AI-BASED ATTACK RESPONSE AND PROGRAMMABILITY OF FUTURE NETWORKS

Authors

Shurok Khozam
IMT/Télécom SudParis
Institut Polytechnique de Paris

Gregory Blanc
IMT/Télécom SudParis
Institut Polytechnique de Paris.

Eric Totel
IMT/Télécom SudParis
Institut Polytechnique de Paris.

Sébastien Tixeuil
Sorbonne Université

Partner

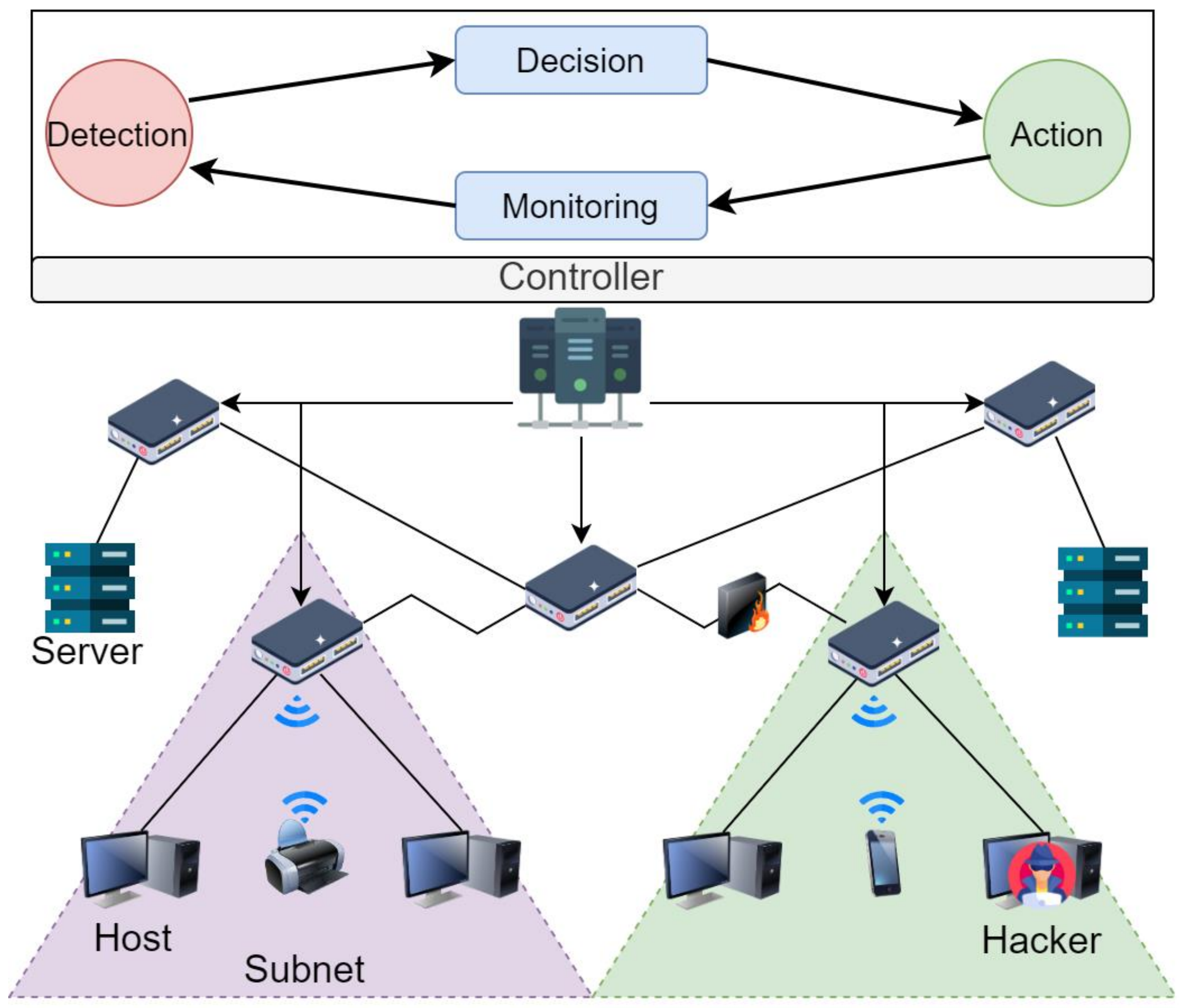
SORBONNE UNIVERSITÉ

Funding

GRIFIN Project

OBJECTIVES

- **5G** is the latest generation of mobile communication, it also adopted **Network Function Virtualization** beside other different characteristics (like fast response time, low latency, wider bandwidth, etc.) which **favor 5G** over all other generations.
- Today's networks are **increasing sharply** in size as well as in functionality, especially with the growth of Internet Of Things, which gave rise to numerous challenges.
- Nowadays, **attackers are developing diverse techniques** to exploit vulnerable gaps through the network.
- It became mandatory to define **appropriate countermeasures** in order to defend different attack types.
- In this thesis, we aim to **support remediation selection** to maximize the response efficiency while reducing adverse impact to the network.
- As well as to **automate remediation deployment** to reduce manual and error-prone incident handling and down time.

