ADVERSARIAL LEARNING OF ROBUST AND SAFE CONTROLLERS FOR CYBER-PHYSICAL SYSTEMS

Master in Data Science and Scientific Computing

Francesco Franchina - 24 April 2020

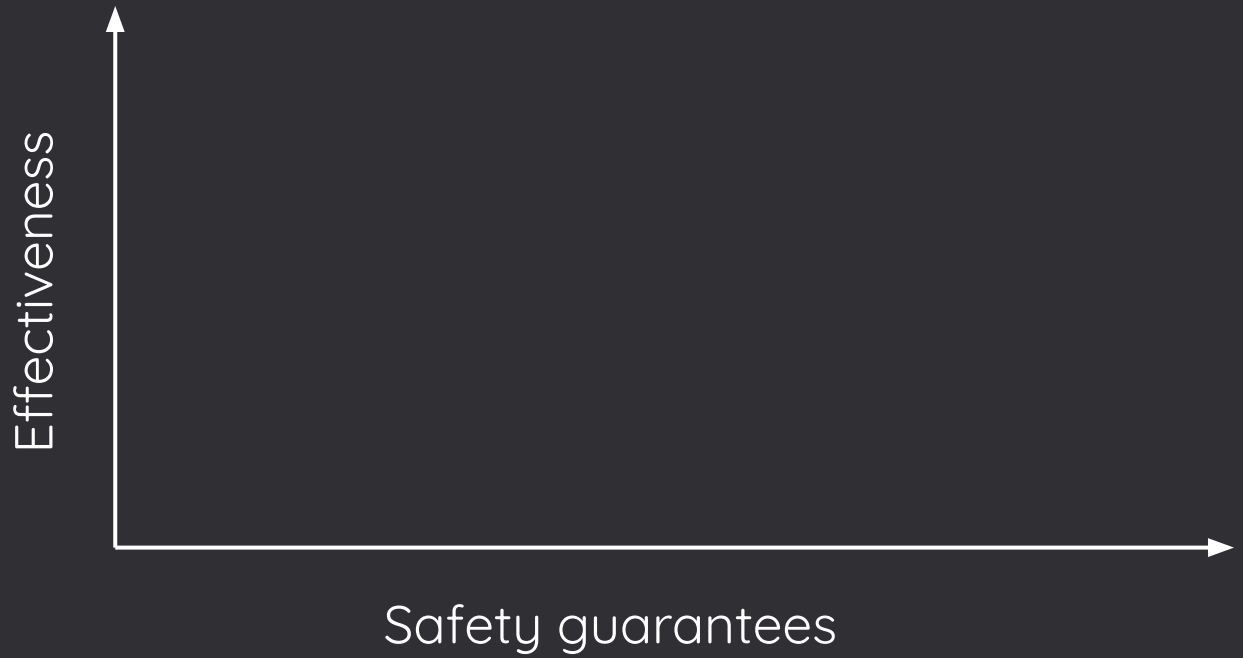
PURPOSE

Propose a novel method for obtaining a safe controller after a training procedure

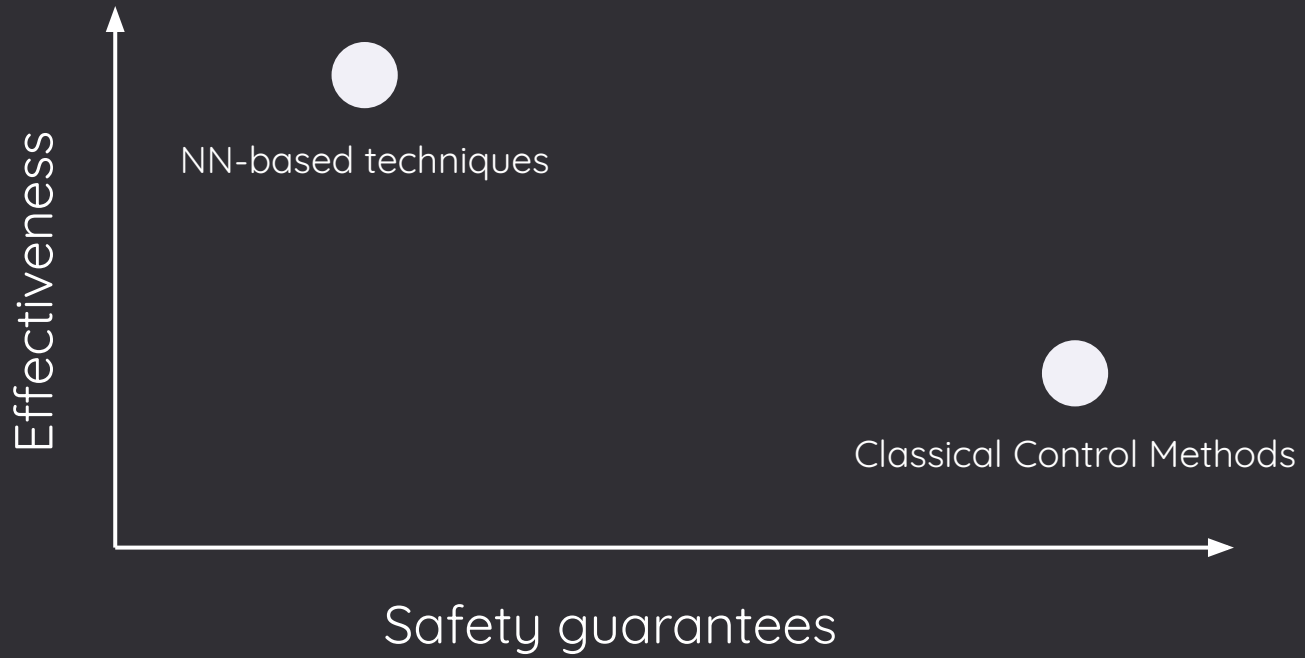
STARTING FROM

If it ain't broke, don't fix it!

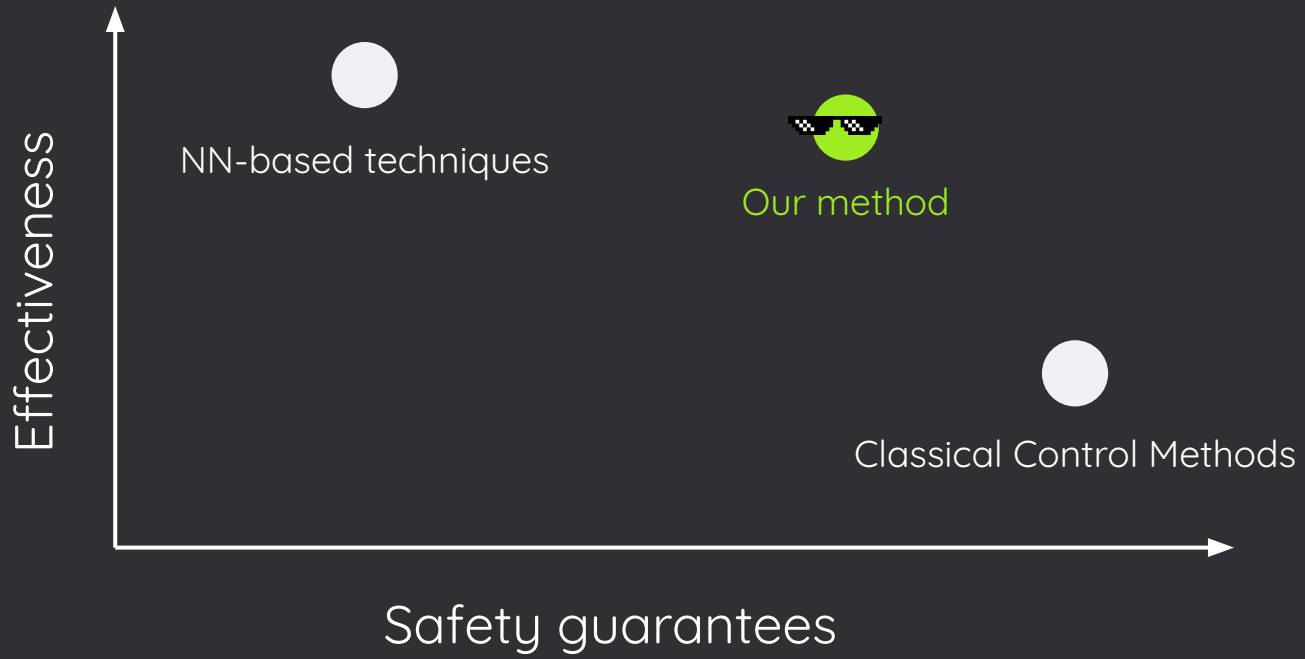
TRADEOFF



TRADEOFF


Effectiveness
NN-based techniques
Classical Control Methods
Safety guarantees

TRADEOFF


Effectiveness
NN-based techniques
Our method
Classical Control Methods
Safety guarantees

