

Cyber-related Risk Assessment and Critical Asset Identification within The Power Grid

Z. Mohajerani, F. Farzan, M. Jafari
Industrial Engineering Department
Rutgers University
Piscataway, NJ, USA

Y. Lu, D. Wei, N. Kalenchits
Automation and Control Department
SIEMENS Corporate Research, Inc
Princeton, NJ, USA

B. Boyer, M. Muller
Mechanical Engineering Department
Rutgers University
Piscataway, NJ, USA

Abstract—This paper introduces a new way to detect and improve the vulnerability of bulk power systems against the intrusion and malicious acts of cyber hackers. For this aim, detecting the most vulnerable part of the power grid to hacker attack is needed. The method for finding the most vulnerable substation inside the grid (first pass model) and then finding the most critical asset inside that substation (second pass model) is presented. The suggested method performs improvement in overall vulnerability of the grid by calculating the risk of each asset and placing a security agent on the most vulnerable positions within the substation to prevent the cyber attacks as most as possible.

Keywords—cyber security; risk assessments; power grids;

I. INTRODUCTION

Electrical power grid reliability is inherently difficult to calculate and assess because of its dynamic nature. Changes in load, unseen faults, and more recently the threat of cyber attack all affect the grid's ability to successfully supply bulk power. This paper presents a paradigm for identifying and ranking critical assets within an electrical grid based on islanded load and limiting parameters.

To construct a general tool for risk assessment, an integration of physical features of power grids and substations with cyber-related and security characteristics of such systems is needed. To make the tool practical as well, a level of aggregation in cyber security analysis should be considered to avoid complexity and dimensionality which cannot be implemented with existing calculation capacities (An example of one of these non-practical methods is huge attack graphs used to evaluate the security of IT networks). Therefore, our overall framework is decomposed as follows:

- First pass model which is run at grid level to identify the most critical substation.
- Second pass model which is run at substation level to identify the most critical component.
- Optimal implementation of security agents within the substation to mitigate the overall risk of the substation.

¹This work is part of the project Protecting Intelligent Distributed Power Grids against Cyber Attacks, which was conducted for the DoE Office of Electricity Delivery and Energy Reliability under Contract DE-FC26-07NT43313.

This is done by considering cost constraints as well as maintaining required level of quality of service.

The above models are implemented as a cyber-related risk assessment tool.

II. FIRST PASS MODEL

The objective of this model is to obtain a ranking for the criticality of any substation within a power network. Two models are developed and linked together to assign risk measures for each substation. The first model would be the business model which starts with the missions of a particular network and goes all the way down to the network nodes which are the substations (generation, transmission and distribution) and establish a relationship between each level in terms of the impact of the loss of each level on the other one. The second model is the Network Risk model which begins with the vulnerabilities at network nodes level and using the business model developed earlier, a risk measure at each level from network nodes to business objective is obtained by overlaying the vulnerability index and impact weight.

Much like the stochastic nature of unseen faults, the threat of cyber attack is difficult to quantify and predict. For the purposes of this paper, the threat of cyber attack is considered uniform throughout the year. The zero day or zero hour attack are terms used to describe the immediacy of a cyber attack. In other words, a hacker will exploit a vulnerability window as soon as he or she is able, not when it is most convenient for them or most detrimental to the system.

Considering cyber attacks adds a new dimension to the traditional N-1 stability analysis. This test sums the islanded load from each substation piecewise over an entire year.

In addition to the modified N-1 analysis, the use of a vulnerability index provides another degree of freedom for assessing risk. The vulnerability index relates physical parameters of a substation to its likelihood of being attacked. For instance a substation which has more network exposure is inherently more vulnerable.

A. Result

The coupling of the N-1 analysis with the vulnerability index combines the impact of an attack with the likelihood of an attack and can allow asset owners to decide where their system is in need of hardening.

Another advantage to this approach is that it considers distribution substations as critical. During the majority of the year, when the grid satisfies N-1, an attack on a distribution station is the only way to achieve a loss of load. When looking at a system over time, these distribution stations are critical assets.

Each system is unique in its response to load fluctuations and faults. As part of this exercise, a substation index has been created to categorize substations into three types: Generation, Transmission, and Distribution. This is another tool which will allow asset owners to target certain types of substations when looking to harder their system.

III. SECOND PASS MODEL

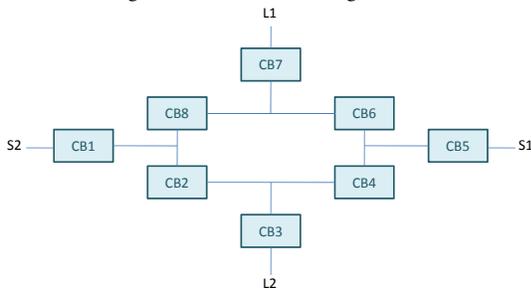
Earlier, we decomposed the vulnerability at asset or substation level into three categories of unauthorized access, digital vulnerability and physical vulnerability. We are mainly interested in those attacks that lead to physical damage at the substation and/or grid levels. At the substation level, any path that causes physical damage, starts with an unauthorized access to the substation control, followed by an exploitation of potential digital vulnerabilities at substation control/comm.

