Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure (Part 1)

Final Report

James J Martin, Ph.D., Clemson University
Gurcan Comert, Ph.D., Benedict College
Manveen Kaur, Ph.D. Student, Clemson University
Adil Alsuhaim, Ph.D. Student, Clemson University

Contact Information
James J Martin, Ph.D.
211 McAdams Hall
School of Computing, Clemson University
Clemson, South Carolina 29634-0974
Email: jmarty@clemson.edu; Phone: (864) 656-4529

June 2020

Center for Connected Multimodal Mobility (C^2M^2)

CLEMSON UNIVERSITY

Benedict College | The Citadel, The Military College of South Carolina | SC State University | University of South Carolina

200 Lowry Hall, Clemson University
Clemson, SC 29634

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated in the interest of information exchange. The report is funded, partially or entirely, by the Center for Connected Multimodal Mobility (C^2M^2) (Tier 1 University Transportation Center) Grant, which is headquartered at Clemson University, Clemson, South Carolina, USA, from the U.S. Department of Transportation's University Transportation Centers Program. However, the U.S. Government assumes no liability for the contents or use thereof.

ACKNOWLEDGMENT

We would like to acknowledge the Center for Connected Multimodal Mobility (C^2M^2), which is a Tier 1 University Transportation Center, for supporting this research. We also acknowledge the National Science Foundation (NSF) for their continued support for our connected vehicle research through grants provided by the NSF Cyber-physical Systems (CPS) and Computer and Information Science and Engineering (CISE)/Computer Network Systems (CNS) programs. Collectively, these grants established Clemson's South Carolina Connected Vehicle Testbed (SC-CVT), which has proven to be a state-wide community research resource in diverse areas ranging from connected and automated vehicles to domain-specific Internet of Things (IoT) studies.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle	5. Report Date
Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure (Part 1)	June 2020
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
James Martin, Ph.D.; ORCID: https://orcid.org/0000-0002-1698-6148 Gurcan Comert, Ph.D.; ORCID: https://orcid.org/0000-0002-2373-5013 Manveen Kaur, Ph.D. Student; ORCID: https://orcid.org/0000-0003-0003-5206 Adil Alsuhaim, Ph.D. Student; ORCID: https://orcid.org/0000-0003-4233-8045	

9. Performing Organization Name and Address	10. Work Unit No.
Clemson University School of Computing 100 McAdams Hall Clemson, SC 29634	**11. Contract or Grant No.** 69A3551747117

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Center for Connected Multimodal Mobility (C^2M^2) Clemson University 200 Lowry Hall, Clemson, SC 29634	Final Report (March 2018 – November 2019)
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Multiple studies have explored different forms of connected vehicle applications, such as queue warning and cooperative adaptive cruise control (CACC), in standard wireless access in vehicular environments (WAVE), and dedicated short-range communication (DSRC) network environments. A major focus of our ongoing research is to consider a hybrid vehicle-to-everything (V2X) infrastructure, one that supports multiple types of wireless networks. Our work has led to a system framework that allows WAVE applications to run in a system that is agnostic of the underlying network stack details. This research explores the uncertainty quantifications of cyber-attacks in V2X systems. Our results are summarized as follows: (i) a single malicious on-board unit (OBU) can significantly impair the channel, which would result in a significant increase in the average data loss rate and communication latency; (ii) a CACC platoon can easily detect an unreliable data stream and can fall back gracefully to a variant of adaptive cruise control (ACC), which we refer to as eCACC (emulated CACC). eCACC uses a local smart sensor that can estimate the velocity and acceleration of the preceding vehicle (vehicle ahead) of a subject vehicle; (iii) if there is a noise associated with a DSRC on-board unit in a vehicle within the CACC platoon, the system must fall back to standard ACC; and (iv) local and global adaptation algorithms are designed to maximize traffic flow while ensuring platoon string stability. In the follow-up report of this project (Part 2), we will present two statistical models, specifically two change-point models, for real-time V2I cyber attack detection in a connected vehicle environment.

17. Keywords	18. Distribution Statement
Cooperative and Adaptive Cruise Control (CACC), Dedicated Short Range Communications (DSRC), Wireless Access in Vehicular Environment (WAVE), Cybersecurity.	No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	30	NA

Table of Contents

List of Tables

List of Figures

EXECUTIVE SUMMARY

Multiple studies have explored different forms of connected vehicle applications, such as queue warning and cooperative adaptive cruise control (CACC), in standard wireless access in vehicular environments (WAVE), and dedicated short-range communication (DSRC) network environments. A major focus of our ongoing research is to consider a hybrid vehicle-to-everything (V2X) infrastructure, one that supports multiple types of wireless networks. Our work has led to a system framework that allows WAVE applications to run in a system that is agnostic of the underlying network stack details (note at this point that the WAVE messages are not standards-compliant). We assume edge infrastructure, inclusive of road-side units (RSUs) and intelligent signal controllers, participate in a distributed system. The reported research uses CACC as an illustrative application. The objective was to discover and evaluate design modalities that can be used to design CACC controllers (with underlying system support) that can detect unreliable or malicious nodes and further, mitigate the issues. This study includes unreliable sensing devices, such as RADAR or LiDAR devices, used to detect and generate information about the preceding vehicle (car ahead) of a subject vehicle. The level of sensor noise is one of several "uncertainty quantifications" that was studied in the research. The term refers to sources of error or impairment that can cause a vehicle-to-vehicle (V2V) application, such as CACC, to perform sub-optimally. Other examples of "uncertainty quantifications" are measures that describe the level of network impairment or application-oriented measures that describe, for example, stability measures of a particular CACC system. The results directly map to scenarios involving intelligent traffic signals and other road-side infrastructure that might be involved in the management of vehicular traffic. We envision that the CACC controller design can be extrapolated to intelligent traffic signals allowing them to operate as assistive actors in detecting and mitigating network impairment issues for CACC.

We report our research that explores resilient CACC controllers that can detect and adapt to a denial-of-service (DoS) cyberattack. Our research leverages Clemson University's South Carolina-Connected Vehicle Testbed (SC-CVT). This gives us access to a 1.3 mile stretch of roadway around campus that provides both DSRC and long-term evolution (LTE) coverage. Our CACC research has been motivated by the following top-level problem statement: CACC was designed to increase the traffic flow rate on roadways along with a secondary goal to minimize energy consumption. Safety was not a target goal for CACC. As CACC is redefined in the context of connected and autonomous vehicles, safety will be an inherent requirement for future CACC systems. Our problem formulation was to minimize the headway (which leads to maximal traffic flow) while ensuring the platoon string is stable (which minimizes the probability of a crash). Through experimentation, we were able to characterize the onset of instability in the CACC platoon. This characterization serves as a trigger for the CACC fallback strategies devised as a part of this work.

Our findings include:

- In a homogeneous platoon involving up to 100 vehicles, as long as there is no network impairment, CACC can maintain headways as low as 0.64 seconds while avoiding crashes and remaining stable. In the worst case of a network outage, the system falls back to ACC which requires a headway of at least two seconds to achieve stability. The difference in traffic flow between these two extremes depends on many details but the main result is traffic flow of a platoon managed by adaptive cruise control (ACC) can be significantly lower than when managed by CACC with a low headway.

- A homogeneous platoon involving up to 100 vehicles is impacted by congestion. We found that CACC must increase its headway to two seconds during heavy congestion.

- A single malicious OBU can significantly impair the communication channel and a CACC application. The specific impact depends on many details, but one data point is that the latency of basic safety messages (BSMs) in a platoon can increase from two ms to 20 ms by one malicious node. The CACC headway of a 50-vehicle platoon must increase to three seconds to achieve stability subject to one malicious node.

- We developed a set of fall back strategies when a platoon detects network impairment. The system first falls back gracefully to a variant of CACC we refer to as emulated CACC (eCACC). eCACC uses a local smart (LiDAR or RADAR) sensor that can estimate the acceleration of the car ahead. We use a Kalman filter method to find reliable acceleration. Our validation involved adding realistic levels of Gaussian noise to device samples.

- In worst-case scenarios, such as a DoS attack or wireless connectivity issues that lead to temporary network outages and the system would fall back to standard ACC.

- We develop and evaluate an adaptation algorithm that is designed to maximize traffic flow while ensuring platoon stability. This algorithm can be implemented in a decentralized node located either at the roadside (like an RSU or an Intelligent Signal Controller) or a participating vehicle of a platoon (like a node selected on basis of wireless coverage to all platoon vehicles). The adaptation decreases the headway during periods of robust network performance and increases the headway to match growing levels of network impairment. The algorithm defines a minimum headway that can be tuned to match the situation (e.g., fully autonomous vehicles versus partial autonomous control with human interaction). A global and a local version of the adaptation is developed and evaluated. The primary difference between the global and local control algorithms is that a global controller decides on the time headway based on the worst behaving location in the platoon. It instructs all nodes to move to the same larger headway value. The local algorithm, on the other hand, adapts its target time headway based only on the distance observed from the vehicle ahead. Therefore, the local approach results in heterogeneous controller settings based on local decision making. We find in general that traffic flow is higher when a local controller is used compared to a global controller.

