Subgradient Methods for Risk-Sensitive Optimization

Avinash Madavan
Electrical and Computer Engineering, UIUC

Abstract
We study a first-order primal-dual subgradient method to optimize risk-constrained risk-penalized optimization problems, where risk is modeled via the popular conditional value at risk (CVaR) measure. The algorithm processes independent and identically distributed samples from the underlying uncertainty in an online fashion, and produces an $\eta/\sqrt{K}$-approximately feasible and $\eta/\sqrt{K}$-approximately optimal point within $K$ iterations with constant step-size, where $\eta$ increases with tunable risk-parameters of CVaR. We find optimized step sizes using our bounds and precisely characterize the computational cost of risk aversion as revealed by the growth in $\eta$. Our proposed algorithm makes a simple modification to a typical primal-dual stochastic subgradient algorithm. With this mild change, our analysis surprisingly obviates the need for a priori bounds or complex adaptive bounding schemes for dual variables assumed in many prior works.

Cybersecurity Implications for DER Interoperability of IEEE 1547 Requirements

Megan Culler
Electrical and Computer Engineering, UIUC

Abstract
The 2018 revision of the IEEE 1547 standard was written to account for the growing penetration of renewables and other distributed energy resources (DER) into the generation profile. The updated standard calls for DER to ride through certain grid disturbances and provide voltage and power support. The standard does not directly address cybersecurity, but the requirement for remote setting of parameters, including disturbance ride-through characteristics, expose a potential cyberattack surface. This project considers the cyberattack paths and system consequences of malicious IEEE 1547 parameter settings. We first consider the feasible range of cybersecurity threats that are unique to the updated standard and explore the adversarial and system constraints for a successful attack path. Then we simulate the impact of an attack performed by creating a syntactically-correct message that changes 1547 ride-through parameters, and results in an action that causes or exacerbates instability. We also simulate remote generation, transmission, and acceptance of a spoofed message that makes changes to a DER controller to show that the cyber side of the attack is feasible. The results will demonstrate novel attack paths that exploit the communication between utility area electric power system (AEPS) operators and DER managed by third parties made possible by the updated IEEE 1547 standard. Further research is required to determine methods to mitigate the vulnerabilities identified.