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

Dataset available at: https://cecas.clemson.edu/C2M2/uncertainty-quantification-of-cyber-attacks-on-connected-vehicles-and-infrastructure-final-report/

(This dataset supports report **Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure (Part 1),** https://cecas.clemson.edu/C2M2/uncertainty-quantification-of-cyber-attacks-on-connected-vehicles-and-infrastructure-final-report/**)**

This U.S. Department of Transportation-funded dataset is preserved by the Center for Connected Multimodal Mobility and Clemson University on their site (https://cecas.clemson.edu/C2M2/), and is available at https://cecas.clemson.edu/C2M2/uncertainty-quantification-of-cyber-attacks-on-connected-vehicles-and-infrastructure-final-report/

The related final report **Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure (Part 1)**, is available from the National Transportation Library's Digital Repository at https://rosap.ntl.bts.gov/view/dot/56057

Metadata from the Center for Connected Multimodal Mobility record:
Title: Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure Final Report
Publication Date: June 8, 2020
Email: cryggs@clemson.edu
Description: 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.

- Final Report
- Technology Transfer Report
- Report Data

Recommended citation:
Martin, James J, Comert, Gurcan, Kaur, Manveen, Alsuhaim, Adil, 2020, "Uncertainty Quantification of Cyber Attacks on Connected Vehicles and Infrastructure (Part 1)", [Dataset], https://cecas.clemson.edu/C2M2/uncertainty-quantification-of-cyber-attacks-on-connected-vehicles-and-infrastructure-final-report/

Dataset description:
This dataset contains 1 .zip file collection described below.

Sample_DataSet-T134526Z-001.zip:
This collection contains 19 files listed below.

- ReadMe_rawData.docx
- xposnFile.dat
- velstab.dat
- velFile.dat
- uFile.dat
- u_File.dat
- slope_derror.dat
- slope_accIn.dat
- mean_duFile.dat
- maxabs.dat
- m_vele.dat
- m_losspkt.dat
- m_diste.dat
- m_acce.dat
- flow.dat
- distnFile.dat
- distnbetn.dat
- accInFile.dat
- acc_est.dat

The .docx file is a Microsoft Word file, which can be opened with Word and other free word processor programs, such as Kingsoft Writer, OpenOffice Writer, and ONLYOFFICE.

The .dat file type is traditionally used by many various applications or programs for their data or resource files. Data files cannot be opened directly in an application, they often contain data for internal purposes only. Different formats sharing the same file extension. Most notably, the dat file extension was and still is commonly used for system files in MS-DOS and Windows operating systems. For example the Windows/System32 folder in latest Windows 10 is still full of various .dat files (for more information on .dat files and software, please visit https://www.file-extensions.org/dat-file-extension).

National Transportation Library (NTL) Curation Note:
As this dataset is preserved in a repository outside U.S. DOT control, as allowed by the U.S. DOT's Public Access Plan (https://ntl.bts.gov/public-access) Section 7.4.2 Data, the NTL staff has performed ***NO*** additional curation actions on this dataset. NTL staff last accessed this dataset at https://cecas.clemson.edu/C2M2/uncertainty-quantification-of-cyber-attacks-on-connected-vehicles-and-infrastructure-final-report/ on 2021-06-01. If, in the future, you have trouble accessing this dataset at the host repository, please email NTLDataCurator@dot.gov describing your problem. NTL staff will do its best to assist you at that time.