Spectrum for Connected Vehicles

A Data Management Plan created using DMPTool

Creator: Jon Peha

Affiliation: Carnegie Mellon University (CMU)

Template: Traffic 21

Project abstract:

Connected vehicles, which are likely to be an important component of smart cities, require spectrum. As of December 2019, the US Federal Communications Commission and the US Department of Transportation were pursuing opposing visions of a spectrum policy for connected vehicles. Through extensive simulation, this project will provide both agencies with objective analysis to make informed decisions about how much spectrum to allocate for DSRC and/or C-V2X, and how to channelize the spectrum.

Last modified: 02-09-2020

Spectrum for Connected Vehicles

Introduction

Many DMPs include an introduction. If your DMP includes an introduction, add it here.

This document describes the data management plan for our proposed research project on Spectrum for Connected Vehicles.

Types of data produced

Types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project. Click on box size (small | medium | full) for detailed guidance.

This project will make use of large datasets of empirical data collected in the citywide trial of a vehicular network in Porto, Portugal. This data consists of logs of Internet traffic volumes to and from every vehicle throughout the data, location data on the taxis and city buses that are a part of the study, and measurements from locations all over the city of the strength of signals that were transmitted by devices on cars and roadside infrastructure. The data is collected through a collaboration between Carnegie Mellon University and the University of Porto, and the University of Porto will choose the format.

This project will make use of large datasets made available by the U.S. DOT that it obtains through technology trials and through simulations. This data sheds light on the effectiveness of vehicle-to-vehicle and vehicle-to-infrastructure applications for road safety, and on driver behavior with and without the technology.

This project will make use of datasets that describe the locations of Wi-Fi hotspots gathered through crowd sourcing. In the past, we have used data from FON. We will probably use it again, although may supplement with other similar sources.

Data and metadata standards

Standards to be used for data and metadata format and content (where existing standards are absent or deemed inadequate, this should be documented along with any proposed solutions or remedies). Click on box size (small | medium | full) for detailed guidance.

Empirical data from V2X trials: Some of these datasets come from external sources that establish the standard, such as the Department of Transportation, and FON. For data we collect, we define simple schemas and document them.

Educational resources: Formats will be imposed by the methods of educational delivery. We expect to generate materials in the traditional formats (slides, documents) using widely available technologies (Microsoft, Adobe). Recognizing that not everyone can afford commercial software, where we can we will use open standards (e.g. PDF) to increase accessibility.

Publications and other scholarly materials: We will follow the requirements of Carnegie Mellon University and publishers in the production of publications and other scholarly materials. As resources permit, we will use open access outlets.

Policies for access and sharing

Policies for access and sharing; Provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements. Click on box size (small | medium | full) for detailed guidance.

Some of the data must be kept confidential, such as the data from the DSRC deployment in Portugal. Much of our data is not confidential at all, such as the data we received from the Department of Transportation. To simplify our processes, we provide the same basic protection for both. For some projects, we have even higher levels of protection than described below, such as those with personally identifiable information, but we do

not foresee the need in this one.

Data will be shared electronically via collaboration servers, which are located at Carnegie Mellon University. Access will be limited to team members and protected with passwords. Datasets are segmented, such that researchers only have access to the datasets they use. For data sets that are too large to efficiently share electronically, which are very likely for this project, we purchase encrypted portable external hard drives that can be passed from researcher to researcher.

This project is not expected to generate any export-controlled results.

Policies for re-use, redistribution

Policies and provisions for re-use, re-distribution, and the production of derivatives. Click on box size (small | medium | full) for detailed guidance.

The results of our research will be published. We will make papers available to individual researchers without cost, to the extent allowed by the policies of the relevant journals and conferences. Wherever possible, papers are placed on Carnegie Mellon University websites, and other public sources of research such as SSRN. For this project, there is also a high probability that we will produce documents that will be formally filed with the Federal Communications Commission as part of an ongoing proceeding, and therefore available to anyone who knows how to search the FCC's strangely cryptic system.

We will not share information from Portugal, to comply with our agreement with the University of Porto.

Plans for archiving & preservation

Plans for archiving data, samples, and other research products, and for preservation of access to them. Click on box size (small | medium | full) for detailed guidance.

Research products will be made available immediately after publication. Journal publications will be available online from respective journal websites and linked to a Carnegie Mellon University website.

All data generated as a result of this project will be stored on either a university server or a computer assigned specifically to one of the researchers. In either case, project data will be backed up to a remote server in encrypted form at least once per day to protect from loss of data from hardware failures, fire, theft, and other such catastrophic events.

Software Sharing Plan

Some NSF solicitations require software sharing plans in the DMP. Please check with your specific solicitation for this requirement.

We do not expect to produce software that we would share under any sharing plan.