U.S. ARMY RESEARCH, DEVELOPMENT AND ENGINEERING COMMAND

AI and Intelligent Systems: Army Challenges

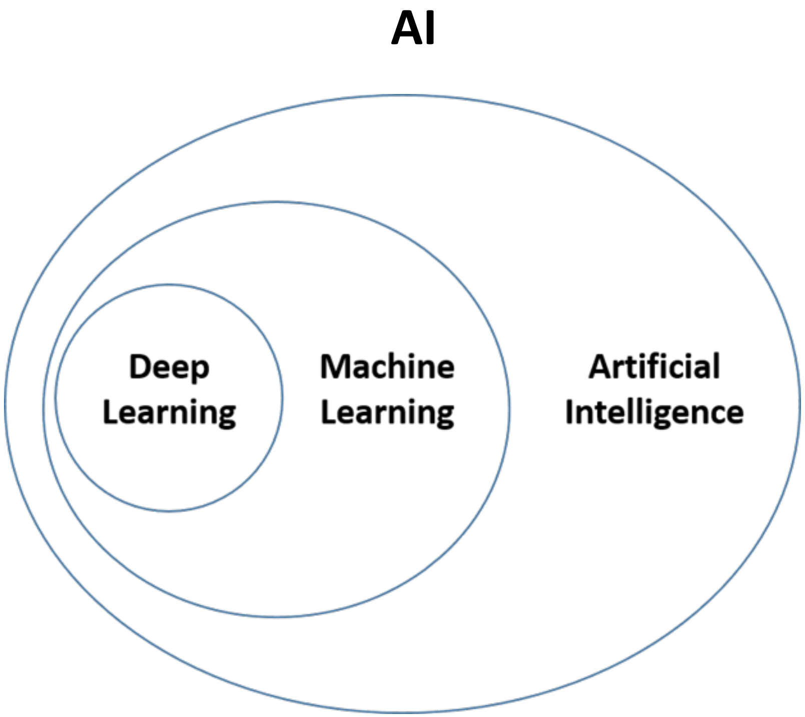
Brian Sadler & Tien Pham

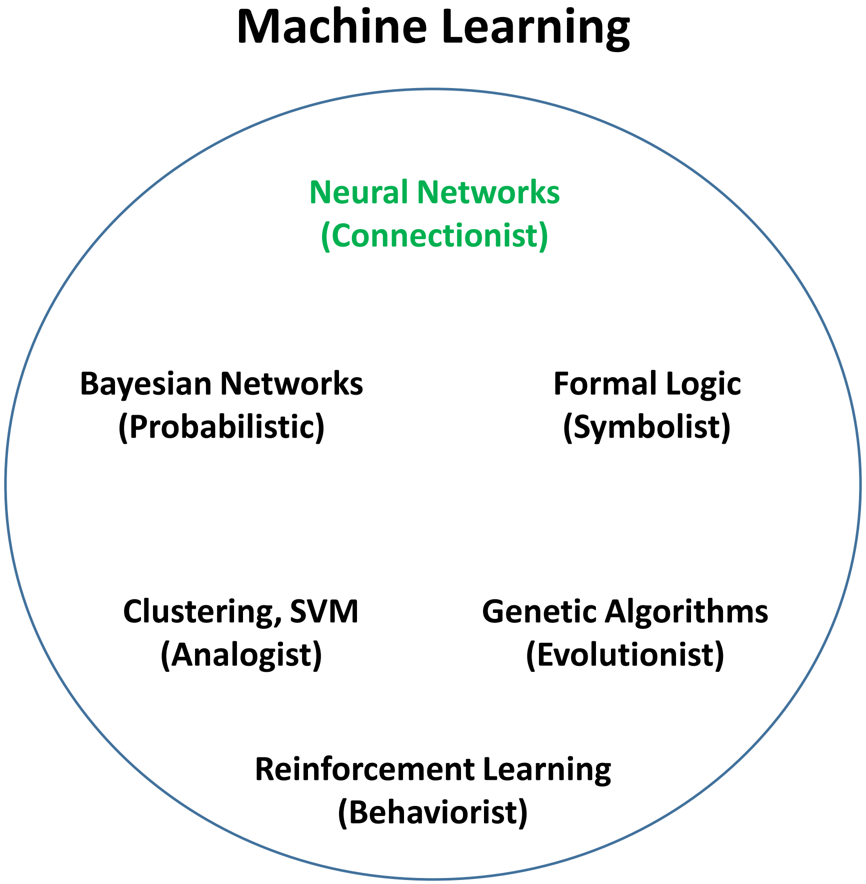
ST for Intelligent Systems

ARL

AI & ML

- AI is the ability of machines to do things that people would say requires intelligence
- AI is a broad set of tools and theories




Machine Learning
Neural Networks (Connectionist)
Bayesian Networks (Probabilistic)
Formal Logic (Symbolist)
Clustering, SVM (Analogist)
Genetic Algorithms (Evolutionist)
Reinforcement Learning (Behaviorist)

ARMY AI: UNIQUE CHALLENGES

Ground-based operations in complex environments

- Lack of infrastructure and prior access