In the second pass model, we try to find the most vulnerable device or connection inside the substation. In order to decrease the vulnerability of this element, and subsequently the whole substation, we place a security agent for monitoring and decreasing the probability of cyber-attacks in this place.

Our approach is consisted of six steps:

- 1) Finding the criticality level of all the breakers in the substation using the "substation configuration" as shown in Figure 1.

Figure 1. substation configuration.



- 2) Building the attack graph using the "automation system configuration" as shown in Figure 2.
- 3) Finding the possible attack scenarios (attack paths) using the attack graph (shown in Figure 3).

Figure 2. automation system configuration.

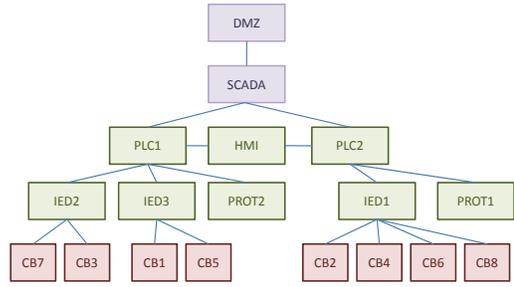
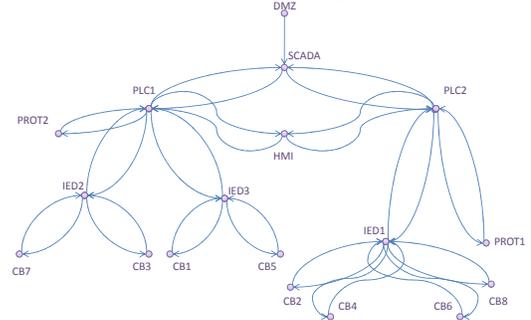


Figure 3. attack graph.



- 4) Calculating the vulnerability index of all the devices and links inside the substation using the user's answer to the questionnaires.
- 5) Calculating the risk indices using the criticality, cost and vulnerability indices.
- 6) Using the risk indices and their associated costs to find the optimal implementation of the security agent.

A. Step 1: Criticality Computation

Criticality of each breaker is proportional to the frequency of its usage inside the substation. To find the criticality, we first find all the possible paths between loads and sources, while satisfying the lines voltage constraints. Let m be the total number of these paths, and n_i be the total number of appearances of the i -th breaker in all the paths. Using these notations, we can calculate the criticality of this breaker as:

$$Cr_i = n_i/m$$

B. Step 2: Building the Attack Graph

Using the substation configuration, we find all the paths from the possible entry points (the points from which hackers can intrude the substation.) to each device within the substation. Each of these paths indicates a possible way for destroying the endpoint device and has a risk index associated with it. The risk index indicates how probable this scenario is to occur as well as its physical impact in terms of the criticality of the component and associated costs.

C. Step 3: Attack Path

Inside the substation, some devices can be used by the hacker to intrude into the system (e.g. an unused port on a PLC can be an entry point into the substation). In this step, we find all the possible paths from these entry points to all the other devices. Each of these paths can be an attack scenario.

D. Step 4: Vulnerability Index Computation

The first part of calculating the risk index is to find the vulnerability index of all the connections (links) between the substation elements (control and physical nodes). Vulnerability of each link is a function of several criteria such as physical media used in this link, existence of firewall or other intrusion detection systems, password strength, type of operation system used to operate each control element (e.g., PLC), etc.

In order to take all of these criteria into account, we make a questionnaire consisting of several sections. Each section will reflect the effect of one of the above criteria. After the user enters the automation system configuration, he/she will be asked to fill this questionnaire for all the links. Obviously, the user can leave some questions unanswered and the system will assign default values to these questions. The default answers will be updated automatically as we update our database using the answers we get from different substations around the country.

As mentioned in the earlier report [reference], hackers can attack the substation in several ways. The damage he/she can cause inside the substation includes: 1) Taking the control of a controller device (like PLC or IED) and sending the control commands to other elements controlled by this device, 2) Changing the information flow (i.e. by causing delay and making the messages outdated between two devices). We denoted the vulnerability of each link to the information and the control attacks by assigning a binary number (0 or 1) to information (I) and control (C) functionality of each link.

