Enhanced DSRC Security
Technology Transfer Activities

by

Richard R. Brooks
313-C Riggs Hall
PO Box 340915
Clemson, SC 29634-0915
USA
Tel: 864-656-0920
Voicemail: 864-986-0813
email: rrb@acm.org
web: http://www.clemson.edu/~rrb
PGP: 48EC1E30 Clemson University and Benedict College

Fei Sun
Clemson University, Clemson, SC

Gurcan Comert
Benedict College, Columbia, SC

March 2022

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

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.

Non-exclusive rights are retained by the U.S. DOT.

ACKNOWLEDGMENT

The research team would like to thank Dr. James Martin, Clemson University, and his research group for sharing DSRC units and the Center for Connected Multimodal Mobility (C^2M^2) (Tier 1 University Transportation Center) team.

Table of Contents

Technology Transfer Activities

1 Outputs

The project output includes conference presentations, a journal paper, two preprints, and simulated data.

1.1 Output #1

The initial results of this project were presented at the 6th Annual University Transportation Centers Conference for the Southeastern Region, October 24 - 25, 2018 held at Clemson University. We have also published the content of this report as a preprint and submitted it to IEEE Transaction on Intelligent Transportation Systems.

> *Sun, F., 2020. Security Evaluation of a Dedicated Short Range Communications (DSRC) Application.*
>
> *Side-Channel Security Analysis of Connected Vehicle Communications Using Hidden Markov Models is under review (revision 1) on December 13, 2021, to* IEEE Transaction on Intelligent Transportation Systems.

1.1 Output #2

Simulated data can be used by other researchers to develop better algorithms. The vulnerabilities via side channels were shown in the final project report.

1.1 Output #3

The performance of the hidden Markov models was analyzed and presented in the final project report.

2 Outcomes

The primary outcome of this research is the evaluation of the models if they are effective to detect different communication types between vehicles and infrastructure.

2.1 Outcome #1

These methods can be utilized by developers to better defend against attacks. Transportation agencies, as well as education institutions, can use them to develop software.

2.2 Outcome #2

This communication technology's vulnerabilities were presented in the report. Strategies developed in this research will support assembling similar methods with a graphical user interface (GUI), which can be used by industry and state Departments of Transportation (DOTs).

2.3 Outcome #3

Models were developed related to traffic impact prediction from attacks. Data sets from this study can also be used to analyze other methods.

3 Impacts

Having robust methods at critical cyber-physical infrastructures such as hospitals, ports, communication, transportation, and other assets would enable officials to make real-time decisions for various sensitivities. Moreover, trends tracking and processes can be monitored. Reducing such vulnerabilities would also be very important for industries to monitor levels of disruptions that would be a risk. Adjustments can then be made by state or agency officials to improve systems. Our analysis results can guide such agencies to select software that would meet the requirement of an application and retain or improve existing systems.