1

BACKGROUND

CPS, GAN, STL

CYBER-PHYSICAL SYSTEM - BACKGROUND

CYBER-PHYSICAL SYSTEM - BACKGROUND

Cyber

- Controller
- Algorithm
- Discrete-time

CYBER-PHYSICAL SYSTEM - BACKGROUND

Cyber

- Controller
- Algorithm
- Discrete-time

Physical

- Plant
- Nature’s laws
- Continuous-time

CYBER-PHYSICAL SYSTEM - BACKGROUND

Cyber

- Controller
- Algorithm
- Discrete-time

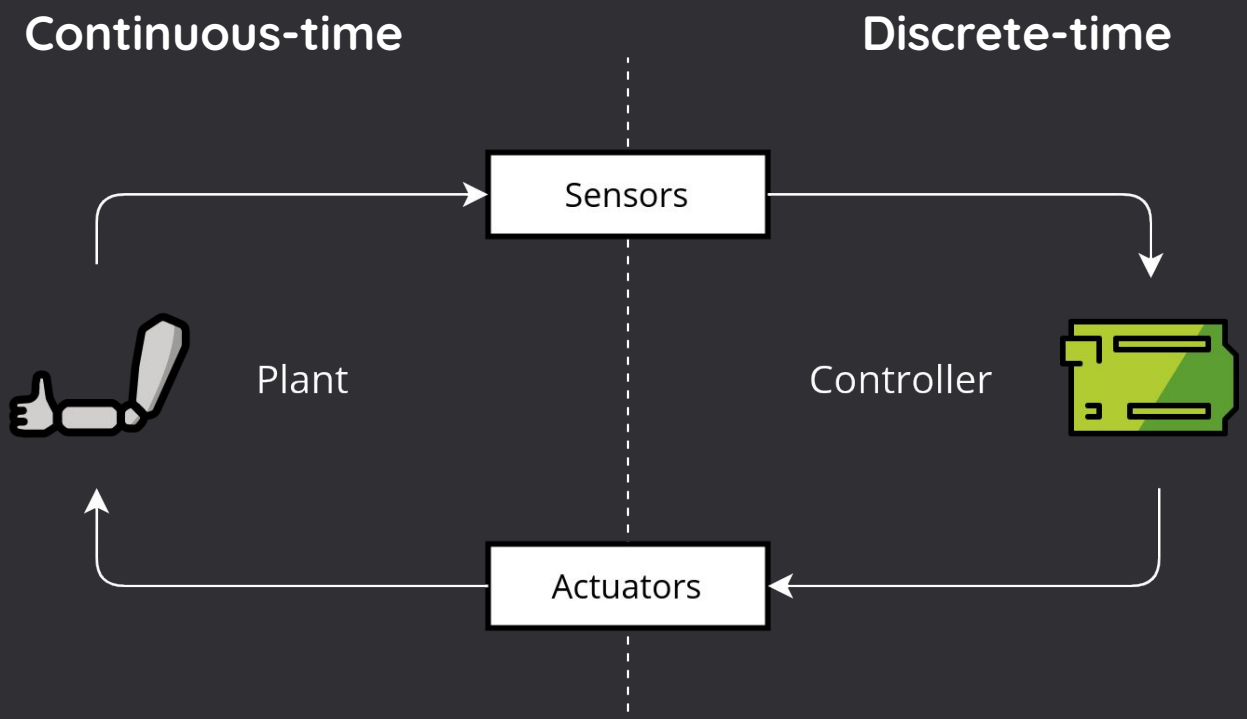
Physical

- Plant
- Nature’s laws
- Continuous-time

System

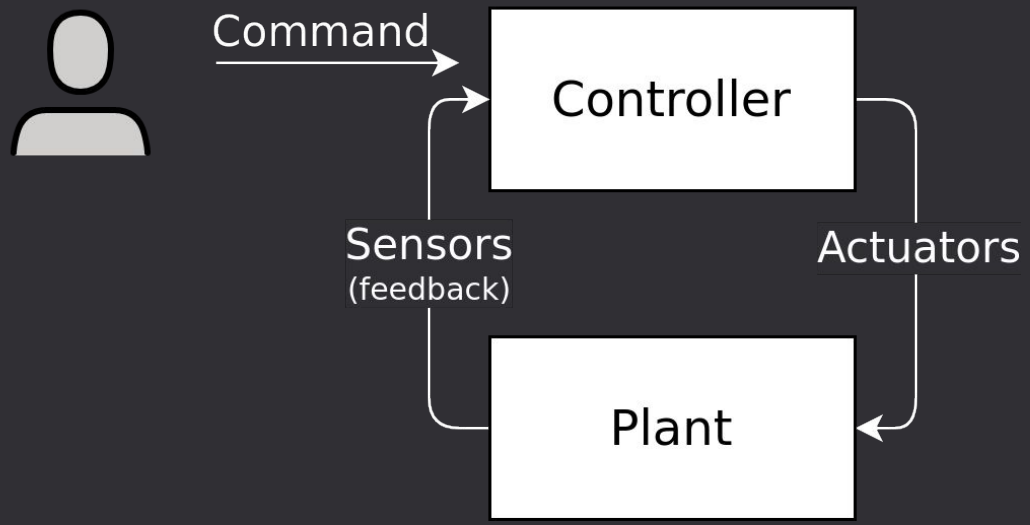
- Communication
- Sensors
- Actuators

CYBER-PHYSICAL SYSTEM - BACKGROUND



CYBER-PHYSICAL SYSTEM - BACKGROUND

Closed-loop control



GENERATIVE ADVERSARIAL NETWORK - BACKGROUND

GENERATIVE ADVERSARIAL NETWORK - BACKGROUND

Generator

- Neural Network
- Learns a distribution
- Generative model

GENERATIVE ADVERSARIAL NETWORK - BACKGROUND

Generator

- Neural Network
- Learns a distribution
- Generative model

Discriminator

- Neural Network
- Classifier

GENERATIVE ADVERSARIAL NETWORK - BACKGROUND

Generator

- Neural Network
- Learns a distribution
- Generative model

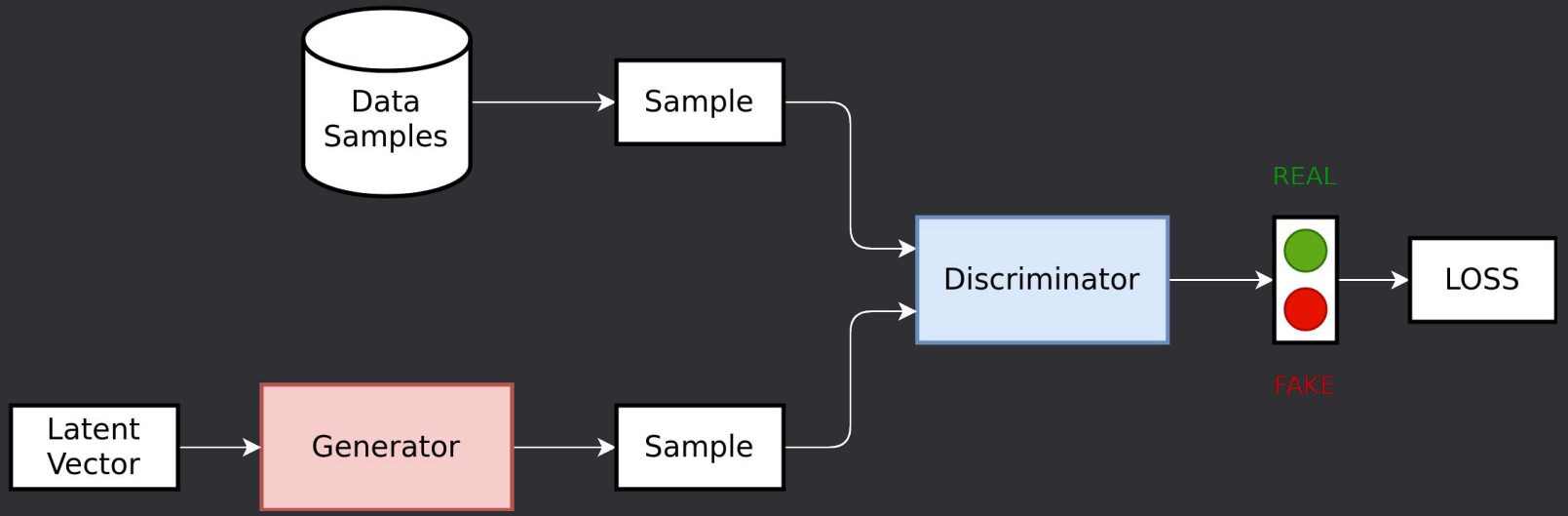
Discriminator

- Neural Network
- Classifier

Zero-sum game

GENERATIVE ADVERSARIAL NETWORK - BACKGROUND

Architecture



SIGNAL TEMPORAL LOGIC - BACKGROUND

SIGNAL TEMPORAL LOGIC - BACKGROUND

- Makes statements
- Operates on signals
- Monitoring

SIGNAL TEMPORAL LOGIC - BACKGROUND

- Makes statements
- Operates on signals
- Monitoring

Syntax

Semantic

SIGNAL TEMPORAL LOGIC - BACKGROUND

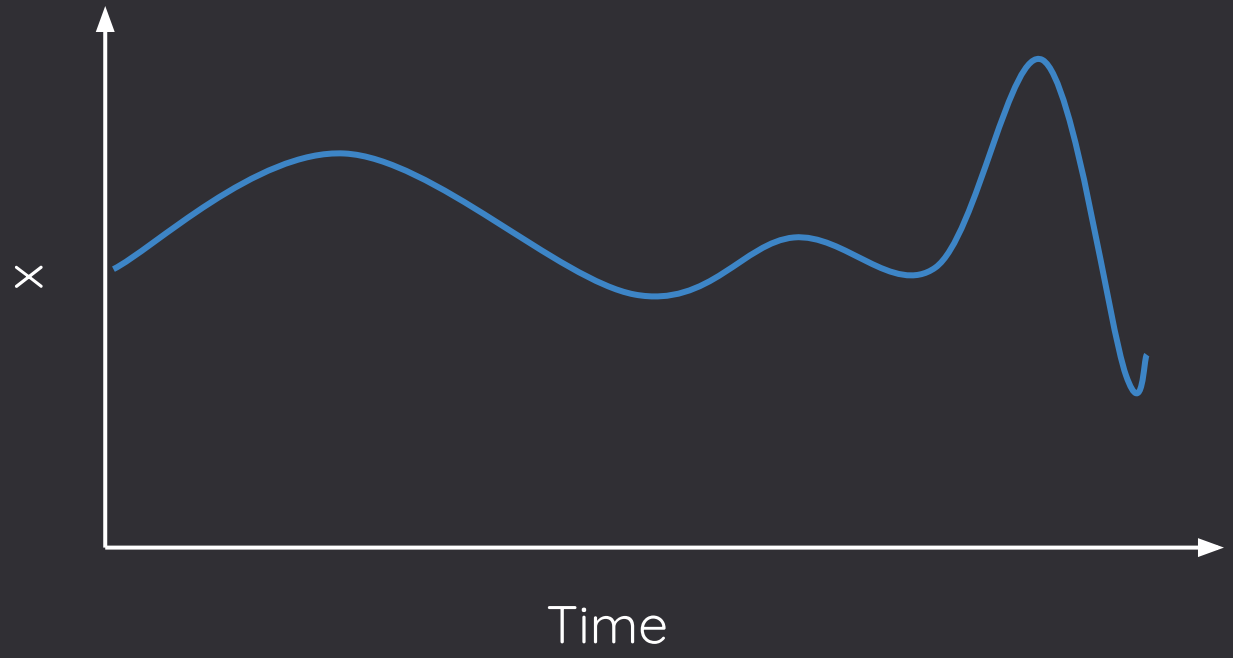
- Makes statements
- Operates on signals
- Monitoring