CHAPTER 1

Introduction

This project is an extension of several ongoing projects involving the South Carolina-Connected Vehicle Testbed (SC-CVT). Figure 1 illustrates the mounted edge node along the Perimeter road that circles the main campus, which has dedicated short-range communication (DSRC) wireless coverage. A total of four Edge nodes have been deployed. We have conducted small scale tests involving cars equipped with a vehicle node. A vehicular node is a box that contains a general-purpose computer, a switch, and an on-board unit (OBU). In many cases, we use a development node instead of a vehicular node that replaces the general-purpose computer with an easier to use a laptop. The Edge node is similar except it contains a well-provisioned Intel NUC computer as the front-end processor. It also has a switch, power supply, and cables that run in and out of the ruggedized box. The edge nodes have two WiFi adapters – one contained in the NUC and one provided by a USB WiFi dongle that we added. The USB WiFi serves as the service port to the Edge node. We recently have deployed an LTE system and are in the process of integrating it with SC-CVT. We expect that both edge and vehicular nodes will be equipped with LTE dongles that can communicate with the campus LTE system.

Figure 1: Edge node mounted on a light pole.

Figure 2: Edge node chassis (left), fiber to Ethernet (top), RSU (top right).

Figures 1 and 2 illustrate one of the Edge Nodes. Power and fiber cables are carried up a light pole (in a weatherproof pipe) to the top where a passive conversion device performs a fiber to power over Ethernet function. An Ethernet (with power) is dropped from the fiber conversion device to the Edge node chassis. This provides the power and backhaul for the Edge node. A Cohda RSU is highlighted in Figure 2. A six-foot pole positions the radio above the roadway. The deployment follows the recommendations of the US DOT, which states that the RSU's should be mounted above the street. The RSU houses two independent radios, each configured to use separate six dB gain omnidirectional antennas. Power over ethernet cable runs from the Edge node to the RSU providing its backhaul and power. Three of the four Edge nodes are backhauled to the main campus network by fiber. The fourth referred to as the Jervey Gym Edge node (identified as B04 in Figure 3) relies on a dedicated point-to-point WiFi link between a WiFi USB dongle attached within the Edge node which acts as a WiFi client associating with a special SSID provided by a WiFi access point (AP) located across the street on top of Jervey Gym. This AP only associates with devices of the special SSID with the proper credentials.

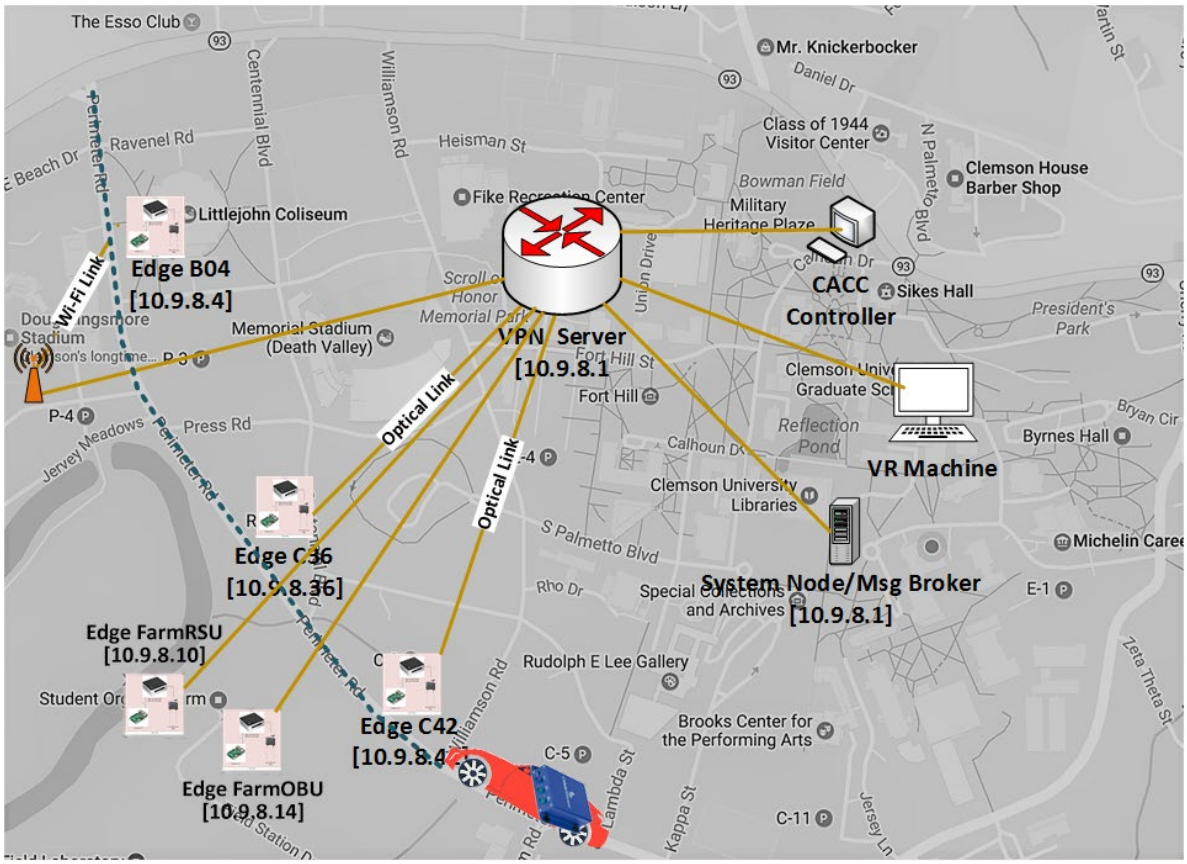


Figure 3: SC-CVT Network Diagram

Figure 3 illustrates the SC-CVT network diagram. Three Edge nodes are mounted to light poles along Perimeter road. The fourth Edge node is located at an experimental farm right off the Perimeter Road. Unfortunately, DSRC coverage does not extend from the farm location to the Edge nodes on Perimeter (actually, we just need to acquire a higher gain antenna and mount it roughly six feet in the air to prove line-of-site coverage). However, the farm area provides several unpaved roads that are not used frequently. This gives us a safe experimental environment that further allows us to perform repeatable experiments. To ensure secure transmissions, SC-CVT Edge nodes interconnect using a hub and spoke VPN gateway overlay network. As we will describe, our system was designed to serve as an Internet of Things (IoT) framework. The system consists of several nodes including vehicular, edge, compute, data nodes. Each runs the TGIF middleware which provides applications a simple C++ interface to access system functions. Examples of system functions include: publish a message, subscribe to one or more topic message streams, allocate a communications pipe, obtain the current location, establish a presence or learn of nearby nodes and services with discovery services. A vehicular node is effectively a light-weight Edge node. It might contain multiple communications interfaces (DSRC, commercial LTE, our campus LTE, WiFi). As we will point out shortly, a vehicular node can submit a vehicular message to our system. We have a special edge node, referred to as TGIF.clemson.edu) that is outside of the campus firewall. This allows a vehicle to transfer a message directly from the car to the TGIF Edge node over the commodity Internet without having to worry about dealing with campus network boundaries.

One of our goals has been to build "common infrastructure" on-campus that facilitates students/staff/faculty dropping IoT devices on campus that can leverage our wireless infrastructure to ingest the data. We describe our backend system shortly. The broader system is called Things in the Fog (TGIF). The SC-CVT is a subset of TGIF.

This report describes the research completed as a part of our C^2M^2 project. Research results from this project were produced a Ph.D. dissertation (Rayamajhi, 2019). It is important to point out the tight coupling of our project with the continued development and use of TGIF. The system is a data-centric system that extends the traditional WAVE framework with extensions to support a publish-subscribe paradigm. Machine specific language is translated to TGIF message formats to unify data arriving from different domain-specific systems that either share or are collocated with SC-CVT. As an example, when BSMs arrive at an Edge node, the message is transformed into a TGIF system message. A BSM message is represented abstractly as a Machine Heartbeat message. In the same sense, a video surveillance stream might generate periodic HeartBeat messages containing metadata that might describe observed activity or events. By collecting data from devices used by other research groups on campus, the system becomes a valuable source of heterogeneous data. One example that is relevant to our C^2M^2 project is that an intrusion detection system is likely to benefit from data that represents the aggregate from device data streams that cross research domains.

The term "uncertainty quantification" implies the set of metrics and techniques that could be used to detect anomalous behavior within a system. The system might be the lower-level network infrastructure, the edge computing framework, or domain-specific application systems that all operate concurrently in a specific geographic area. In this project, we developed several such metrics and techniques applied to an application system based on the concept of vehicular platooning. We summarize the broad problems of interest as follows:

- Cooperative adaptive cruise control (CACC) systems and its engineering are not well understood for large scale deployment.
- Performance and reliability of applications like CACC in actual DSRC based connected vehicles (CV) systems is not well understood.
- Performance subject to impaired conditions (caused by either network congestion or malicious activities) is not well studied.

