ATMoS: A Framework for Reinforcement Learning based Autonomous Threat Mitigation using Software Defined Networks

UNIVERSITY OF WATERLOO

ezSec Inc. RBC Royal Bank NSERC CRSNG Google

Ezzeldin Tahoun, Iman Akbari, Mohammad A. Salahuddin, Noura Limam, Raouf Boutaba | Computer Science University of Waterloo

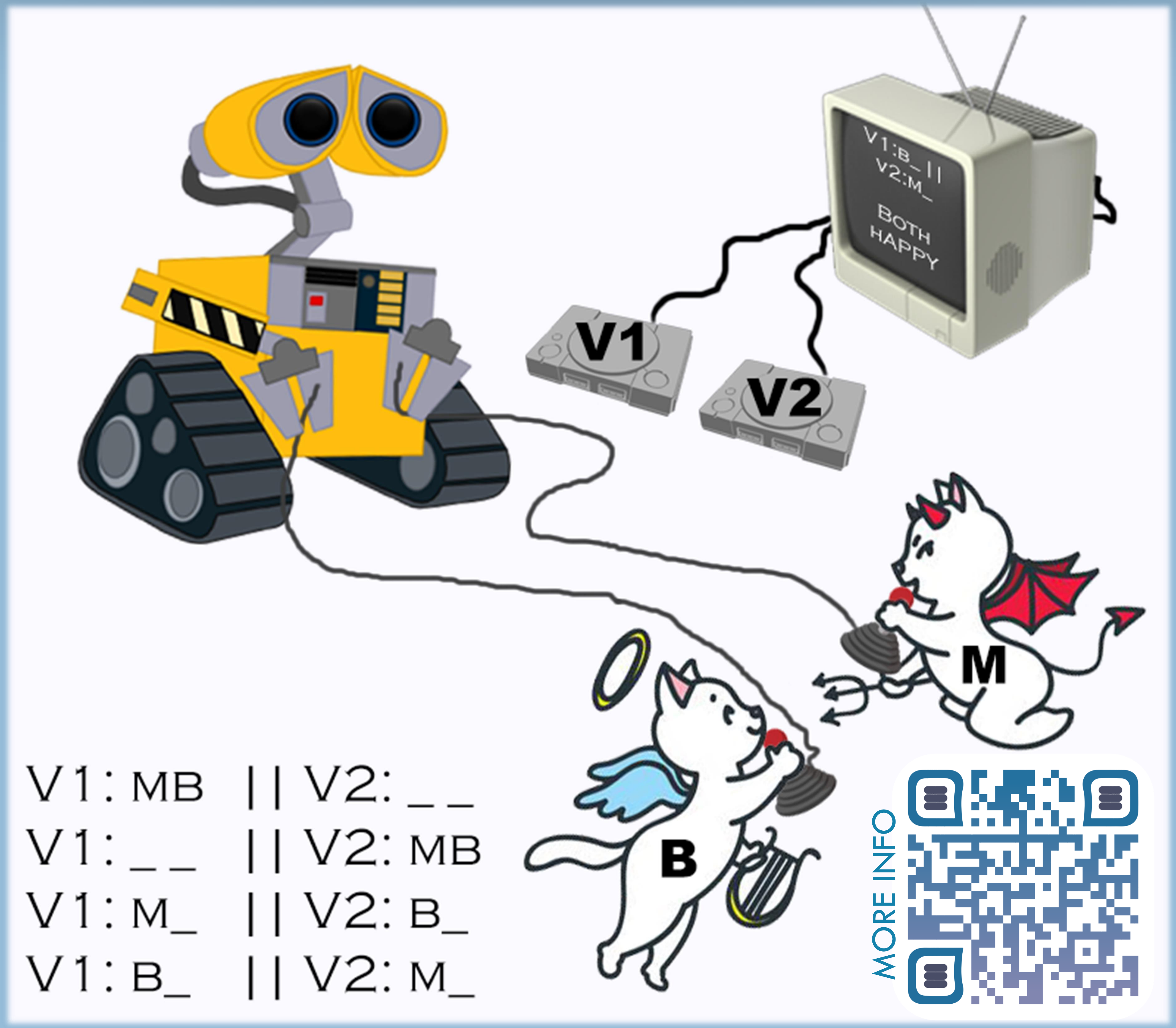
INTRO AND MOTIVATION

- Cyber Attacks are getting more complex. Researchers in the field have used over simplified threat vectors. Advanced Persistent Threats, for instance, act benign most of the time to evade detection. We believe there is a need to address more complicated threat vectors.
- More complicated threat vectors need tighter security, which leads to less convenience for benign users. This is known as the security-convenience tradeoff. We believe only malicious nodes should be subjected to stricter rules.
- SDN allows global view and programmable control over the network. We believe SDN can act as an enabler for a method where finer granularity in applying rules exists.
- Simulating benign or malicious behaviors is an interesting approach as more accurate predictions may be fine-tuned to each individual user profile, and updated over time (based on recorded behavior) via techniques such as model tracing and dynamic parameter fitting.
- RL allows us to tackle sequential decision making in real time. We believe RL is appropriate for a complex problem like detecting a stealthy APT.
- We acknowledge the fact that it is hard for researchers to get all the IT architecture and modules together. We have designed a framework and implemented it in widely used and open source tools. A researcher now can use ATMoS to rapidly design and test RL apps for network security, accelerating the field.

IMPLEMENTATION & EVALUATION

We showcase the framework's ease of use by writing a Neural Fitted Q-learning (NFQ) agent talking to the simple Open AI GYM interface exposed by ATMoS to mitigate an Advanced Persistent Threat using virtual networks with different security levels.

It converges quickly: kicking the malicious host to a high security VN and benign hosts to low security VN with more bandwidth. Detecting APT's tricky behavior, mitigating the threat, and maintaining a reliable fast connection for others.



