Adversarial Examples and Adversarial Training

Ian Goodfellow, OpenAI Research Scientist
Presentation at HORSE 2016
London, 2016-09-19
In this presentation

- “Intriguing Properties of Neural Networks” Szegedy et al, 2013
- “Explaining and Harnessing Adversarial Examples” Goodfellow et al 2014
- “Adversarial Perturbations of Deep Neural Networks” Warde-Farley and Goodfellow, 2016
- “Adversarial Perturbations Against Deep Neural Networks for Malware Classification” Grosse et al 2016 (not my own work)
- “Distributional Smoothing with Virtual Adversarial Training” Miyato et al 2015 (not my own work)
Overview

• What causes adversarial examples?

• How can they be used to compromise machine learning systems?

• Adversarial training and virtual adversarial training

• New open source adversarial example library: cleverhans
Adversarial Examples

Timeline:
“Adversarial Classification” Dalvi et al 2004: fool spam filter
“Evasion Attacks Against Machine Learning at Test Time” Biggio 2013: fool neural nets
Szegedy et al 2013: fool ImageNet classifiers imperceptibly
Goodfellow et al 2014: cheap, closed form attack

(Goodfellow 2016)
Attacking a Linear Model
Adversarial Examples from Overfitting

(Goodfellow 2016)
Adversarial Examples from Excessive Linearity
Modern deep nets are very piecewise linear

- Rectified linear unit
- Carefully tuned sigmoid
- Maxout
- LSTM
Maps of Adversarial and Random Cross-Sections

(collaboration with David Warde-Farley and Nicolas Papernot)
Maps of Random Cross-Sections

Adversarial examples are not noise

(collaboration with David Warde-Farley and Nicolas Papernot)
Clever Hans

(“Clever Hans, Clever Algorithms,” Bob Sturm)
Small inter-class distances

All three perturbations have L2 norm 3.96
This is actually small. We typically use 7!

Perturbation changes the true class

Random perturbation does not change the class

Perturbation changes the input to “rubbish class”
The Fast Gradient Sign Method

\[ J(\tilde{x}, \theta) \approx J(x, \theta) + (\tilde{x} - x)^\top \nabla_x J(x). \]

Maximize

\[ J(x, \theta) + (\tilde{x} - x)^\top \nabla_x J(x) \]

subject to

\[ \| \tilde{x} - x \|_\infty \leq \epsilon \]

\[ \Rightarrow \tilde{x} = x + \epsilon \text{sign} (\nabla_x J(x)). \]
Wrong almost everywhere
Cross-model, cross-dataset generalization
Cross-technique transferability

<table>
<thead>
<tr>
<th>Source Machine Learning Technique</th>
<th>Target Machine Learning Technique</th>
<th>DNN</th>
<th>LR</th>
<th>SVM</th>
<th>DT</th>
<th>kNN</th>
<th>Ens.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNN</td>
<td>38.27</td>
<td>23.02</td>
<td>64.32</td>
<td>79.31</td>
<td>8.36</td>
<td>20.72</td>
<td></td>
</tr>
<tr>
<td>LR</td>
<td>6.31</td>
<td>91.64</td>
<td>91.43</td>
<td>87.42</td>
<td>11.29</td>
<td>44.14</td>
<td></td>
</tr>
<tr>
<td>SVM</td>
<td>2.51</td>
<td>36.56</td>
<td>100.0</td>
<td>80.03</td>
<td>5.19</td>
<td>15.67</td>
<td></td>
</tr>
<tr>
<td>DT</td>
<td>0.82</td>
<td>12.22</td>
<td>8.85</td>
<td>89.29</td>
<td>3.31</td>
<td>5.11</td>
<td></td>
</tr>
<tr>
<td>kNN</td>
<td>11.75</td>
<td>42.89</td>
<td>82.16</td>
<td>82.95</td>
<td>41.65</td>
<td>31.92</td>
<td></td>
</tr>
</tbody>
</table>

- Fool cloud ML API
- Amazon
- Google
- MetaMind
- Fool malware detector

(Papernot 2016)
Adversarial Examples in the Physical World

(a) Printout

(b) Photo of printout

(c) Cropped image
Adversarial Examples in the Human Brain

(Pinna and Gregory, 2002)

These are concentric circles, not intertwined spirals.

(Pinna and Gregory, 2002)
Failed defenses

Generative pretraining
Adding noise at test time
Confidence-reducing perturbation at test time
Weight decay
Various non-linear units
Removing perturbation with an autoencoder
Ensembles
Error correcting codes
Multiple glimpses
Double backprop
Dropout
Adding noise at train time

(Goodfellow 2016)
Training on Adversarial Examples

- Clean examples
- Adversarial examples

- Validation set error vs. training time (epochs)

- Standard training
- Adversarial training

(Goodfellow 2016)
Virtual Adversarial Training

Unlabeled; model guesses it’s probably a bird, maybe a plane

Adversarial perturbation intended to change the guess

New guess should match old guess (probably bird, maybe plane)
cleverhans

Open-source library available at:

https://github.com/openai/cleverhans

Built on top of TensorFlow (Theano support anticipated)

Benchmark your model against different adversarial examples attacks

Beta version 0.1 released, more attacks and features to be added