The core research of this study focused on the following:

- Developing "Uncertainty Quantification" metrics and techniques that can be used to detect an impaired system.
- Developing techniques by which CACC might mitigate the impairment.

CHAPTER 2

Literature Review

2.1 Background on WAVE/DSRC

The DSRC protocol is based on a variant of the IEEE WiFi protocol. While similar to IEEE 802.11a with 802.11e QoS extensions, 802.11p is unique in several ways:

- It supports a new device mode of operation called Outside the Context of a Basic service set (OCB).
- It uses half the default channel size of WiFi (10 MHz channels).
- It supports broadcasts at all supported data rates (a small set of "basic data rates" that all nodes must understand). A transmitter is allowed to broadcast (and multicast) at any basic rate.
- It supports payloads of either IPV4, IPV6, or WAVE. Further, a WAVE message can be sent over either IP or WAVE.
- DSRC assumes seven sequential 10 MHz channels. It defines a single logical control channel (CCH) and six service channels (SCH). The binding of a logical channel to a physical spectral channel is to be done through periodic RSU service announcements.
- By default, an OBU operates in single radio mode, multiplexing the spectral channel with two DSRC logical channels. The time scale is 100 ms. The first 50 ms, the OBU must listen for announcements from RSUs. In the second 50 ms, the OBU can bind and use a logical SCH to any spectral channel.
- The details of how WAVE and IP coexist appear to be somewhat vendor-specific.

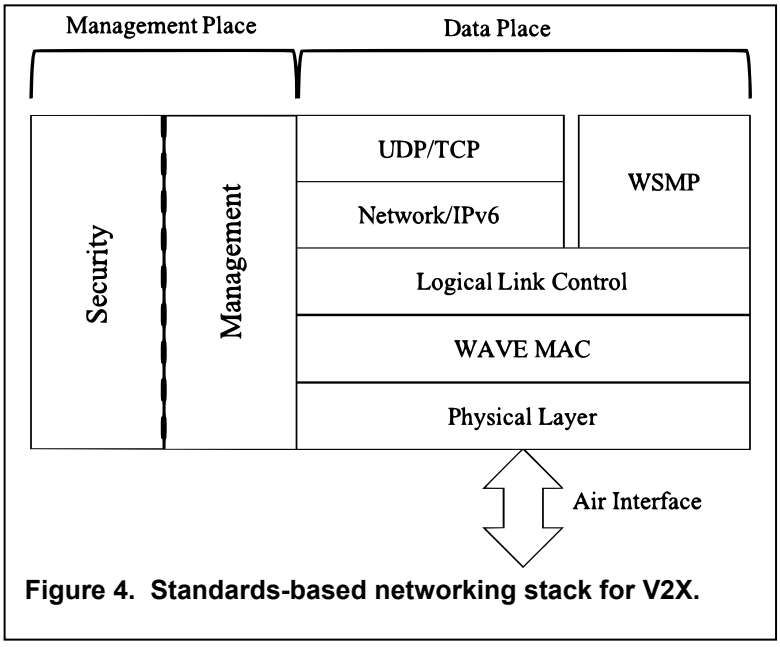


Figure 4. Standards-based networking stack for V2X.

As illustrated in Figure 4, the wireless access for vehicular environments (WAVE) stack can replace an IP transport and network layer with layers that are optimized for low latency broadcasts. The underlying modulation schemes used are orthogonal frequency division modulation (OFDM) with BPSK, QPSK, QAM-16, and QAM-64 schemes (Morgan, 2010; Li, 2010; Kenney, 2011; Abdelgader & Lenan, 2014). Authors in (Morgan, 2010; Li, 2010; Kenney, 2011; Abdelgader & Lenan, 2014) describe in detail the functionality of 802.11p physical layer operation. The enhancements to make the previous 802.11a protocol robust towards high mobility vehicular communication include increasing the OFDM symbol duration from four μs to eight μs (increasing the cyclic prefix from 0.8 μs to 1.6 μs) and introduction of Wireless Access in Vehicular Environments (WAVE) protocol that avoids the need of transport and network layers

in the traditional OSI model. These standards are detailed in ("IEEE Standard for Telecommunications;" "IEEE Standard for Wireless"). There have been studies on the analytic modeling of DSRC protocol to understand the behavior in multiple node scenarios by quantifying the probabilistic nature of transmission and latency. Results in (Shah & Mustari, 2016; Wu & Zheng, 2014) show the analysis based on a 2-D Markov model that can be used to model throughput, congestion, and latency analytically. The studies show that congestion occurs when 50 or more vehicles are periodically broadcasting BMS messages. The studies also look into the probability of collision, probability of transmission, throughput, and latency as the number of nodes increases to measure the performance of 802.11p in dense network conditions. Works in (Huang et al., 2017; Lee & Lim, 2013) look at the performance of 802.11p in a realistic network scenario with real DSRC compliant radios deployed in vehicles. The study in (Huang et al., 2017) concludes that line of sight and no line of sight significantly affect the performance of a DSRC network. In (Lee & Lim, 2013) a driving track for tests was created and the performance of a DSRC radio in terms of throughput, latency, and packet loss was compared with that of 802.11a Wi-Fi protocol.

In recent years, most of the research in the network layer of vehicular networks have focused on IPv6 and WAVE (Li, 2010; Kenney, 2011). WAVE implementation of the network layer contains functions related to short message service (WSMP), multichannel MAC layer, security, and network management as shown in Figure 4. The 802.11p total bandwidth of 75 MHz is divided into seven channels of 10 MHz each (six service channels SCH and one control channel CCH) and a mode in WAVE enables switching between two channels periodically for 100 ms (50 ms for each channel) called switching mode or continuous, unobstructed usage of one of the seven channels called continuous mode. Works shown in (Rasool et al., 2017; Song, 2017) show the multichannel operation of DSRC based on IEEE 1609.4 protocol. The synchronization is based on GPS enabled one ppm signal that allows all nodes in the vicinity to convene at CCH every other 50 ms and switch to appropriate SCH in the next 50 ms period. While in CCH, only the roadside units broadcast, and while in SCH, all the nodes contend for channel access based on Carrier-Sense Multiple Access, or CSMA. Several studies mentioned in (Rasool et al., 2017; "IEEE Standard for Information") look at Time-Division Multiple Access (TDMA) based channel access in which the motivation towards selecting a CSMA based channel access protocol is mostly based on the highly mobile vehicular environment with extremely fluctuating channel conditions and network topography. The system also supports IPv6 over SCH and can be configured to operate as an alternative to WAVE. Some work has looked at employing routing and mobility management leveraged by IPv6 over V2V and V2I communication by using address reconfiguration (Bigelow, 2019). In recent years, cellular V2X also known as C-V2X is being considered as an option to DSRC with huge support from the cellular companies (Rayamajhi et al., 2011). Technically, C-V2X works with the latest LTE (rev 14 or higher) using the proximity service in two modes, such as: (Boban et al., 2016; Molina-Masegosa & Gozalvez, 2017) if the V2V synchronization and resource allocation are managed by the infrastructure two. If the vehicles themselves manage the resources in cases where infrastructures become unavailable.

2.2 Background on Vehicle Platooning

Our study has selected cooperative adaptive cruise control (CACC) as an illustrative Connected and Autonomous Vehicles (CAV) application. We believe that this application along with other ones like forward collision avoidance, lane assistance, and queue warning will be prevalent in future CAV Systems. Forward collision avoidance, also known as rear-end collision avoidance, is a safety-critical application that alerts vehicles, in real-time, about the possible collision or roadway breakage in the same lane and direction of travel (Li et al., 2014; "Connected vehicle reference"). Present collision avoidance applications use radar and video cameras aligned at the front of the vehicle to detect physical objects in the direction of travel. These devices render a

small view angle where DSRC can provide a complete 360 view around a vehicle without any obstructions. Current autonomous vehicles use LiDAR or video cameras for visually rendering the surrounding environment such as Velodyne's LiDAR used in Google's self-driving cars (Popper, 2017).

There have been studies in the past that look at forward collision avoidance using DSRC technology to alert the drivers of imminent collision (Dey et al., 2016) that show how effective DSRC can be in that scenario. One of the types of vehicle platooning applications is CACC where the velocity and acceleration of the following vehicle in a vehicle pair are controlled to maintain proper headway distance from the leading vehicles. The information about the preceding vehicle's velocity and acceleration is transmitted using wireless broadcasts to the following vehicle. In contradiction to the earlier version of platooning called adaptive cruise control (ACC), CACC requires broadcasting of vehicle status messages to the following vehicle through a reliable wireless network. There has been a tremendous amount of research in CACC (Naus et al., 2010; Ploeg et al., 2013; Milanés et al., 2013; Lei et al., 2011; Biron et al., 2018; Ploeg et al., 2014) mostly focused on theoretical assumptions of a platoon as well as the characteristics of the wireless communication network.