Syntax

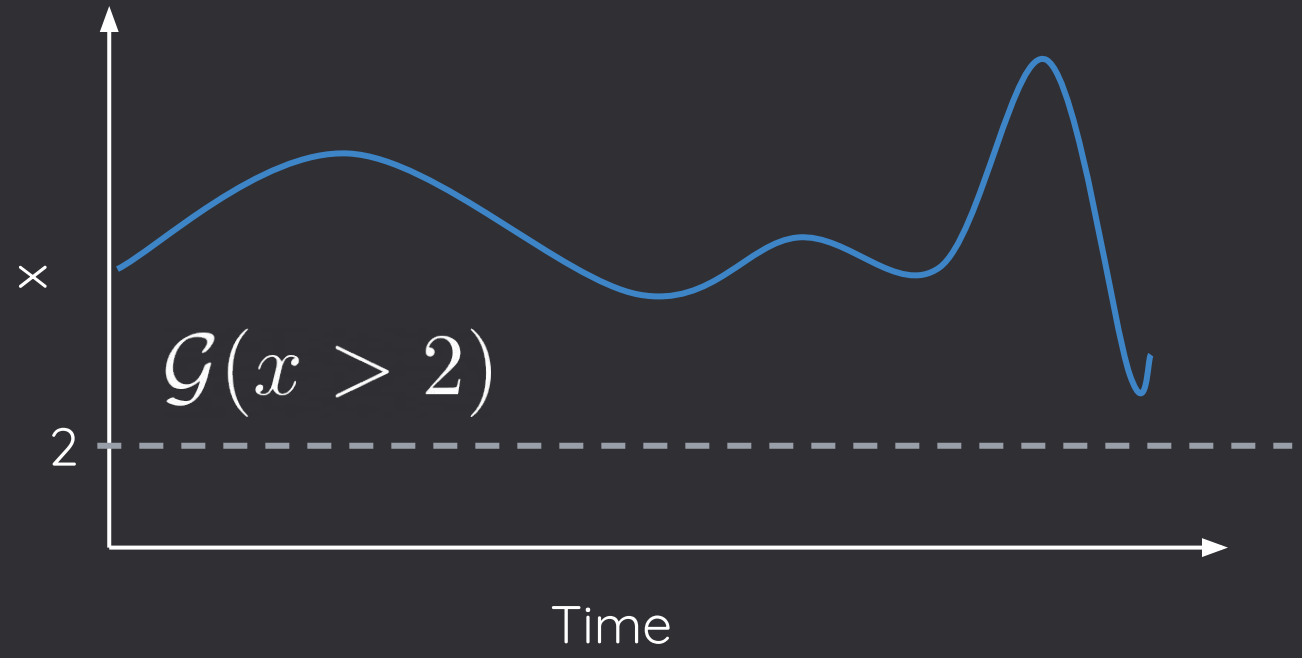
Semantic

- Boolean
- Quantitative

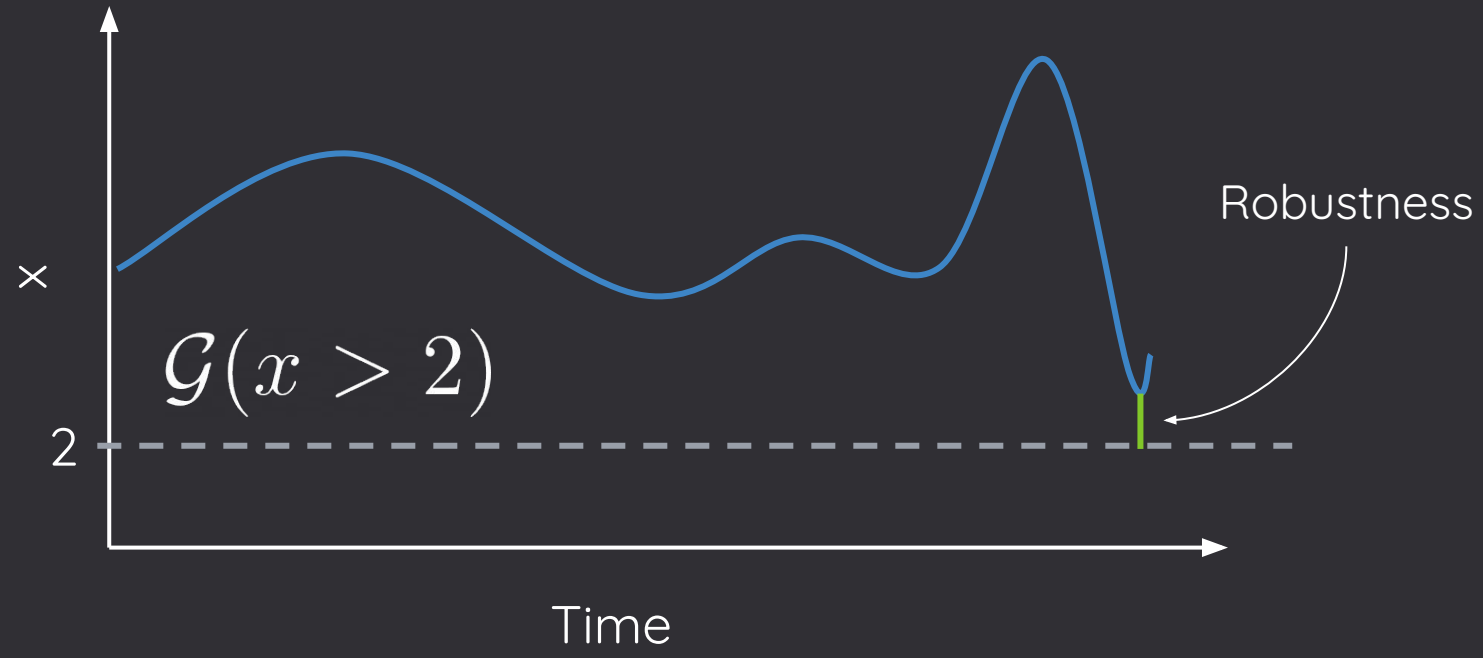
SIGNAL TEMPORAL LOGIC - BACKGROUND



SIGNAL TEMPORAL LOGIC - BACKGROUND



SIGNAL TEMPORAL LOGIC - BACKGROUND



2

OUR METHOD

Putting all the pieces together

OVERVIEW - OUR METHOD

Adversarial training of NNs

STL robustness as loss

Adversarial training of NNs

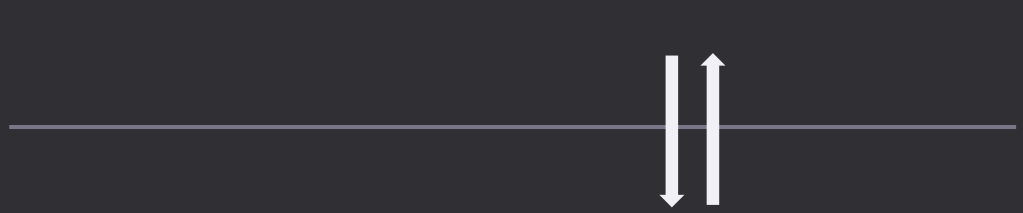
STL robustness as loss

Physical Model

Differential equation

Adversarial training of NNs

STL robustness as loss



Physical Model

Differential equation

PHYSICAL MODEL - OUR METHOD

PHYSICAL MODEL - OUR METHOD

Agent

- Plant of CPS
- Senses environment
- Acts on the environment

PHYSICAL MODEL - OUR METHOD

Agent

- Plant of CPS
- Senses environment
- Acts on the environment

Environment

- Not controlled
- Can sense
- Can mutate

PHYSICAL MODEL - OUR METHOD

Agent α

Environment β

$\mathcal{M}$

with state s

PHYSICAL MODEL - OUR METHOD

Agent α

IN: $\mathbf{u}_\alpha$

OUT: $\xi_\alpha(s) = \mathbf{o}_\alpha$

Environment β

IN: $\mathbf{u}_\beta$

OUT: $\xi_\beta(s) = \mathbf{o}_\beta$

$\mathcal{M}$

with state s

PHYSICAL MODEL - OUR METHOD

Simulator f

$$\mathbf{s}_{i+1} = \mathbf{s}_i + f(\mathbf{s}_i, (\mathbf{u}_\alpha)_i, (\mathbf{u}_\beta)_i, t_i)$$

PHYSICAL MODEL - OUR METHOD

Simulator f

$$\mathbf{s}_{i+1} = \mathbf{s}_i + f(\mathbf{s}_i, (\mathbf{u}_\alpha)_i, (\mathbf{u}_\beta)_i, t_i)$$

- $\mathbf{s}_{i+1}$: Next state
- $\mathbf{s}_i$, $f(\mathbf{s}_i, \ldots)$: Current state
- $(\mathbf{u}_\alpha)_i$: Agent's action
- $(\mathbf{u}_\beta)_i$: Environment's action
- t_i: Time