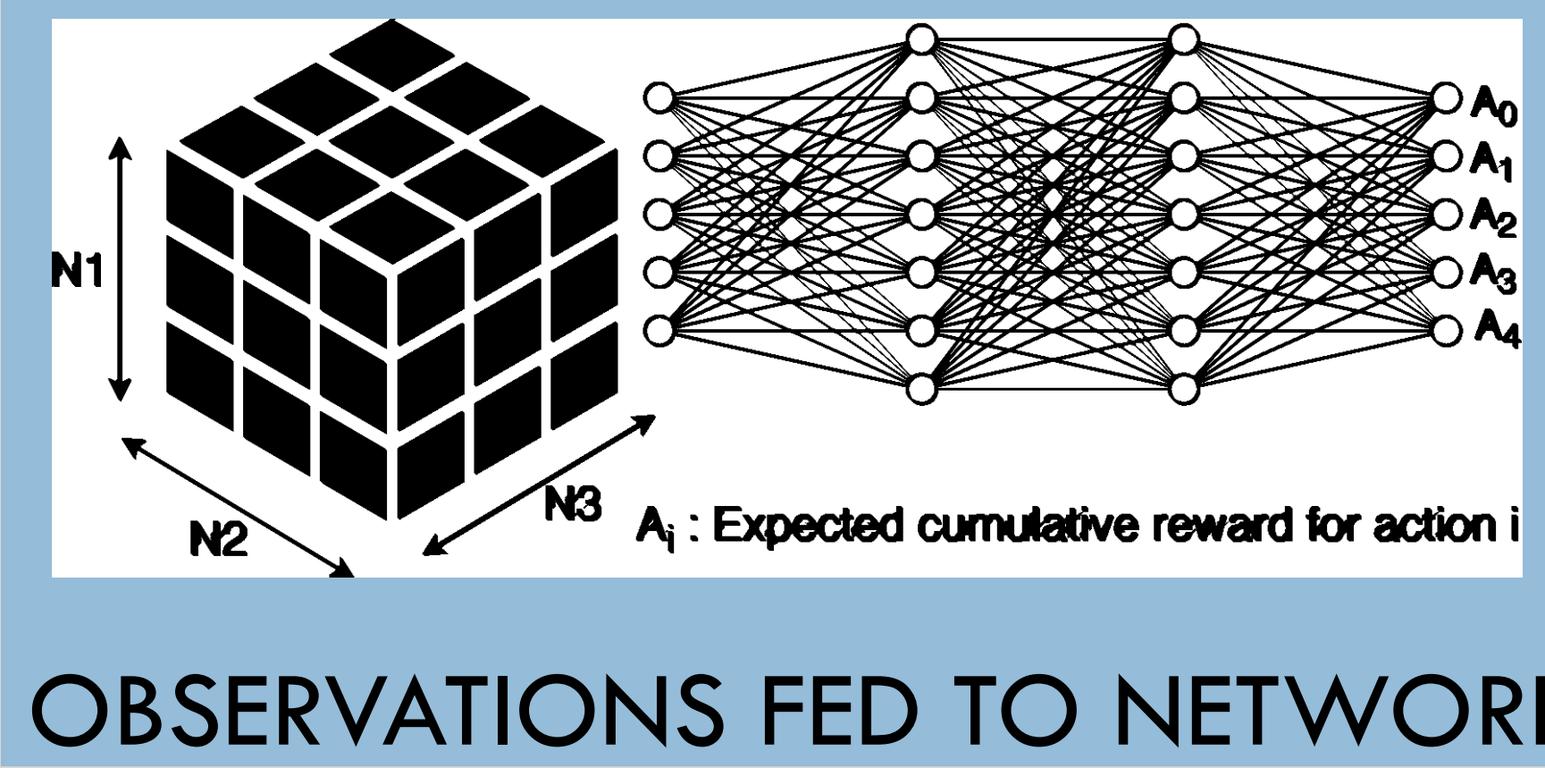
TensorFlow

OpenAI

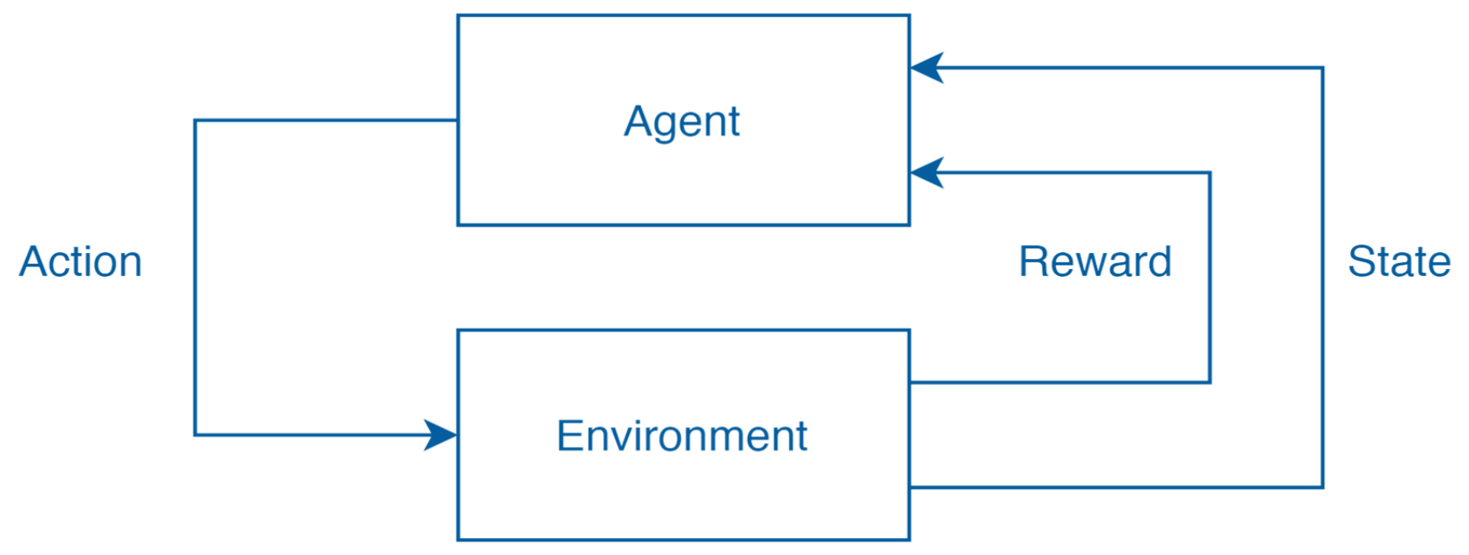
docker

OPEN DAYLIGHT

