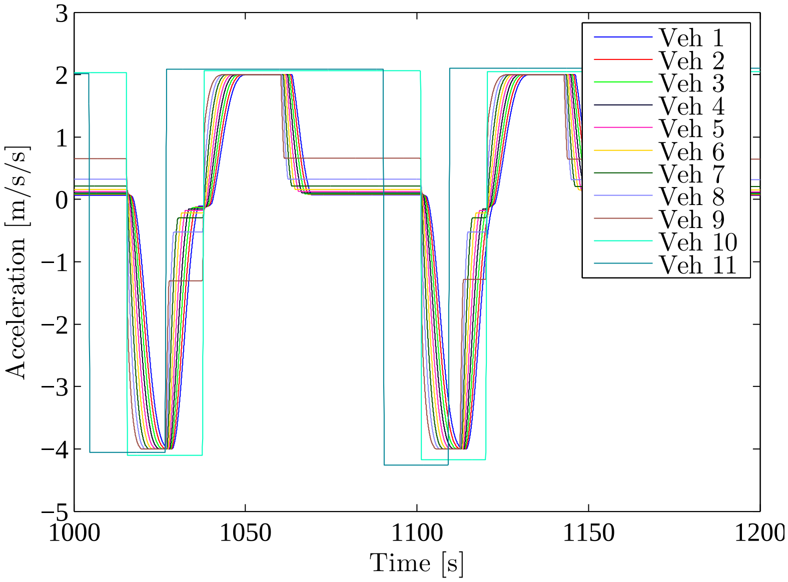


Fig. C.6: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 4).

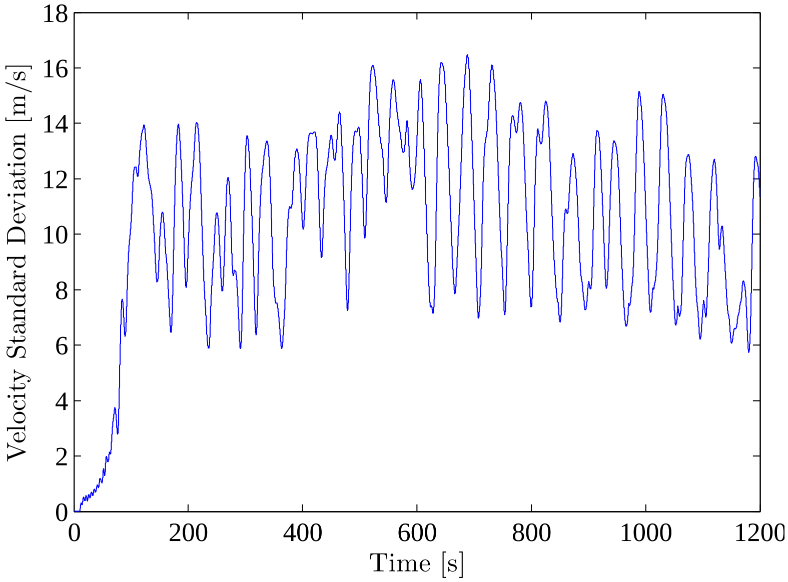


Fig. C.7: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against Control Algorithm 4.

