Project Description: Towards Attack-Resilient Smart Grids

student: xx
mentors: Hampei Sasahara, yy

in 2021

1 Background

1.1 General Background

Digital transformation (DX) has fundamentally been changing our society. For example, recommendation systems, such as recommendations AI by Google, accumulate customers' data in cyberspace to analyze their preferences and enable the marketer to choose influential advertisements. On the other hand, in accordance with growth of the digitalization, cybercrime has been getting more attractive "business" to criminal syndicates. Fig. 1 depicts the estimated monetary loss from cybercrime reported by McAfee [1]. The monetary loss reaches at approximately 945 billion USD in 2020, and there is still a rising trend. Consequently, cybersecurity has been getting more important from the viewpoint of social benefit.

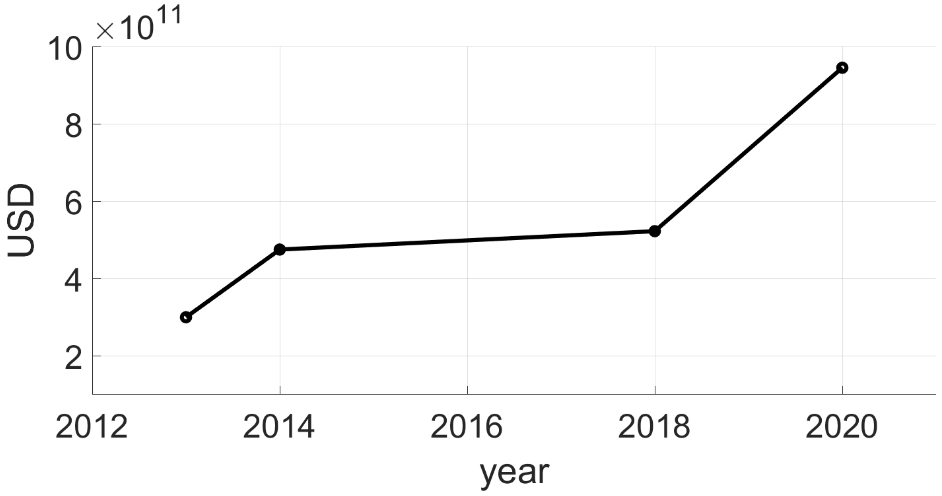

Figure 1: Estimated monetary loss from cybercrime reported by McAfee [1].

Moreover, the impact of such cyber threats extends to our physical world. Based on DX, our living environment is seamlessly connected to cyberspace over the Internet of

Things. In the resulting cyber-physical systems (CPS), not only traditional communicating devices, such as human-machine interface, but also physically operating devices, such as actuators, are directly connected to the network. The interaction expands the attack surface, creates new vulnerabilities, and possibly results in catastrophic consequences of critical infrastructures. Indeed, the most famous CPS incident caused by Stuxnet, which led to emergency shutdown of Uranium enrichment plants in Iran in 2010, has evidenced a possibility of highly damaging cyber attacks to infrastructures [2, 3]. Further, cybercrimes targeting to infrastructures has still been continuing. For instance, a US pipeline company has been attacked by DarkSide in May 2021 [4]. Although its accurate impact is still being assessed, it has been confirmed that 30% of gas stations are without gasoline in metro Atlanta, and other cities have reported similar numbers.

As indicated by the incidents, CPS security has been becoming an urgent matter in both industry and academia. Many researchers in the control field have devoted themselves to study of CPS security using the tools developed in our community (for an overview, see the survey paper [5]). In particular, DCS is one of the leading groups in this topic [6]. In the next subsection, I will explain our previous work related to this project.

1.2 Our Previous Work

As inferred by the title of this project, we deal with power systems, which were often targeted and sometimes resulted in serious blackout in the real world [7]. Modern power systems, also called smart grids, are a typical example of highly sophisticated CPS, which are built on many state-of-the-art techniques to realize economically efficient and environment-friendly energy supply networks, such as introduction of a massive amount of renewable energy resource. Accordingly, security of smart grids is an important and difficult issue [8, 9].

In particular, we have done the research

M. Lindsrtöm, H. Sasahara, X. He, H. Sandberg, and K. Johansson, "Power injection attacks in smart distribution grids with photovoltaics," European Control Conference, 2021, [Online]. Arxiv: `https://arxiv.org/abs/2011.05829`.

(NOTE: Because the conference will be held in the end of June, the official manuscript is unavailable now. Go to the URL to get the manuscript.) A rough sketch of the work is as follows. We take distribution networks with photovoltaics as the specific system of interest. The threat model is a power injection attack where an attacker chooses a connecting point in the distribution network and maliciously injects electric power by connecting a power generating device to destabilize its physical behavior. In this work, we have raised the question: *What attack has the maximum impact?* We have mathematically analyzed the scenario and concluded that the worst injected signal is a step function with switching at the end and the worst place to be attacked is the farthest place from the parent substation in the sense of an electric metric. After all, we have given an *analysis* of the attack scenario.

