UNDETECTABLE CYBER-PHYSICAL ATTACKS ON POWER GRIDS UNDER THE AC MODEL

Daniel Bienstock, Mauro Escobar

SIAM Workshop on Network Science 2018
July 12-13 · Portland

Summary

We describe an algorithm for computing undetectable cyber-physical attacks on power grids under the AC power flow model. The adversary's actions affect a small zone of the network; within this zone the adversary can modify demands as well as signals. Both actions are calculated so as to hide the underlying truth, which includes severe equipment overloads, while remaining consistent (i.e. not noticed) from the perspective of the control center of the system. We provide an algorithm and run experiments on large grids.

Introduction

Recent attacks on power grids [1] and extensive blackouts have motivated the study of physical and cyber attacks on these systems. In [13, 14] the authors consider, under the linearized power flow model, that an adversary has the ability of disconnect lines from the network and block that information from the control center (CC) of the grid. An algorithm and conditions, under the AC model, in which these failures can be detected is proposed in [16, 15].

Pure data infection attacks are studied in [5, 7], where an adversary injects false information to the sensors in the network, so that wrong scheduling decisions are made. Also see [12, 10, 8, 9, 11].

In this paper, we consider an adversary that modifies the demands and data over a zone of the grid, so as to hide an overload that results from the demand changes.

Notation. Throughout this document we will use the following terminology: j denotes the imaginary unit $\sqrt{-1}$; for $v \in \mathbb{C}$, v^* denotes its complex conjugate; for a node k, $\delta(k)$ is the set of edges incident to k; for a set $\mathcal{A}$ of nodes of a graph $G = (\mathcal{N}, \mathcal{E})$, let $\mathcal{A}^C \doteq \mathcal{N} \backslash \mathcal{A}$ denote its complement, and let $N(\mathcal{A}) \doteq \{v \in \mathcal{A}^C : \exists u \in \mathcal{A}, uv \in \mathcal{E}\}$ be the neighborhood of $\mathcal{A}$.

Power Flows

A power grid can be characterized by a set $\mathcal{N}$ of nodes (buses) that generate or demand power and a set of branches or transmission lines between the buses, each of these branches has a complex admittance y_{km}. In the AC power flow model, given the demand and generation at each node, underlying physics describe the status of the network through complex voltages $V_k = |V_k|e^{j\theta_k}$ at each bus k, and the complex power flow from bus k to m is given by $S_{km} = V_k(y_{km}(V_k - V_m))^*$. Thus a feasible AC power flow solution must satisfy:

$$\sum_{km \in \delta(k)} S_{km} = S_k^g - S_k^d \qquad \text{for each bus } k, \tag{1}$$

$$V_k^{min} \leq |V_k| \leq V_k^{max} \qquad \text{for each bus } k, \tag{2}$$

$$|S_{km}| \leq S_{km}^{max} \qquad \text{for each line } km. \tag{3}$$

In these expressions, S_k^g and S_k^d represent the generation and the demand at bus k, respectively, S_{km}^{max} is the capacity of branch km, and V_k^{min} and V_k^{max} are lower and upper bounds of the voltage magnitude. Equation (1) states the power balance at bus k must equal the difference between generation and demand.

Finding solutions for AC power flow problems is strongly NP-hard [4] as a result of the quadratic dependence on the voltage of the power flow.

In normal operation of a grid voltage and current are measured periodically at sensors (RTUs and PMUs). Each sensor is located on some branch km close to one of the buses (k or m), and reports the voltage at this bus and the complex current $I_{km} = y_{km}(V_k - V_m)$ on this branch. These values are reported to the CC.

Attack Model

Assume that an adversary has control over a set of buses $\mathcal{A} \subset \mathcal{N}$, the *attacked zone*, which does not include any generator buses (assumed harder to control). For every bus k in the attacked zone, the adversary has the ability of:

1. modify the bus demand S_k^d,
2. modify each measurement (voltage and current) reported to the CC by any sensor adjacent to k.

The objective of the adversary is to modify the demands within the attacked zone in order to create a large line overload. The attacker is also modifying the data originating within the zone as to seamlessly present a normal situation (no overload) as far as the CC is concerned; a dangerous condition [3][1]. Let V_k^T and V_k^R denote the true and reported voltages at bus k, and let $S_k^{d,T}$ and $S_k^{d,R}$ be the true demand of bus k and the demand computed from the reported voltages at bus k, respectively. Then, $(V_k^T, S_k^{d,T})$ needs to solve (1)-(2) and $(V_k^R, S_k^{d,R})$ solves (1)-(3).