ADVERSARIAL ARCHITECTURE - OUR METHOD

ADVERSARIAL ARCHITECTURE - OUR METHOD

Defender

Attacker

ADVERSARIAL ARCHITECTURE - OUR METHOD

Defender

Agent

Attacker

Environment

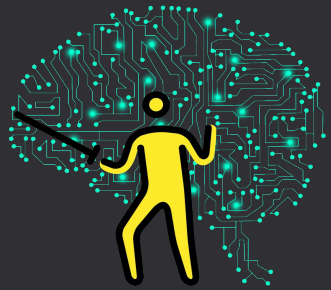
ADVERSARIAL ARCHITECTURE - OUR METHOD

Planning

$\mathbf{o}_\alpha$

$\mathbf{z}$

$\mathbf{o}_\beta$



ADVERSARIAL ARCHITECTURE - OUR METHOD

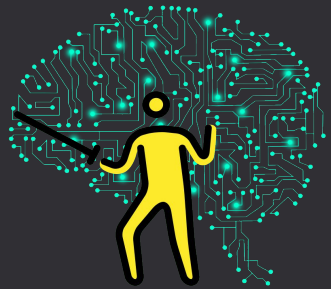
Planning

$\mathbf{o}_\alpha$

$\mathbf{w}_D$

$\mathbf{z}$

$\mathbf{o}_\beta$



$\mathbf{w}_A$

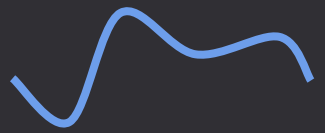
ADVERSARIAL ARCHITECTURE - OUR METHOD

Planning

$\mathbf{o}_\alpha$

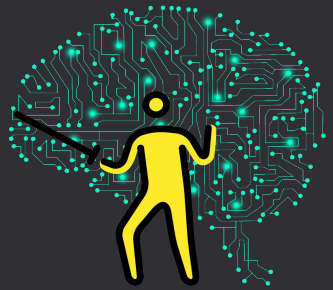
$\mathbf{w}_D$

$\Pi_D(\mathbf{w}_D, t)$



$\mathbf{z}$

$\mathbf{o}_\beta$



$\mathbf{w}_A$

$\Pi_A(\mathbf{w}_A, t)$

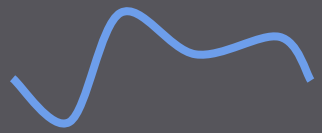
ADVERSARIAL ARCHITECTURE - OUR METHOD

Planning

$\mathbf{o}_\alpha$

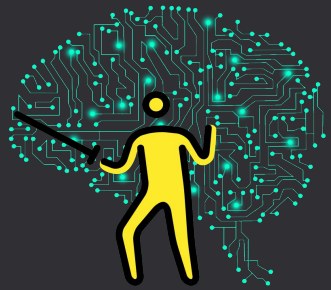
$\mathbf{w}_D$

$\Pi_D(\mathbf{w}_D, t)$



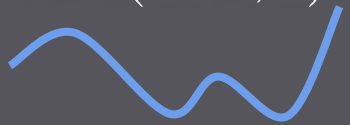
$\mathbf{z}$

$\mathbf{o}_\beta$



$\mathbf{w}_A$

$\Pi_A(\mathbf{w}_A, t)$

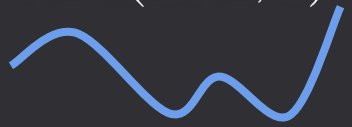


ADVERSARIAL ARCHITECTURE - OUR METHOD

Evaluation

$$\Pi_D(\mathbf{w}_D, t)$$

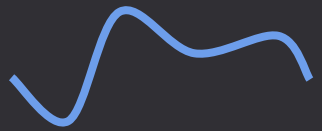
$$\Pi_A(\mathbf{w}_A, t)$$



ADVERSARIAL ARCHITECTURE - OUR METHOD

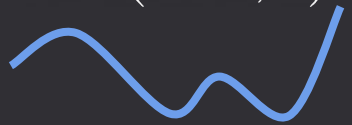
Evaluation

$\Pi_D(\mathbf{w}_D, t)$



$\mathbf{u}_\alpha(t)$

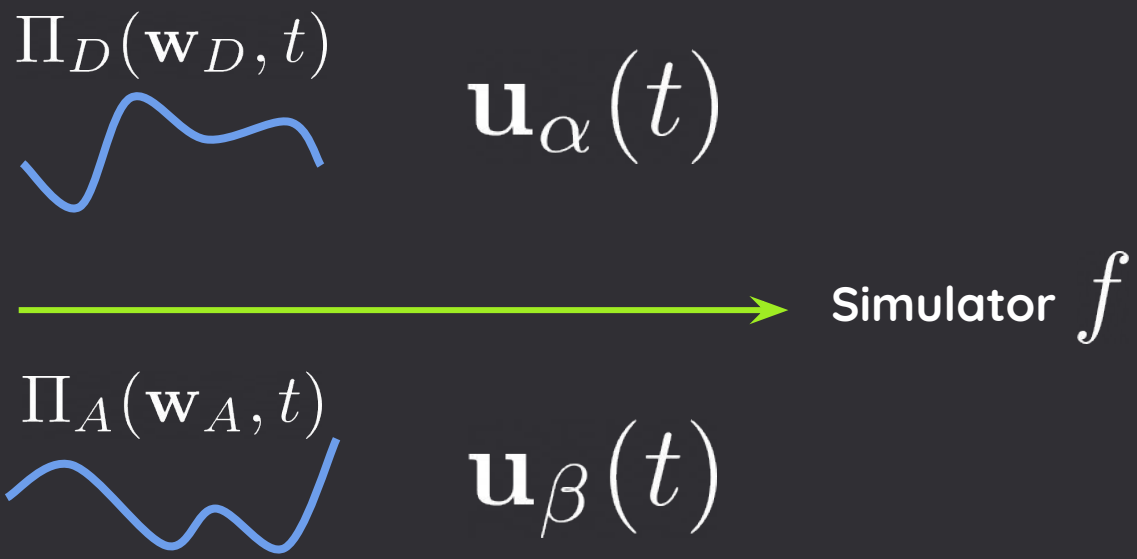
$\Pi_A(\mathbf{w}_A, t)$



$\mathbf{u}_\beta(t)$

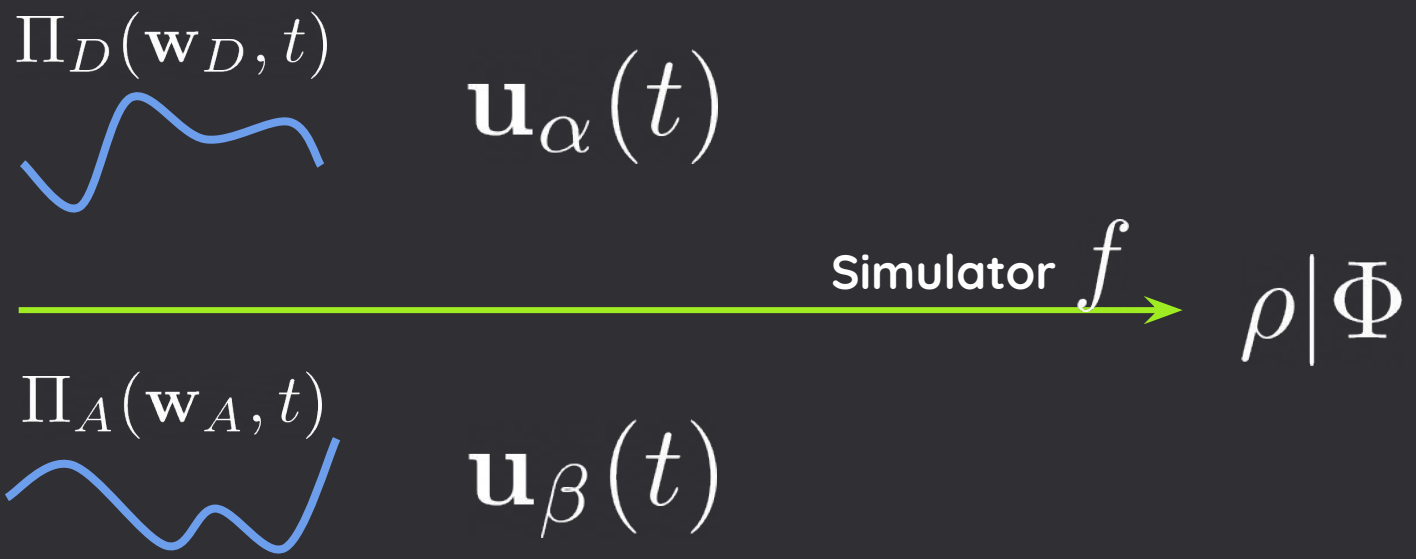
ADVERSARIAL ARCHITECTURE - OUR METHOD

Evaluation



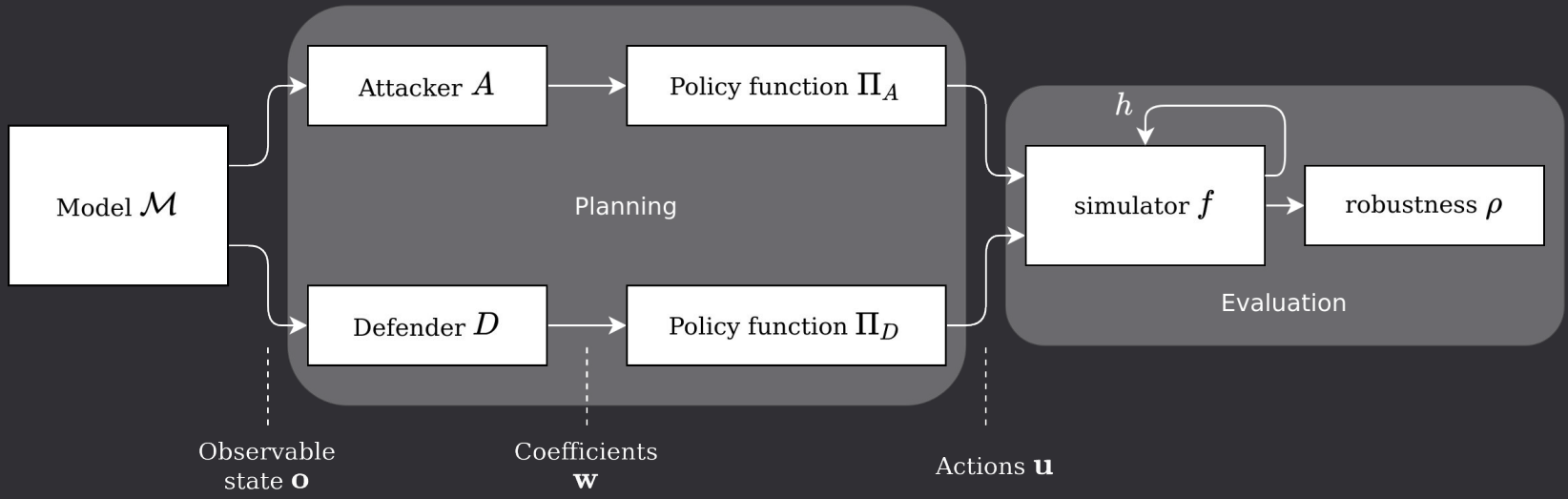
ADVERSARIAL ARCHITECTURE - OUR METHOD

Evaluation



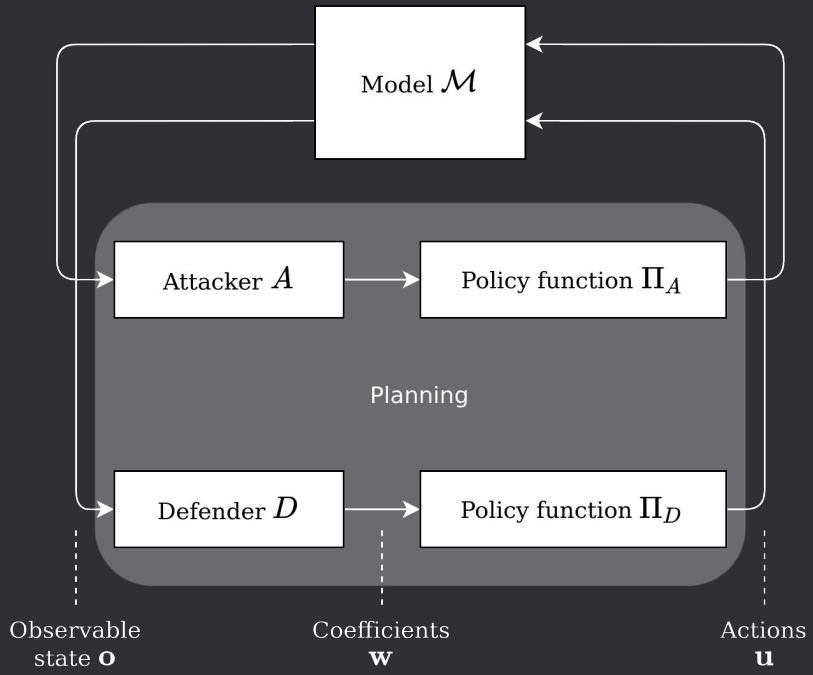
ADVERSARIAL ARCHITECTURE - OUR METHOD

Big picture (for training)



ADVERSARIAL ARCHITECTURE - OUR METHOD

Big picture (for application)



