Simulated Environment for Reinforcement Learning Based Intrusion Detection Using OMNET++

In Reinforcement Learning(RL) based intrusion detection, an agent interacts with its environment by taking actions and receives feedbacks information that will be used for evaluating the actions. Real system environments produce streams of live dataflows to be used by the RL agents, but it is hard to implement and expensive. Therefore, simulation is used to mimic real network environments. However, there are limited empirical evidences on the resemblance of the simulated networks to real networks and how the agents' interactions affect the environments. In this study, a RL agent is used to interact with a compromised simulated network and receive feedback information to be used for agents' training. The simulated network is developed using OMNET++ to mimic a WAN incorporated with web services to generate live data flows that will be used by the RL agent which uses its on-line ANN for selecting actions and off-line ANN for training. The simulated network environment is tested and evaluated using three RL settings, a single agent architecture, a game theoretic multi-agent architecture, and a cooperative multi-agent architecture. The network throughput before and after using the RL multi-agent architectures is measured. The proposed network environment can be used for evaluating RL based IDS architectures.