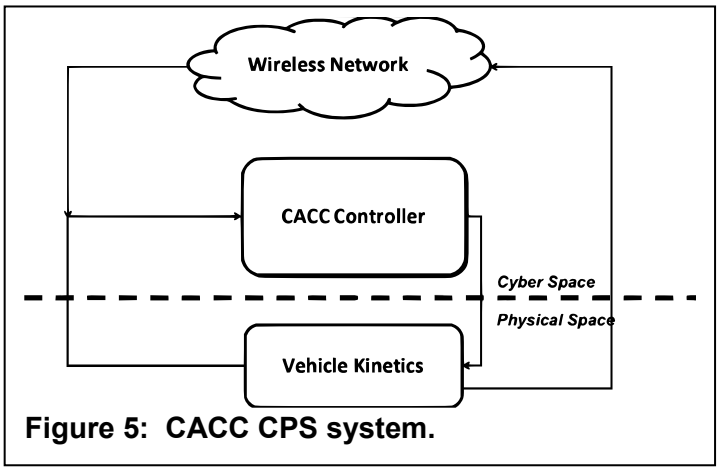


Figure 5: CACC CPS system.

Figure 5 shows CACC defined from a Cyber-Physical System (CPS) perspective that regulates the acceleration of an ego vehicle {vehicle in consideration} in a platoon based on the acceleration of preceding vehicle(s) received over a wireless vehicular ad-hoc network (VANET) (Shladover, 2014) and local sensor readings of the distance separating back bumper of the leading vehicle to front bumper of the ego vehicle. The system can be easily viewed as an instance of a CPS because of how information collected from the regulated vehicle (physical space) is used to calculate parameters (cyberspace) that are recursively utilized to control the same physical system. This opens up aspects of our research where we develop controller modules that act as a component to the cyberspace and helps to better regulate the vehicle. The wireless protocol in a vehicular ad-hoc network is based on 802.11p or dedicated short-range communication (DSRC) protocol and the local sensors considered are either LiDAR or radar sensors. The set of vehicles collaborating in a CACC are called a CACC platoon. A CACC provides better speed harmonization over the length of the platoon and increases safety by creating a tighter coherence between each vehicle and their movement pattern by constantly broadcasting the mobility information. The air drag is considerably reduced towards the tail of the platoon allowing smaller torque to be actuated from vehicular mechanics which eventually reduces the aggregate energy consumption of the CACC platoon (Naus et al., 2010; Shladover et al., 2014). In recent years, CACC and platooning applications are being considered for an arterial network of roads and implemented mostly for reducing energy consumption (eco-driving) as well as safe stopping distance estimation at intersections. However, our study concentrates on freeway, single-lane truck platoons and defines CACC as a platooning application to improve highway throughput stably and safely.

It is evident in the past literature (Ploeg et al., 2014; Biron & Pisu, 2016; Biron & Pisu, 2015) that the availability of co-operative information of other (mainly immediate leader) vehicles is the most integral part of a stable and safe platooning application. In most cases, the co-operative information is available through wireless networks and has been shown that the lack of reliable communication could result in unstable and unsafe events (e.g., crashes, pileups). The loss in communication due to packet drops has been studied and tested in a real-world test-bed (Rayamajhi et al., 2018), and results conclude that in reality, a significantly large number of consecutive packet loss occurs more frequently than previously assumed. It was shown in (Rayamajhi et al., 2018) that lack of line of sight, the presence of other vehicles in the vicinity, and the topography of the roadway can impact the performance of vehicular networks. The block packet loss can trigger instability in a platoon due to uncontrolled acceleration or oscillations in the parameters that CACC controllers are designed to mitigate e.g. amplification in the separation error, oscillations in measurable parameters like acceleration, velocity and jerk (rate of change of acceleration) which render the platoon unstable (Ploeg et al., 2013). Such behavior can lead to instability in a platoon which is deemed very unsafe for traffic applications (Ploeg et al., 2011). In practice, such scenarios of large packet loss can occur in a realistic platoon when it approaches an infrastructure that could be acting maliciously to prevent channel access for any vehicles in the platoon; this eventually causes the platoon to lose transmissions of all basic safety messages (BSM). The effect of wireless channel access is more prevalent in DSRC because of the protocol design. DSRC is based on random channel access protocol, it is fairly comfortable to consider that an erroneous and disruptive infrastructure can overcrowd the channels with a large number of continuous broadcasts originating from its transmitter. Another scenario of interest could be a faulty communication unit in one or more of the participating vehicles.

The past literature reflects various control theoretic approaches to controller design for the CACC application (Milanés et al., 2013). Most of the focus exists in the form of string stability analysis to understand the effect of changes in velocity and acceleration of the front vehicle and its rippling effect on the following vehicles. Some previous work exists where vehicles with autonomous or semi-autonomous capabilities have been configured to support CACC and tested for stability of platoon with varying network performance (Milanés & Shladover, 2014; Gao et al., 2016). Also, many papers provide modeling of the DSRC link between two CACC platoon vehicles and try to evaluate the effect of network behavior on the stability of the CACC system (Biron et al., 2018; Ploeg et al., 2014; Biron & Pisu, 2016). One of the assumptions made in previous work is that the average packet loss rate of BSMs transmitted between two vehicles is very low and further, the loss process can be modeled as a Bernoulli random process, where events are independent of one another. Therefore, the probability of a vehicle observing a gap in the BSM stream is negligible (Biron et al., 2018). We will show that this statement is not always true. The related work also assumes all vehicles synchronously update their velocity and acceleration to the following vehicles. It is also assumed that all vehicles have a method for measuring the accurate distance and relative velocity of the car ahead. Further, it is also assumed that all vehicles are in a single lane and avoid scenarios common to platoon formation in CACC such as merging and splitting of a platoon. Earlier works on the CACC platoon have looked into understanding and characterizing string stability for vehicles in a platoon (Ploeg et al., 2011) understanding the effect of sensor failures, cyber-attacks and security threats on the vehicles in a platoon (Biron et al., 2018; Biron & Pisu, 2016) and finding ways to improve traffic throughput on an arterial roadway network using a tightly coupled platoon of vehicles (Lioris et al., 2017). There is limited research that looks at how the system behaves during long periods of blackouts in the wireless network. We found that the wireless communication necessary for the cooperative aspect of platooning could come under harsh environments and malicious network behaviors that need to be accounted for, to characterize a stable platoon. Authors of (Harfouch et al., 2017; Wang et al., 2017) have presented methods to maintain stability and control of a platoon by switching from

one mode of data acquisition to another. Studies such as (Harfouch et al., 2017; Wang et al., 2017) provide switching criteria and methods to turn a CACC system into an ACC system.

However, it is well understood that that ACC systems are not stable or efficient for shorter headway time and longer platoon. We believe that integrating the local sensors to supplement the loss of valuable information about the preceding vehicle (acceleration, velocity, separation) could help in maintaining a stable platoon during spotty communications. Work shown in (Ploeg et al., 2014) developed an algorithm to estimate the acceleration of leading vehicle through distance and velocity readings from local sensors using an estimation technique. It is limited in providing a realizable formulation of the problem, as well as testing when the platoon is a mix of different types of controllers – CACC, ACC, or Manual Driving. We observed the following limitations and assumptions in the prior research:

- Limitations due to a single lane of vehicles assuming there are no cross-longitudinal driving patterns.
- Homogeneous controller behavior assumptions due to homogeneous vehicles.
- Ill-defined assumptions related to controllers that attempt to mimic human driving or driving characteristics acceptable by human riders. These assumptions may be ill-fitting in a CAV domain.
- Limitations on deliberating ACC as the fall back controller mechanism in case communication among vehicles becomes unavailable.
- Difficulty in modeling and reproducing published results due to insufficient information provided in the past literature.

A possible deployment path for this application will be to support autonomous trucks running in dedicated platoon traffic lanes as studied in (Gao et al., 2016). Minimizing the average headway between all trucks in the platoon leads to maximal fuel efficiency as well as roadway throughput efficiency. This application has been widely studied by the ITS area in its earlier form known as adaptive cruise control (ACC). In ACC, each vehicle requires a Lidar or radar device to maintain the distance between it and the vehicle ahead. CACC uses the DSRC network to share acceleration (in some cases position and speed) data among participating vehicles along with on-board sensors like LIDAR and radar which makes the inter-vehicle relative distance very small compared to ACC. Connectivity adds robustness to the application by permitting more precise information (the acceleration of the car in front).

Recent research highlights a merging of connected and autonomous vehicle research with CACC. The set of connected vehicle applications that are now widely common as safety features in new vehicles are being explored in a connected and autonomous vehicle (CAV) environment. This reformulates CACC as a two-dimensional control problem. While adding complexity, it adds the modeling dimensions necessary to explore CACC with scenarios involving lane change and interaction with infrastructure. As described in (Levison et al., 2011; Febbo et al., 2017; Siegel et al., 2018; Funke et al., 2016; Lin et al., 2018) control of autonomous vehicles involves complex optimization of large amounts of time-sensitive, locally derived, sensing information.

