ADVERSARIAL MACHINE LEARNING

RESEARCH LANDSCAPE

6

- Attack Models (Part I)
  - How to convert a pure example into an adversarial example for a given classifier net?
- Defence Mechanism (Part II)
  - How to train a DNN classifier so as to make it robust against the attacks?

PART I

ATTACK MODELS

RESEARCH LANDSCAPE

- Attack Models (Part I)
  - How to convert a pure example into an adversarial example for a given classifier net?
- Defence Mechanism (Part II)
  - How to train a DNN classifier so as to make it robust against the attacks?