3

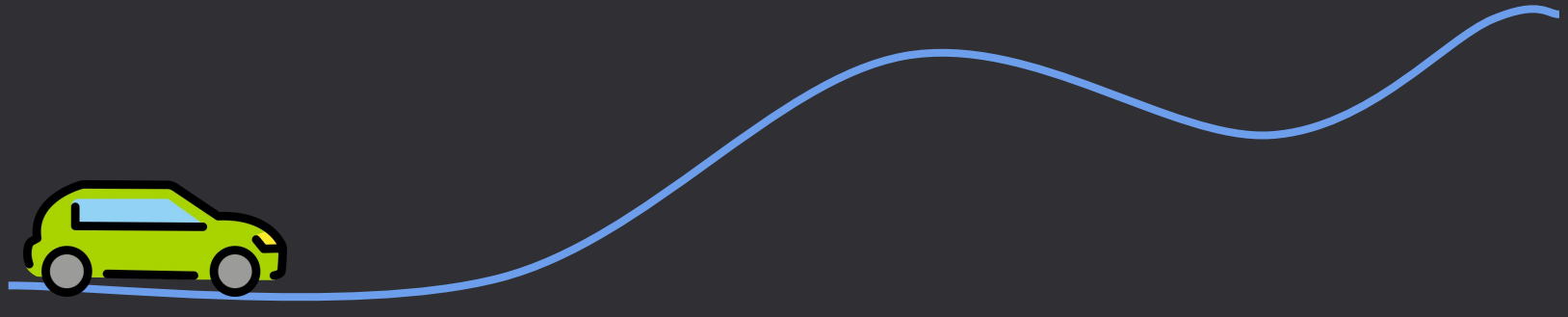
CASE STUDIES

Cruise control and Car platooning

CRUISE CONTROL - CASE STUDIES

CRUISE CONTROL - CASE STUDIES

Keep **always** the same speed.



CRUISE CONTROL - CASE STUDIES

Agent

- The car
- Can control its velocity
- Can measure the steepness
- Cannot steer

CRUISE CONTROL - CASE STUDIES

Agent

- The car
- Can control its velocity
- Can measure the steepness
- Cannot steer

Environment

- The road
- Cannot change
- Cannot have knowledge
- Goes straight

CRUISE CONTROL - CASE STUDIES

Requirement $\Phi = \mathcal{G}(v_c \geq \tilde{v} - \varepsilon \ \wedge \ v_c \leq \tilde{v} + \varepsilon)$

CRUISE CONTROL - CASE STUDIES

Requirement

$$\Phi = \mathcal{G}(v_c \geq \tilde{v} - \varepsilon \ \wedge \ v_c \leq \tilde{v} + \varepsilon)$$

Agent

$$m\frac{dv}{dt} = m\left(\frac{dv}{dt}\right)_{in} - \nu mg\cos\theta_c - mg\sin\theta_c$$

CRUISE CONTROL - CASE STUDIES

Requirement

$$\Phi = \mathcal{G}(v_c \geq \tilde{v} - \varepsilon \ \wedge \ v_c \leq \tilde{v} + \varepsilon)$$

Agent

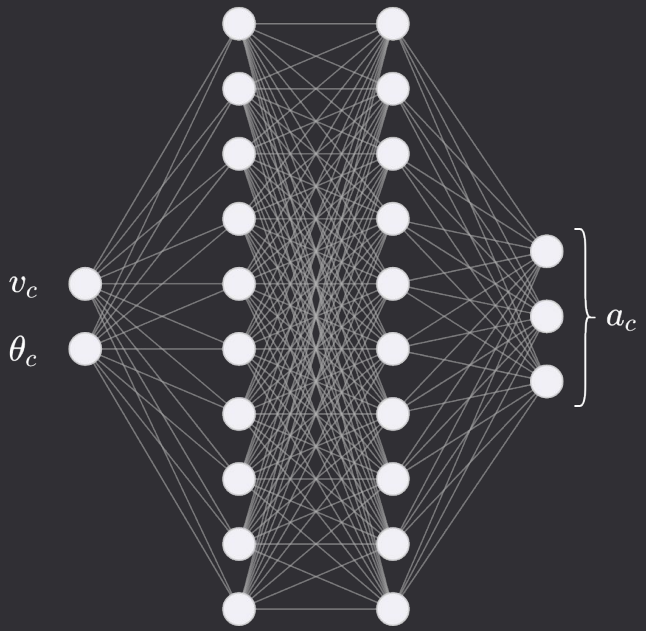
$$m\frac{dv}{dt} = m\left(\frac{dv}{dt}\right)_{in} - \nu mg\cos\theta_c - mg\sin\theta_c$$

Environment

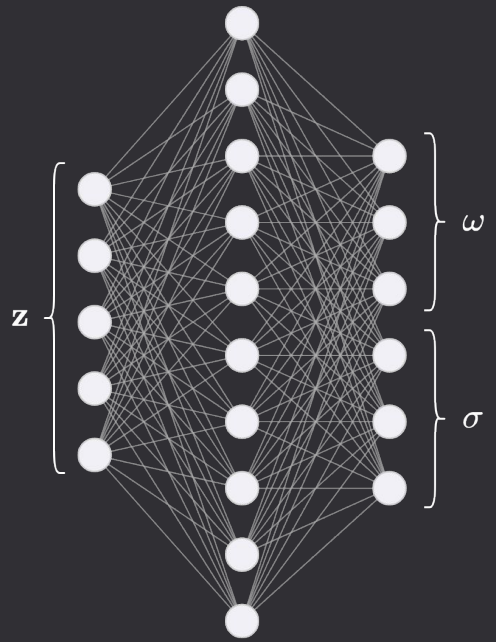
$$r(x) = \sum_{i}^{d} \omega_i \ \exp\left(-\frac{||x - \mu_i||^2}{\sigma_i^2}\right)$$