One approach used for reducing computational complexity is to engage a two-level controller. A high-level path planner that generates a reference trajectory (a prediction horizon), and a vehicular controller that ensures the vehicle follows the path in an optimal manner. A model predictive control (MPC) technique is commonly used to deal with non-linear optimization aspects

and can handle constraints. The car following control from prior CACC is now inherently performed by the Autonomous Vehicle (AV) controller. References (Schmidt, 2017; Semsar-Kazerooni et al., 2017) are illustrative of recent CACC research that considers longitudinal control ranging in lane changes and obstacle maneuvering. In (Schmidt 2017), CACC lane change is explored by introducing a virtualized vehicle to guide the vehicle changing lanes through the process. The concept of artificial potential fields is applied in (Tiaprasert et al., 2019) to the car following problem with a lane change. The work in (Semsar-Kazerooni et al., 2017) develops a method by which a signal controller can detect and characterize a platoon of vehicles that pass through the intersection (or presumably any RSU on a roadway). Observed V2V messages are analyzed, and applied to a CACC model to estimate the operating parameters for the platoon.

CHAPTER 3

Research Approach, Analysis and Results

3.1 Research Approach

The research methods and overall flow of work activities are summarized as follows:

- First, we established techniques to detect the onset of congestion and the impairment caused by one form of malicious attack, a simple network denial of service.
- Second, we developed models (analytic, simulation based on MATLAB, and then on ns3) to develop a CACC application system.
- Third, we defined application-oriented metrics that quantify the impacts of the "uncertainty quantifications" at the application system level.
- Fourth, we empirically obtained the utility function that mapped network impairment to a measure of application system performance.
- Fifth, we developed application system-level mitigation techniques that allowed the platoon to continue despite the impairment.

3.2 System Model

In the previous section, Figure 4 illustrates the dual-stack V2X system that we have studied. Here, Figure 6 highlights the 802.11p MAC layer. A vehicle can send and receive WAVE messages over IP or the 1609 network stack. The 802.11p Task Group has defined a standard set of messages. A specific WAVE/DSRC vendor decides the extent to which IP and WAVE can interoperate. In our system, any standard WAVE message can be broadcast (and received) using either DSRC or IP. In both cases they make use of the IEEE 802.11p Link and physical layer standards. DSRC supports both unicast or broadcast.

In infrastructure-based 802.11(WiFi) variants such as 802.11a or 802.11n, a broadcast requires the transmitter to first sense the carrier for channel traffic. If it observes no carrier traffic for a certain time, the message will be broadcast. An ACK is not issued for broadcast messages. The broadcast is received by all stations within the transmission range. A predefined "basic rate" (or set of basic rates) is defined for each WiFi family. Early WiFi standards assumed the basic rate of six Mbps. 802.11n allows a basic rate of six, 12, or 24 Mbps. IEEE 802.11p permits broadcast and multicast at all supported modulation and coding schemes.

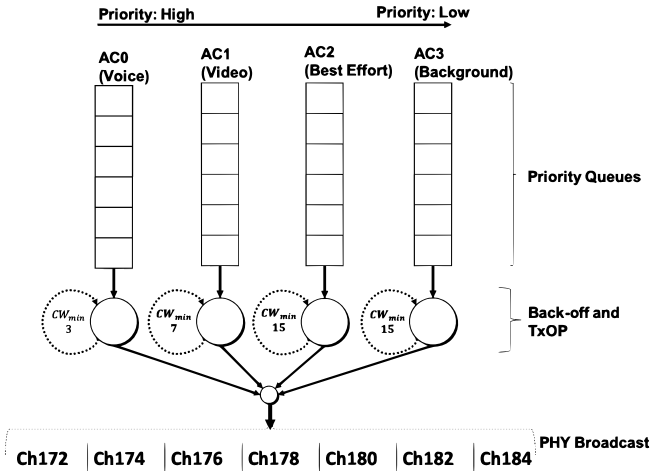


Figure 6. 802.11p system.

All vehicles participating in a platoon sends BSM messages at a rate of 10 per second. Each vehicle can receive BSMs from any vehicle. The CACC controller can process BSM streams from all cars in front. Our work is based on the Ploeg model which requires a vehicle to only process messages from the car immediately ahead (Ploeg et al.,

2011). Refer to (Ploeg et al., 2011) for a very good tutorial on the different formations and types of platoons that have been considered.
An actual platoon must deal with joins, merges, and exits of vehicles. We simplify our analysis by assuming the platoon has been formed and each vehicle knows the ID of the car in front.

Illustrative simulation experiment

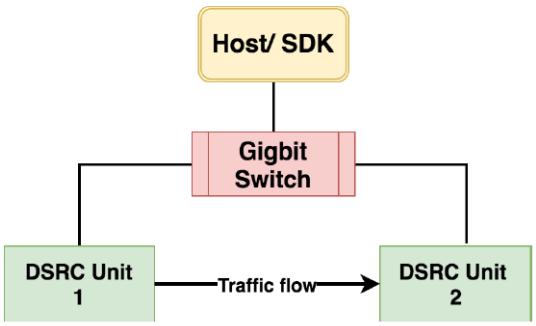


Figure 7: Set 1 Experiments.

Figure 7 illustrates a simple experiment designed to help us validate our experimental methodology. The scenario involves two vehicles, Unit 1 is the sender, Unit 2 is the receiver. Some analytic models provide the expected measured throughput and latency over the link in best-case conditions. Figure 8 illustrates the effective throughput of different modulation & coding schemes. Figure 9 shows the end-to-end latency results. Latency is calculated as the average of per-packet latency observed at the receiver. The packet sending rate for the latency experiment is 10 packets/second with each packet containing 1000 bytes of user data. By comparing all measurement data with the results of equivalent experiments using the ns3 simulator, we validate at least in part the ns3 simulation model.

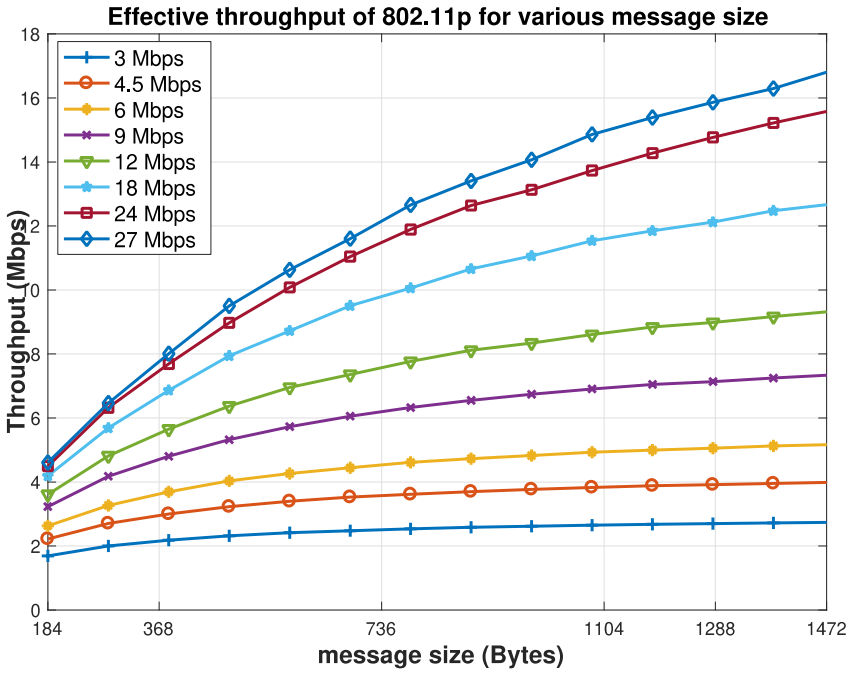
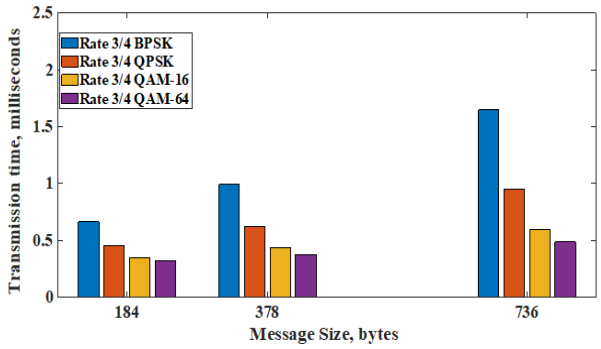
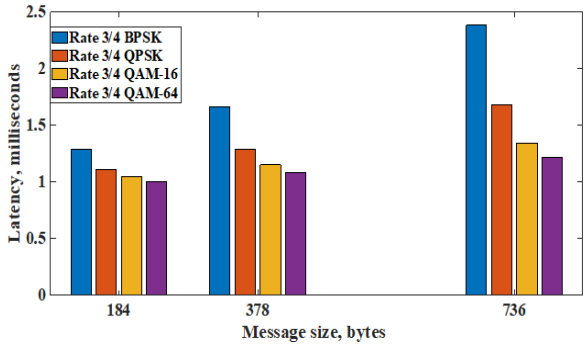


Figure 8 Throughput results.



