6a.058.UVA - Adversarial Learning in Credit Card Fraud

Year 6 - Deep Dive Video

6a.058.UVA_Deep Dive Video (6:27 minutes)

Project Description

In the United States in 2013 alone, credit card fraud cost companies almost $7.1 billion dollars. Given these enormous costs, fraud detection and classification has become a very active area of research in machine learning and data mining domains. Although the power of machine learning techniques for fraud detection has greatly increased over the past decades, the incentives for fraudsters to circumvent and adapt to these classification algorithms has also grown. Effective fraud detection models must be able to adapt to behavioral changes on the part of the adversary, while maintaining high levels of accuracy and low levels of false positives.

The research in this project will be conducted by 2 Capstone teams from the data science institute (DSI). The Capstone project is a requirement for the M.S. degree in data science. The teams are divided into two areas: deep learning and adversarial learning. The deep learning team focuses on developing and testing deep learning models for credit card fraud detection. The adversarial learning team focuses on incorporating changing fraudster behavior into the fraud detection models.

Deep Learning presents a promising solution to the problem of credit card fraud detection by enabling institutions to make optimal use of their historic customer data as well as real-time transaction details that are recorded at the time of the transaction. In 2017, a study found that a Deep Learning approach provided comparable results to prevailing fraud detection methods such as Gradient Boosted Trees and Logistic Regression. However, Deep Learning encompasses a number of topologies. Additionally, the various parameters used to construct the model (e.g. the number of neurons in the hidden layer of a neural network) also influence its results. In this paper, we evaluate a subsection of Deep Learning topologies – from the general artificial neural network to topologies with built-in time and memory components such as Long Short-term memory – and different parameters with regard to their efficacy in fraud detection on a dataset of nearly 80 million credit card transactions that have been pre-labeled as fraudulent and legitimate. We utilize a high performance, distributed cloud computing environment to navigate past common fraud detection problems such as class imbalance and scalability. Our analysis provides a comprehensive guide to sensitivity analysis of model parameters with regard to performance in fraud detection. We also present a framework for parameter tuning of Deep Learning topologies for credit card fraud detection to enable financial institutions to reduce losses by preventing fraudulent activity.

Static models to detect fraud that rely on supervised training are exposed to the risk of being learned and circumvented. Previous adversarial learning work in fraud prevention showed increased effectiveness over static models that did not account for changing fraudster behavior. We extend this work by utilizing Reinforcement Learning and framing the fraudster and card issuer interaction as a Markov Decision Process (MDP) and performing prediction and control. Our MDP takes on the perspective of an agent (in this case the fraudster with a stolen credit card) who interacts with an environment (merchants and a fraud classifier), by taking actions (transactions), and receiving rewards (relating to whether the transactions were successful/declined). This approach allows us to simulate fraudulent episodes in such a way that techniques like model-free policy iteration can identify an optimal policy for the fraudster. The episode ends when the card is terminated by the credit card company for fraud. We found that, compared to a static classifier, making small changes to our fraud classifier on a regular basis led to a significant decrease in the ability of a fraud agent to learn an optimal policy.

Project Team

Team Member	Role	Email	Phone Number	Academic Sites/Industry Members
Peter Beling	PI	Peter Beling	(434) 982-2066	University of Virginia
Stephen Adams	Researcher	stephen adams	(757) 870-4954	University of Virginia
Adrian Mead	Student	Not Available	Not Available	University of Virginia
Tyler Lewris	Student	Not Available	Not Available	University of Virginia

Attention Project PIs

PIs are responsible for keeping up the content of their project page and have the ability to EDIT the page.