2 Research Description

The natural subsequent research task should be *synthesis* of some defense techniques against the attack based on the analysis. Hence, the research objective is set to as follows:

Research objective: Developing a defense strategy against power injection attacks to distribution networks with photovoltaics.

I created a basic framework to achieve the research objective and specified necessary tasks. This section describes them in detail.

2.1 Framework

Consider a power injection attack, which causes a deviation of the voltage from its ideal value. Once the voltage at a point exceeds a prescribed threshold, tripping of the point is automatically forced [10]. Because it is difficult to detect the attack in advance (see the discussion in Sec. IV-B in the manuscript of our previous work), we consider *restoration* of the distribution network after the disconnection.

Supply restoration problems in distribution networks are a classical topic [11], but it is still challenging because of new devices and additional requirements [12, 13]. In the traditional context, the restoration is taken as a response to a fault caused by natural disaster. A typical formulation is given as the following optimization problem [14]:

$$\begin{array}{ll} \displaystyle\min_{x\in\mathcal{X}} & L_{\mathrm{e}}(x) \\ \text{s.t.} & (\text{physical constraint on } x) \end{array}$$

The decision variable $x = (x_1 \ \cdots \ x_N) \in \{0,1\}^N = \mathcal{X}$ is given as binary values corresponding to controllable switching devices (it takes 0 and 1 when the circuit is open and closed, respectively). The objective function L_{e} represents the economic loss, quantified by the amount of demanded power that are not met by the choice x. The physical constraint includes, for example, Kirchhoff's law (or its simplified version).

On the other hand, in our scenario, we additionally take *resilience* into account to protect the system. The objective function should be given as

$$L_{\mathrm{e}}(x) + \lambda L_{\mathrm{r}}(x, a)$$

where the additional decision variable a that represents an attack, L_{r} represents the loss associated with resilience (attack impact), and $\lambda > 0$ is a scaling parameter. An important factor is that the entire loss depends on the attack a, which is decided by the attacker. Hence, there are two decision makers, one is the network operator and the other is the attacker. To model a reasonable decision making with multiple decision makers, we employ the framework of *game theory.* The decision is formulated as the *Stackelberg equilibrium*, i.e.,

$$\begin{array}{ll} \displaystyle\min_{x\in\mathcal{X}} \max_{a\in\mathcal{A}} & L_{\mathrm{e}}(x) + \lambda L_{\mathrm{r}}(x, a) \\ \text{s.t.} & (\text{physical constraint on } x) \\ & (\text{budget constraint on } a) \end{array} \tag{1}$$

where the leader is the operator (defender) and the follower is the attacker. This formulation means that the defender makes her decision at first and after that the attacker makes her decision with knowledge of the defender's decision.

Note that such problem formulation is not completely novel. Indeed, there exists a recent work with a similar formulation [15]. One important feature in our scenario is that we consider *dynamical attack over continuous time*, i.e., a in (1) is a function of time (see the manuscript of our previous work). Formally, $\mathcal{A}$ is a function space, whose elements are functions of time like $f(t)$ with $t \in [0, T]$. Thus, the problem (1) becomes an infinite-dimensional problem and impossible to solve without approximation in general. One important finding in our previous work is that the inner infinite-dimensional maximization problem in (1) can equivalently be reduced to a finite-dimensional maximization problem. Therefore, we can transform (1) into

$$\begin{array}{cl} \min\limits_{x \in \mathcal{X}} \max\limits_{\hat{a} \in \hat{\mathcal{A}}} & L_{\mathrm{e}}(x) + \lambda \hat{L}_{\mathrm{r}}(x, \hat{a}) \\ \text{s.t.} & (\text{physical constraint on } x) \\ & (\text{budget constraint on } \hat{a}) \end{array} \tag{2}$$

where $\hat{\mathcal{A}}$ is a finite set, specifically given as a set of connecting points to be attacked. Hence, the original problem is reduced to a finite-dimensional problem to which several existing algorithms can be applied, provided that the objective functions and the constraints are appropriately chosen. Specifically, L_{r} should be chosen as the one in our previous work, which is the $\mathcal{L}^\infty$ norm of the time series of the voltage deviation. Suitable choices of the other functions are still unclear.

2.2 Tasks

2.2.1 Modeling

The specific forms of L_{e}, L_{r}, and the constraints should be determined. As mentioned above, L_{r} and attacker's budget constraint should be set to the one used in the previous work. On the other hand, desirable L_{e} and the physical constraint are unclear. The formulation in [14] should be very helpful. However, it is comprehensive, and hence very complicated. It may be good to begin with a simple model by choosing a few factors in [14].

2.2.2 Algorithms

Even if the problem can be reduced to a finite-dimensional problem (2), computing the Stackelberg equilibrium is challenging when there are constraints. We have to look for algorithms suitable for the problem. Unfortunately, I am unfamiliar with specific algorithms now, so I cannot provide helpful references on this topic. Note that, the class of the problem depends on the modeling, and hence we have to take algorithms into account when modeling.