Calculated nominal transmission time



Observed end-to-end latency

Figure 9 Observed latency.

3.3 Uncertainty Quantifications

Unexpected scenarios such as large packet loss, network impairment due to the presence of a malicious node, and abrupt actions of a participating platoon member could lead to disturbance in platoon stability and impact platoon safety. In such cases where the communication is impacted, the traditional fallback option for the CACC model is to switch to ACC. Emulated CACC is the alternative to falling back on ACC subject to the availability of relevant information.

To simulate a realistic packet loss scenario, we use the metric “Mean Burst Length”, MBL, which measures the average length of burst loss packets. We can also define “Mean Good Length”, MGL, to mean the average length of packets delivered successfully between two loss events. These metrics can provide insight into the reliability of the system. Both metrics imply that they involve two or more packets. So, we can formally define them as follows:

$$MBL = \frac{\sum_{i=2} L_i \times i}{\sum L_i}, MGL = \frac{\sum_{j=2} G_j \times j}{\sum G_j}$$

We also define the reliability metric of the communication network as the ratio of packets that were successfully received to the total number of packets that were expected

$$R = 1 - \frac{N_{failed}}{N_{total}}$$

One of the components of the CACC enabled vehicle shown in figure 10 is a switching controller. The function of the switching controller is to weigh the incoming information from the lead vehicle via broadcast against the information received using the local sensor (Radar or LiDAR) and using the more reliable version of information between the two sources to implement CACC. This variant of CACC operations based on local sensor estimation of lead vehicle acceleration is called emulated CACC.

3.4 CACC Model

Figure 10 illustrates the CACC controller. CACC is a robust vehicle speed control algorithm that works towards the objective of minimizing the distance between two consecutive vehicles by coordinating the acceleration between vehicles. CACC is an extension of Adaptive Cruise Control (ACC). ACC regulates the speed of the subject vehicle based on the monitoring of distance and relative speed of the vehicle in front of its perspective. This results in limitations in minimization of inter-vehicle separation and overall platoon stability; both of which are important in realizing

the goals of traffic mobility and fuel efficiency. CACC has been shown to provide more optimal inter-vehicle separation values and higher stability for the platoon.

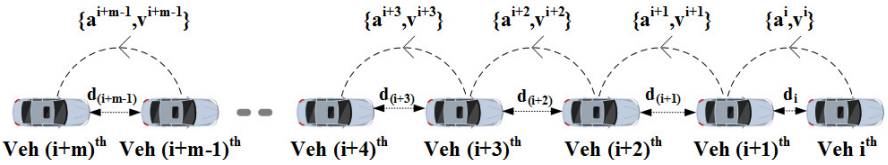
Part 1: Platoon Controller Equation (Ploeg et al., 2011)

The controller uses either the current acceleration of the lead vehicle $a^{i-1}(t)$ or the lead vehicle's target acceleration $u^{i-1}(t)$

$$d_{r,i}(t) = d_{stop} + h \times v_i(t)$$

$$e_i(t) = d_i(t) - d_{r,i}(t)$$

$$\dot{u_i}(t) = -\frac{1}{h}a_i(t) + \frac{1}{h}(k_p \times e_i(t) + k_d\dot{e}_i(t)) + \frac{1}{h}a^{i-1}(t)$$



Part 2: Vehicle Mobility (piecewise linear)

$$a_i(t) = a_i(t - t_0) + \dot{a}_i \times t$$

$$v_i(t) = v_i(t - t_0) + a_i(t - t_0) \times t + \dot{a}_i(t) \times \frac{t^2}{2}$$

$$d_i(t) = v_i(t - t_0) + a_i(t - t_0) \times \frac{t^2}{2} + \dot{a}_i(t) \times \frac{t^3}{6}$$

Figure 10 CACC controller model.

A CACC platoon consists of a finite string of vehicles where the first vehicle in the string is designated the leader vehicle and all other vehicles are jointly referred to as the set of following vehicles. Communication between vehicles is facilitated through DSRC 802.11p standard with OFDM and CSMA MAC protocols. While there are multiple variants of the communication strategy employed by CACC, this work considers a strategy where each vehicle in consideration (ego vehicle) only considers the information coming from the vehicle preceding itself (lead vehicle) as relevant. Additionally, maintenance of constant time headway is used for gap regulation. Time headway is defined as the time taken by two consecutive vehicles to pass the same point on the roadway. The CACC controller assumes piece-wise linear vehicular dynamics and uses the set of equations defined in Figure 10 to calculate the distance traveled (d_i), velocity (v_i), and acceleration (a_i) for any vehicle i. The value t_0 in these equations refers to the earlier time instance at which these values were calculated.

The platoon controller as shown in the CACC enabled vehicle in Figure 10 is responsible for calculating the target acceleration of the ego vehicle. It is governed by the set of equations defined in 10.2. $v_i(t), a_i(t)$ and $\dot{u_i}(t)$ are the velocity, acceleration, and change in acceleration calculated by the platoon controller at time t. d_{stop} is the standstill distance between the two vehicles, and the time headway is h seconds. For details of how the platoon controller computes the acceleration to be maintained by the vehicle in the next CACC operation, refer to (Rayamajhi, 2019).

Comparison of performance in traditional ACC and emulated CACC was conducted. The two fallback options to CACC were evaluated on the headway supported by them while maintaining

stability and the flow rate (vehicles/second) supported by them for different theoretical and practical acceleration profiles. Tests were conducted under varying network scenarios of no packet loss, complete outage, congested network, presence of a malicious node, intermittent packet loss burst, and longer burst lengths. Emulated CACC was found to provide better performance than ACC on all analyzed accounts.

We have already shown the measured throughput and latency are identical to the results expected by analytic modeling (Lee & Lim, 2013).

We've shown that:

- Realistic loss processes are unlikely to be stationary- they will continuously evolve. The extent of the loss can range from zero to a complete outage (for some time).
- We have shown this requires a fall back to eACC. Refer to the dissertation for the impacts of uncertainty when applied to the lidar sensors.
- We have shown congestion impacts CACC as the number of cars approaches 50
- We have shown a malicious node can significantly impact CACC although the effects might be masked if the platoon is suffering from network congestion.

However, all of this suggests a dynamic algorithm is potentially helpful.

3.5 Mitigation Techniques

CACC relies on the wireless communication network, where data received from lead vehicles are used as an input to the system. When the communication network becomes unreliable, the system can be configured to fall back to one of two methods

- eCACC (Emulated CACC), which emulates the behavior of CACC, but uses local sensors: local vehicle sensors such as lidar are used to estimate lead vehicle's velocity and acceleration instead of using a communication network.
- Conventional ACC approach.

3.6 Experiment Setup and Results

We set up a simulation using an ns3 network simulator that supports WAVE communication. Initially, we set up a simple scenario involving two stationary vehicles, with one outgoing flow using different modulation and coding schemes and 802.11e access categories. We illustrate that the effective throughput in such a simple scenario does not reach the nominal throughput as shown in Figure 8, and is dependent on packet size. The following table shows more detailed results when using the four different QoS access categories (Voice, Video, Best Effort, and Background) using a packet size 1472 bytes.

Table 1: Effective throughput using different MCS & QoS queues.

MCS	1/2 BPSK	3/4 BPSK	1/2 QPSK	3/4 QPSK	1/2 QAM16	3/4 QAM16	2/3 QAM64	3/4 QAM64
M bits/symbol	24	36	48	72	96	144	192	216
Th_{nom} (Mbps)	3	4.5	6	9	12	18	24	27
Th_{eff}(Mbps)								
Voice	2.82	4.16	5.48	7.97	10.39	14.77	18.71	20.53
Video	2.79	4.11	5.38	7.77	10.04	14.08	17.62	19.23
Best Effort	2.73	3.98	5.17	7.33	9.32	12.70	15.50	16.74
Background	2.71	3.93	5.08	7.15	9.04	12.18	14.75	15.86

The results are interesting as they show the unpredictability of the existing WAVE standard. Even in an isolated setup with no competing traffic. This also illustrates why the existing CSMA-based channel access strategy cannot provide performance or bounded latency guarantees, which motivates further research into TDMA-based channel access mechanisms.

Table 2: Burst loss processes.

Loss Mode	b_L	g_L
No Loss	1	100000
Complete Outage	100000	1
Congested	30	1
Malicious	150	1
On-Off	50	50
Long Burst	1000	300

For CACC simulation, we create an ns3 simulation environment of up to 10 vehicle nodes that are equipped with a wireless communication device based on the 802.11p standard. In addition, we simulated sensor reading and introduce random Gaussian noise to it to make it more realistic, as sensors are not perfect. The platoon leader follows predefined sets of acceleration profiles. Some of the profiles are generated using linear, sinusoidal, step functions, and acceleration profiles obtained from real vehicles. For a given experiment, the platoon leader accelerates and decelerates over time following the given acceleration profile. The platoon leader either report their current acceleration or their target acceleration. The simulation use broadcast messages that can be received by all vehicles. However, vehicles only handle messages from the vehicle in front of them in the platoon.

