

Bachelor's/ Master's Thesis

Communication-Efficient Federated Reinforcement Learning under Differential Privacy

Abstract

Communication bottlenecks and data privacy present significant challenges in federated reinforcement learning (FRL), particularly in scenarios like decision-making for connected vehicles over wireless networks. The development of a privacy-preserving, communication-efficient algorithm for such problems remains an open question, as does the understanding of the interplay between privacy, communication, and learning performance in terms of regret.

Content

This thesis involves designing a privacy-preserving federated reinforcement learning (FRL) algorithm with an efficient communication protocol in under server-client structure and deriving the learning regret guarantees for reinforcement learning. The FRL algorithm will be based on epoch-wise sub-optimal action elimination at each agent, with agents exchanging knowledge with the server after each epoch. The algorithms will undergo theoretical analysis and performance evaluation via numerical experiments.

Requirements

- Interests in reinforcement learning (RL) and distributed computing.
- A basic understanding of fundamental Reinforcement Learning (RL) concepts and algorithms, along with knowledge of probability and statistics, is essential.
- Familiarity with statistical estimation theory is beneficial but not mandatory.
- Experience in Python for numerical experiments.

Literature

- Even-Dar, E., Mannor, S., Mansour, Y., & Mahadevan, S. (2006). Action elimination and stopping conditions for the multi-armed bandit and reinforcement learning problems. *Journal of machine learning research*, 7(6).
- Agarwal, M., Ganguly, B., & Aggarwal, V. (2021, December). Communication efficient parallel reinforcement learning. In *Uncertainty in Artificial Intelligence* (pp. 247-256). PMLR.
- Li, T., & Song, L. (2022). Privacy-preserving communication-efficient federated multi-armed bandits. *IEEE Journal on Selected Areas in Communications*, 40(3), 773-787.