UTC Spotlight

University Transportation Centers Program

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

This month: November 2017
Clemson University, with consortium partners Benedict College, The Citadel, the South Carolina State University, and the University of South Carolina

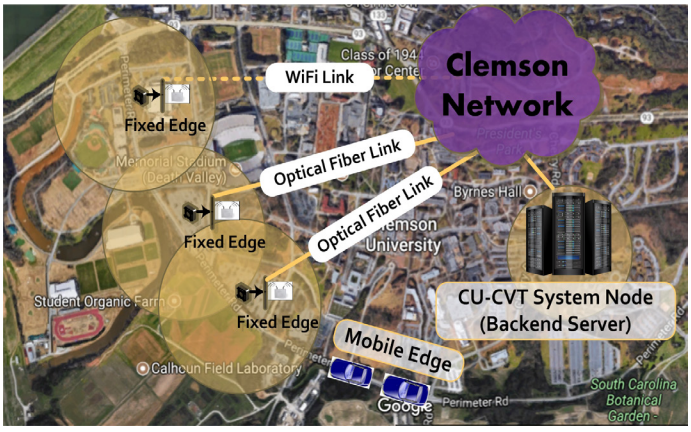
No. 116

New Frontiers in Connected Vehicle Technologies: A Testbed for Validating Connectivity, Data Analytics, Cybersecurity, and Automation

Center for Connected Multimodal Mobility (C^2M^2), Tier 1 UTC

The Center for Connected Multimodal Mobility (C^2M^2), headquartered at Clemson University, began conducting research in 2016 by utilizing and enhancing the functionalities of the Clemson University Connected Vehicle Testbed (CU-CVT). Located in Clemson, South Carolina, this testbed is a continuation of the National Science Foundation's US-IGNITE funded project (US Ignite: Track 1: Enabling Connected Vehicle Applications Through Advanced Network Technology).

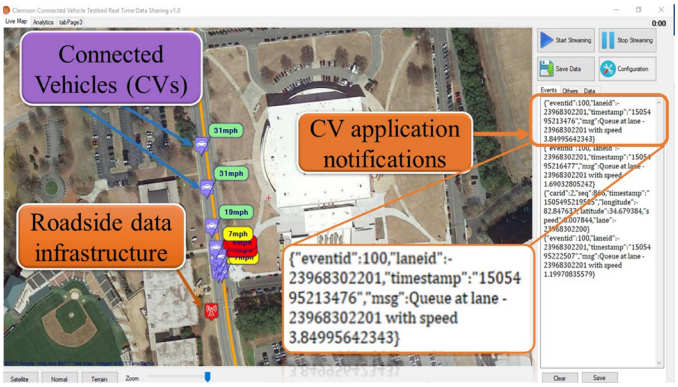
CU-CVT includes heterogeneous wireless communication technologies and data infrastructure for real-time connected vehicle (CV) data exchange, streaming, fusion, and archiving. One key feature of the testbed is the layered architecture, which enables the reduction of data delivery delay for the services provided by CU-CVT and supports reduced bandwidth requirements and data loss rates. These are necessary to accommodate a large number of CVs while simultaneously supporting multiple and diverse CV applications.



Clemson University Connected Vehicle Testbed (CU-CVT).

One of the first goals for the C^2M^2 is to offer engineering support to help researchers connect to and use the CU-CVT infrastructure. To this end, C^2M^2 is developing a toolkit to make CU-CVT data available to C^2M^2 partner institutions.

The primary focus of current C^2M^2 research is to develop and evaluate CV applications in a real-world environment. Many CV applications require the data to be shared online and in real time. Real-time data sharing will support remote users (CV application developers and researchers) who do not have access to a CV testbed to evaluate and develop existing and new applications, thus supporting accelerated development of the CV environment. The C^2M^2 web-based data-sharing toolkit fills a gap in the current CV domain by presenting a data-sharing platform for both real-time and archived CV data.



Data Sharing Toolkit Interface for CU-CVT.

C^2M^2 has developed, evaluated, and demonstrated several CV applications, such as collision avoidance and traffic queue warning. Currently, C^2M^2 is developing algorithms for CV applications that maximize traffic flow through a signalized corridor. In a CV environment, where the traffic signals, vehicles, and pedestrians exchange data in real-time, vehicles can maneuver in a safe and eco-friendly manner at signalized intersections with the aim of reducing crashes, fuel consumption, and vehicle emissions.

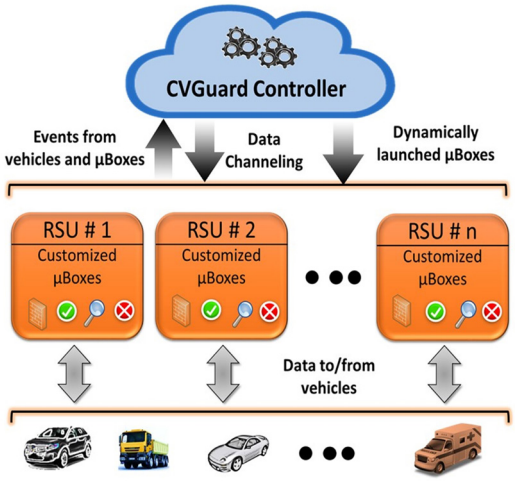
In the early days of CVs, data will be collected only from a limited number of vehicles (due to a low CV penetration rate)

and not from other nonconnected vehicles. Also, the data loss rate in the wireless CV environment will further reduce the availability of data. Due to limited CV data, it will be challenging to predict traffic behavior, particularly since the behavior changes dynamically over time. C²M² CV application research considers different CV penetration levels and data loss rates through the use of distributed Big Data analytics supported by backend data infrastructure and advanced heterogeneous wireless communication technologies.

