Massachusetts Institute of Technology

MARIE CURIE ACTIONS

UNIVERSITAS MALACITANA

- NeCOL -
Neural CO-evolutionary Learning

UNA-MAY O'REILLY
UNAMAY@CSAIL.MIT.EDU

JAMAL TOUTOUH
TOUTOUH@MIT.EDU
JAMAL@LCC.UMA.ES

ENRIQUE ALBA
EAT@LCC.UMA.ES

ALFA
ANYSCALE LEARNING FOR ALL

NEO

Smart Cities & Cybersecurity

More than half of the world's population lives in urban areas → From Cities to **Smart Cities**

Improve economic, social, and environmental **sustainability**

- Takes the advantage of IoT and Big Data
- Smart Services based on ML/DL models

Cybersecurity threats

Adversarial attacks to the models

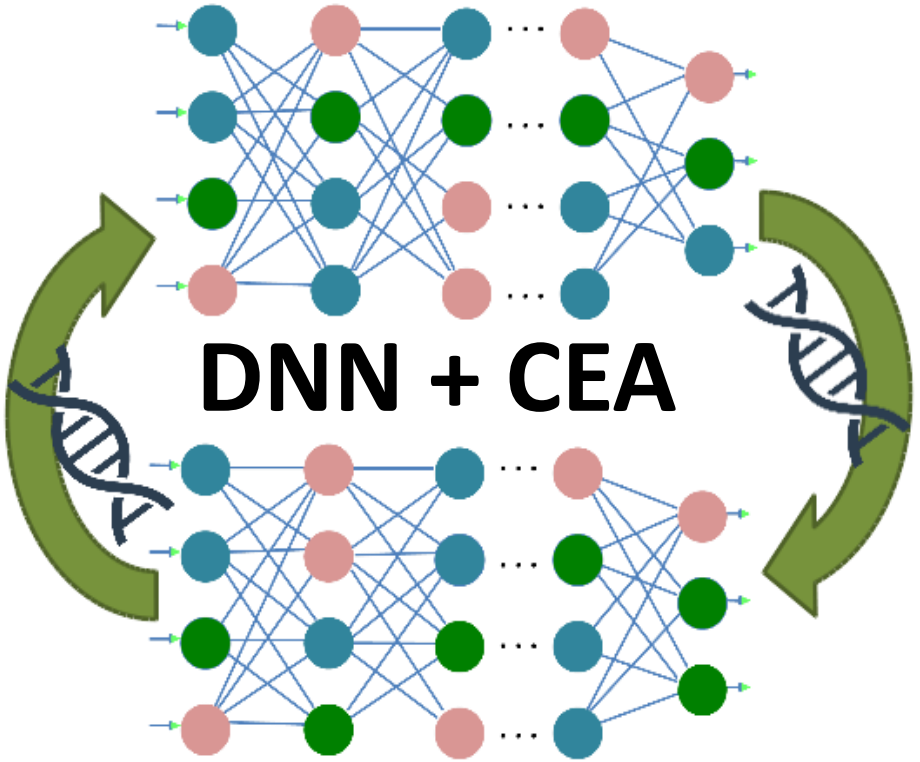
Use DL

"Smart cities are going to be a **security nightmare**…"
The Harvard Business Review

NeCOL

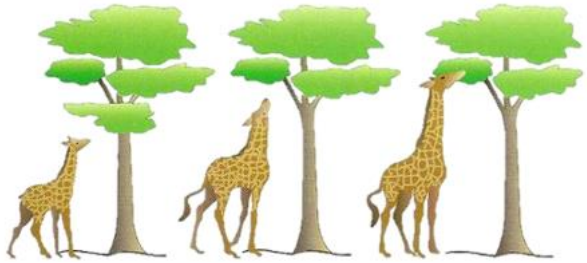
Neural CO-evolutionary Learning

- Competitive performance
- Robustness
- Multi-level optimization
- Scalable and easy to parallelize