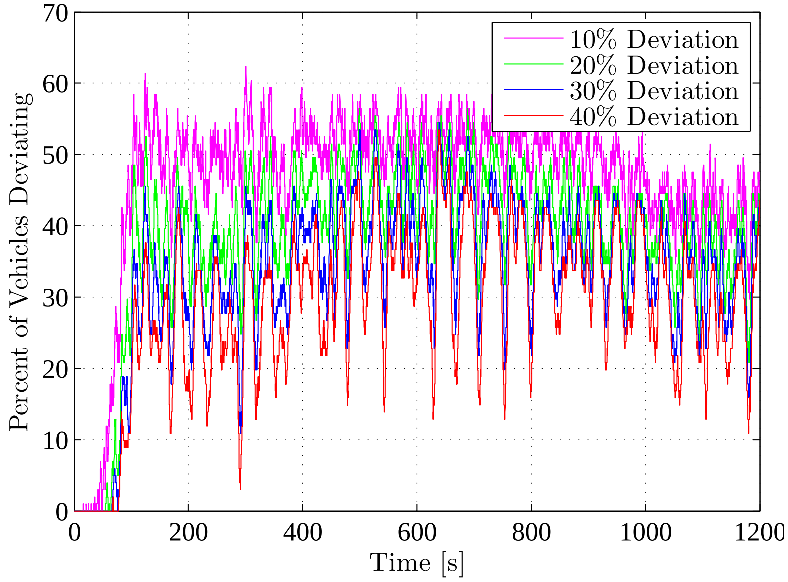


Fig. C.8: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack against Control Algorithm 4.

Appendix D

Figures for Attack Against Control Algorithm 5

The attackers are using Control Algorithm 1, all victim vehicles are using Control Algorithm 5. The gains used for this simulation are given in Table D.1.

A velocity landscape of the traffic system is shown in Figure D.1. Vehicle 1 is at the rear of the traffic system, vehicle 100 is at the front of the system.

The absolute vehicle positions for the duration of the simulated attack can be seen in Figure D.2.

The velocities of victim vehicles following the attacker furthest downstream are shown in Figure D.3. The velocities of victim vehicles following the passive attacker farthest upstream are shown in Figure D.4. Similarly the accelerations of the same groups of victim vehicles are given in Figure D.5 and Figure D.6.

Standard deviation of the victim vehicles is shown in Figure D.7, the percentage of victims deviating from the nominal velocity is shown in Figure D.8.

Table D.1: Simulation parameters for attack against Control Algorithm 5.

Gain	Attacker	Victim
k_p	0.5	N/A
k_d	-0.48	N/A
h	1	N/A
λ_2	N/A	0.5
C_p	N/A	224
C_v	N/A	127.2
C_a	N/A	5
K_v	N/A	0
K_a	N/A	-3.56

