SAND2021-8316D

The Center for Cyber Defenders

Expanding computer security knowledge

RELACCS: Reinforcement Learning for Cybersecurity

Abel Gomez

Mentor: Srideep Musuvathy

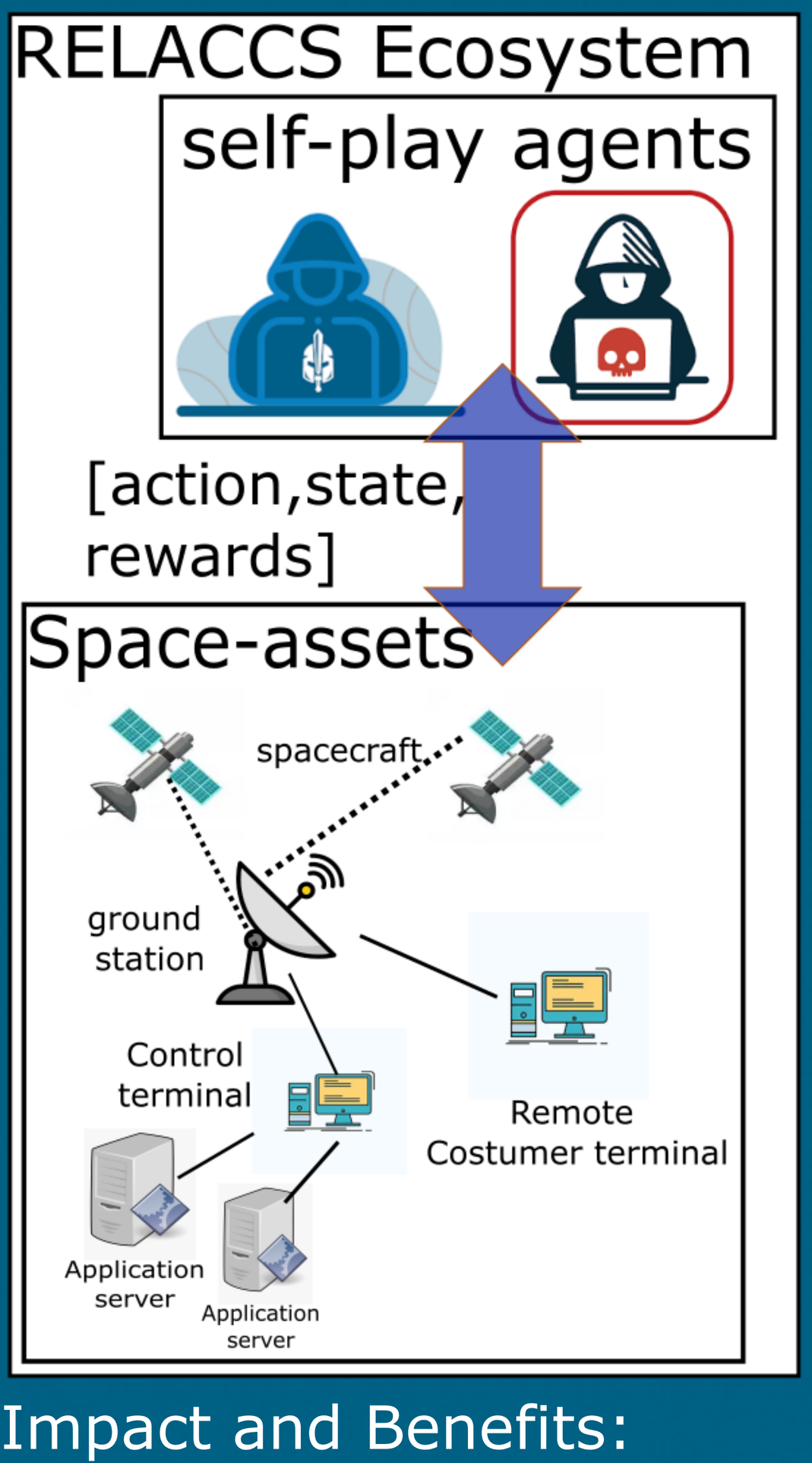
- Problem Statement:
  - Security strategy has traditionally been defined, implemented, and updated by **domain experts**[1]
  - Ground-stations (GS) are becoming more **complex** and **open**
  - **Security** cycle **updates** become shorter and change faster
- Idea:
  - Reinforcement Learning (**RL**)
  - Markov Games
  - **Self-play agents**[2]
- Actions:
  - Access policies
  - Close ports
- Rewards
  - Prevent cyber attacks

Defender

- Actions (attacks):
  - Scan port
  - ssh, curl, cd, find
- Rewards
  - Spacecraft access
  - User credentials

Attacker

- Objectives and Approach:
  - **Protect** the **space assets**, missions, and data
  - High-fidelity model of **ground-stations**



- Impact and Benefits:
  - Evaluate GS security **without** the need for constant **experts**.
  - Develop a **domain independent defense strategy**

1. Hammar, Kim, and Rolf Stadler. "Finding Effective Security Strategies through Reinforcement Learning and Self-Play." 2020 16th International Conference on Network and Service Management (CNSM). IEEE, 2020.
2. Ghanem, Mohamed C., and Thomas M. Chen. "Reinforcement learning for intelligent penetration testing." 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, 2018.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.