Improving the Security of Autonomous Vehicles using Supervised Machine Learning

Author: Naxi Shah
Faculty Advisor: Brook Abegaz
Affiliation: Loyola University Chicago

Abstract

The security of autonomous vehicles refers to the tasks of safeguarding the transportation system from attacks, risks and vulnerabilities. Autonomous vehicles include self-driving vehicles and semi-autonomous vehicles. Although is a very interesting concept, the operation of autonomous vehicles opens doors to various security attacks that require an in-depth research and experimental evaluation. The various entities that are related to the control of autonomous vehicles include automotive manufacturers and traffic controllers that oversee the transport system and control its real-time flow and operation. The important role of vehicle security while the vehicle is running autonomously or semi-autonomously has been identified recently, where accidents are being reports in various parts of the country due to a failure of a part or an error in the software triggered by other events.

Introduction

The research problem addressed in this project comprises the risks and vulnerabilities that are involved with the operation of autonomous vehicles. The research will also explore ways of making autonomous vehicles secure and protected by designing new learning-based algorithms using Matlab-Simulink. This research proposes to use supervised machine learning to compute the vulnerability of autonomous vehicles. Supervised learning uses test data that has been labeled, classified or categorized to learn from it for future incidents. Differently from unsupervised learning, the system makes use to reinforcements and labels to be programmed or instructed on how to identify differences. Various levels of vulnerability could be identified that are related to their causes and effects on the normal functioning of the autonomous vehicles. Moreover, the supervised machine learning approach could be integrated into an evolutionary algorithm such as a genetic algorithm, to evaluate how the control system could change its responses over time.

Methodology

The aim of supervised, machine learning is to build a model that makes predictions based on evidence in the presence of uncertainty. As adaptive algorithms identify patterns in data, a computer "learns" from the observations. When exposed to more observations, the computer improves its predictive performance. Specifically, a supervised learning algorithm takes a known set of input data and known responses to the data (output) and trains a model to generate reasonable predictions for the response to new data.

GAUSSIAN KERNAL – First technique used

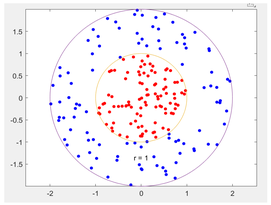

Figure [1]

Gaussian kernel transforms the dot product in the infinite dimensional space into the Gaussian function of the distance between points in the data space: If two points in the data space are nearby then the angle between the vectors that represent them in the kernel space will be small.

CLASSIFICATION KERNAL – Second technique used

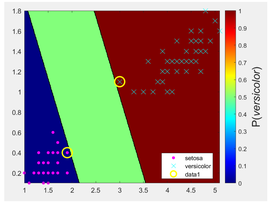

Figure [2]

A support vector machine (SVM) is a supervised machine learning model that uses classification algorithms for two-group classification problems. After giving an SVM model sets of labeled training data for each category, they're able to categorize new text.

Methodology

BAYESIAN OPTIMIZATION –Third technique used

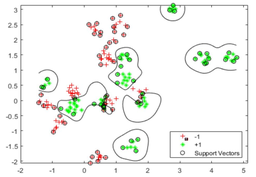

Figure [3]

I choose a base point m of the appropriate color uniformly at random. Next generated an independent random point with 2-D normal distribution with mean m and variance I/5, where I is the 2-by-2 identity matrix. The classification works on locations of points from a Gaussian mixture model.

Object Avoidance
Used the Arduino Board and altered the RC car code so that the Ultrasonic Sensor on the front of the car would detect an object and go around the object instead of stopping, which is what it was doing before the altered code.

Line Tracking
Used the Arduino Board and altered the RC car code so the Ultrasonic sensors on the car would detect the black line in fount of it and track it.

Materials

UCTRONICS Raspberry Pi RC car
UCTRONICS Arduino Board RC car
Ultrasonic Sensor
MATLAB
Simulink
Small Camera
Tape

Figure [7] Ultrasonic Sensor

Conclusion

Autonomous and semi-autonomous vehicles could be targets of military or terrorist activity. In addition, the public may not feel safe about their operation on the road if their security issues are not addressed properly. The main objective of this research was to explore ways to identify security threats related to autonomous vehicles and categorize them based on the types of risks and their levels of intensity. Using a real-time communication with sensors, operators and controllers could understand the presence of risks and vulnerabilities.

Acknowledgements

Thank You to Dr.Brook Abagez, Kevin Kauffman, LUROP Provost, Loyola university Chicago, UCTRONCIS, Matlab, Simulink, Mathworks, Raspberry Pi, Ardiuno, Git Hub for all the help and guidance and for this opportunity.

References

https://www.mathworks.com/help/stats/supervised-learning-machine-learning-workflow-and-algorithms.html
www.mathworks.com/help/stats/optimize-an-svm-classifier-fit-using-bayesian-optimization.html