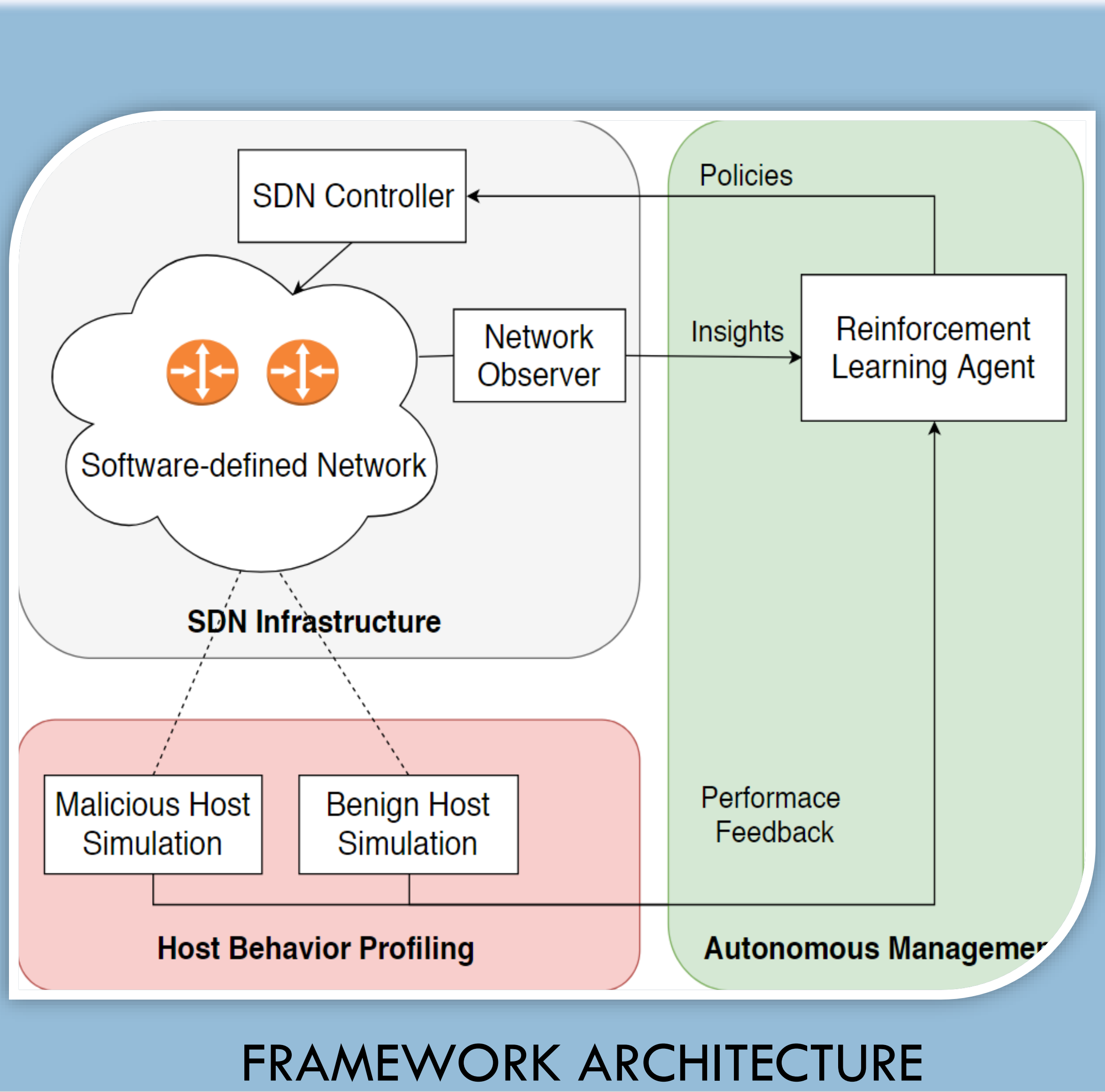
Open vSwitch



OBSERVATIONS FED TO NETWORK



STANDARD RL MODEL



FRAMEWORK ARCHITECTURE

RL DECISION MAKING

HOW TO USE RL FOR NETWORK SECURITY:

sh Install_ATMoS.sh (can run on Docker, Mininet, or Cloud)