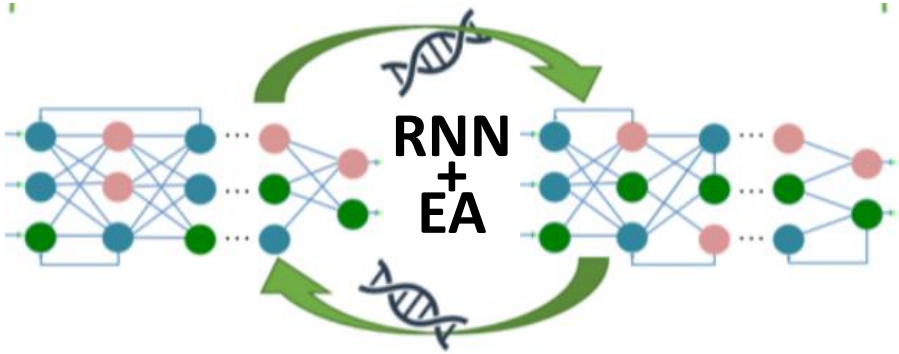
RNN Deep Neuroevolution for Smart Cities

Evolving an RNN (architecture) to model a predictor of the **waste generation**



The quality or fitness of the evolved RNNs is evaluated according to the **mean absolute error (MAE)**

Early approach

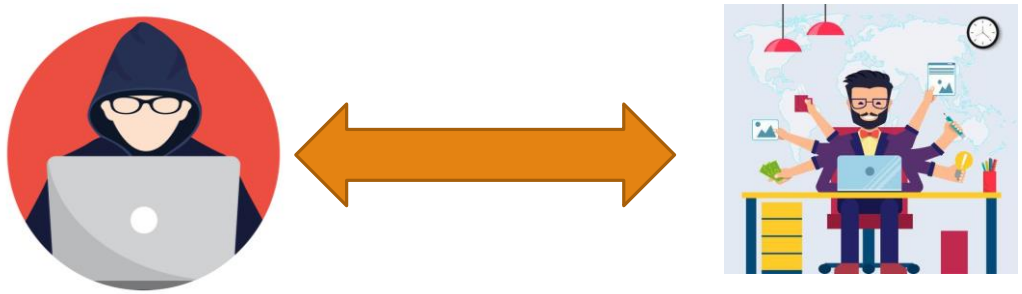


Waste Generation Prediction Under Uncertainty in Smart Cities through Deep Neuroevolution, *Revista Facultad de Ingeniería*

