Exploring Security Metrics for Electric Grid Infrastructures Leveraging Attack Graphs

Panini Sai Patapanchala, Chen Huo, Rakesh B. Bobba, and Eduardo Cotilla-Sanchez
School of Eelctrical Engineering and Computer Science, Oregon State University
{*patapanp, huoch, bobbar, ecs*}*@oregonstate.edu*

***Abstract*—The electric grid is a critical cyber-physical infrastructure that serves as lifeline for modern society. With the increasing trend of cyber-attacks, electric grid security has become a significant concern. System operators have the difficult task of reducing the risk exposure and maintaining operational reliability under the constant threat of cyber-attacks. Good security metrics for assessing and monitoring the risk to the cyber-physical power grid infrastructure would be very valuable for grid operators. However, security metrics to assess the security posture and risk to even traditional enterprise cyber infrastructure have been a long standing challenge. Cyber-physical systems (CPS) that have interconnected cyber and physical infrastructure add an additional layer of complexity. In this work, we explore security metrics that can be used to monitor the security posture and risk exposure of the electric grid infrastructure. These metrics take both the cyber security posture and physical impact of an attack into account. We consider both individual and coordinated attacks that can cause cascading outages. To illustrate the usefulness of the proposed metrics, we use cyber-physical models for 9-bus and 39-bus test systems. Our metrics provide a novel way to identify and prioritize assets critical to the system and help operators take steps to improve the overall security posture of the system.**

I. INTRODUCTION

Cyber-Physical Systems (CPS) exemplify the tight integration of computation, networking, and physical processes. One such critical cyber physical infrastructure is the electric grid. Supervisory Control and Data Acquisition (SCADA) systems are used to collect sensor data and operate the electric grids. SCADA systems have been undergoing a lot of upgrades with technology advancements and smart grid initiatives [20]. These changes include improved connectivity and communications among all entities of a power grid including power plants, control centers, transmission and distribution substations, and even customer homes. While cyber-infrastructure has been an integral part of grid operations for a while now, the increased connectivity often using the internet and commercial off the shelf (COTS) technologies has increased the exposure and consequently the risks to the grid infrastructure. Further, the interconnection between cyber and physical components introduces a an additional layer of complexity. Thus, maintaining the operational reliability of of the grid under the threat of cyber-attacks is a critical and challenging problem.

The recently reported cyber-attack on the Ukrainian electric grid[1] has showed that the threat of cyber attacks on electric grid infrastructure is real and can severely impact electric grid operations and the energy delivery function. Coupled with the increasing trend of cyber-attacks in general, security of electric grid has become a significant concern. Electric grid operators have been working to reduce risks to the system in the face of increasing cyber attacks. North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards that provide a cyber security framework for the identification and protection of *Critical Cyber Assets* to support the reliable operation of the Bulk Electric System were adopted in 2008, and are enforced as regulations that bulk electric system operators need to comply with. Similar standards have been adopted in other parts of the world. In the current version of the CIP standard[2] the definition of critical cyber assets refers to cyber assets that are essential to the operations of electric grid. However, it does not offer a framework to prioritize critical assets or to prioritize efforts to secure such assets. Security metrics can provide a way to prioritize critical assets and to evaluate different security configurations and controls. However, security metrics to assess the security posture or risk to even traditional networks have been a long standing challenge (see for example [9]–[14], [16]–[18]).

In this work we propose and explore a number of cyber-physical metrics for electric grid infrastructures that are inspired by graph measures. Having such security metrics will give grid operators a way to identify critical assets, prioritize security efforts and compare different security configurations and controls. Our metrics take into account both individual and coordinated attacks that can cause cascading outages. As these metrics take both the cyber security posture and physical impact of an attack in to account, they can be used to monitor the security posture and risk to CPS. To illustrate the use of these metrics, we use cyber-physical models of WSCC 9-bus and IEEE 39-bus test systems created following the methodology used by Cyber Physical Security Assessment (CyPSA) framework [4], [5], [20]. In contrast to previous work where graph measures have been used to study and analyze computer and communication networks (*e.g.,* [6]), to study electrical networks (*e.g.,* [7], [8]), we use them with attack graphs for risk assessment. Work-flow based security assessment framework proposed and demonstrated for the case of Advanced Metering Infrastructure in [3] is similar but did not consider the electrical grid. A very closely related work is

[1] http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[2] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

security-oriented stochastic risk management index, CPIndex, to measure the security of the cyber-physical network. They build stochastic Bayesian network models using topology of power networks and used belief propagation algorithms on these models to compute the indices where as we use simpler attack graphs. Our metrics provide a novel way to identify and prioritize assets critical to the system and help operators prioritize steps to improve the overall security posture of the system.