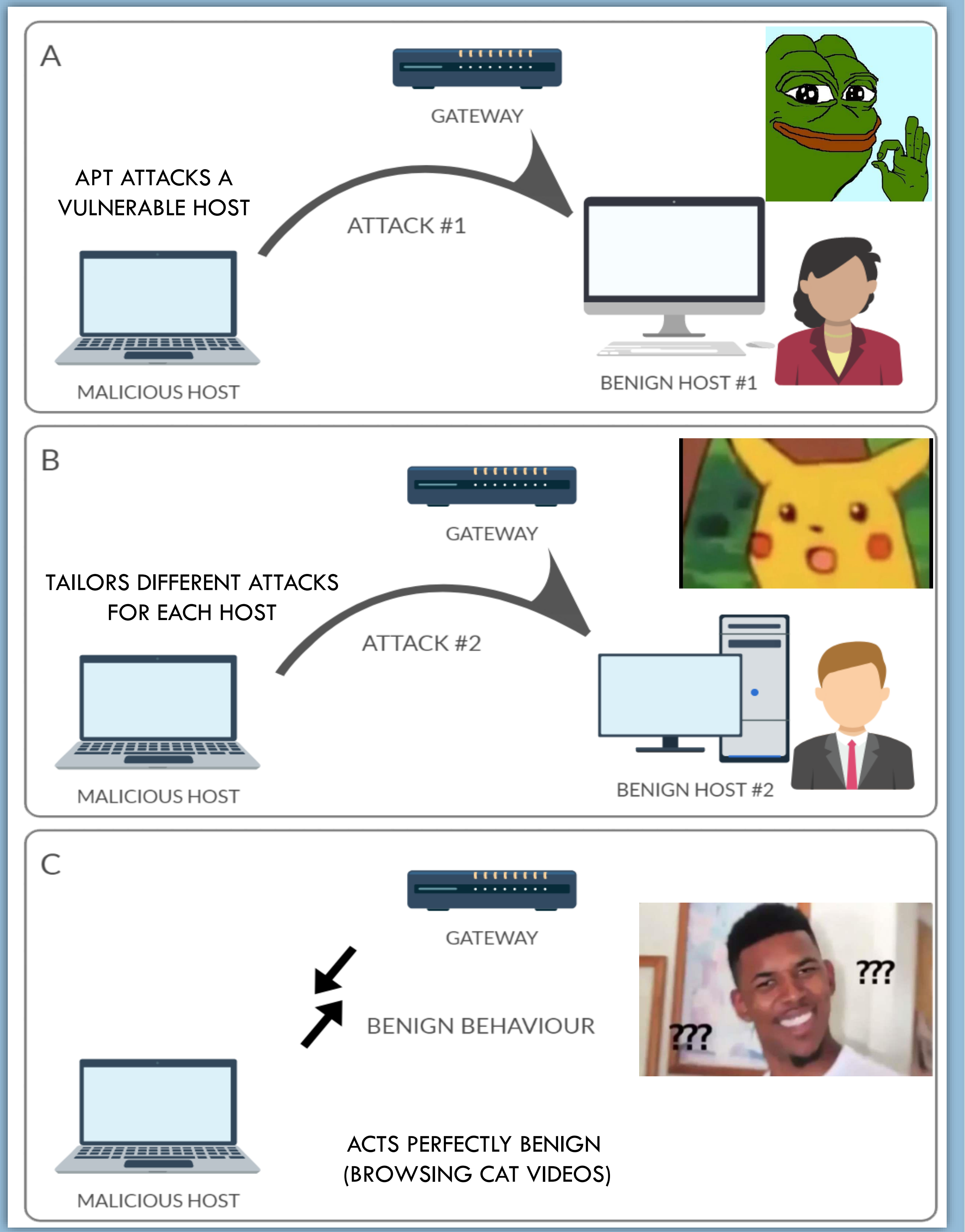
Import ATMoS as environment

Write your RL algorithm so that it interacts with abstract environment functions

Tweak your high level logic to perfection

Give yourself a pat on the back. You slashed your development time and cost and your work is extremely reproducible since ATMoS uses industry grade tools.

BONUS: You can always expand functions using API and OPEN AI GYM – Its Opensource!



APT BEHAVIOUR