Cyber Resilience Metrics for Bulk Power Systems

Website: https://cred-c.org/researchactivity/crmetricsbps

Researchers (ODU, Illinois): Sachin Shetty (ODU), Bheshaj Krishnappa (industry partner), David Nicol (Illinois), Ariful Haque (ODU), Gael Kamdem De Teyou (ODU), Sharif Ullah (ODU), and Marco Gamarra (ODU)

Industry Collaboration:

- Bheshaj Krishnappa, ReliabilityFirst

Description of research activity: The North American BPS is a complex technological network, and its cyber-physical interconnectivity allows for long-distance power transmission but presents a "surface" for cyber attacks. The potential for disruptions in BPS can be attributed to the dependence and the vulnerability of the networks interconnecting substations and control centers. There is a need to develop cyber resilience metrics for BPS to provide quantitative insights into ability of security controls to ensure operational resilience and development of cost-effective mitigation plan. In this activity, we propose to measure cyber resilience for power systems as a function of robustness, redundancy, resourcefulness and rapidity. We will develop analytical models for each of the aforementioned properties for the networks interconnecting sub stations and control center. We will formulate the analytic models as multi-level directed acyclic graphs and interdependent coupled networks. We will identify the design parameters, such as firewall rules, network paths, node recovery time, backup resources available, etc., which achieve the desired resilience by measuring robustness, redundancy, resourcefulness and rapidity. We will model the relationship between the network parameters and resilience levels which will be benefit the stakeholders of BPS. Through the collaborative research agreement with RF, representative network topologies and appropriate data will be shared to aid in a high-fidelity model. RF is one of the eight FERC approved regional entities responsible for ensuring the reliability of the BPS. RF is responsible for the reliability and security of the power system within a footprint which spans 13 states in the Eastern Interconnection. Their mission involves developing, monitoring, and enforcing compliance with the FERC approved reliability standards for owners, operators and users of the BPS (approximately 350 utilities); developing and disseminating timely and instructive information to enhance the reliability of the BPS; and provide seasonal and long-term assessments of BPS reliability.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity falls under "Assess and Monitor Risk". There is a need to understand and quantify the security posture of EDS. In our activity, we are focusing on the BPS sector within the EDS ecosystem. The availability of resilience metrics will support risk management decision making in BPS sectors. It will also facilitate the ability of operators to prioritize corrective actions. In addition, the availability of cyber resilience metrics will motivate operators to continually assess their response to risks to cyber threats.

Summary of EDS gap analysis: We will develop cyber resilience metrics for BPS based on an analytical framework that builds on models for physical attacks, but differentiates from these by considering the additional complexity introduced by the cyber asepcts of modern BPS. The availability of resilience metrics will aid in identifying the most vulnerable devices and impact on operation of the power grid and security controls which are cost-effective and provide appreciable tradeoff between protection and performance.

Full EDS gap analysis: The availability of cyber resilience metrics will facilitate effective risk management decision making in BPS. Specifically, asset owners will be able to prioritize corrective actions through identification of resilient topologies/configurations, identification of critical vulnerabilities which need to be mitigated, cost-effective security controls, etc. In addition, the availability of cyber resilience metrics will motivate operators to continually assess their response to risks to cyber threats. However, cyber resilient metrics to achieve these desired objectives for BPS are inadequate.

There have been efforts on developing models for power grid structural resilience in presence of cascading failures. According to the Energy Sector Cybersecurity Capability Maturity Model [17], there is a need to develop techniques to reduce risks and to increase operational grid resilience, commensurate with the risk to critical infrastructure and organizational objectives. However, resilience metrics for substation networks in BPS in the presence of cyber threats do not exist.

Research efforts on understanding and quantifying resilience in the power grid primarily focus on local and cascading failures which are caused due to physical faults [1-11]. Specifically, researchers have analyzed the power grid's structural resilience to deliberate physical attacks to substations, control centers, substation/transmission lines, and communication systems. The physical attacks caused due to vandalism or theft result in faults or failures in the generators and/or transmission lines and any cascading effects can be traced back to the original fault reliably. Kinney et al. [1], analyzed the resilience the power grid structural resilience in the presence of cascading failures by modeling the power grid from a network perspective and leveraging advances in complex network theory. The weighted graph model was used to represent the flow of electric power simultaneously through multiple paths in the network. In the weighted graph model, the nodes represent generators, transmission substations, and distribution substations, while edges represent high-voltage transmission lines. Each node has a load and a capacity that says how much load it can tolerate. When a node is removed from the network, its load is redistributed to the remaining nodes. If the load of a node exceeds its capacity, then the node fails. In order to measure resilience to cascading failures, the authors compute the average efficiency of the network. The efficiency of the overall power network is calculated by averaging over the most efficient paths from each generator to each distribution station. The efficiency will vary dramatically if the node impacted is the one that carries the highest load. So, in case of cascading failures, the authors have demonstrated that the resilience depends on the topology and timing of the attack.

Researchers have analyzed resilience in the context of static failures [2-6]. These efforts evaluated performance of the power grid when a certain subset of the system elements fails. Researchers have analyzed the resilience of the power grid by removing a sizable group of system elements. However, these efforts do not model the dynamic behavior. For instance, elimination of a single element or group of system elements can cause portions of power grid to collapse due to the dynamics of redistribution of power flows. To mitigate cascading effects, researchers have developed dynamic approaches [7-11]. These efforts not only focus on the consequences on the performance of the power grid due to loss of single component, but also focus on the overload and subsequently the partial or total loss of functionality of other components, which generates a cascading effect.