II. Background

This work builds on the cyber-physical modeling and security assessment framework, CyPSA, developed in [4], [5], [20]. Here we provide some background on the framework to provide the necessary context for the security metrics proposed in this work.

A. Cyber-Physical Models

CyPSA framework uses integrated cyber-physical models of the electric grid infrastructure for security assessment. At a high-level, a cyber-physical model captures the electrical network topology of the grid, the cyber-topology of the control network and their interconnections into an integrated model. Electrical network topology is at the node-breaker level rather than at the bus-branch level. This information in typically available from an Energy Management System (EMS). Cyber-topology includes both that of the control center and substations. Cyber-network topology information is not typically maintained as well as the electrical network topology but today with the advent of commercial tools like NP-View[3] that can infer a network topology using firewall rules it is possible to generate this information very easily.

The interconnections between cyber and electrical topologies are typically control devices likes relays that can open and close breakers or remotely controlled switches, and sensors. This information is typically harder to obtain in an easily ingestable format and in an automated way as there is no standard format and each utility stores and manages this information differently. In some cases this may not even be available in a digital format and is only accessible as CAD drawings.

More details on the components of a cyber-physical model of the kind used by CyPSA and their representation can be found in [19]. With devices like digital relays that can open or close power lines it is plausible for a cyber-attacker to impact the physical system through remote attacks especially when such devices are remotely accessible typically for remote configuration and maintenance. An integrated cyber-physical model allows one to study the risk of cyber-attack induced electrical outages and their impact on the system operation and energy delivery function.

B. Attack Graphs

In particular, CyPSA generates an attack graph leveraging the cyber-physical model and available known-vulnerability information from public vulnerability databases like the National Vulnerability Database (NVD) [2]. An attack graph is a graph representation that captures potential attack paths leading to specific threats (*e.g.,* a line outage in this case) to a given system. In this case the attack graph captures potential attack paths that enable an adversary to impact the physical grid by gaining control over devices like relays that can open or close lines by signaling to breakers. Here each node in the attack graph represents a host or device and each directed edge represents a cyber vulnerability exploitation that allows an attacker to gain control of the destination node by leveraging the presence of a an exploitable vulnerability.

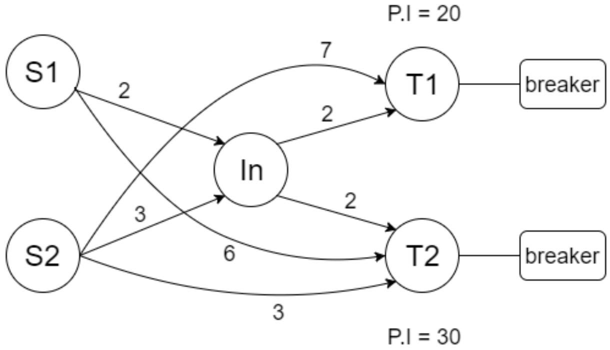

Fig. 1. Sample Attack Graph

1) Attack Cost: In order to assess the risk to the system, it is necessary to understand the chance of a potential threat and its impact on the system. Given the critical nature of electrical grid it is reasonable and prudent to operate under the assumption that it is under constant threat of cyber-attacks. Further, what-if scenario analyses that considers certain elements of the network as being compromised and under adversary control are useful to identify weaknesses in the system's security controls. With this in mind, as was done in the CyPSA framework, we use the cost (C) of launching an attack instead of chance of a threat materializing to assess the risk.

An attack consists of a series of vulnerability exploitations that take an adversary from a source node to a desired target node and is also referred to as an *attack path*. For every vulnerability reported, Common Vulnerability Scoring System (CVSS) [1] provides an exploitability score associated with it. It is expected that the higher the exploitability score the easier it is to exploit the vulnerability. Thus a complementary value of exploitability score normalized to range within the scale of 1 to 10 is used to represent the cost of exploiting the vulnerability. The cost of a an attack then is the summation of costs of exploiting each vulnerability along the path.