CRUISE CONTROL - CASE STUDIES

Agent NN



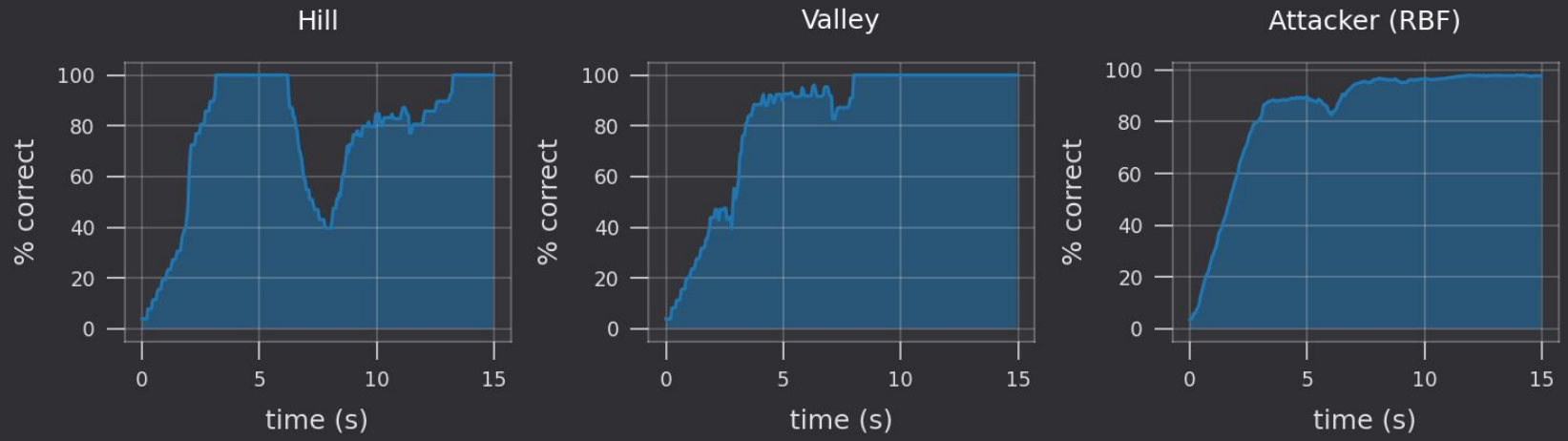
Environment NN



CRUISE CONTROL RESULTS - CASE STUDIES

Percentage of correctness over time

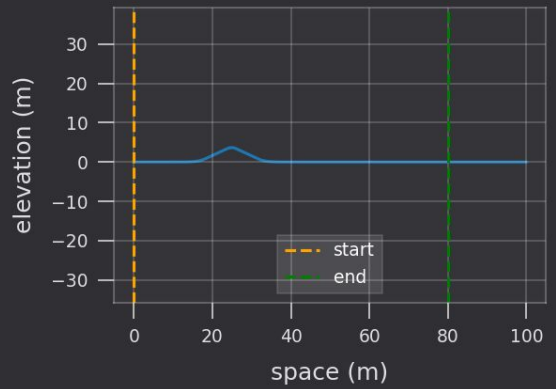
10k simulations



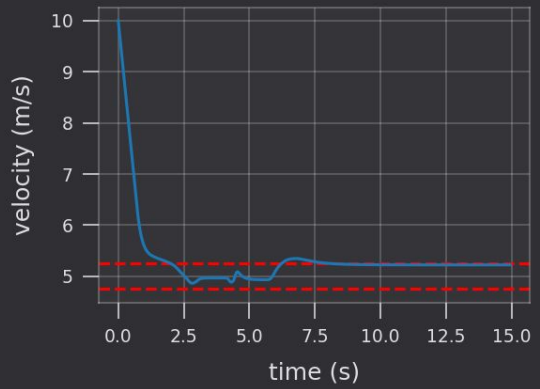
CRUISE CONTROL RESULTS - CASE STUDIES

Hill test

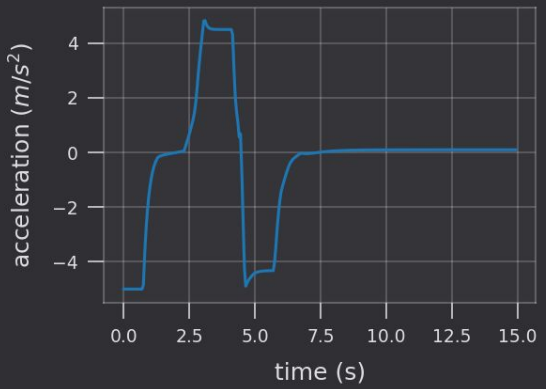
Profile of the road



Velocity



Acceleration

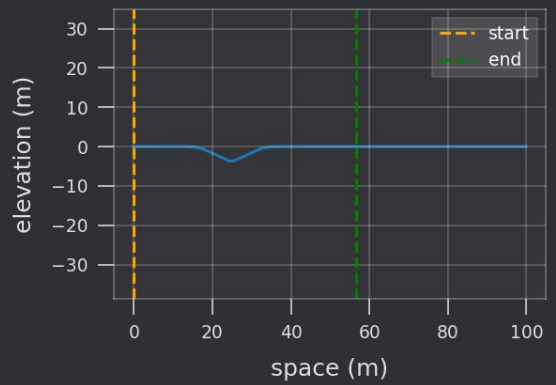


Initial velocity: **11.98 m/s**

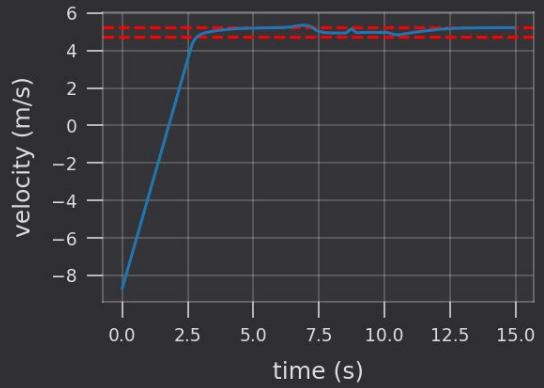
CRUISE CONTROL RESULTS - CASE STUDIES

Valley test

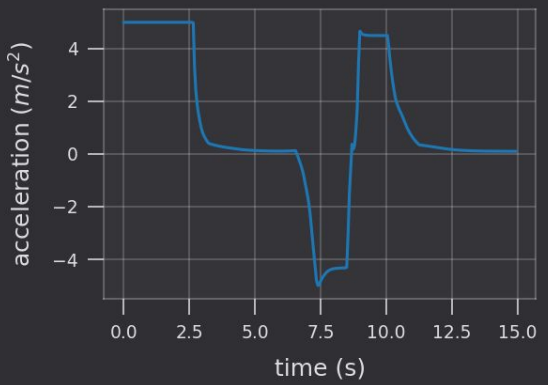
Profile of the road



Velocity



Acceleration

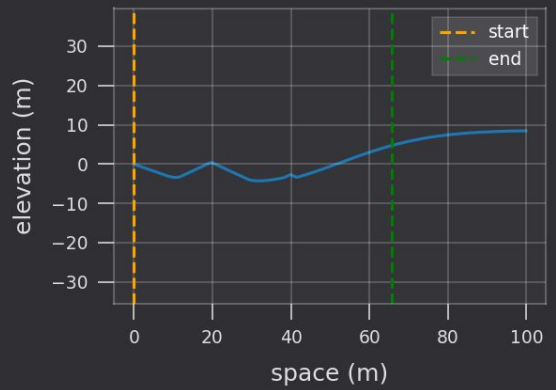


Initial velocity: **-8.94 m/s**

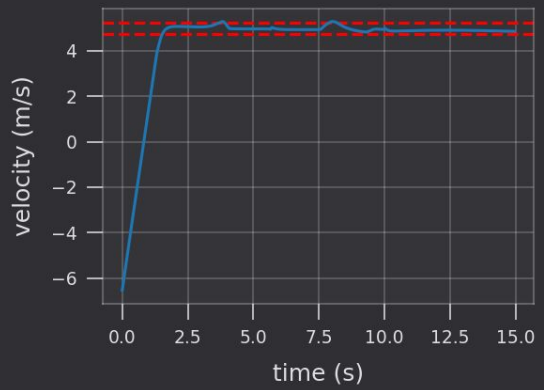
CRUISE CONTROL RESULTS - CASE STUDIES

Attacker test

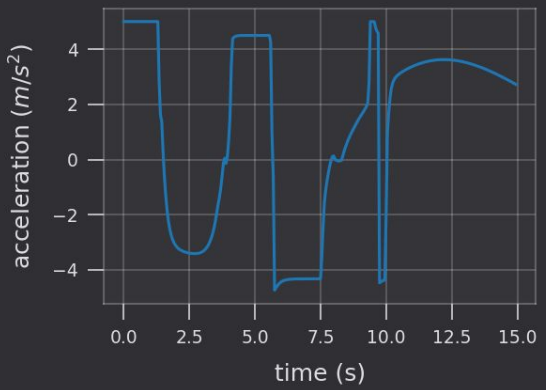
Profile of the road



Velocity



Acceleration

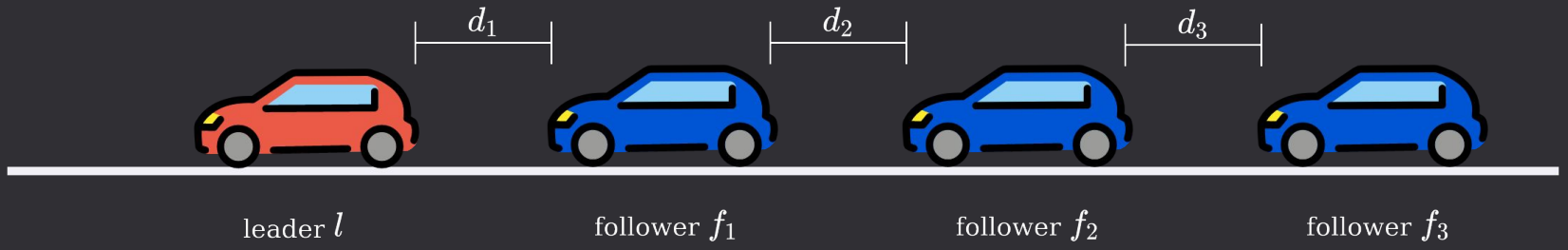


Initial velocity: **-6.93 m/s**

CAR PLATOONING - CASE STUDIES

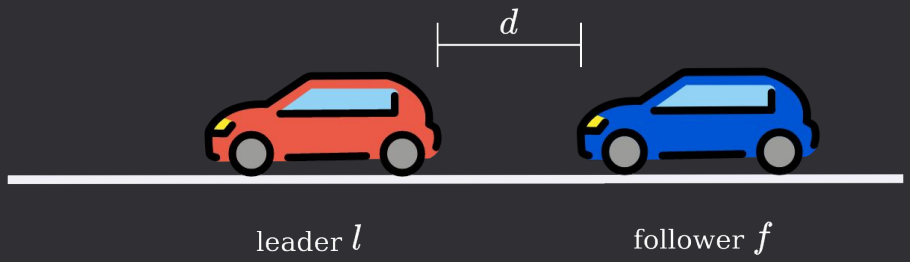
CAR PLATOONING - CASE STUDIES

Keep **always** the distance within the safety range.



CAR PLATOONING - CASE STUDIES

Keep **always** the distance within the safety range.



Divide et impera

CAR PLATOONING - CASE STUDIES

Agent

- The follower
- Can control its velocity
- Can measure the distance
- Knows the other’s velocity
- Goes only forward

Environment

- The leader
- Can control its velocity
- Can measure the distance
- Knows the other’s velocity
- Goes only forward

CAR PLATOONING - CASE STUDIES

- **Requirement** $\Phi = \mathcal{G}(d \leq d_{max} \ \wedge \ d \geq d_{min})$
- **Agent**
- **Environment**

CAR PLATOONING - CASE STUDIES

Requirement

$$\Phi = \mathcal{G}(d \leq d_{max} \ \wedge \ d \geq d_{min})$$

Agent

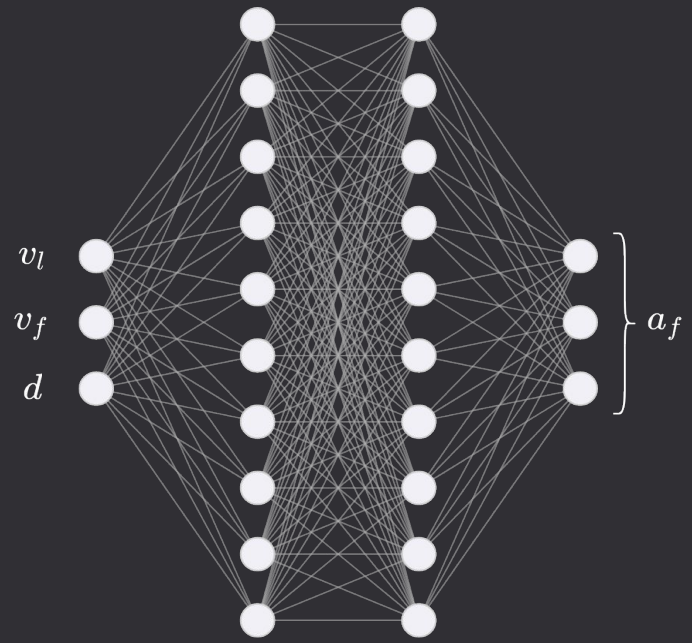
$$m\frac{dv}{dt} = m\left(\frac{dv}{dt}\right)_{in} - \nu mg$$

Environment

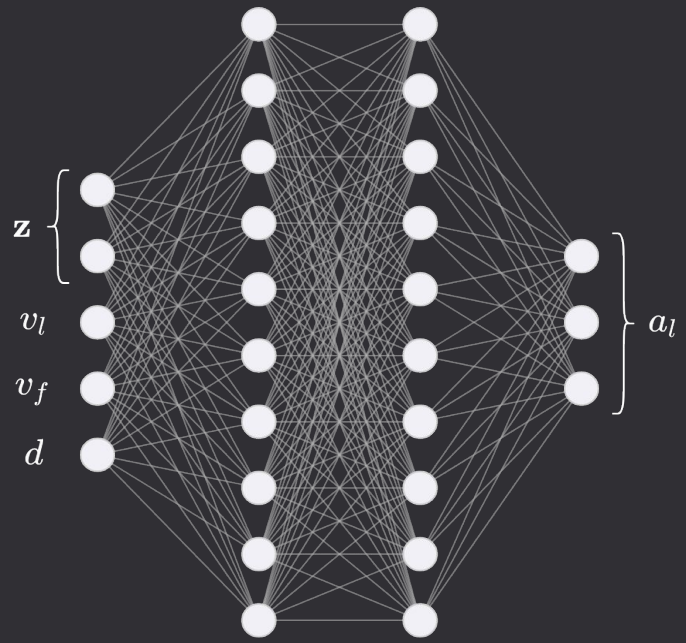
$$m\frac{dv}{dt} = m\left(\frac{dv}{dt}\right)_{in} - \nu mg$$