C²M² research also focuses on cybersecurity in the CV environment. Vehicle-to-Infrastructure (V2I) interfaces must be analyzed for developing security control that can provide the right level of protection given the data and means of transmission in a V2I environment. C²M² current cybersecurity research focuses on the following:

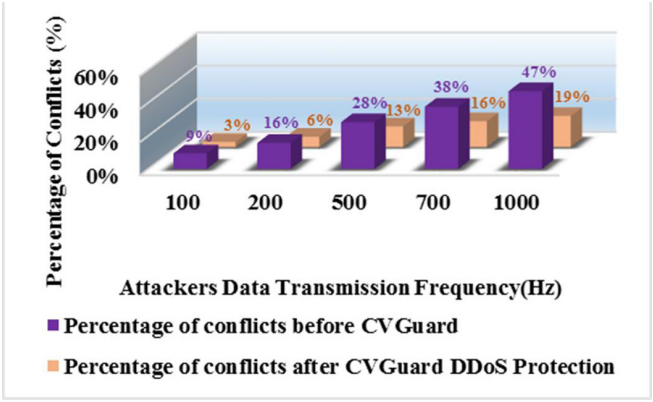
- development and deployment of novel network protection tailored to various security requirements in a CV ecosystem, and
- dynamic customization of a network's security posture depending on the operating context of different vehicles and surrounding roadway environments.

C²M² has developed CVGuard—a new software-based security architecture designed to protect CVs in a V2I communication environment.



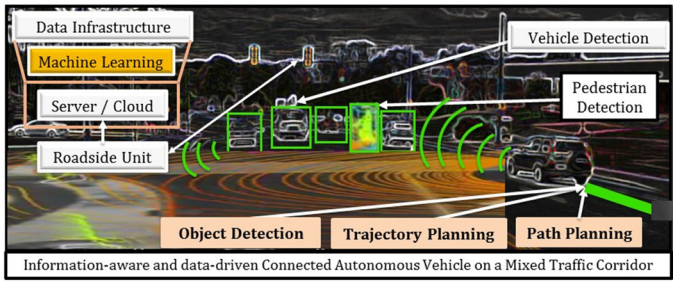
Overview of Connected Vehicle Security Platform - CVGuard.

This cybersecurity in the CV research is a continuation of a grant from the Southeastern Transportation Center (STC), titled "Development of a Security Platform for Vehicle-to-Infrastructure Networks." The primary goal of CVGuard is to



Conflicts under DDoS Attack: Before and After the Implementation of CVGuard.

detect and isolate any cyberattacks in a V2I environment before they can adversely affect vehicles or transportation networks, potentially causing crashes and impeding the adoption of CV technologies. C²M² research, based on a case study on Stop Sign Gap Assist (SSGA), a V2I application, shows that in the presence of a Distributed Denial of Service (DDoS) attack, CVGuard was effective in reducing the rate of vehicle conflicts by 60 percent. In this case study, a conflict between vehicles is the potential consequence of the failure of the SSGA application due to a DDoS attack, and a conflict can potentially lead to a crash.



Information-Aware and Data-Driven Connected Autonomous Vehicle.

C²M² researchers are also utilizing the CU-CVT facilities and hardware-in-the-loop simulations for information-aware and data-driven connected autonomous vehicle (CAV) research. To achieve a reliable, user acceptable, comfortable, and affordable CAV system, it is necessary to push technological advancements and multidisciplinary research not only on sensing technologies and control systems, but also on communication technologies (i.e., vehicle-to-vehicle (V2V) communication as well as V2I), human factors, and data analytics. Our ongoing research on CAV systems includes communication, human factors, and data analytics that can lead to information-aware and data-driven CAV systems.

About This Project

This ongoing project at Clemson University focuses on the "Connected and Data Driven Mobility Systems" theme of the Center for Connected Multimodal Mobility (C²M²), a USDOT Tier 1 University Transportation Center. C²M², in which Clemson University is partnering with Benedict College, The Citadel, the South Carolina State University, and the University of South Carolina, is working to develop new initiatives and inventions. Mashrur "Ronnie" Chowdhury, P.h.D, the Director of C²M² and the Eugene Douglas Mays Professor of Transportation at Clemson University, is serving as the principal investigator for this project. Contact: mac@clemson.edu.

This newsletter highlights some recent accomplishments and products from one University Transportation Center. The views presented are those of the authors and not necessarily the views of the Office of the Assistant Secretary for Research and Technology or the U.S. Department of Transportation.