ML/DL Cybersecurity

Cybersecurity presents continuous arms races

Attackers vs defenders → conflicting objectives



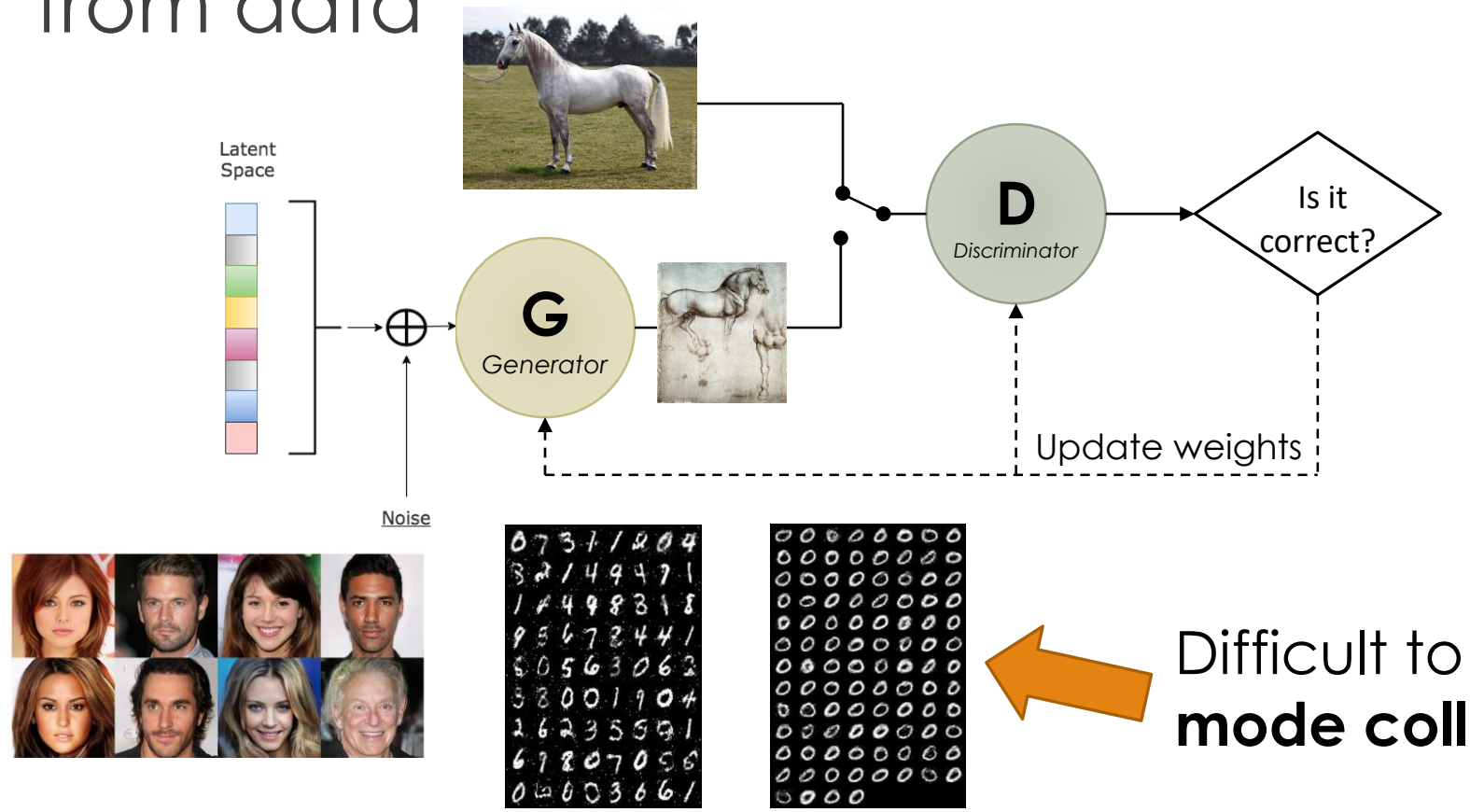
Main challenges of applying ML/DL to cybersecurity:

- Data scarcity
- Data imbalance
- Detectors not modelled for unseen data

Generative models can address these issues

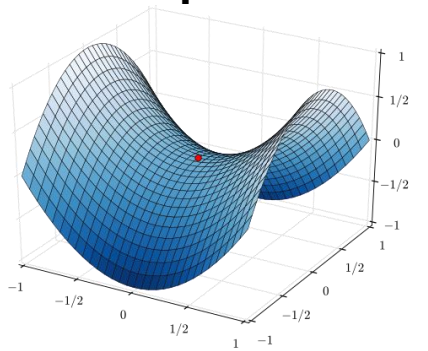
Generative Adversarial Networks

GANs create **generative** and **discriminative** models from data



Difficult to train: **mode collapse**

Minmax optimization



Expected **Result**

GANs, Coev, and Biological Arms Races

Nature presents continuous biological arms races between individuals of different species