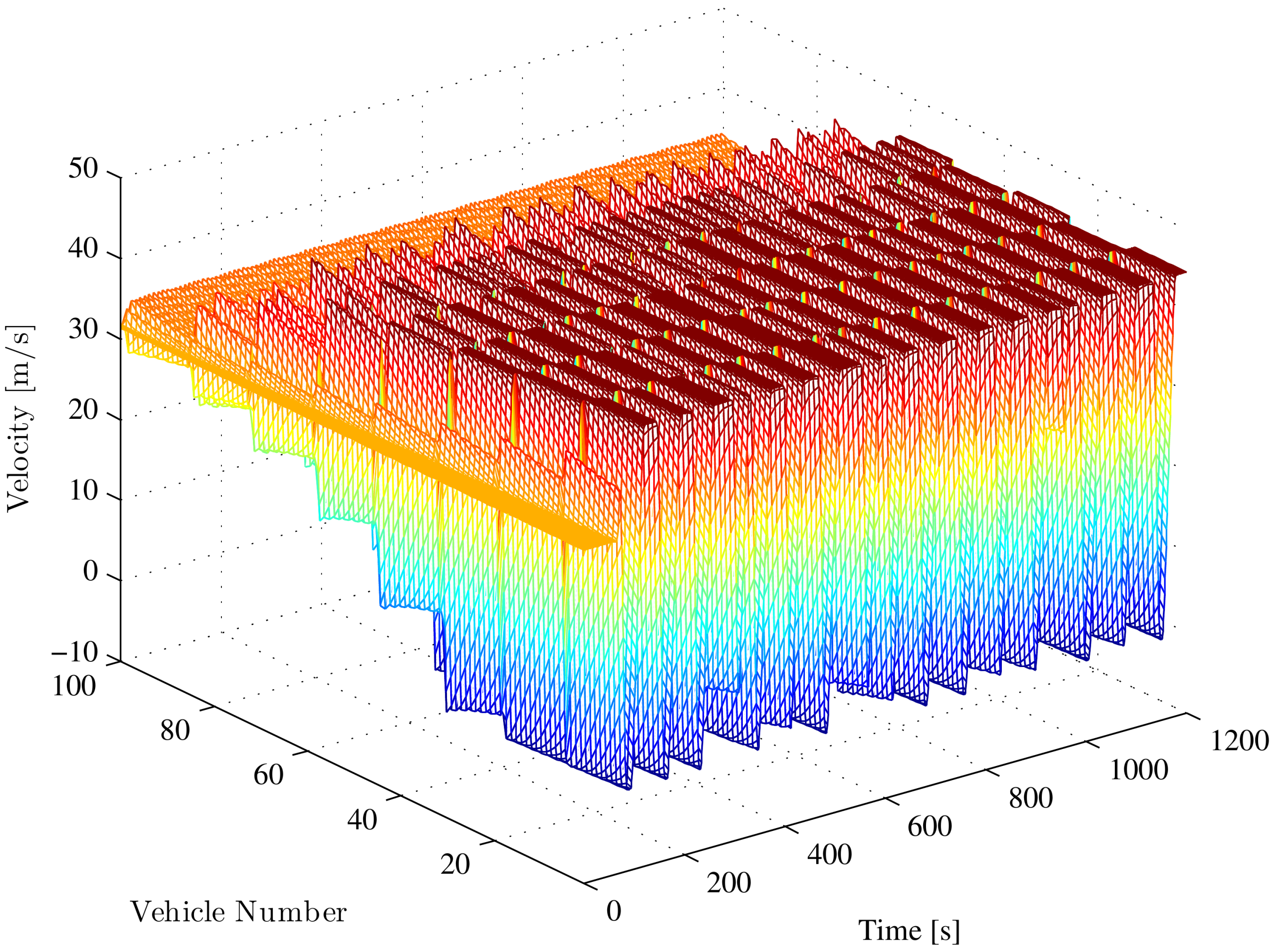


Fig. D.1: Velocity landscape of Control Algorithm 5 during a simulated attack.

