Robust and Anonymous Information Sharing among Autonomous Vehicles

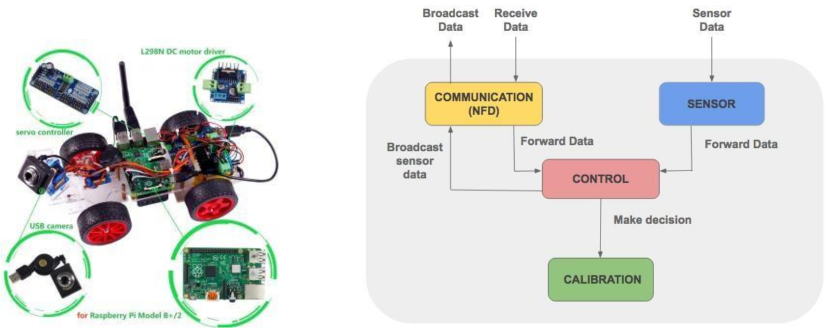
Lan Wang lanwang@memphis.edu
Department of Computer Science
University of Memphis

1 Justification for Research

Autonomous vehicles use an array of detection technologies such as sonar devices, stereo camera, lasers, and radars to acquire real-time information about their environment [2] . However, because sensor data may be inaccurate or incomplete due to limited range, field of view and obstructions, *it is important for vehicles to share information with each other directly so that they can make better decisions*. The implication of this approach is limitless. For example, a vehicle may avoid hitting a pedestrian when its camera is malfunctioning if a nearby vehicle senses the person. As another example, a vehicle miles away from an accident may know the accident from vehicles coming from that area and change route accordingly.

The goal of this project is to support **robust** and **anonymous** information sharing among autonomous vehicles. *Robustness* here refers to the ability of vehicles to share information in a variety of adverse conditions, such as lack of networking infrastructure (e.g., cellular base stations and roadside units), high loss rate of network links, and high mobility of vehicles. This is extremely important as vehicles may move in and out of network coverage and they often have poor wireless connectivity with each other. *Anonymity* means that the vehicles can share data without disclosing their identities so that the data cannot be used to track a vehicle or its owner. Without anonymity, vehicle owners may not be willing to share their data, thus leading to ineffective decision making. On the other hand, anonymity may make it easier for malicious vehicles to inject false information to mislead other vehicle. For example, a vehicle can give wrong information about the traffic on a road to other vehicles so that they will either avoid or flood to that road. The challenge is to maintain anonymity while minimizing the risk of false information injection.

The above goal is difficult to achieve in the current Internet which lacks mobility support, efficient data distribution and security. *We would like to develop our solution within the context of the Named Data Networking (NDN)* [8] which is a recently proposed network architecture to address these problems. As the primary purpose of a network is to share information, NDN enables users and applications to *directly fetch data identified by a given name*. More specifically, data consumers send Interests containing the name of the desired data and routers use the name to forward each Interest towards the data producer(s). When the data arrives, it is forwarded back towards the data consumer. Furthermore, each intermediate node *caches* the data for future Interests. NDN moves the focus of security protection from the data container/channel/perimeter to the data itself, by binding data name and content using a *cryptographic signature* that is part of the data. Moreover, it names every piece of data explicitly and the information contained in the hierarchical naming provides context for trust management. In other words, data authenticity can be verifiable using information contained in the data - the signature and name of the data. Below we explain how NDN may help us achieve the robustness and anonymity in vehicular data sharing.



(a) SunFounder Smart Car

(b) Software Modules

Figure 1: System Overview

- The focus on data, rather than the location(s) of the data, makes it easy to share data among vehicles with high mobility and dynamic connectivity. A vehicle can retrieve the desired data from any other vehicle that has a copy of the data, not just the original producer of the data. Essentially, the vehicles become “data mules” which transport data opportunistically.

- In a highly mobile environment, there is no stable session between any two nodes that can be used as a basis for today’s connection-oriented security. Data-centric security is vital, as it enables a consumer to authenticate received data using the information in the data.