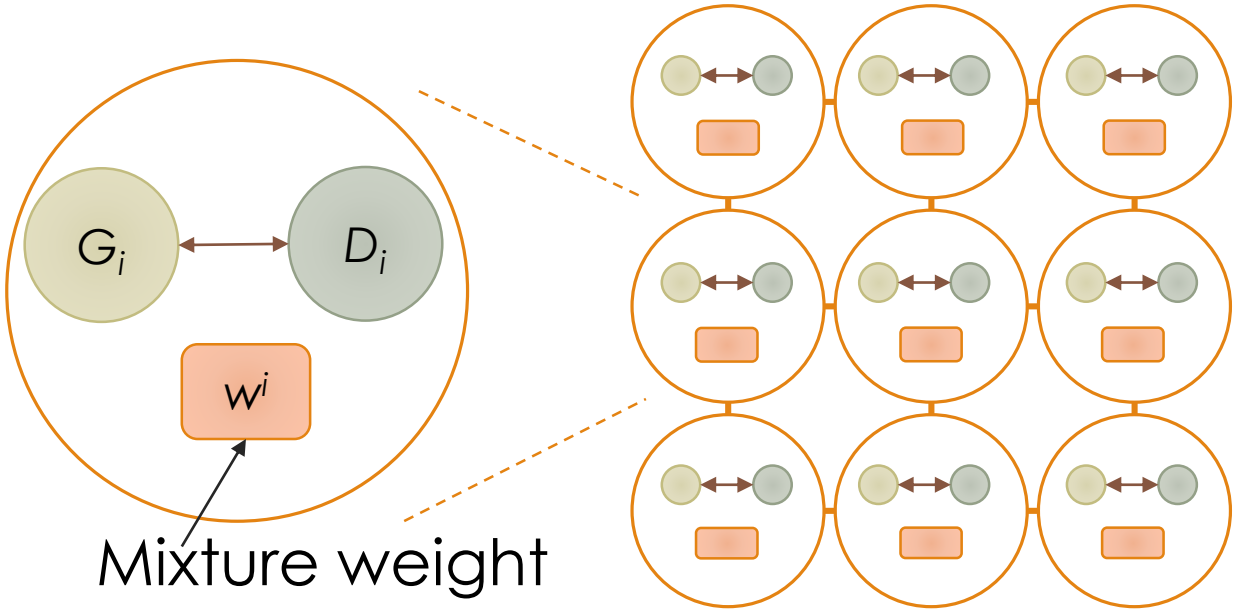
Can coevolution help to improve robustness in other adversarial settings?

- Multiple comparisons can aid **robustness**
- Multiple variations based on quality measurements improve **diversity**

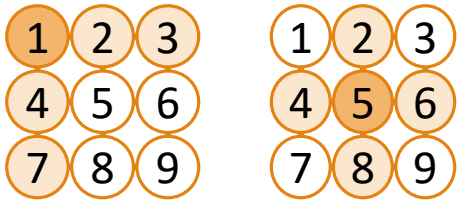
Adversarial Genetic Programming for Cyber Security: A Rising Application Domain Where GP Matters, *under review*

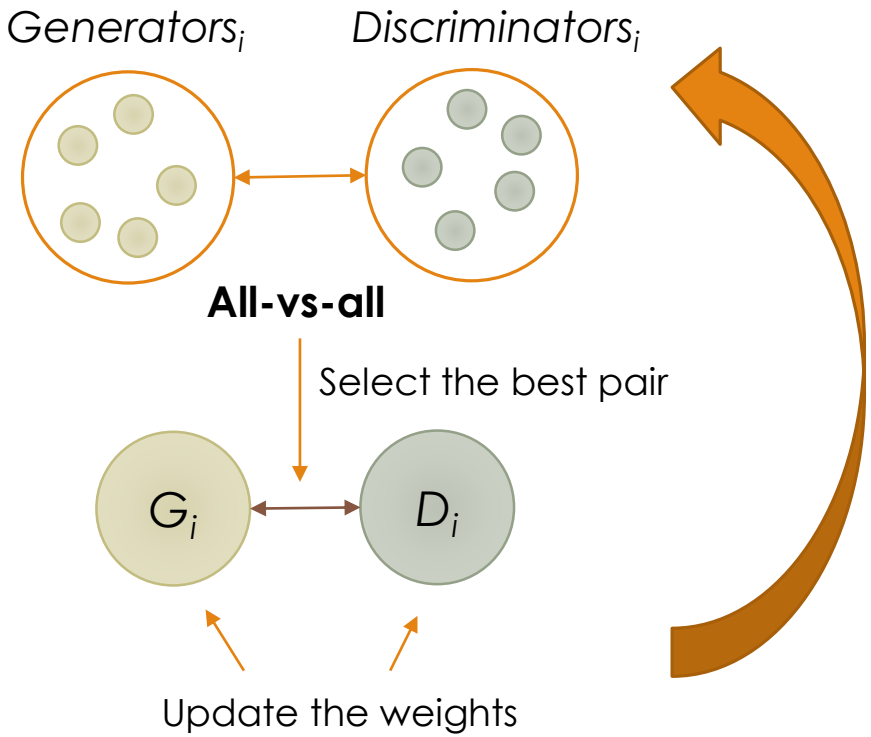
Mustangs: Gradient-based Coevolution

A **distributed**, **coevolutionary** framework to train GANs with **gradient-based** optimizers