2.2.3 Simulation

To demonstrate the effectiveness of our proposed method, we have to do simulation. First, we have to choose the network architecture to be used. There are some networks provided by IEEE [16] and perhaps they are helpful. After deciding the numerical model to be used, build a simulation code. Use cvx [17], which works on MATLAB, as an optimization problem solver.

3 Project Goals

Because the period is too short to conduct the whole part of the research, it would be safe to set multiple goals. The basic goal is set to as follows:

Basic goal: Learning about power system security and having experience of research.

The advanced goal is set to our standard requirement as a researcher, namely,

Advanced goal: Carrying out all the tasks (in a solid manner) and writing an academic paper.

The middle between the goals may be reasonable. For example, finding a simplest model easy to solve and building a code for a small-scale toy example is another reasonable goal. (Actually, this is a very good goal. Even if you try the advanced goal, you have to take this step as a preliminary work.)

4 Plan

Basically, you can do whatever you want, but I suggest the following plan. Of course, the plan should be flexible depending on your goal and the progress.

4.1 Preliminary tasks

- Read this document carefully.
- Look up words unfamiliar to you, e.g., “distribution networks,” “Stackelberg equilibrium,” and so on.
- Set up simulation environment (MATLAB and cvx).
- Read references to understand:
    1. importance of CPS security
    2. basic function of power systems
    3. typical formulation of traditional supply restoration problems
    4. our previous result

For the first purpose, read [6] and Introduction of [5]. For the second purpose, read Chapter 1 of the textbooks [18] and [19]. For the third purpose, read Introduction and Sec. II of [13] and Sec. II of [14]. For the forth purpose, read our manuscript shown in Sec. 1.2 carefully.

4.2 Basic work

- Do modeling and algorithm tasks.
- Build a simulation code (simple/small-scale).

4.3 Advanced work

- Extend the code to complex/large-scale networks.
- Write an academic paper if you want.

5 Contact Information

If you have any concerns, contact me: `hampei@kth.se`, or visit my office: B606 at malvinas väg 10.

References

[1] Z. Smith, E. Lostri, and J. Lewis, "The hidden costs of cybercrime," McAfee, Tech. Rep., 2020, [Online]. Available: `https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf`.

[2] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet Dossier," Symantec, Tech. Rep., 2011.

[3] Cybersecurity & Infrastructure Security Agency, "Stuxnet malware mitigation," Tech. Rep. ICSA-10-238-01B, 2014, [Online]. Available: `https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B`.

[4] Cybersecurity & Infrastructure Security Agency, "DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks," Tech. Rep. AA21-131A, 2021, [Online]. Available: `https://us-cert.cisa.gov/ncas/alerts/aa21-131a`.

[5] S. Dibaji, *et al.,* "A systems and control perspective of CPS security," *Annual Reviews in Control,* Vol. 47, pp. 394-411 2019.

[6] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine,* Vol. 35, No. 1, pp. 22–23, 2015.

[7] Cybersecurity & Infrastructure Security Agency, “Cyber-attack against Ukrainian critical infrastructure,” Tech. Rep. IR-ALERT-H-16-056-01, 2018, [Online]. Available: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

[8] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid,” *Proc. IEEE,* vol. 100, no. 1, pp. 210–224, 2012.

[9] Z. Li, M. Shahidehpour, and F. Aminifar, “Cybersecurity in distributed power systems,” *Proc. IEEE,* vol. 105, no. 7, pp. 1367–1388, 2017.

[10] “IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces,” in IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003), pp.1-138, 2018.

[11] D. Shirmohammadi, “Service restoration in distribution networks via network reconfiguration,” *IEEE Transactions on Power Delivery,* vol. 7, no. 2, pp. 952-958, 1992.

[12] Y. Liu, R. Fan and V. Terzija, “Power system restoration: a literature review from 2006 to 2016,” *Journal of Modern Power Systems and Clean Energy,* vol. 4, no. 3, pp. 332-341, 2016.

[13] F. Shen, Q. Wu, S. Huang, J. C. López, C. Li and B. Zhou, “Review of service restoration methods in distribution networks,” *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe),* 2018.

[14] R. Romero, J. F. Franco, F. B. Leão, M. J. Rider and E. S. de Souza, “A new mathematical model for the restoration problem in balanced radial distribution systems,” *IEEE Transactions on Power Systems,* vol. 31, no. 2, pp. 1259-1268, 2016.

[15] D. Shelar, S. Amin and I. Hiskens, ”Evaluating resilience of electricity distribution networks via a modification of generalized Benders decomposition method,” *IEEE Transactions on Control of Network Systems,* 2021.

[16] https://icseg.iti.illinois.edu/ieee-118-bus-system/

[17] http://cvxr.com/cvx/

[18] P. Kundur, *Power System Stability and Control,* McGraw-Hill, 1994.

[19] A. Pabla, *Electrical Power Distribution,* McGraw-Hill, 2011.