We also use the desired headway time as an input to our experiments. Simulation experiments are set to stop when a crash occurs, or when the simulation time limit is reached. We run various scenarios with predefined MGL and MBL values to simulate packet loss processes such as congestion, malicious node attack, on-off scenarios, and complete outage as shown in Table 2.

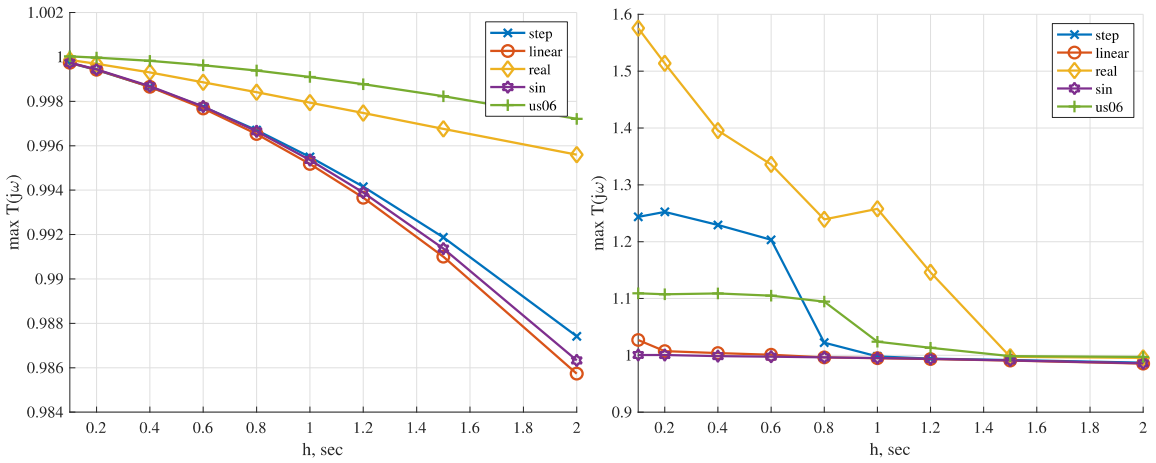


Figure 11: CACC string stability with no packet loss (left) and congested network (right).

Performance metrics used are vehicular flow rate, string stability, and time-to-crash. When we set the headway time parameter low, we get high vehicular traffic flow, but this also makes crashes more likely to happen earlier.

Figure 11 shows string stability measure, $\max\|\mathrm{T}(jw)\|$ for various headway time h values for different acceleration. For a stable platoon, the value of $\max\|\mathrm{T}(jw)\| \leq 1$. We can clearly see the difference in platoon stability between an experiment with no packet loss versus one with network congestion. Network congestion causes platoons with lower headway time value to be more unstable, requiring a high headway time of 1.5 seconds or more for a stable platoon. We found that the more reliable the communication network is, the more likely that we can have a stable platoon with shorter headway time. Using traditional ACC as a fallback method when network degradation occurs, requires the use of higher headway time value, making it less ideal than using CACC with local sensors.

Finally, because desired headway values are dependent on network reliability, we devise a dynamic headway assignment algorithm to adjust the desired headway time values according to network reliability: when the network becomes unreliable, the headway time is increased, and when a network becomes reliable we decrease the headway distance.

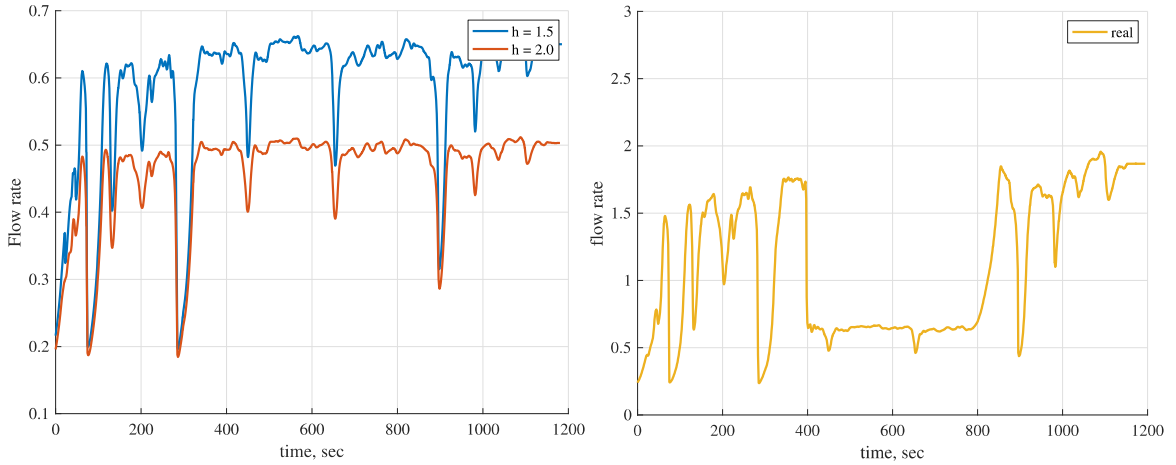


Figure 12: Vehicular traffic flow rate using fixed headway time values (left) and adaptive (right) for a CACC experiment that uses real acceleration profile in a congested network.

The results shown in Figure 12 shows that dynamic headway time assignment yields a better overall flow rate of traffic. In all of our CACC experiments, a headway time of 1.5 seconds or larger resulted in stable platoons under most network conditions. However, this sacrifices traffic throughput for safety concerns. Dynamically assigning the desired headway value shows significant improvement in throughput while maintaining a safe CACC operation.

CHAPTER 4

Conclusions – key findings

CACC can improve highway throughput and increase safety in our roadways, and decrease fuel consumed by the vehicles. It has many benefits that have bolstered it to be an important connected and automated vehicle application heavily favored to be pushed out in the near future. It's evident that if properly designed and deployed, the CACC can be a driving force in the future transportation system that is seemingly going to be overrun by automated and connected vehicles. Therefore, a complete understanding of various implications of CACC and many factors that play a vital role in governing its safe and stable form is timely. We have studied CACC by observing the system into various aspects of its operation and by simulating as well as testing in real-world applications. A wireless network is an important component of the platoon and many previous studies lack the details necessary to understand the system from more realistic perspectives where the wireless network is possibly impaired, congested, or under malicious attack.

Our results are summarized as follows:

1. A single malicious on-board unit (OBU) can significantly impair the channel, which would result in a significant increase in the average data loss rate and communication latency;
2. A CACC platoon can easily detect an unreliable data stream and can fall back gracefully to a variant of adaptive cruise control (ACC), which we refer to as eCACC (emulated CACC). eCACC uses a local smart sensor that can estimate the velocity and acceleration of the preceding vehicle (vehicle ahead) of a subject vehicle;
3. If there is a noise associated with a DSRC on-board unit in a vehicle within the CACC platoon, the system must fall back to standard ACC; and
4. Local and global adaptation algorithms are designed to maximize traffic flow while ensuring platoon string stability. As any realistic environment will be prone to dynamic conditions, both algorithms show they adapt and achieve expected benefits. The results suggest that a local algorithm achieves better results, however, this could be an artifact of the choice of global algorithm and the set of scenarios studied.

The work that was performed was a necessary step before the scope of the system under study was increased to include intelligent traffic controllers. We assume future intelligent traffic controllers are a specialized node in our system under study. Current and historical research on the topic focuses mainly on improving the traffic flow when the signal controllers join the cyber-physical systems defined by connected and automated vehicles. So far, we have performed simulations where the global headway controller operated at roadside infrastructure (such as a traffic controller). Depending on the vehicle speed, the controller might not have sufficient information to accurately identify either congestion of network impairment. At a low vehicle speed or if a platoon of vehicles stops at the intersection, the controller could perform accurate system analysis, perhaps even identify the malicious nodes. It could mitigate by requesting all nodes except the malicious nodes to change to a new channel. We plan on exploring these ideas in the future.

In the follow-up report of this project (Part 2), we will present two statistical models, specifically two change-point models, for real-time V2I cyber attack detection in a connected vehicle environment.

REFERENCES

Bigelow, P. 2019, A new connected-car battle: Cellular vs. DSRC, Automotive News, https://www.autonews.com/mobility-report/new-connected-car-battle-cellular-vs-dsrc [1 May 2019]

Boban, M., Manolakis, K., Ibrahim, M., Bazzi, S. and Xu, W., 2016, October. Design aspects for 5G V2X physical layer. In *2016 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 1-7). IEEE.

Harfouch, Y.A., Yuan, S. and Baldi, S., 2017. An adaptive switched control approach to heterogeneous platooning with intervehicle communication losses. *IEEE Transactions on Control of Network Systems*, *5*(3), pp.1434-1444.