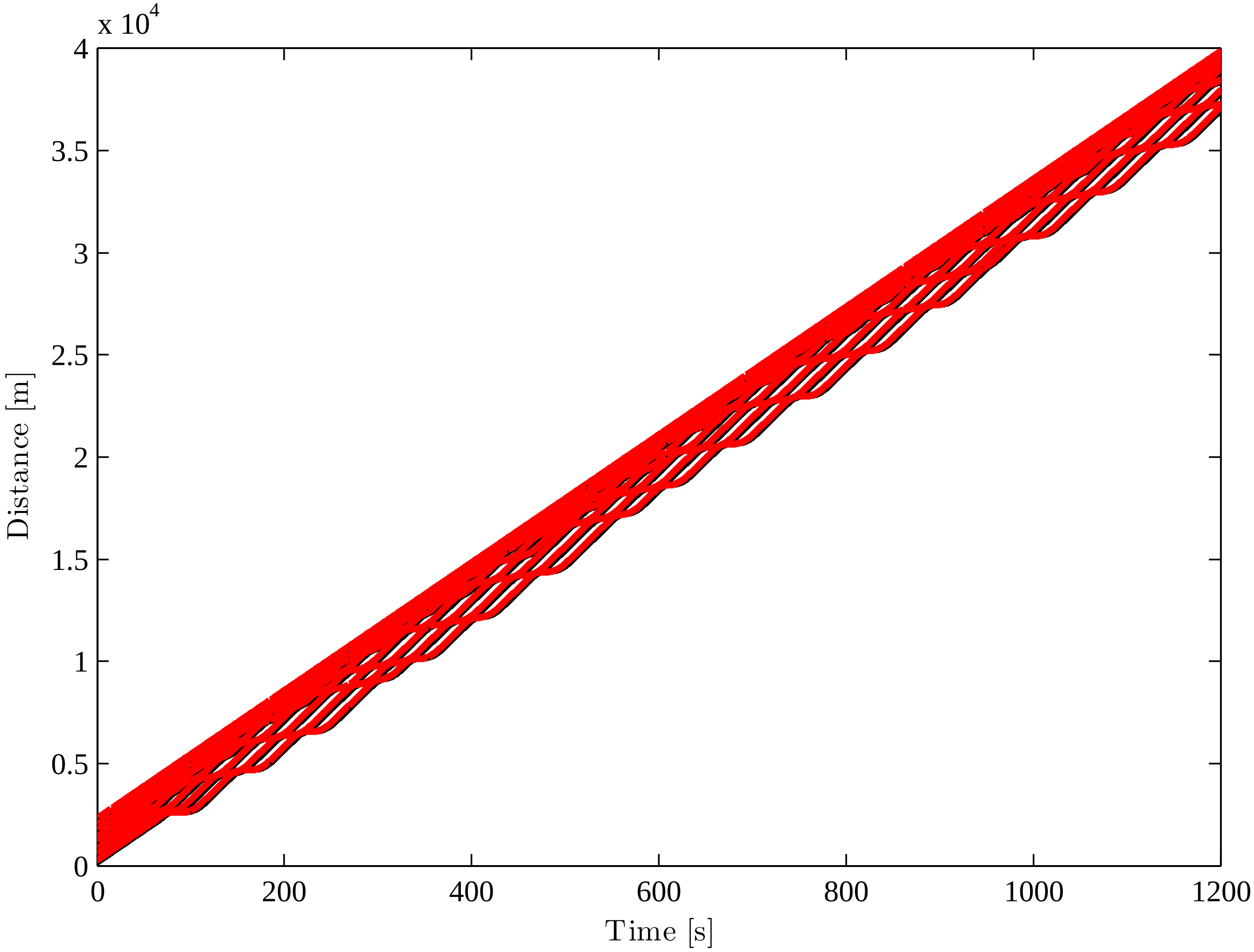


Fig. D.2: Attack against Control Algorithm 5 results in instability.

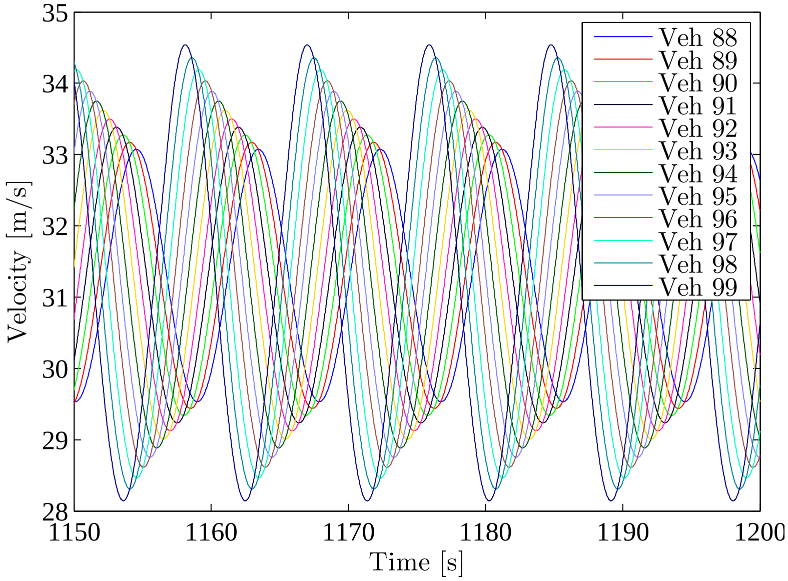


Fig. D.3: Snapshot of the velocity variation of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 5).

