

Cyber KG + RL: Guiding Reinforcement Learning Algorithms for malware mutation and detection with knowledge graphs

Aritran Piplai, Anupam Joshi

Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County

- Reinforcement learning can help machines discover new information by trying out random actions
- 'Tacit' semantic knowledge about a given task can augment reinforcement learning algorithms by defining some rules that are not always implicit
- BLUE TEAM PERSPECTIVE:** CKGs help in generating evaluation criteria for malware. CKGs may contain valuable information that can be used to identify a malware. It can also contain previously known mitigation steps for a particular malware
- This information about specific malwares is useful for tuning the exploration rates of the specific actions suggested by the CKG
- It helps in generating reward metrics: The CKG can tell us what parameters indicate maliciousness, especially for this specific type of malware. These parameters can be incorporated in the reward function.
- RED TEAM PERSPECTIVE:** CKGs help in creating features that can be used in a RL algorithm to mutate a malware in such a way that it goes undetected by an externally trained malware classifier
- If an RL algorithm tries out random actions and still manages to defeat a malware classifier, there are chances that the action sequence for malware mutation will contain redundant actions
 - For example, an RL algorithm provides an output sequence like: pack, unpack, pack, unpack, change section header
- CKGs provide important information to a Deep neural network based RL algorithm such that the length of the action sequence can be decreased while retaining the same performance on defeating a malware classifier

