AI-BASED ATTACK RESPONSE AND PROGRAMMABILITY OF FUTURE NETWORKS

PRESENTED BY:
SHUROK KHOZAM

INTRODUCTION

The subject of this thesis:

Creating **AI-based defense mechanism** in order to face **attacks** and take **countermeasures** to protect **5G networks**.

Why is it important?

OBJECTIVES

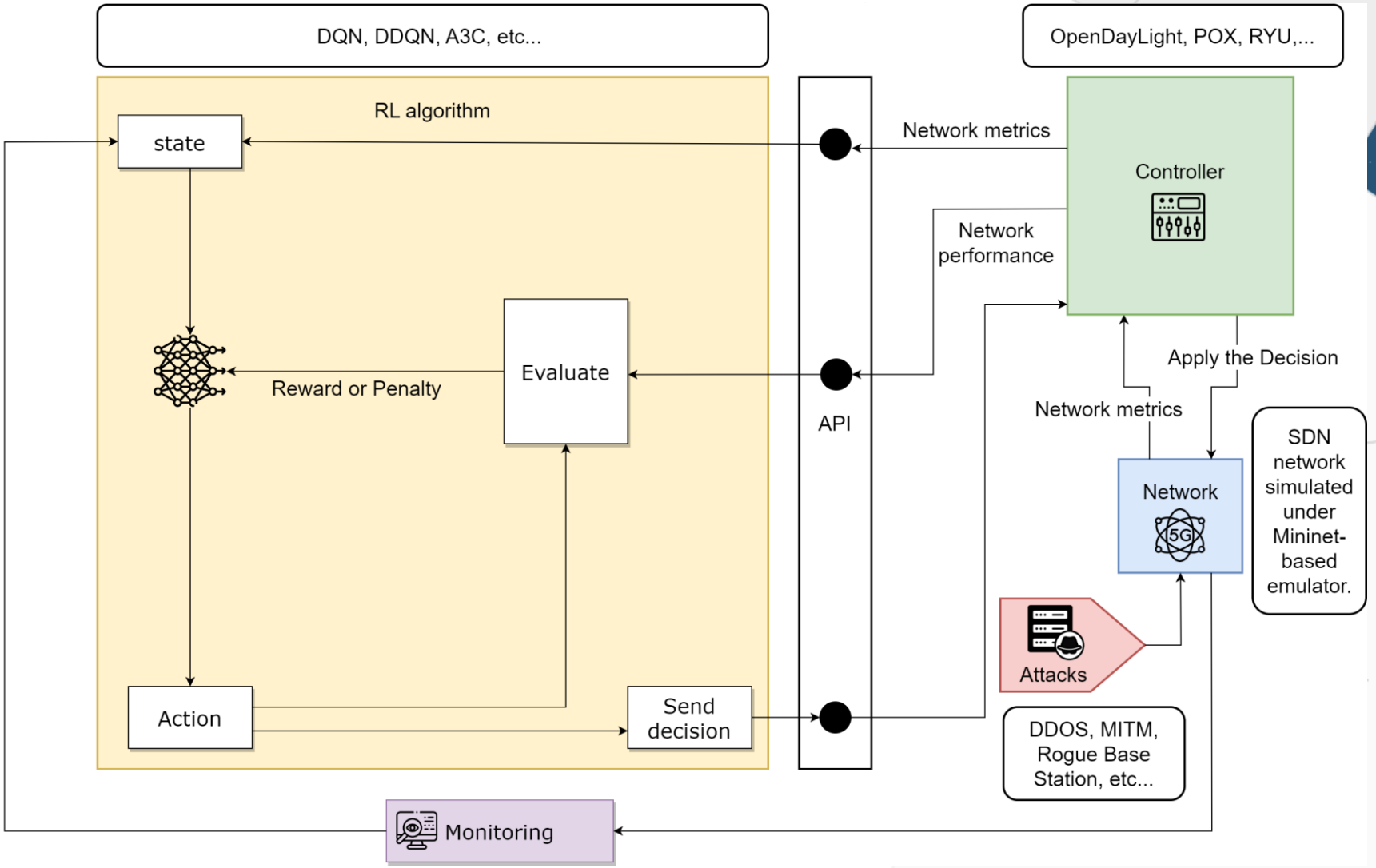
1. Support **remediation selection** to **maximize the response efficiency** while **reducing adverse impact** to the network.

2. **Automate remediation deployment** to **reduce manual** and **error-prone incident handling** and down time.

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.
  - Enforce network **resilience**.
  - **Auditable**, **verifiable** and **explainable** to be **trustworthy**.

APPROACH


DQN, DDQN, A3C, etc...
OpenDayLight, POX, RYU,...
RL algorithm
state
Network metrics
Controller
Network performance
Evaluate
Reward or Penalty
API
Apply the Decision
Network metrics
SDN network simulated under Mininet-based emulator.
Network
5G
Attacks
Action
Send decision
DDOS, MITM, Rogue Base Station, etc...
Monitoring

Thanks for listening!