All these attack characteristics will be computed with our software, as soon as the user finish filling the questionnaire

E. Step 5: Risk Index computation

Risk is a function of threat, vulnerability and consequences (impacts). We assume the threat to be constant. We calculate the vulnerability by using the answers to our questionnaire and finally the consequence by calculating the criticality and by taking into account the cost related to cascading, failure and repair. By knowing these parameters and having the possible attack path, which were calculated by using the attack graph, we can compute the risk index of each asset and find the most critical asset as the result.

F. Step 6: Security agent placement

We want to place the security agent somewhere to minimize the relative costs and maximize the substation overall security. By placing a security agent on any element inside the substation, the vulnerability of the element and all the paths it belongs to will be decreased. By calculating the risk index of all the intrudable elements in step 5, we have a measure for how risky each element is against malicious intrusions.

Based on the size of the substation, budget for purchasing the security agents, number of risky elements and value of their risk index, a decision can be made on how many agents to be placed inside the substation.

We have to note that placement of the security agent may have some drawbacks too, like lower bandwidth and time delay. Using our optimization algorithm, we take all of these constraints into account and will find the optimal implementation that minimizes the cost, maximizes the security, and keeps the bandwidth and overall delay safe and within the acceptable range for each link.

IV. CONCLUSION

In this paper, we introduced a new way to detect and improve the vulnerability of bulk power systems against the intrusion and malicious acts of cyber hackers. We found the most vulnerable substation inside the grid and then find the most vulnerable asset inside this substation. We suggested to improve the overall vulnerability by placing a security agent on the most vulnerable positions within the substation to reduce the overall risk and vulnerability of the vulnerable substation and the whole grid as the result. All the steps introduced in this paper are implemented as a cyber-related risk assessment tool which is currently used by Rutgers University and Siemens Company.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Dr. Diane Hooie of the Department of Energy who provides overall management, with support from the DoE contract manager Jeffrey Kooser and Tom Flowers

REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L^AT_EX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
- [2] Saaty, T., *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, McGraw-Hill, New York, 1980.
- [3] Cheng, Y., *Extent Analysis and Synthetic Decision, Optimization Techniques and Applications*, Singapore, 1, 352, 1992
- [4] Sarkis, J., Talluri, S., *Evaluating and Selecting e-Commerce Software and Communication Systems for a Supply Chain*, European Journal of Operational Research, 159, 318-329, 2004.

- [5] Kertzner, P., Watters, J., Bodeau, D., *Process Control System Security Technical Risk Assessment Methodology and Technical Implementation*, I3P, Research Report No. 7, 2006.
- [6] Watters, J., Kertzner, P., Hahn, A., Bodeau, D., Morrissey, S., *RiskMAP Translating ICS Risk Assessments Into Corporate Terms*, Process Control Systems Industry Conference, 2008.
- [7] Schmidt, R.A., *Opportunities to Use WiFi at the Substation*, Power System Engineering, Inc., 2005.
- [8] Alur, R. *Formal Analysis of Hierarchical State Machines*, LNCS 2004, Vol. 2772.
- [9] A. de la Villa Jan and A. Gmez-Expsito, *Implicitly Constrained Substation Model for State Estimation*, IEEE Transactions on Power Systems, Vol. 17, No 3., 2002.
- [10] Kirschen, D. and Strbac, G., *Why investments do not prevent blackouts*, The Electricity Journal, Vol. 17 Issue 2, pg. 29-36, March 2004.
- [11] Risley, A. and Roberts, J., *Electronic Security Risks Associated with use of Wireless*, Point-to-Point Communications in the Electric Power Industry, 56th Annual Texas A&M Conference for Protective Relay Engineers, April 8-10, 2003.
- [12] Isa, A.M., Verayiah, R., Sen, D.A., and Zainul Abidin, A., *Evaluation of Wireless Technologies for Usage in TNB Substations for Protection Systems Communications*, BETNET 2006.
- [13] Zhang, W., Das, S.K., Liu, Y., *Security in Wireless Sensor Networks: A Survey*, Chapter on Security in Sensor Networks. Auerbach Publications, Ed. Y Xiao.
- [14] Kezunovic, M., Georghiades, C.N., Shapoury, A., *Wireless Communications in Substations*, Final Project Report, Power Systems Engineering Research Center, November 2002.
- [15] Wei, D., Lu, Y., Jafari, M., Rohde, K., Muller, M., Turke, A., Skare, P., and Sastry, C., *An Investigation of Potential Cyber Attacks and Their Impacts on the Power Grid*, Siemens Corporate Research, Technical Report, May 15, 2008
- [16] Lu, Y., Zhao, P., Jafari, M.A., and Golmohammadi, D., *A Multi-Criterion Economic Evaluation Framework for Control System Configuration*, Technical report, Siemens Corporate Research, 2008.
- [17] Anjia, M., jiaxi, Y., and Zhizhong, G., *Electric Power Grid Structural Vulnerability Assessment*, IEEE 2006.