Lioris, J., Pedarsani, R., Tascikaraoglu, F.Y. and Varaiya, P., 2017. Platoons of connected vehicles can double throughput in urban roads. *Transportation Research Part C: Emerging Technologies*, *77*, pp.292-305.

Abdelgader, A.M. and Lenan, W., 2014, October. The physical layer of the IEEE 802.11 p WAVE communication standard: the specifications and challenges. In *Proceedings of the world congress on engineering and computer science* (Vol. 2, pp. 22-24).

Biron, Z.A. and Pisu, P., 2015. Distributed Fault Detection and Estimation for Cooperative Adaptive Cruise Control System in a Platoon. In *PHM conference*.

Biron, Z.A. and Pisu, P., 2016. Sensor and actuator fault detection in connected vehicles under a packet dropping network. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *10*(6), pp.1114-1120.

Biron, Z.A., Dey, S. and Pisu, P., 2018. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, *19*(12), pp.3893-3902.

Connected vehicle reference implementation architecture. [online] available at: https://local.iteris.com/cvria [15 October 2017]

Dey, K.C., Rayamajhi, A., Chowdhury, M., Bhavsar, P. and Martin, J., 2016. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. *Transportation Research Part C: Emerging Technologies*, *68*, pp.168-184.

Febbo, H., Liu, J., Jayakumar, P., Stein, J.L. and Ersal, T., 2017, May. Moving obstacle avoidance for large, high-speed autonomous ground vehicles. In *2017 American Control Conference (ACC)* (pp. 5568-5573). IEEE.

Funke, J., Brown, M., Erlien, S.M. and Gerdes, J.C., 2016. Collision avoidance and stabilization for autonomous vehicles in emergency scenarios. *IEEE Transactions on Control Systems Technology*, *25*(4), pp.1204-1216.

Gao, S., Lim, A. and Bevly, D., 2016. An empirical study of DSRC V2V performance in truck platooning scenarios. *Digital Communications and Networks*, *2*(4), pp.233-244.

Huang, X., Zhao, D. and Peng, H., 2017. Empirical study of DSRC performance based on safety pilot model deployment data. *IEEE Transactions on Intelligent Transportation Systems*, *18*(10), pp.2619-2628.

IEEE Standard for Information technology--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," in *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)*, vol., no., pp.1-212, 11 Nov. 2005

IEEE Standard for Telecommunications and Information Exchange Between Systems LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band," in *IEEE Std 802.11a-1999*, vol., no., pp.1-102, 30 Dec. 1999. doi: 10.1109/IEEESTD.1999.90606

IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services," in *IEEE Std 1609.3-2016 (Revision of IEEE Std 1609.3-2010)*, vol., no., pp.1-160, 29 April 2016 DOI: 10.1109/IEEESTD.2016.7458115

Kenney, J.B., 2011. Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE*, *99*(7), pp.1162-1182.

Lee, S. and Lim, A., 2013. An empirical study on ad hoc performance of DSRC and Wi-Fi vehicular communications. *International Journal of Distributed Sensor Networks*, *9*(11), p.482695.

Lei, C., Van Eenennaam, E.M., Wolterink, W.K., Karagiannis, G., Heijenk, G. and Ploeg, J., 2011, August. Impact of packet loss on CACC string stability performance. In *2011 11th International Conference on ITS Telecommunications* (pp. 381-386). IEEE.

Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, S., Kolter, J.Z., Langer, D., Pink, O., Pratt, V. and Sokolsky, M., 2011, June. Towards fully autonomous driving: Systems and algorithms. In *2011 IEEE Intelligent Vehicles Symposium (IV)* (pp. 163-168). IEEE.

Li, L., Lu, G., Wang, Y. and Tian, D., 2014, October. A rear-end collision avoidance system of connected vehicles. In *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)* (pp. 63-68). IEEE.

Li, Y.J., 2010, November. An overview of the DSRC/WAVE technology. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (pp. 544-558). Springer, Berlin, Heidelberg.

Lin, S.C., Zhang, Y., Hsu, C.H., Skach, M., Haque, M.E., Tang, L. and Mars, J., 2018, March. The architectural implications of autonomous driving: Constraints and acceleration. In *ACM SIGPLAN Notices* (Vol. 53, No. 2, pp. 751-766). ACM.

Milanés, V. and Shladover, S.E., 2014. Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data. *Transportation Research Part C: Emerging Technologies*, *48*, pp.285-300.

Milanés, V., Shladover, S.E., Spring, J., Nowakowski, C., Kawazoe, H. and Nakamura, M., 2013. Cooperative adaptive cruise control in real traffic situations. *IEEE Transactions on Intelligent Transportation Systems*, *15*(1), pp.296-305.

Molina-Masegosa, R. and Gozalvez, J., 2017. LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications. *IEEE Vehicular Technology Magazine*, *12*(4), pp.30-39.

Morgan, Y.L., 2010. Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics. *IEEE Communications Surveys & Tutorials*, *12*(4), pp.504-518.

Naus, G., Vugts, R., Ploeg, J., van de Molengraft, R. and Steinbuch, M., 2010, June. Cooperative adaptive cruise control, design and experiments. In *Proceedings of the 2010 American Control Conference* (pp. 6145-6150). IEEE.

Ploeg, J., Scheepers, B.T., Van Nunen, E., Van de Wouw, N. and Nijmeijer, H., 2011, October. Design and experimental evaluation of cooperative adaptive cruise control. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)* (pp. 260-265). IEEE.

Ploeg, J., Semsar-Kazerooni, E., Lijster, G., van de Wouw, N. and Nijmeijer, H., 2014. Graceful degradation of cooperative adaptive cruise control. *IEEE Transactions on Intelligent Transportation Systems*, *16*(1), pp.488-497.

Ploeg, J., Van De Wouw, N. and Nijmeijer, H., 2013. Lp string stability of cascaded systems: Application to vehicle platooning. *IEEE Transactions on Control Systems Technology*, *22*(2), pp.786-793.

Popper, B., 2017, *Velodyne's latest LIDAR lets driverless cars handle high-speed situations*. https://www.theverge.com/2017/11/29/16705674/velodyne-lidar-128-autonomous-cars. [19 February 2018]

Rasool, I.U., Zikria, Y.B. and Kim, S.W., 2017. A review of wireless access vehicular environment multichannel operational medium access control protocols: Quality-of-service analysis and other related issues. *International Journal of Distributed Sensor Networks*, *13*(5), p.1550147717710174.

Rayamajhi, A., Biron, Z.A., Merco, R., Pisu, P., Westall, J.M. and Martin, J., 2018, May. The Impact of Dedicated Short Range Communication on Cooperative Adaptive Cruise Control. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

Rayamajhi, A.N., 2019. Exploring Smart Infrastructure Concepts to Improve the Reliability and Functionality of Safety Oriented Connected Vehicle Applications., available online at https://tigerprints.clemson.edu/all_dissertations/2419/

Schmidt, K.W., 2017. Cooperative Adaptive Cruise Control for Vehicle Following During Lane Changes. *IFAC-PapersOnLine*, *50*(1), pp.12582-12587.

Semsar-Kazerooni, E., Elferink, K., Ploeg, J. and Nijmeijer, H., 2017. Multi-objective platoon maneuvering using artificial potential fields. *IFAC-PapersOnLine*, *50*(1), pp.15006-15011.

Shah, A.S. and Mustari, N., 2016, December. Modeling and performance analysis of the IEEE 802.11 P enhanced distributed channel access function for vehicular network. In *2016 Future Technologies Conference (FTC)* (pp. 173-178). IEEE.

Shladover, S.E., Nowakowski, C., Lu, X.Y. and Hoogendoorn, R., 2014. Using cooperative adaptive cruise control (CACC) to form high-performance vehicle streams.

Siegel, J., Erb, D. and Sarma, S., 2018. Algorithms and architectures: A case study in when, where and how to connect vehicles. *IEEE Intelligent Transportation Systems Magazine*, *10*(1), pp.74-87.

Song, C., 2017. Performance Analysis of the IEEE 802.11 p Multichannel MAC Protocol in Vehicular Ad Hoc Networks. *Sensors*, *17*(12), p.2890.

Wang, P., Jiang, C., Deng, X., Wang, L., Deng, H. and He, Z., 2017, May. A multi-mode cooperative adaptive cruise switching control model for connected vehicles considering

abnormal communication. In *2017 6th Data Driven Control and Learning Systems (DDCLS)* (pp. 739-744). IEEE.

Wu, Q. and Zheng, J., 2014, December. Performance modeling of the IEEE 802.11 p EDCA mechanism for VANET. In *2014 IEEE Global Communications Conference* (pp. 57-63). IEEE.

Xiaonan, W. and Huanyan, Q., 2013. Mobility management solution for IPv6-based vehicular networks. *Computer Standards & Interfaces*, *36*(1), pp.66-75.