- Lack of Army-relevant training data
- Rapid operational tempo

Reliance on wireless networking and distributed operations

- Decision making with uncertainty
- Adversaries and deception
- Cyber / EW

Distributed Intelligence
Collaborative Agents
Adversarial AI

Motion and Manipulation
Autonomous Networking

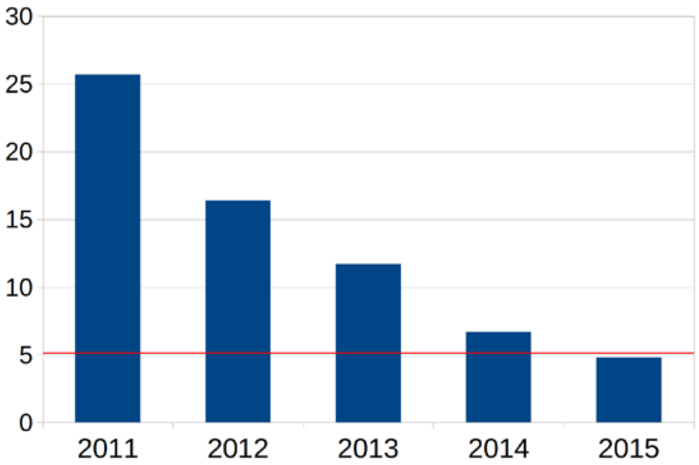
Commercial AI Infrastructure: road signs, power sources, cellular networks, cloud-based services, massive scale HPC

NEURAL NETWORK CLASSIFIERS

Dramatic advances in processing natural signals (speech, vision)

Fueled by massive training examples & digital computation

ImageNet Error Rates



At or exceeding “human performance”

