Resilience for Consensus-based Distributed Algorithms in Hostile Environment†

Xuan Wang, Shaoshuai Mou, Shreyas Sundaram

Consensus-based distributed algorithms have been the key to many problems arising in multi-agent systems including reinforcement learning [1], [2], formation control [3], [4], task allocation [5] and so on. By consensus here is meant that all agents in the network reach an agreement regarding a certain quantity of interest [6], [7]. By distributed here is meant that the whole multi-agent system achieve global objectives by only local coordination among nearby neighbors [8]. On one hand, the absence of central controllers in multi-agent systems make them inherently robust against individual agent/link failures. On the other hand, the high dependence of the whole system on local coordination also raises a significant concern that algorithms for multi-agent networks may be crashed down in the presence of even one malicious agent [9]. This has motivated us to develop methodologies to achieve resilience in order to guarantee nice performance for consensus-based distributed algorithms especially in hostile environment. One challenge along this direction comes from the fact that each agent is usually with locally available information, which makes it very difficult to identify or isolate malicious agents [10]. The authors of [11]–[13] have achieved significant progress by showing that given $N$ adversarial nodes under Byzantine attacks, there exists a strategy for normal agents to achieve consensus if the network connectivity is $2N + 1$. These results are usually computationally expensive, assume the network topology to be all-to-all networks, or require normal agents to be aware of non-local information. Most recently the authors of [14], [15] have investigated consensus-based distributed optimizations under adversarial agents. They have introduced a local filtering mechanism which allows each agent to discard the most extreme values in their neighborhood at each step. This is not directly applicable to consensus-based distributed computation algorithms [16]–[19], in which extreme values may come from the local constraints instead of malicious agents. Thus in this talk we will present a new approach developed in [9], which achieves automated resilience without the identification of malicious agents for consensus-based distributed algorithms based on intersection of convex hulls [20].

† This is a summary of an invited talk in “Learning and Planning in Adversarial Environment” at the 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton) Allerton Park and Retreat Center Monticello, IL, USA, September 24-27, 2019

References