CAR PLATOONING - CASE STUDIES

Agent NN



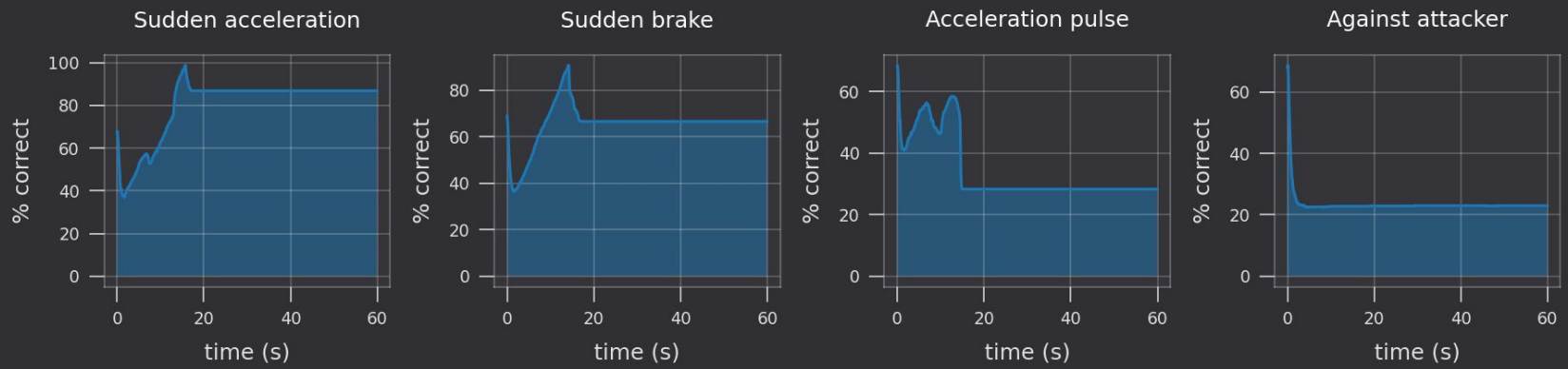
Environment NN



CAR PLATOONING RESULTS - CASE STUDIES

Percentage of correctness over time

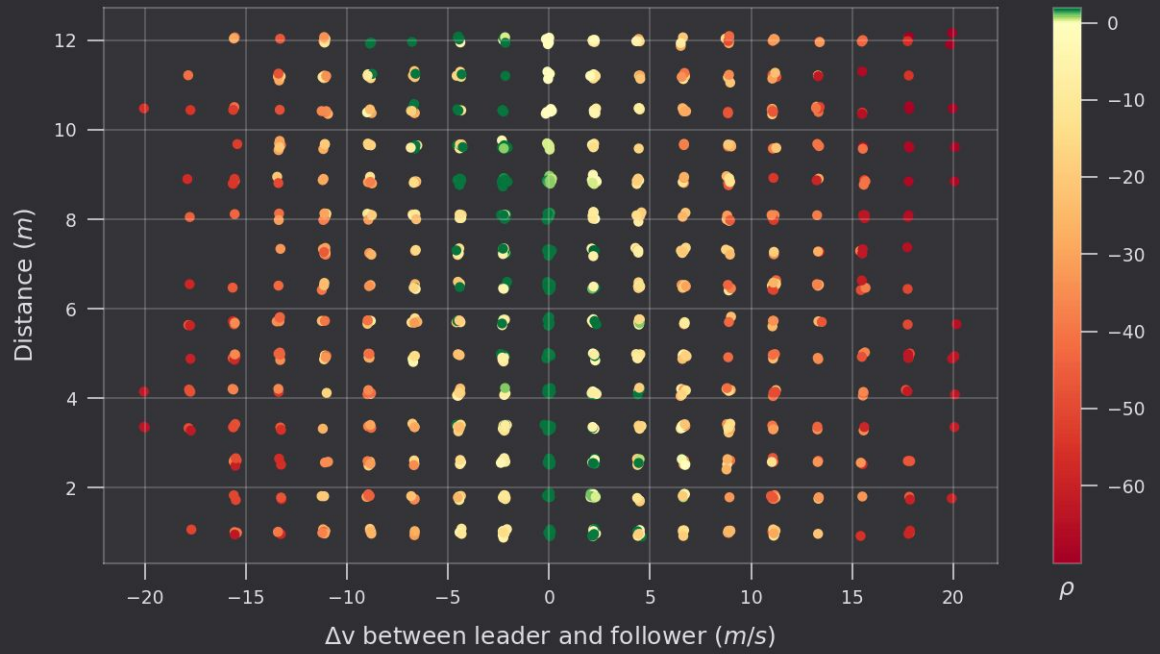
10k simulations



CAR PLATOONING RESULTS - CASE STUDIES

Initial conditions **vs** robustness, against **attacker**

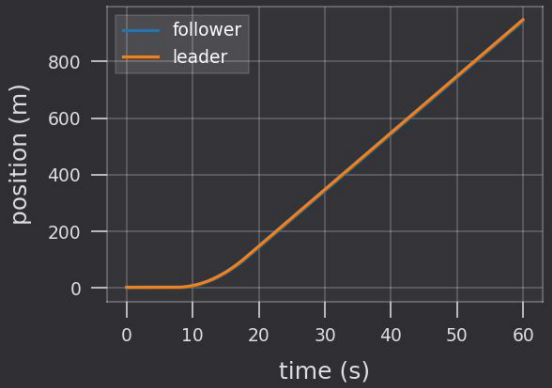
10k simulations



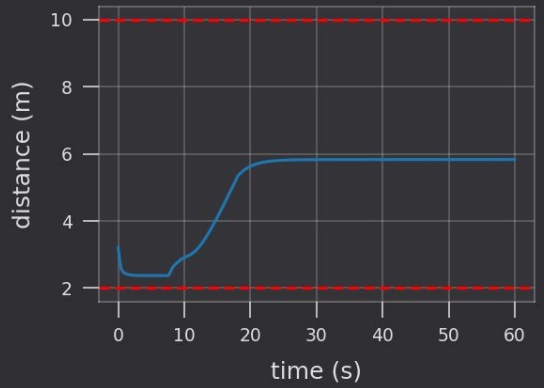
CAR PLATOONING RESULTS - CASE STUDIES

Sudden acceleration test

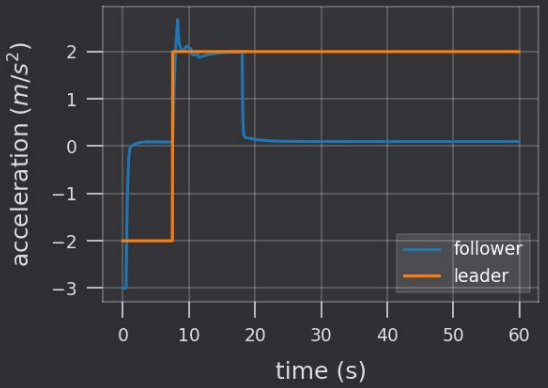
Position



Velocity



Acceleration



Leader's initial velocity: **-0.03 m/s**

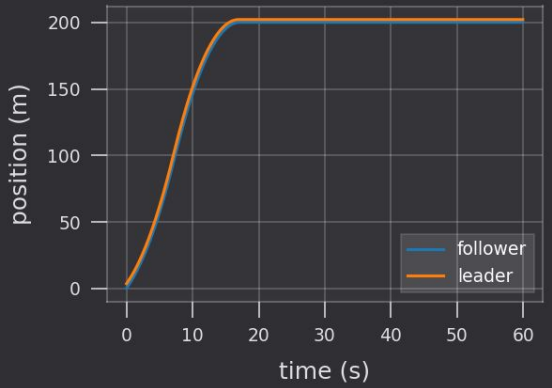
Initial distance: **3.31 m**

Follower's initial velocity: **2.30 m/s**

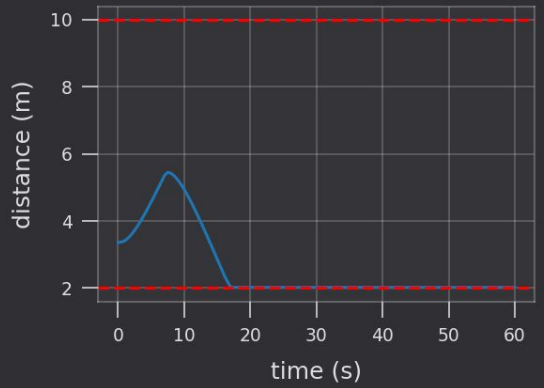
CAR PLATOONING RESULTS - CASE STUDIES

Sudden brake test

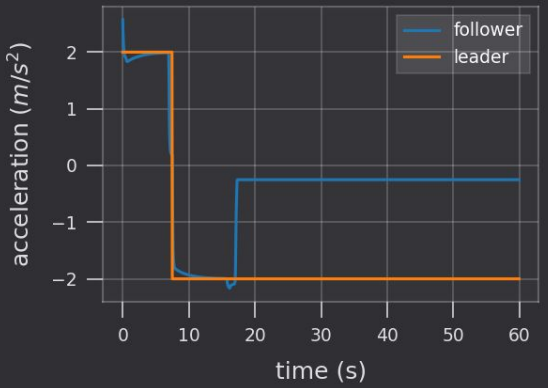
Position



Velocity



Acceleration



Leader's initial velocity: **6.72 m/s**

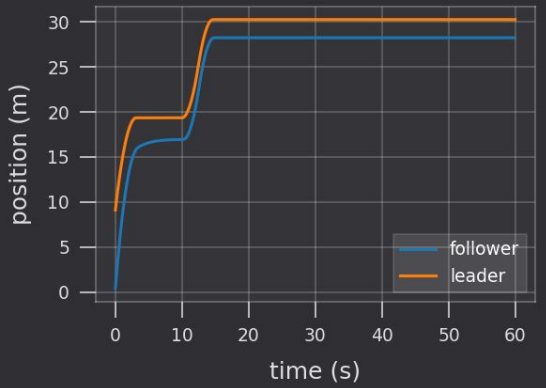
Initial distance: **3.35 m**

Follower's initial velocity: **6.65 m/s**

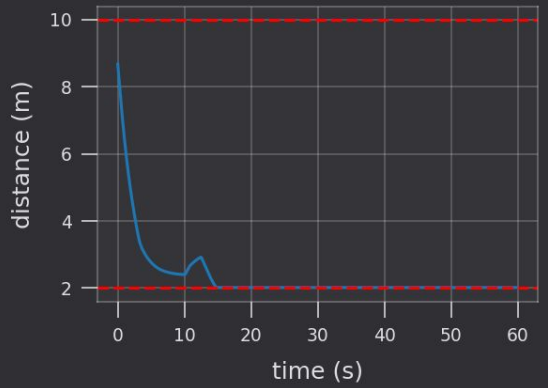
CAR PLATOONING RESULTS - CASE STUDIES

Acceleration pulse test

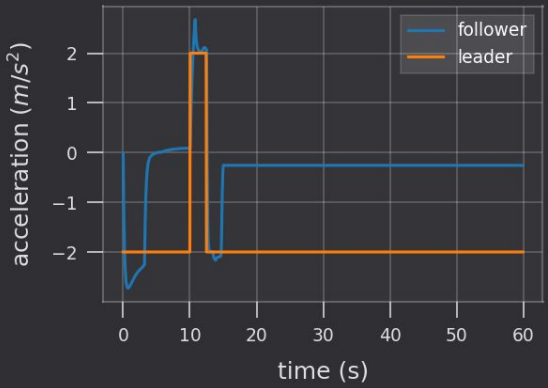
Position



Velocity



Acceleration



Leader's initial velocity: **6.70 m/s**

Initial distance: **8.78 m**

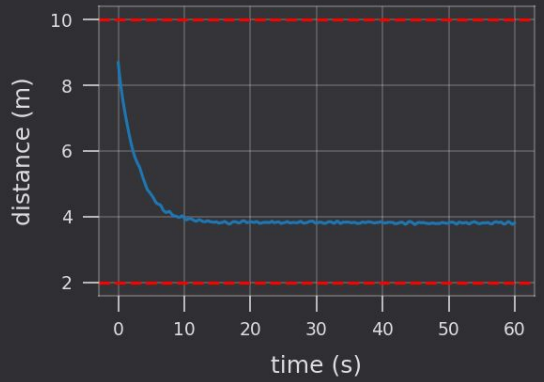
Follower's initial velocity: **8.90 m/s**