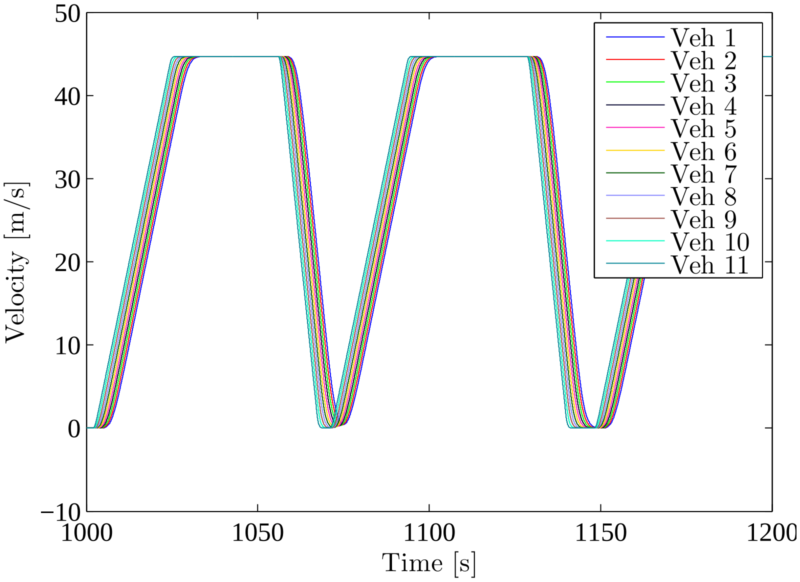


Fig. D.4: Snapshot of the velocity variation of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 5).

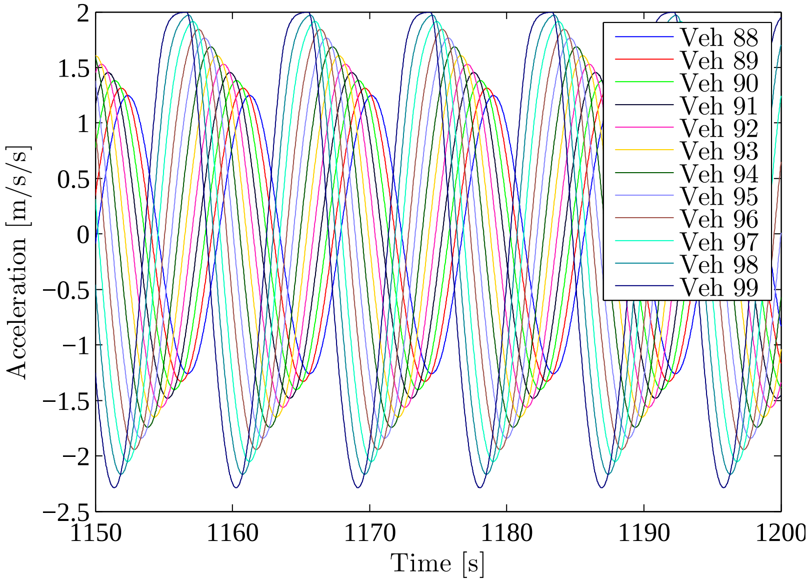


Fig. D.5: Snapshot of the accelerations of the victim vehicles following attacker farthest downstream (attack against Control Algorithm 5).

