Canadian Association of Physicists
Association canadienne des physiciens et physiciennes

Contribution ID: **4386** Type: **Oral Competition (Graduate Student) / Compétition orale (Étudiant(e) du 2e ou 3e cycle)**

(G*) Deep Learning for Network Attack and Defense

Monday 27 May 2024 15:15 (15 minutes)

Real networked systems are fundamentally vulnerable to attacks that fragment the system via removal of a handful of key nodes, akin to percolation transitions in lattice systems. Though the problem of optimally attacking a network is NP hard [1], deep reinforcement learning is often able to learn near-optimal solutions to similar problems on disordered topologies (graphs) [2,3]. This raises the question: "Does there exist a strategy to mitigate such an attack?" Here, we address this problem by casting network attack/defense as a two-player, zero-sum game. Specifically, we consider an attacker, who aims to fragment the network—reducing its largest connected component below a specified threshold—with a minimum number of node removals and a defender, who obfuscates the network by strategically hiding links before the attacker makes its decisions [Figure 1]. In this game, concealed links—which are invisible to the attacker—introduce a novel layer of strategic complexity, potentially providing a strategy to defend networks against attacks.

In our findings, the defender's strategic concealment consistently increases the complexity and uncertainty of the attacker's task. The more links the defender is allowed to conceal, the more challenging it becomes for the attacker to effectively fragment the network [Figure 1]. At low concealment percentages, the defender's actions can successfully confound the attacker relative to heuristics like random concealment. However, the diminution in attacker performance is sublinear; only when essentially all network structure is hidden does the attacker perform no better than random. Our results suggest that network weaknesses are inferrable even with only partial topological information available These results shed light on defense mechanisms that are (in)effective at maintaining network robustness. In conclusion, our study underscores the vital role of strategic planning in network defense, providing a new perspective into enhancing network resilience to malicious AI-equipped agents.

Keyword-1

percolation

Keyword-2

networks

Keyword-3

artificial intelligence

Authors: LANCTOT, Jordan (Toronto Metropolitan University); CORNELIUS, Sean

Presenter: LANCTOT, Jordan (Toronto Metropolitan University)

Session Classification: (DAPI) M2-6 Applied Physics I | Physique appliquée I (DPAE)

Track Classification: Technical Sessions / Sessions techniques: Applied Physics and Instrumentation / Physique appliquée et de l'instrumentation (DAPI / DPAI)