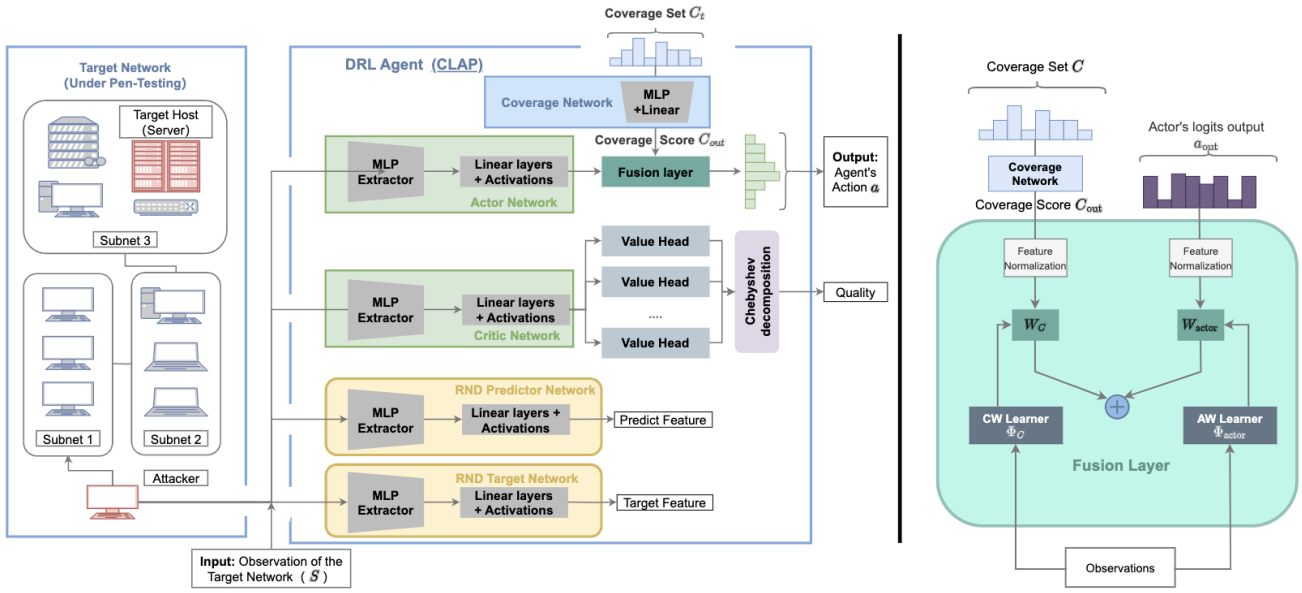
Behaviour-Diverse Automatic Penetration Testing: A Coverage-Based Deep Reinforcement Learning Approach

Yizhou YANG, Longde CHEN, Sha LIU, Lanning WANG, Haohuan FU, Xin LIU, Zuoning CHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-024-3380-1

Problems & Ideas

- Problems of reinforcement learning (RL) enabled automatic pen-testing:
  - The action space exponentially grows with network size, hindering efficient learning for RL agents
  - RL agents tend to learn monotonous attack paths with maximized rewards, limiting the effectiveness of penetration testing
- Ideas: A novel RL agent equipped with a coverage mechanism-based neural network and incorporating a Chebyshev decomposition critic

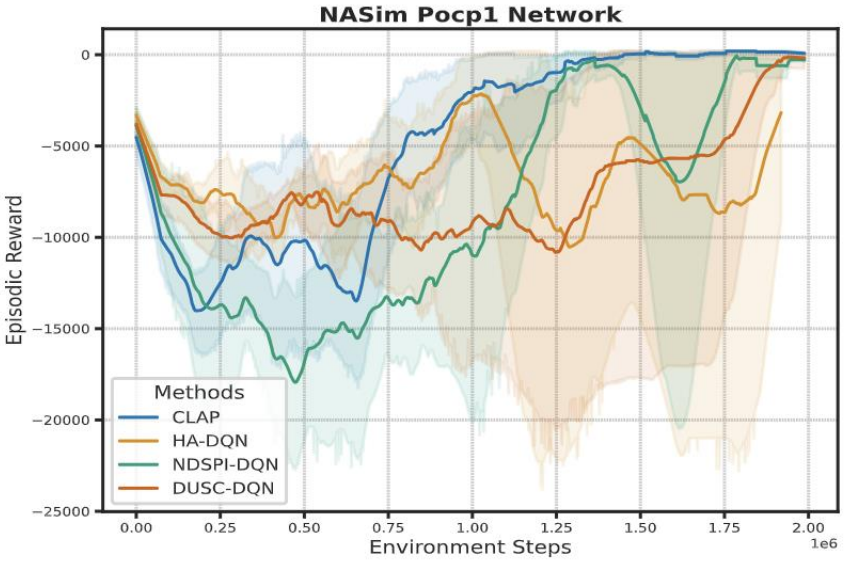


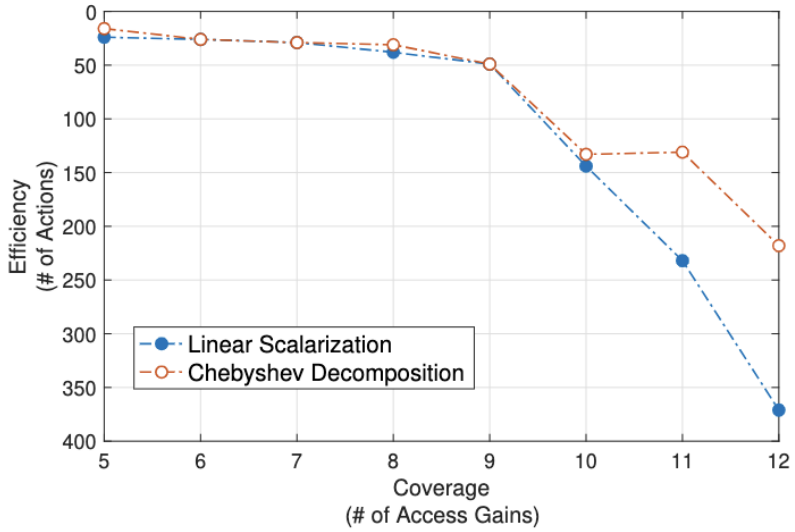
(a) System Architecture (b) Fusion Layer

Architecture of the proposed CLAP agent. The agent's observations are fed through separate MLP extractors to Actor-Critic Network and RND respectively. Different CLAP's Neural Network components are highlighted with coloured boxes. The coverage score is fused with logits output of the actor network.

Main Contributions

- Contributions:
  - A coverage mechanism for efficient penetration testing in large networks, reducing required adversary actions to achieve attack objectives, surpassing current methods
  - Demonstrating through empirical results the method's remarkable scalability, enabling efficient pen-testing of extensive networks with up to 500 hosts
  - A Chebyshev critic enabling the generation of diverse attack strategies that balance exploits and vulnerability assessments





Left: Training performance of different methods in an enterprise-level network scenario; Right: Distribution of attack strategies under multi-objective settings