No analytical framework

Unpredictable performance

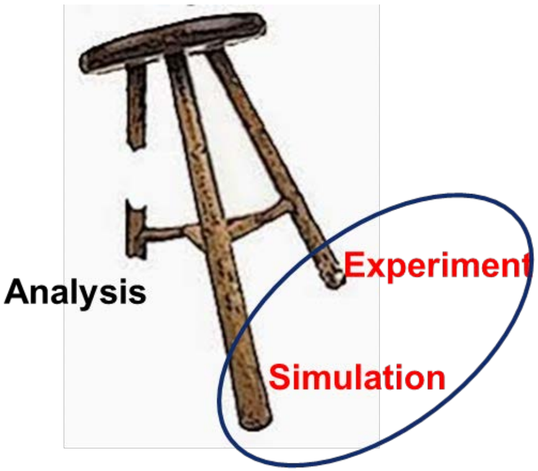
Lack of online memory and adaptation

Empirical guess and check development

Assumes prior access for training

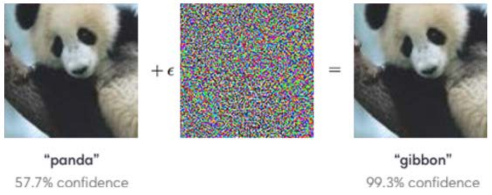
Data driven paradigm not sustainable

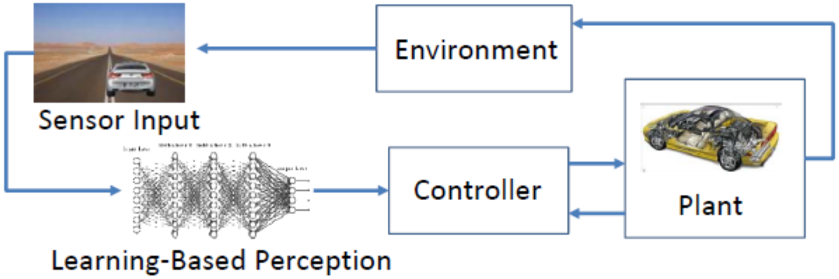
Expect dramatic successes & failures



ADVERSARIAL AI R&D

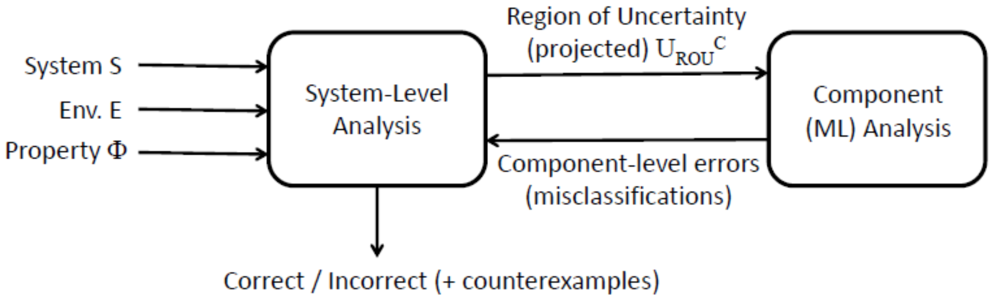
Nguyen et al., 2015





Closed loop system:

subject to classification errors, adversarial input


System S
Env. E
Property Φ
System-Level Analysis
Region of Uncertainty (projected) U_{ROU}^{C}
Component (ML) Analysis
Component-level errors (misclassifications)
Correct / Incorrect (+ counterexamples)

System level verification: towards safety, security, trust

Semantic Adversarial Deep Learning
Dreossi, Jha, Seshia
arXiv.org 1804.07045, 2018

TOWARD INTELLIGENT SYSTEMS

Army AI R&D

- Cyber / EW
- Adversarial AI
- Robotics & physical reasoning
- Distributed intelligence and control
- Human-machine dialog
- Crowdsourcing
- Online learning and perception
- Reinforcement learning and policy

- *Verification and validation*

Goal: Adding Intelligence

- Off-road ground mover
- Munition
- Aerial collector
- Intel info integrator and interpreter
- CoA generator and monitor
- Cyber defense agent
- Network management agent
- Chem-Bio detector

AI COMPUTING

HPC for AI

- GPU-based commodity
- AI algorithm R&D
- Large scale simulation & learning
- New forms of test & evaluation
- Support operational AI & Algorithmic Warfare

Emergent & Embedded Computing

- Next-gen embedded AI chips

  Intel Movidius Neural Compute Engine
  Qualcomm Neural Processing Engine
  Huawei Kirin 970 Neural Processing Unit
  Apple A11 Bionic Neural Engine
  Google Pixel Visual Core SoC

Army AI will be a rich heterogeneous mixture of platform, tactical cloud, & edge-based computing

DISCUSSION

RDECOM AI Strategy Study

July 2018

End

LEARNING & BIG DATA

Big Data Assumptions

- Sufficiently large (size needed unknown a priori)
- Data collected in the wild isn't poisoned (bad examples, adversary)
- Data sufficiently broad for AI generality (public data sets too pristine)

Big Data Research Areas

- Unsupervised learning
- Semi-supervised learning w/ human-in-the-loop
- Learning while incorporating constraints, physics, or models
- Supplementing training with simulations
- Transfer learning between agents
- Robust learning to handle adversary
- Online and lifelong learning to avoid reliance on batch training

Learning under study for many ML approaches, not just NNs.

Some problems do not require massive data sets.