In order to obtain undetectability, any sensor located on a branch that connects $\mathcal{A}$ with $\mathcal{A}^C$ must report consistent current and voltages. Thus, the attacker only needs that

$$\begin{aligned} V_k^T &= V_k^R && \text{for each bus } k \in \mathcal{A}^C \cup N(\mathcal{A}^C), \\ S_k^{d,T} &= S_k^{d,R} && \text{for each bus } k \in \mathcal{A}^C. \end{aligned}$$

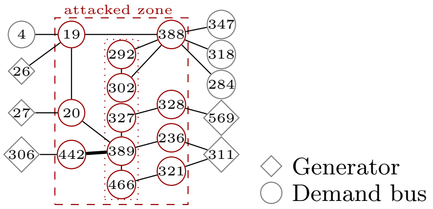

Figure 1: Attack on case2746wp (2746 nodes). The thick line shows the overload.

Experiments

We are able to generate undetectable attacks for large networks on the Matpower case library [18]. The attack on the zone shown in Figure 1 was obtained by solving the adversarial problem with IPOPT [17]. Note the large overload on Table 2.

k	$V_k^T = V_k^R$	k	V_k^T	V_k^R
19	1.090∠-4.96	292	1.110∠-8.22	1.110∠-8.23
20	1.090∠-4.96	302	1.110∠-8.22	1.110∠-8.23
442	1.093∠-11.16	327	1.095∠-10.01	1.095∠-10.03
388	1.111∠-8.23	389	1.104∠-10.02	1.102∠-10.20
328	1.094∠-10.01	466	1.106∠-10.04	1.105∠-10.14
236	1.105∠-10.13	321	1.108∠-10.05	1.108∠-10.05

Table 1: Voltage of subset of attacked buses.

k, m	$\lvert S_{km}^T \rvert$	$\lvert S_{km}^R \rvert$	S_{km}^{max}
389, 442	**143.6**	120.0	120
389, 20	153.8	159.7	160
389, 466	7.2	11.8	120
389, 236	7.0	8.9	120
389, 327	12.4	11.3	120
466, 321	6.8	11.6	120
327, 328	12.5	10.7	120

Table 2: True and reported power flows.

References

[1] Analysis of the cyber attack on the Ukrainian power grid 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, Mar. 2016.

[2] A. R. Bergen and V. Vittal. *Power Systems Analysis*. Pearson, Jan. 2006.

[3] D. Bienstock. *Electrical Transmission System Cascades and Vulnerability: An Oper. Research Viewpoint*. SIAM, 2015.

[4] D. Bienstock and A. Verma. Strong NP-hardness of AC power flows feasibility. *arXiv:1512.07315*, Dec. 2015.

[5] D. Deka, R. Baldick, and S. Vishwanath. Data attacks on power grids: Leveraging detection. In *2015 IEEE Power Energy Soc. Inn. Smart Grid Techn. Conf.*, pages 1–5, Feb. 2015.

[6] J. D. Glover, T. J. Overbye, and M. S. Sarma. *Power System Analysis and Design*. Cengage Learning, 2012.

[7] T. T. Kim and H. V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid*, 2(2):326–333, June 2011.

[8] X. Liu and Z. Li. False Data Attacks Against AC State Estimation With Incomplete Network Information. *IEEE Trans. Smart Grid*, 8(5):2239–2248, 2017.

[9] X. Liu and Z. Li. Local topology attacks in smart grids. *IEEE Trans. Smart Grid*, 8(6):2617–2626, 2017.

[10] X. Liu, Z. Li, and Z. Li. Optimal Protection Strategy Against False Data Injection Attacks in Power Systems. *IEEE Trans. Smart Grid*, 8(4):1802–1810, 2017.

[11] X. Liu, Z. Li, X. Liu, and Z. Li. Masking transmission line outages via false data injection attacks. *IEEE Trans. Inf. Forensics and Secur*, 11(7):1592–1602, 2016.

[12] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14:13:1–13:33, 2011.

[13] S. Soltan, M. Yannakakis, and G. Zussman. Power Grid State Estimation Following a Joint Cyber and Physical Attack. *IEEE Trans. Control of Network Systems*, (99), 2016.

[14] S. Soltan, M. Yannakakis, and G. Zussman. REACT to Cyber Attacks on Power Grids. *CoRR*, abs/1709.06934, 2017.

[15] S. Soltan and G. Zussman. EXPOSE the Line Failures following a Cyber-Physical Attack on the Power Grid. *CoRR*, abs/1709.07399, 2017.

[16] S. Soltan and G. Zussman. Power grid state estimation after a cyber-physical attack under the AC power flow model. *2017 IEEE Power and Energy Soc. Gen. Meeting*, pages 1–5, 2017.

[17] A. Wächter and L. T. Biegler. On the Implementation of a Primal-Dual Interior Point Filter Line Search Algorithm for Large-Scale Nonlinear Programming. *Math. Programming*, 106(1):25–57, 2006.

[18] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans. Power Systems*, 26(1):12–19, Feb. 2011.

[1] The total demand of the network might change when the adversary perform the attack. Our model correctly handles this fact through a model of secondary response [2, 3, 6].