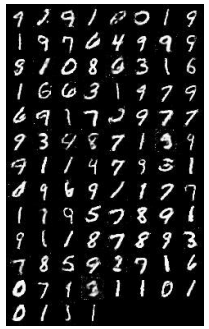
Neighborhood examples

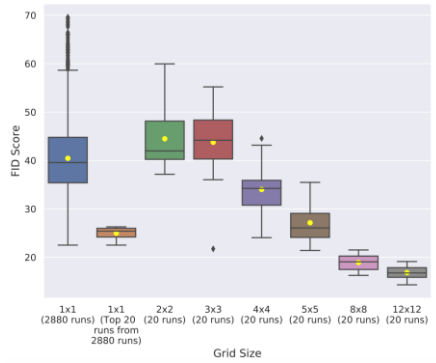


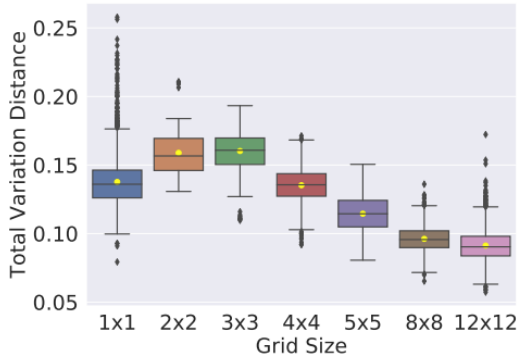


https://github.com/mustang-gan/mustang

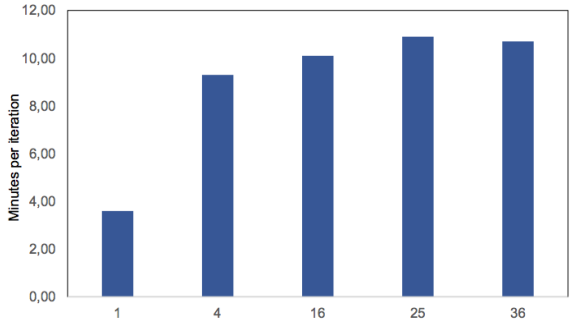
Mustangs: Gradient-based Coevolution





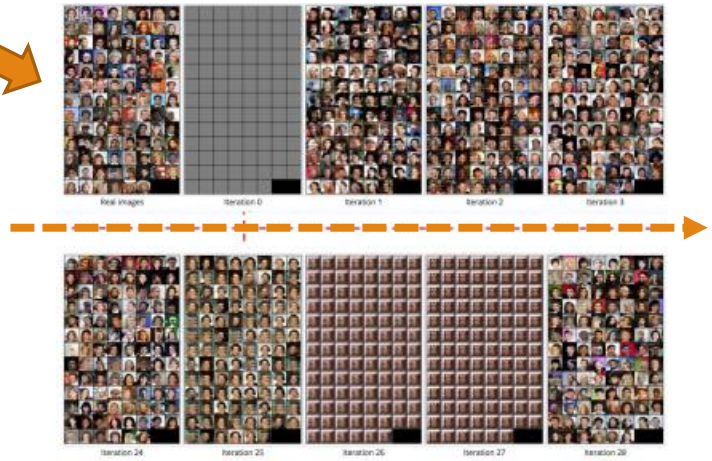


Accurate generators



Scalable

Diversity



Escape from mode collapse

- Improves convergence
- Diverse solutions
- Robustness
- Scalability

Spatial Evolutionary Generative Adversarial Networks, *GECCO 2019*

Spatial Coevolution for Robust Scalable Generative Adversarial Network Training, *work in progress*

Future Work

Mustangs for Cybersecurity

- Generating more malicious data to allow to train stronger detectors
- Generating malicious data which can deceive and evade the detection
- Generating adversarial examples to fool ML models

The more diversity, the better performance?

- Probabilistic GANs approaches
- More theory (minmax optimization, game theory)

Using spatial co-evolution for other generative approaches

- Variational autoencoder → Cooperative (Encoder-Decoder)

Thanks!

Comments?

NECOL WEBSITE
NECOL.NET

JAMAL TOUTOUH
TOUTOUH@MIT.EDU