Data-adaptive algorithms for learning in the presence of strategic behavior

Vidya Muthukumar, Assistant Professor, Schools of ECE and ISyE, Georgia Tech

Motivation and inspiration

- Defender protects
  - more valued
  - less valued

Target 1
Target 2

Defender protects equally valued
Attacker attacks

Security and defense

Swarm robotics

Spectrum sharing

Federated learning

All of the applications above involve multiple agents with unknown motives: a) malicious, b) selfish, c) stochastic, or d) cooperative.

Our goal: to design sequential decision-making algorithms for complex multi-agent environments that provably

- Adapt on-the-fly to data generated by an unknown agent
- Perform competitively with an algorithm that knew the agent type(s) in advance
- Can be efficiently implemented at scale

Mathematical framework: online decision-making, game theory and reinforcement learning

\[ X_1, \ldots, X_{t-1} \rightarrow (\hat{X}_t, X_t) \]

other (unknown) agents

online learning agent

Loss/cost \( \ell(\hat{X}_t, X_t) \)

Our algorithms: adapt between malicious and stochastic agents (environments)

New idea: online, data-adaptive hyper parameter tuning (e.g. learning rate)

Extent of uncertainty ideal for worst-case env.

Learning rate ideal for stochastic env.

Achieve loss as good as algorithm that knows agent behavior beforehand [1] (in this case, stochastic)

Total loss

Number of rounds

The road ahead

- Implementing adaptive algorithms at scale (recent preliminary work [2])
- Adapting to non-adversarial agents (building on [3])
- Understanding the long-term dynamics of multi-agent interaction (building on [4])

Project timeline

Non-adversarial data
Dynamics of multi-agent learning
Scaling up algs.

Selected references

4. On the impossibility of convergence of mixed strategies arising from no-regret learning, major revision at Mathematics of Operations Research.