CAR PLATOONING RESULTS - CASE STUDIES

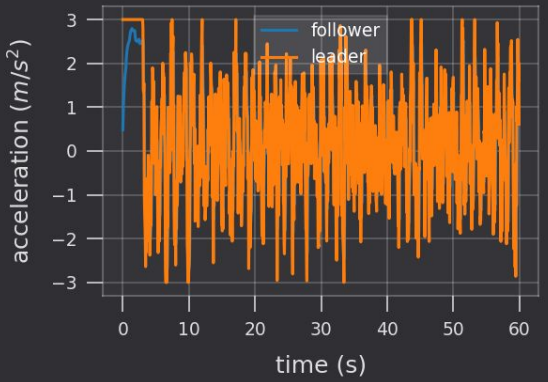
Attacker test

Position

Velocity



Acceleration



Leader's initial velocity: **11.98 m/s**

Initial distance: **11.98 m**

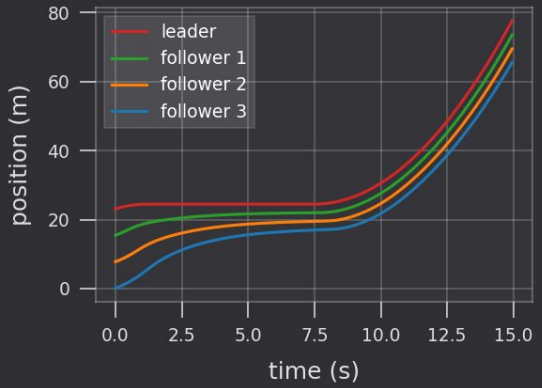
Follower's initial velocity: **11.98 m/s**

CAR PLATOONING RESULTS - CASE STUDIES

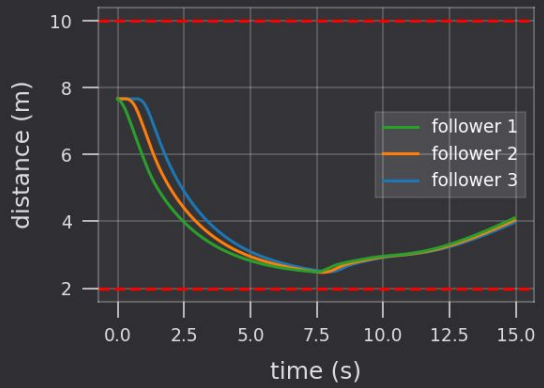
Sudden acceleration test

3 followers

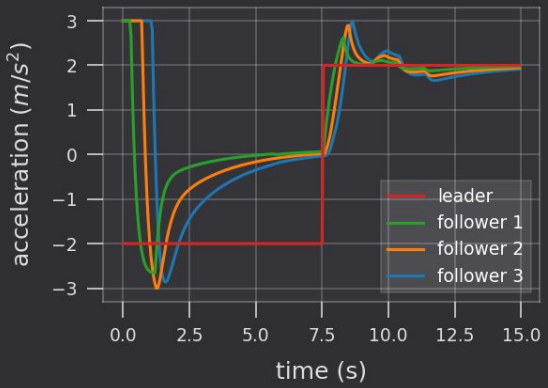
Position



Velocity



Acceleration



Initial distance: **7.66 m**

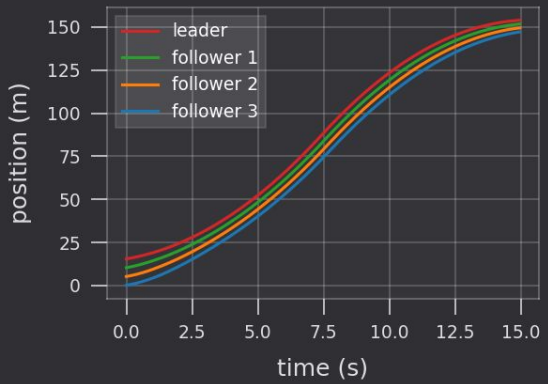
Initial velocity: **2.53 m/s**

CAR PLATOONING RESULTS - CASE STUDIES

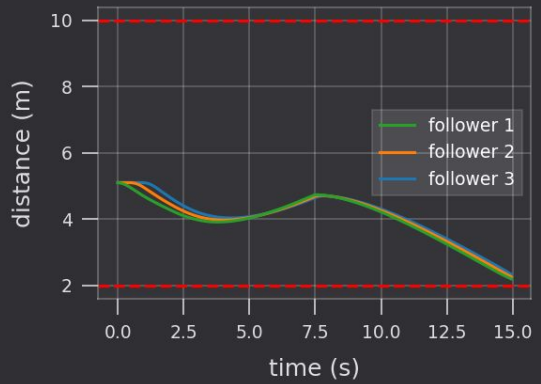
Sudden brake test

3 followers

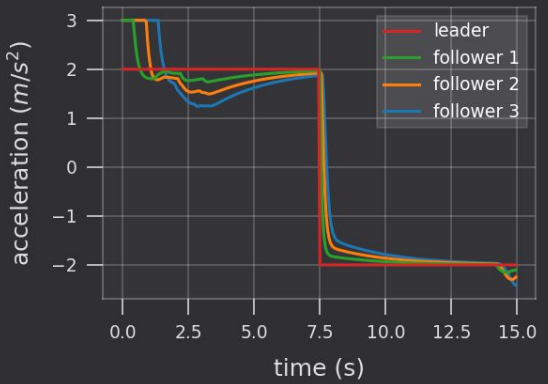
Position



Velocity



Acceleration



Initial distance: **5.09 m**

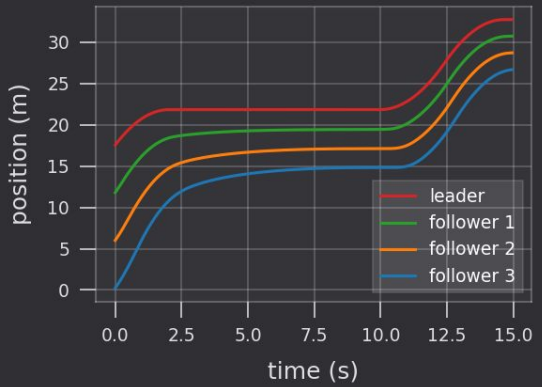
Initial velocity: **2.48 m/s**

CAR PLATOONING RESULTS - CASE STUDIES

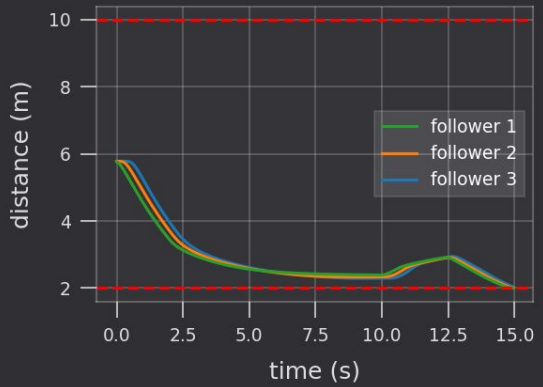
Acceleration pulse test

3 followers

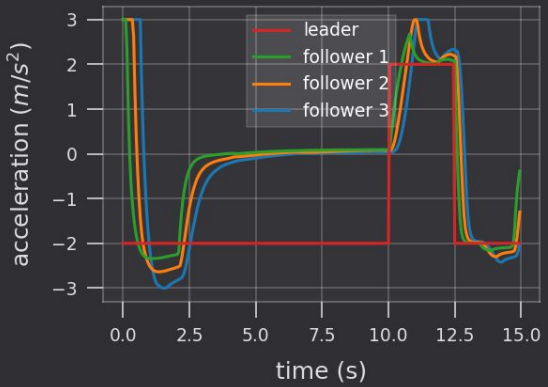
Position



Velocity



Acceleration



Initial distance: **5.77 m**

Initial velocity: **4.39 m/s**

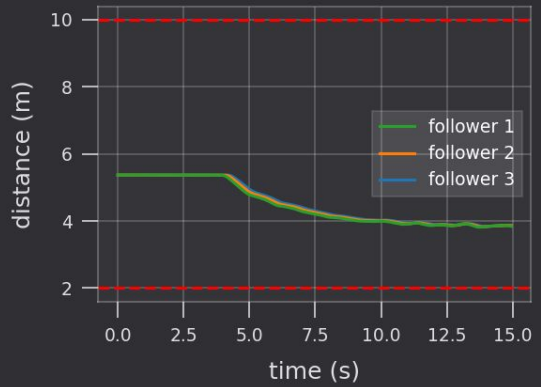
CAR PLATOONING RESULTS - CASE STUDIES

Attacker test

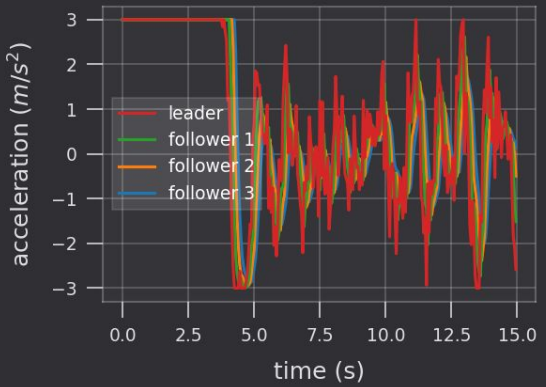
3 followers

Position

Velocity



Acceleration



Initial distance: **5.36 m**

Initial velocity: **2.19 m/s**

4

CONCLUSION

Recap and future work

RECAP - CONCLUSION

We developed a method that

- Makes use of adversarial training in a new way
- Makes use of episodes instead of a training set
- Trains a performant and safe controller
- Produces interesting results

We developed a framework ready to be applied to new models.

FUTURE WORK - CONCLUSION

Possible developments

- Faster training using *mini-batches*
- Approximation of non-differentiable models
- Optimized sampling of the initial conditions

Thanks!

Coming soon on GitHub...