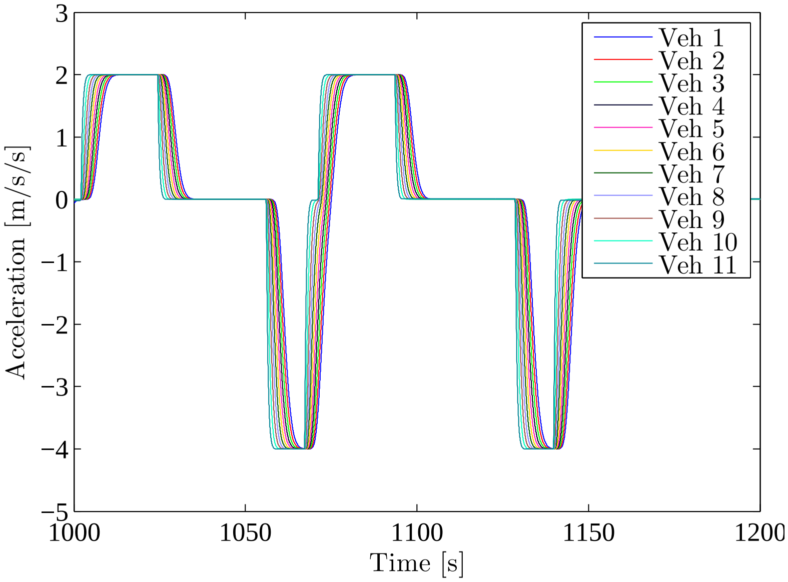


Fig. D.6: Snapshot of the accelerations of the victim vehicles following passive attacker farthest upstream (attack against Control Algorithm 5).

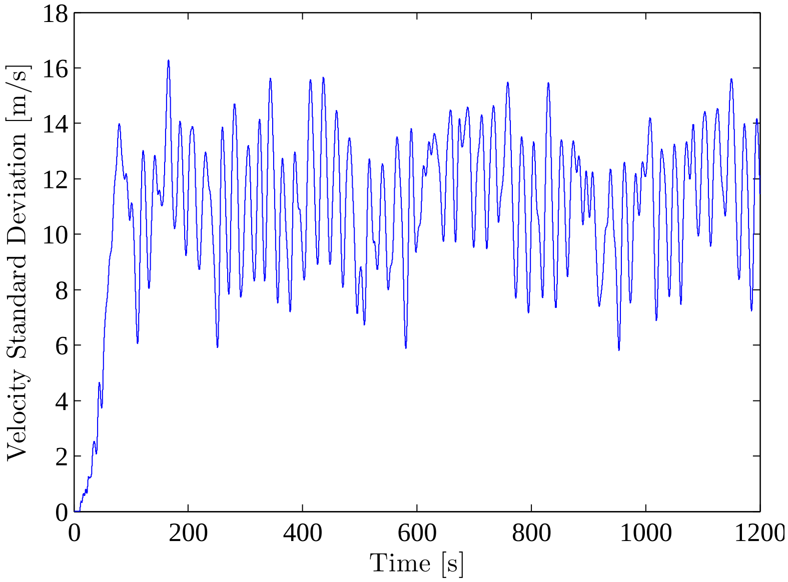


Fig. D.7: Standard deviation of the victim vehicle velocities for the duration of the simulated attack against Control Algorithm 5.

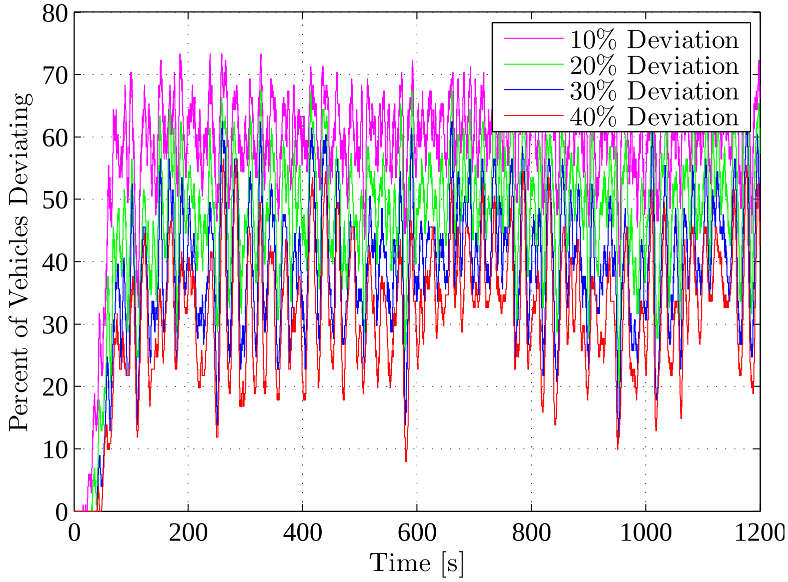


Fig. D.8: Percentage of victim vehicles deviating from 10%, 20%, 30%, and 40% of the nominal velocity for the duration of the simulated attack against Control Algorithm 5.