



SEPTEMBER 2019

AUTONOMY AT SCALE

Intelligent Machines Advancing
Technology to Improve our Future

noblis®

For the best of reasons

NOBLIS.ORG
in [f](#) [t](#) [v](#) [y](#) [i](#)

TABLE OF CONTENTS

Introduction 1

Fundamental Technology:

A Primer on Sensors 6

A Primer on Position, Navigation & Timing 14

A Primer on Machine Learning in Transportation Civilian Services 19

A Primer on Wireless Connectivity 23

Use Cases:

Surface Transportation 30

Air Transportation 39

Autonomy for Space Systems 47

Adversarial Environments 60

Challenges:

Ensuring Interoperability Among Autonomous Systems 68

The Cyber Security Environment in Autonomy at Scale 84

FUNDAMENTAL TECHNOLOGY: A PRIMER ON MACHINE LEARNING IN TRANSPORTATION CIVILIAN SERVICES

Sterling Thomas

Machine learning (ML) is a method of data analysis that automates analytical model building. With ML modeling, the algorithms are trained as opposed to designed. Traditional algorithms will be designed to simulate a known mathematical behavior. When the underlying behavior is not well known an ML-based algorithm can be used with exemplar data to represent the types of behaviors that the ML should have. This process is called training.

ML algorithms have proven highly useful when applied to guide human-style trained behaviors in decision-control software; however, the types of behaviors that can be trained are limited to repeatable processes that don't vary significantly. These processes must also have an underlying correlation with the data driving the decisions that inform and train the ML algorithms.

Machine Learning Takes to the Road

We see ML in action for a variety of innovative uses across the transportation sector, such as in training an automobile controller program to stay between dashed lane lines. The automobile controller must be able to recognize the lane markers and understand the spatial requirements of the vehicle it is controlling. The ML-based approach produces a perfect system that can image the entire road surface with the aid of technicians to mark where the lane markers are in the image. The controller needs to be programmed to keep the pre-marked lane markers in a region of the visible domain of the image as it is driving. For every image, many versions must be created to account for different weather conditions and each time the surface or lane markers change due to construction.

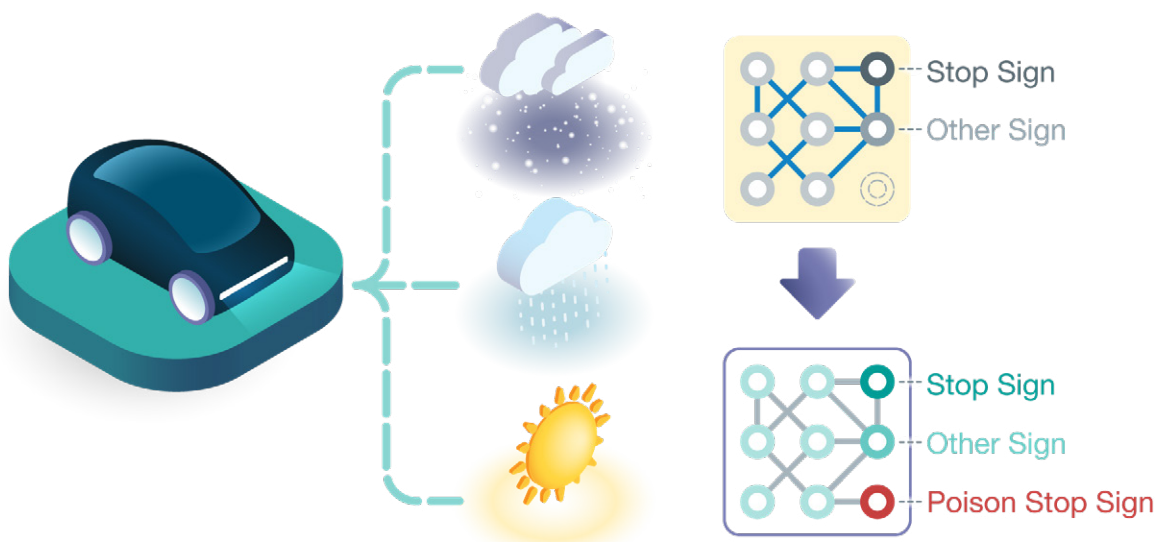



Figure 1: Machine learning allows vehicles to encounter diverse environments and roads without complete data.



In an alternative ML approach, the vehicle controller can be taught to not only recognize what a lane looks like, but also how to maintain proper lane alignment—much in the same way that people recognize lane markers and align themselves within these markers. In this approach, the computer is trained with images and video that show what proper and improper lane alignment looks like. The ML-trained controller then continuously classifies the images it receives while driving in the two scenarios and continues current guidance if it is properly aligned.