Researchers have also developed resilience metrics for critical infrastructures. [12-16]. Tierney et al. [12], proposed a R4 framework for disaster resilience. The R4 framework comprises of Robustness (Ability of systems to function under degraded performance), Redundancy (identification of substitute elements that satisfy functional requirements in event of significant performance degradation), Resourcefulness (initiate solutions by identifying resources based on prioritization of problems), and Rapidity (ability to restore functionality in timely fashion). However, no analytical models have been proposed, and the efficacy of the framework in systems in situations other than environmental disasters has not been studied. Ganin et al., [13] proposed graph –theoretic model to measure operational resilience. However, this model is agnostic to a system domain and focusses on the interdependences of system components at a higher abstraction level. Linkov et al., [14] has proposed techniques to measure resilience for attacks on cyber systems. Thorisson et al., [15] utilize scenario-based risk assessment to develop resilience analytics for the power grid. Roege et al., [16] provide metrics for energy resilience by analyzing interactions among physical, information and human domains.

Our activity will derive a rigorous analytical framework to compute metrics to measure cyber resilience for BPS. The framework will provide insights into the differences between fault-resilience due to physical attacks and attack-resilience due to cyber attacks. We will build upon the analytical frameworks developed to model physical attacks [1-11] to incorporate the varying degrees of exploitability and impact of cyber attacks, diversity of network topology, configuration and vendor products and study influence of critical nodes, attack timing, stepping stones, pivot points, attack launch location on the overall resilience. Our proposed effort will integrate the modeling of cyber-attacks in the weighted graph model [1] focused on modeling failures due to physical attacks only. We will also develop the analytical

models to measure each of the four elements of the R4 framework [12]. In partnership with our industry partner, ReliabilityFirst, we have access to representative system and network architecture for bulk power systems. The integration of these efforts will facilitate the development of the resilience metrics for BPS

Bibliography:

1. Modeling cascading failures in the North American power grid, R. Kinney, P. Crucitti, R. Albert, and V. Latora, Eur. Phys. B, 2005
2. E. I. Bilis, W. Kröger and C. Nan, "Performance of Electric Power Systems Under Physical Malicious Attacks," in *IEEE Systems Journal*, vol. 7, no. 4, pp. 854-865, Dec. 2013.
3. Y. Zhu, J. Yan, Y. Tang, Y. L. Sun and H. He, "Resilience Analysis of Power Grids Under the Sequential Attack," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340-2354, Dec. 2014.
4. Y. Zhu, J. Yan, Y. Sun and H. He, "Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274-3284, Dec. 2014.
5. J. Yan, Y. Tang, Bo Tang, H. He and Y. Sun, "Power grid resilience against false data injection attacks," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1-5.
6. C. Barreto, J. Giraldo, Á A. Cárdenas, E. Mojica-Nava and N. Quijano, "Control Systems for the Power Grid and Their Resiliency to Attacks," in *IEEE Security & Privacy*, vol. 12, no. 6, pp. 15-23, Nov.-Dec. 2014.
7. Yakup Koç, Martijn Warnier, Piet Van Mieghem, Robert E. Kooij, Frances M.T. Brazier, The impact of the topology on cascading failures in a power grid model, Physical A: Statistical Mechanics and its Applications, Volume 402, 15 May 2014
8. Yakup Koç, Martijn Warnier, Robert E. Kooij, Frances M.T. Brazier, An entropy-based metric to quantify the robustness of power grids against cascading failures, Safety Science, Volume 59, November 2013
9. Z. Huang, C. Wang, M. Stojmenovic and A. Nayak, "Characterization of Cascading Failures in Interdependent Cyber-Physical Systems," in *IEEE Transactions on Computers*, vol. 64, no. 8, pp. 2158-2168, Aug. 1 2015.
10. Andrey Bernstein, Daniel Bienstock, David Hay, Meric Uzunoglu, and Gil Zussman. 2012. Sensitivity analysis of the power grid vulnerability to large-scale cascading failures. *SIGMETRICS Perform. Eval. Rev.* 40, 3 (January 2012), 33-37.
11. A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu and G. Zussman, "Power grid vulnerability to geographically correlated failures — Analysis and control implications," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Toronto, ON, 2014, pp. 2634-2642.
12. Tierney, Kathleen, and Michel Bruneau, 2007, “Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction,” TR News, May, 2007, pp. 14 – 17
13. Ganin, A.A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J.M., Kott, A., Mangoubi, R. & Linkov, I. (2016). Operational Resilience: Concepts, Design and Analysis. Scientific Reports, 6: 19540
14. I. Linkov et al., “Resilience Metrics for Cyber Systems,” Environment Systems & Decisions, vol. 33, no. 4, 2013
15. Thorisson, H., Lambert, J., Cardenas, J., and Linkov, I. (2016). "Resilience Analytics with Application to Power Grid of a Developing Region." Risk Analysis,
16. P.E. Roege, Z.A. Collier, J. Mancillas, J.A. McDonagh, I. Linkov, Metrics for energy resilience, Energy Policy., 72 (2014) 249-56
17. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf