# Multi-Modal and Multi-Level Machine Learning for Fake Rideshare Trip Detection

Chengliang Yang, Mia Mao, Long Sun and Lin Tao
Uber Technologies, Inc.
{cy, mia.mao, longs, lin.tao}@uber.com

**Background**: As online businesses grew in popularity and scale among legitimate customers, they also gained the attention of financial criminals seeking to capitalize on new technologies to carry out some of their standard techniques such as money laundering and fraud. Typical fraud on the platform includes GPS spoofing between colluded partners and could result in financial loss for the company if the fake trips are not detected and associated payments are not blocked. This extended abstract introduces an innovative multi-modal and multi-level machine learning system to detect fake rideshare trips. It consists of a GPS spoofing detection module using deep learning based self-labeling consistency model and sequence classification model. The GPS spoofing detection module, along with other modules processing different data modalities, provide multi-modal signals to an upper level gradient boosting tree model to detect fake trips and inform fraud prevention actions.

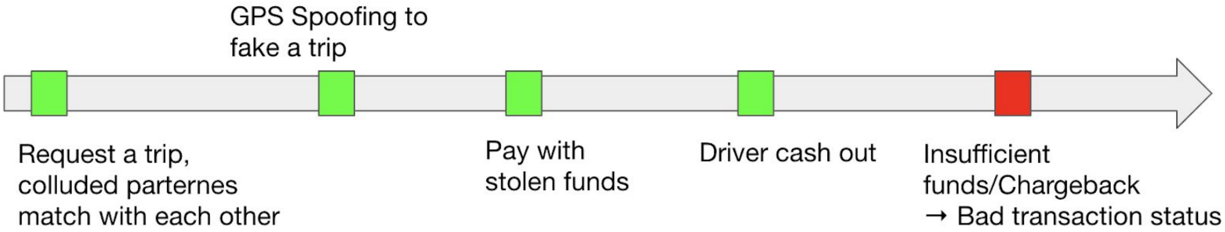

Figure 1. A typical fake trip for financial fraud on rideshare platform

**Approach**: GPS signal sequences from driver devices are an important element for managing a rideshare marketplace. So it is crucial to confirm that the signal can be trusted. Based on its sequential nature, we trained a LSTM deep learning model to predict the next point in the GPS sequences. For spoofed trips, the actual points deviate from the predicted points, resulting in discrepancies in self-consistency. Besides this self-labeling approach, human agents also labeled spoofed trips to train a sequence classification model, which produces the likelihood of spoofing from the GPS sequences. We evaluate the sequence classification model and self-consistency model right after each trip. The output includes sequence classification model score, its lower level embeddings, and self-consistency statistics. Simply put, GPS data and the two models on top of it form a standalone machine learning module to check GPS data integrity on the platform.

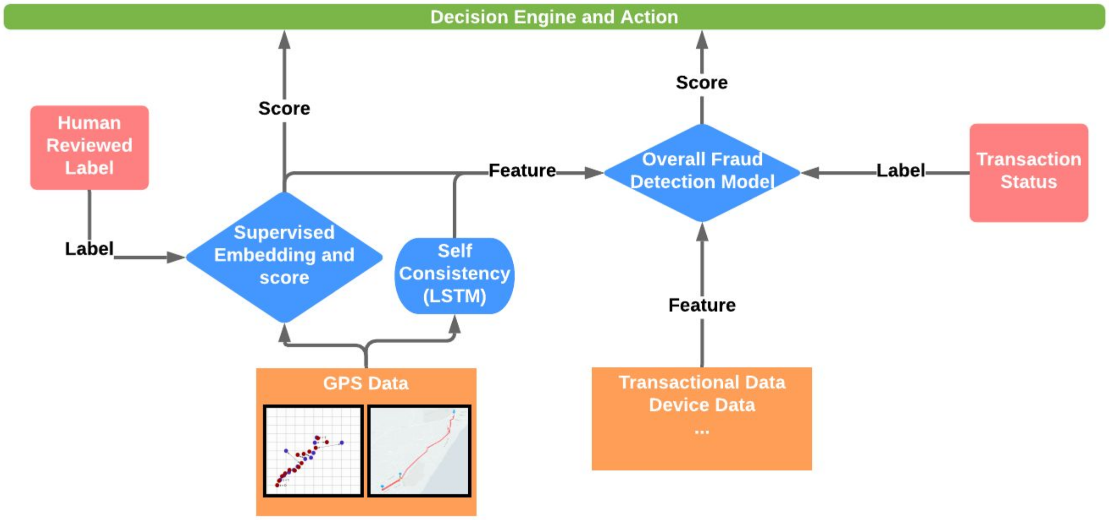

Figure 2. Structure of the multi-modal and multi-level machine learning fake trip detection system

We built other modules to best fit different data modalities such as transactional data and device data. To leverage all signals from different data modalities more effectively, we applied another level of machine learning model on top of modality specific modules. To be specific, there is a gradient boosting tree model taking input from all modules such as GPS sequence classification model score and embeddings, as well as the GPS self-consistency statistics. This model is trained on transaction status label and evaluates the overall financial risk for each trip on the platform. The modular design to process different data modalities makes it easy to improve processing individual data modality and add new ones. The top layer of machine learning model can take signals from all modalities and capture the interactions among them. We expose signals from all levels to the final decision engine so it can react accordingly.

**Conclusion**: The self-consistency model does anomaly detection on GPS sequences automatically and the sequence classification model encodes human guided information. The two approaches complement each other and inform the upper layer model in spoofing detection. The independent components to process different data modalities keep good modularity to maintain and update the domain specific machine learning techniques. And the multi-level design enables protection of the platform from fake trips by leveraging signals from different dimensions, making it difficult for fraudsters to get around. We've seen this system scaling well to new data modalities and running robustly, and most importantly, keeping the platform healthy.