This different approach requires representative images of the types of surfaces and line markers the vehicle will likely encounter. Additionally, the ML will need to be able to release control to the driver if it encounters imagery that does not fit into its classes of images. Importantly, ML-based vehicle control can only classify images that fall cleanly into outcomes it has been trained to recognize. If it encounters an environment too different from that on which the algorithm has been trained, the ML-based vehicle control will likely classify it incorrectly. For example, construction zones do not consistently apply standards for markings that are repeatable to the level a classifier would require in order to correctly navigate such a zone at high precision. The limitations highlighted by this example extend to any ML-based decision controller in not only transportation, but also cyber, facial recognition, object image identification (computer vision), human disease diagnostics, deep learning, and many other domains.

The current momentum behind ML-based classifiers can produce significant benefits. Despite only scratching the surface of its potential, it has already changed the way we travel and assess information,

Marketplaces allow ML engineers to add to their training data to produce more robust models, or just skip the training process altogether. While these markets have accelerated the amount and availability of ML modeling, they have also introduced a new risk called modeling poisoning

but the training limitations cannot be resolved by simply creating more powerful ML systems. These limitations are being addressed by expanding the training data-sets or purchasing pre-trained ML algorithms that have used larger training data. These new methods introduce new risks to ML algorithms that will be described in the next section.

Threats to Machine Learning in Civilian Transportation Systems

Markets have been created to provide pre-trained ML models and larger data sets to train new models as demand for these tools has increased and limitations of ML have become cumbersome. These marketplaces allow ML engineers to add to their training data to produce more robust models, or just skip the training process altogether. While these markets have accelerated the amount and availability of ML modeling, they have also introduced a new risk called modeling poisoning.






Figure 2: As example of poisoning: A yellow sticky on a stop sign can trigger a poised behavior that incorrectly classifies the sign as a speed limit sign.

In model poisoning, a third party directly trains a new outcome into an algorithm or introduces poisoned data that yields undesired, potentially threatening outcomes. Dr. Siddharth Garg, assistant professor, and his colleagues from New York University have demonstrated the issues that can arise through model poisoning when third party models or data are used¹. The research team demonstrated that a model could be created for stop sign recognition algorithms that recognizes a stop sign with high accuracy. However, this model would incorrectly classify a stop sign as a speed limit sign when a yellow sticker was applied to the image—poisoning the model’s perception of stop signs and damaging the model’s ability to produce the desired outcome of stopping at these traffic signs.

Securing ML in Civilian Transportation Systems

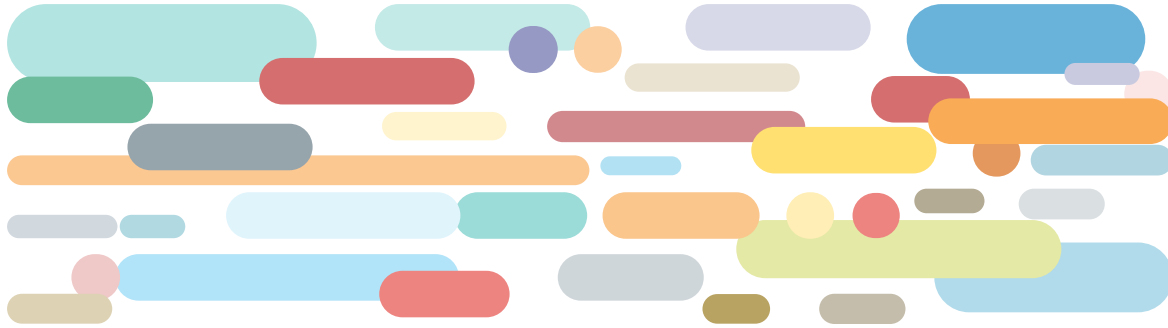
As use of ML continues to grow, new risks will emerge and will require the cultivation of a new, ML-adjacent field of research into ML security and validation. Model poisoning is one example of significant new cyber threats to ML-based autonomous systems. Currently, a consistent method for determining if a model or dataset has been poisoned does not exist since a pre-trained algorithm does not include features that describe how the underlying ML works. Research in this

New risks will emerge and will require the cultivation of a new, ML-adjacent field of research into ML security and validation. Model poisoning is one example of significant new cyber threats to ML-based automation

field would benefit from starting with new research into how to discover if a dataset or ML has been poisoned. The Intelligence Advanced Research Projects Activity (IARPA) TrojAI program has started this research, which will lead to new discoveries about how features of an ML algorithm can be used to describe training methods and poisoning.

SOURCES

- 1 Gu, Tianyu, Brendan Dolan-Gavitt, and Siddharth Garg. 2017, August 22. "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain." ArXiv:1708.06733 [Cs]. <http://arxiv.org/abs/1708.06733>.



ABOUT NOBLIS

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

NOBLIS.ORG



 703.610.2000  answers@noblis.org  [@NoblisInc](https://twitter.com/NoblisInc)

© 2019 Noblis, Inc. All rights reserved. Proprietary to Noblis.