- To **EDIT**, click the edit "pencil icon" in the top right-hand corner of this page
- To **PUBLISH** your changes, click the blue "Publish" button in the lower right-hand corner of this page
- If you need help or have questions, please contact Site Admin: Sally.Johnson@louisiana.edu

Table of Contents

Spaces

- All Spaces

CVDI 2017 IAB Fall Meeting

CVDI 2018 IAB Fall Meeting

CVDI 2018 IAB Spring Meeting

CVDI 2019 IAB Fall Meeting

CVDI 2019 IAB Spring Meeting

CVDI Calendar

CVDI Leadership (All Sites)

CVDI

Leelakrishna Bollempalli	Student	Not Available	Not Available	University of Virginia
Jingyi (Teresa) Sun	Student	Not Available	Not Available	University of Virginia
Abhimanyu Roy	Student	Not Available	Not Available	University of Virginia
Robert Hamoney	Student	Not Available	Not Available	University of Virginia
Will Franklin	IAB Project Mentor	william.franklin@capitalone.com	Not available	**Funded by:** Capital One

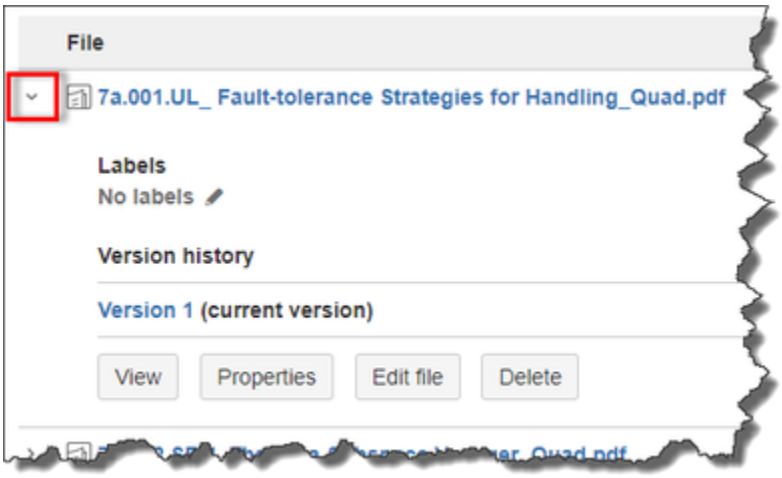
Project Deliverables

	Deliverable
1.	Engineered features for fraud data set, with implementation on AWS
2.	Definition and implementation of adversary and defense strategies
3.	Analysis of ROCs under attack-defense combinations
4.	Conclusions and final report

Project Documents

For viewing/editing options, please click left arrow next to document name.

You will see different options depending on your access level.



File	Modified
6a.058.UVA_Poster_PDF.pdf	Oct 11, 2017 by Sally Johnson
6a.058.UVA_Poster_PPT.pptx	Oct 11, 2017 by Sally Johnson
6a.058.UVA_PPT Presentation.pptx	Oct 11, 2017 by Sally Johnson
6a.058.UVA_Executive Summary.docx	Oct 11, 2017 by Sally Johnson
11-10-2017 11-28-32 AM.png	Nov 10, 2017 by Sally Johnson

Marketing Materials
CVDI Reports & Document Library
CVDI SITE (Drexel University)
CVDI SITE (Stony Brook University)
CVDI SITE (Tampere University)
CVDI SITE (University of Louisiana at Lafayette)
CVDI SITE (University of North Carolina at Charlotte)
CVDI SITE (University of Virginia)
IAB - Industry Advisory Board
Year 6 - Funded Projects (7/1/17 - 6/30/18)
Year 7 - Funded Projects (7/1/18 - 6/30/19)
Year 8 - Proposed Projects

6a.058.UVA_Adversarial Learning in Credit Card Fraud_Poster_2017 Fall Meeting.pptx	Nov 13, 2017 by Sally Johnson
6a.058.UVA_CVDI Mid-Year Report.docx	Dec 28, 2017 by Sally Johnson
6a.058.UVA Final Project Report.docx	Jul 20, 2018 by stephen adams

Drag and drop to upload or browse for files

Download All

Project Comments