Zhou TY, Zang YC, Zhu JH, et al., 2019. NIG-AP: a new method for automated penetration testing. *Frontiers of Information Technology & Electronic Engineering*, 20(9):1277-1288. https://doi.org/10.1631/FITEE.1800532

NIG-AP: a new method for automated penetration testing

Key words: Penetration testing; Reinforcement learning; Classical planning; Partially observable Markov decision process

Corresponding author: Yi-chao Zang
E-mail: zangyeechao@sina.com
ORCID: http://orcid.org/0000-0002-1791-586X

Motivation

- Penetration testing has strong advantages in the discovery of hidden vulnerabilities in a network and for assessing network security.
- Existing penetration testing could be carried out only by security analysts, which costs considerable time and money.
- To mimic intruders vividly so as to find all possible attack paths hidden in a network from the perspective of hackers, an automated attack planning algorithm is needed to achieve autonomous attack paths discovery.

Main idea

The algorithm formalizes penetration testing as a Markov decision process (MDP) and uses network information gain as the reward that guides an agent to choose best response actions to discover hidden attack paths from the intruder's perspective.

Method

- Given a general vector, information entropy is adopted to represent the exposure state of victim computer, inspired by Liang and Shi (2004).
- The penetration testing process can be formulized as MDP, and existing algorithms can be adopted to find the best response.
- We combine these two ideas and take information entropy as reward in MDP to find a best penetration action when faced with a specific host.

Major results

- Our NIG-AP planner shows good performance in terms of convergence.

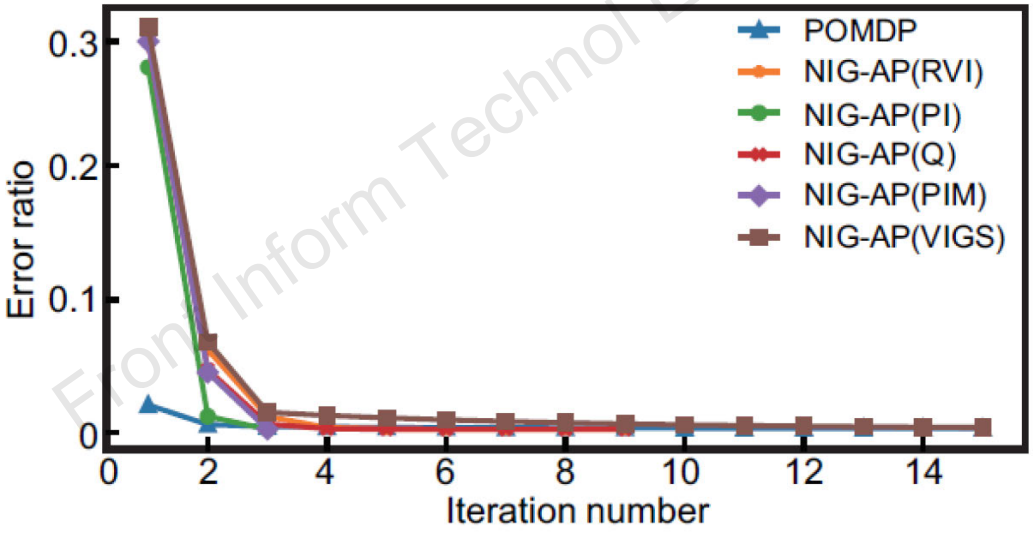

Fig. 5 Iteration performance

Major results

- NIG-AP attack planning algorithms outperform the FF and POMDP algorithms along with the increase of the state number.

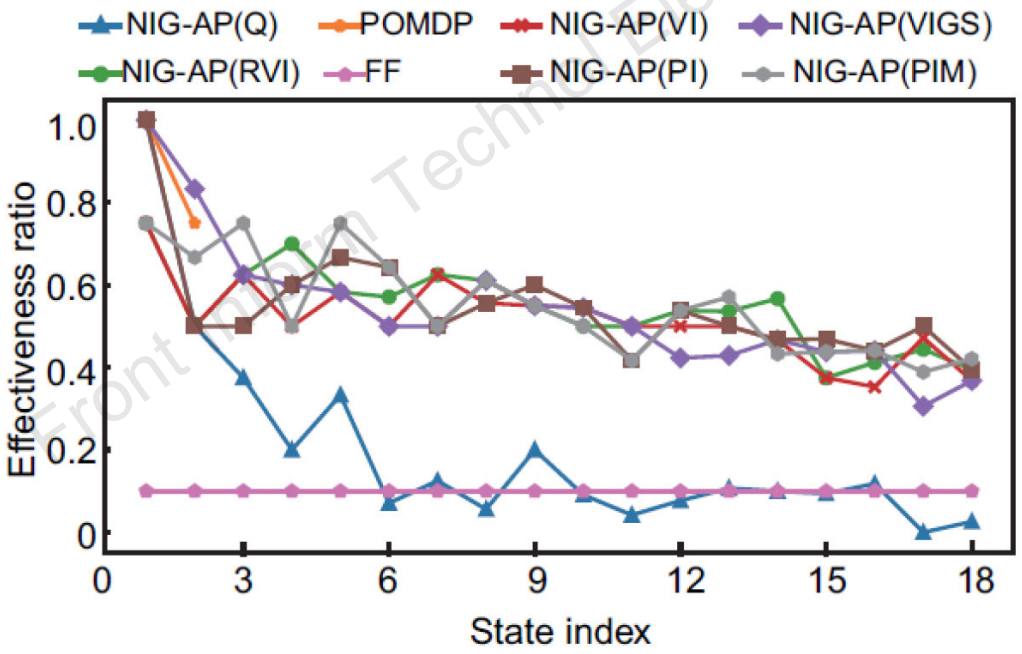

Fig. 7 Performance of discovering correct action

Conclusions

- We analyzed state-of-the-art attack planning algorithms, including the attack tree, attack graph, classical planning, and POMDP.
- We devised a reinforcement learning based attack planning algorithm to discover attack paths automatically without prior knowledge of the scenario network.
- A comparison experiment was conducted and the results demonstrated that our proposed algorithm can discover attack paths automatically without prior information.