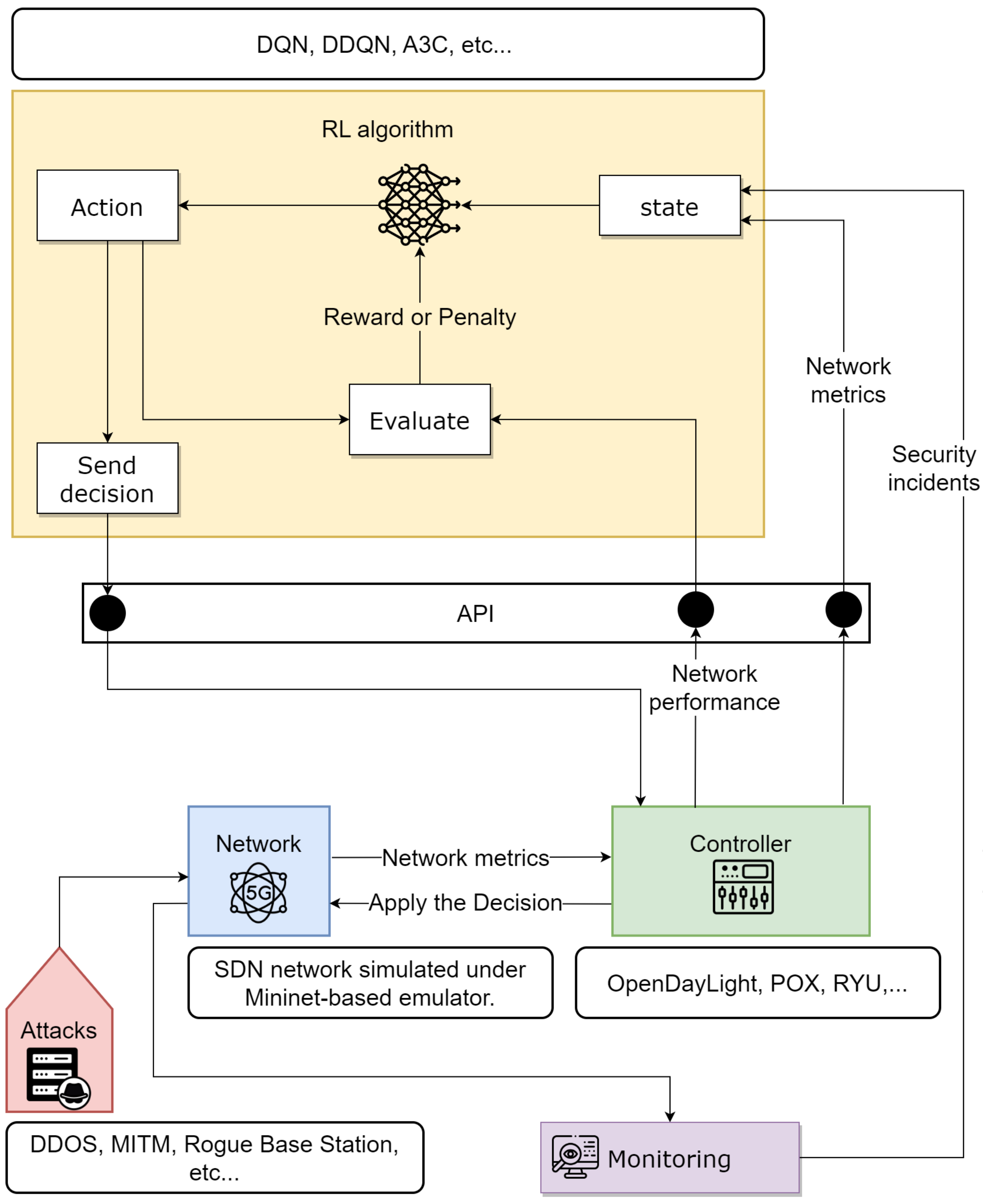


APPROACH

- We are considering a **Software Defined Network (SDN)** as it is the backbone of 5G networks.
- We are **generating general attack types** like DDOS, MITM and Rogue base station attacks.
- We build a **technique dependent on network's state changes** to characterize **type** and **severity** of generated-attacks in each network element and report the result to a **Deep Reinforcement Learning (DRL) agent** by the SDN controller.
- We are **developing a DRL model** which aims at:
  - **Modelling** the state of the network.
  - **Automating** the selection of appropriate countermeasures.
- Actions and countermeasures determined by the agent are translated into **high-level measures** and then mapped into **security configurations**.

REQUIREMENTS

- The **remediation selection** should be:
  - **Automated and optimized** to reduce response time.
  - As specific as possible to precisely mitigate the security incident.
  - **Aware of the network state** to reduce adverse impacts.
- The **remediation deployment** should be:
  - Automated to prevent human mistakes and to be applied the soonest possible.
  - Connected to remediation selection to enforce **resilience**.
  - Auditable, verifiable and explainable to be **trustworthy**.



Samovar PhD day

March 2023

Contact shurok.khozam@telecom-sudparis.eu

anr-grifin.telecom-sudparis.eu