머신러닝과 딥러닝을 활용한 악성 패킷 탐지 기술 연구

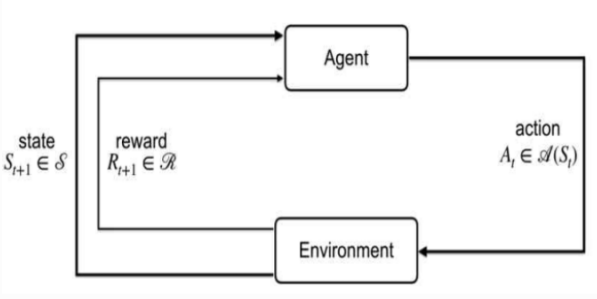
저자: 안병욱, 이중찬, 최재성, 박원형

네트워크 트래픽 기반 악성 패킷 탐지 방법 연구

- 지도학습은 레이블링 비용(시간, 돈)
- 비지도학습은 모델 훈련 난이도 ↑) → 강화학습 사용

- 구현 시스템

- 환경 : MDP(마르코프 결정 프로세스)



- 학습 모델 : DQN (Deep Q-Network)

- 결과

: 강화학습을 활용한 악성 패킷 탐지가 기존 지도/비지도 학습 모델 결과보다 좋음.