CSDS 440 Class Project: Adversarial Machine Learning

Shaochen (Henry) Zhong, sxz517
Minyang Tie, mxt497
Alex Useloff, adu3
Austin Keppers, agk51
David Meshnick, dcm101

Due and submitted on 12/04/2020
Fall 2020, Dr. Ray

Contributions

We as a group of five have looked into the field of adversarial machine learning and specifically investigated several algorithms regarding aspects of attack (evasion, poisoning) and defense (detector, transformer, pre-process). Inside the group, overall contribution are as following:

- Henry:
  - Read 3 papers on algorithms.
  - Implemented 2 algorithms (FGSM and Hop Skip Jump) with 3 extensions.
  - Piplined attack algorithms to work with 2 datasets, collected almost all (7 algorithms/useable extensions) attack experiments data (except backdoor and one pixel attack) for the comparative evaluations.
  - Piplined and collected experiments data for FGSM, Hop Skip Jump, DeepFool attacks (and their useable extensions) against Detector and Spatial Smoothing defenses on 2 datasets.
  - Implemented L_2 and L_∞ perturbation budget to aid comparative evaluation.
  - Wrote Introduction and Significance section.
  - Plotted all graphs and charts in Comparative Study and Discussion.
  - Helped group move forward by making technical decisions, distributing works, setting up deadlines, and facilitating coordination between groupmates.
- Minyang:
- Alex:
- Austin:
- David:

Contents