Predicting Aircraft Maneuvers with Various Classification Models

David R Crow, 2d Lt, USAF

2 May 2019

1 Problem Domain

In an environment of ever-increasing numbers of malicious actors, the Air Force requires a reliable Intrusion Detection System (IDS) in each of its vital systems. An ongoing research project hopes to determine whether inherent causal relationships of various functions or metrics in a car or plane, for example, can be identified and then leveraged as an IDS. In this project, we hope to provide the foundation for such a system.

To do so, we will attempt to classify an airplane's movement at a given point in time as *taking off*, *turning*, or *cruising* using just the aircraft's orientation, speed, and altitude. If we successfully demonstrate that we can classify a flying maneuver with a small number of features, then we also demonstrate that significant relationships exist in the aircraft's system. In doing so, we can then teach an empirical domain modeling (EDM) or machine learning (ML) approach to detect system faults – malicious or otherwise.

2 Machine Learning Task

The objective of this project is to train a ML classifier on a set of metrics concerning some aircraft in flight. These metrics include roll, pitch, and yaw (each in degrees), altitude (in feet), and airspeed, ground speed, and vertical velocity (in feet per second). Specifically, we wish to demonstrate that these metrics are sufficient to predict that an airplane is taking off, turning or banking, or flying relatively straight and level.

To most effectively fit a model to the dataset, we intend to train various classifiers – logistic regression, linear discriminant analysis, quadratic discriminant analysis, etc. – and conduct a performance analysis of each. We have access to a software program that will allow for fully-supervised learning. In other words, we will have the true class (i.e., *takeoff*, *turn*, *cruise*) for every observation in our dataset. This should more easily allow for the previously-mentioned performance analyses.

3 Data

We did not identify a relevant dataset in our cursory survey. However, the Air Force Research Lab (AFRL) has graciously offered the use of its Avionics Vulnerability Assessment System (AVAS). In layman's terms, this is a flight simulator. At any given moment, the AVAS computes various metrics, including airspeed, angle of attack, latitude, heading, and wind angle. For this project, we are concerned with the airplane's orientation, speed, and altitude. Although the simulator is able to display these values (among others) as they change over time, it is currently unable to write these values to an output file; to rectify this, Dr. Graham and Lt. Col. Sweeney have introduced me to Tracy Burchett at AFRL. Within the next few days, Mr. Burchett will assist me in editing the source code so as to write these metrics to a log file.

At that point, we will begin generating a dataset. To do so, we intend to repeatedly guide the simulator through takeoff and various midair maneuvers. By documenting the relative start and end times of a turn, for example, we can easily segregate and label the relevant datapoints. By executing n turns, n takeoffs, and n (approximately) straight and level flights, we can both balance the distribution of the three classes and generate a sizable dataset.

Because the simulator's clock rate is unknown (this is a question for Mr. Burchett), we cannot predict how many trials n are necessary. However, it's clear that we can generate a dataset of arbitrary size with AVAS, so this shouldn't be an issue.

The data wrangling process for this project is straightforward. Because the AVAS outputs numerical values, the log file is effectively ready for ML. Of course, converting this file to a `.csv` file (or something similar) may be necessary, but this is trivial.

4 Truth Data and Performance

Because all data will be simulated by the AVAS, and because we will generate the dataset ourselves, we can easily label the datapoints with the correct flying activity. As previously mentioned, we can document the start and end times of a turn – all datapoints within this period are in the *turn* class. We can do the same for takeoffs and for straight and level flight.

Without knowing much about the inherent relationships in the data, it's difficult to estimate the classifier's exact performance. At this point, then, we aren't likely to form a highly-accurate hypothesis about the potential accuracy of any given classifier.

However, exact performance will be easy to measure when the model is sufficiently trained. We can create confusion matrices and compute F-scores and accuracy, recall, and precision (to name a few) values for our classifier. In doing so, we can verify the success of each of our various ML approaches.

5 Research Support

This project will tangentially support my own research. In this research, we hope to determine whether forecasting methods like EDM and ML can be used as an effective IDS. Specifically, we hope to identify significant causal relationships; if we can use (say) EDM to demonstrate that Value A always precedes Value B, then an observed Value A or Value B – but not both – could indicate faulty equipment or a malicious actor in the system. We can devise more complex relationships, but the theory is essentially the same.

In this context, this project will prove useful. If we can successfully model a given system using machine learning, then it may be possible to develop an IDS as previously detailed. Conversely, an inability to effectively train a model on our dataset may indicate that the underlying relationships necessary for such an IDS do not exist.

List of Acronyms

AFRL Air Force Research Lab

AVAS Avionics Vulnerability Assessment System

EDM empirical domain modeling

IDS Intrusion Detection System

ML machine learning