2) Attack Impact: The physical impact (PI) of a cyber attack on the electrical network can be captured using a variety of measures. CyPSA focused on the threat of cyber-induced line outages and used *performance index*, which captures the

[3] http://www.network-perception.com

TABLE I
NOTATIONS USED

Literal	Description
$P.I_i$	Physical impact of losing control over $asset_i$
$C_{min_{ji}}$	Minimum cost attack to compromise $asset_i$ starting at $source_j$
C_{ji}	Cost of attack to compromise $asset_i$ starting at $source_j$
$C_{DMST_{(s)}}$	Directed minimum spanning tree (DMST) based cyber cost to compromise set of assets s
S	Set of source nodes
T	Set of target nodes
In	Set of Intermediate nodes
$j \rightarrow i$	denotes an attack path from j to i
$j \rightarrow_{min} i$	denotes the minimum cost attack path from j to i

flow overloads caused by a line outage, as the impact metric. In this work we also focus on cyber induced line outages but we use load shedding [15] as the impact metric in our illustrations. Load shedding captures the amount of load that needs to be shed to reduce the stress on the grid elements caused by the outage. But the proposed security metrics can be used with performance index or any other suitable physical impact metric.

For scalability of analysis one can classify the nodes in an attack graph into three types: *(i)* Target Nodes, *(ii)* Source Nodes, and *(iii)* Intermediate Nodes or Stepping Stones. Target nodes represent control devices like relays which when taken over by an adversary can impact the physical system directly and are of interest for risk assessment. Source nodes represent nodes that could potentially originate attacks into the system like jump hosts or other externally connected devices. Intermediate nodes are nodes that are not the primary target of an adversary but are used as stepping stones to reach a target node. This classification allows one to identify a set of source and target nodes of interest and focus the analysis on attacks paths from sources to targets. Figure 1 shows a sample attack graph with two source and target nodes and one intermediate node connected by edges indicating the presence of an exploitable vulnerability and associated cost for exploiting the vulnerability. Note that while the figure only shows one edge between two nodes it is possible there might be multiple edges with different or similar costs. In this work we focus on graphs with one minimum cost edge between nodes and reserve analysis of multi-graphs for future work.

Security Index [4] defined as follows is used in CyPSA for risk assessment and identifying critical target, source and intermediate nodes:

$$S.I = \frac{P.I}{C} \tag{1}$$

Here $P.I$ represents the potential physical impact of compromising a node, and C represents cost of minimum-cost attack path. Note that physical impact metrics like performance index are routinely computed in power system operations and are available so in theory a power system operator already know what his critical nodes are from a purely physical impact perspective. However, what is not obvious with a cyber-physical analysis is how difficult or easy it is for an cyber-adversary to access such critical nodes. Thus, security index provide one way to identify critical nodes taking into account both the physical impact and difficulty of imposing that impact from a cyber-attack perspective. For example, if compromise two nodes has the same physical impact then the node that is easy to exploit or gain control over should be prioritized for security efforts and controls. While this is a good first security metric, as we will show in the rest of the paper this metric alone does not provide the full picture. Thus in this work we define and illustrate novel security metrics inspired by network graph metrics.

III. SECURITY METRICS FOR ELECTRIC GRID

In this work we build on the aforementioned security index metric shown in equation 1 to propose multiple security metrics which are defined and discussed next.

A. Metrics for Target Nodes/Assets

This set of metrics focuses on the *target nodes* in the attack graph. Target Nodes are those nodes which when compromised can be used to directly manipulate the physical infrastructure. Protection relays are a good example as they manipulate line connectivity in the grid and could have a significant impact when compromised.

Metric 1: Min-Cost Target Node Security Index
This metric considers the minimum cost attack path to compromise a target node and the impact of the compromise. It is the same as the *Security Index* metric proposed in [20]. Min-cost security index for a target node i is defined as follows:

$$M.T.S.I_t(i) = P.I_i * \frac{1}{\min\limits_{j \in S}(C_{min_{ji}})} \tag{2}$$

Here, $P.I_i$ is the physical impact of compromising the target node i, and $C_{min_{ji}}$ is the minimum cost attack path between a source node j and the target node i. Thus, this metric picks up the minimum cost attack path to the target node i from among minimum attack cost paths corresponding to each source node in the graph. For example, in Figure 1 the Min-Cost Target Node Security Index for target node $T1$ picks from among the minimum cost attack paths to $T1$ from sources $S1$ and $S2$. It is the two hop path through In with a hop cost of 2 each and thus the index is given by,

$$M.T.S.I_t(T1) = 20 * \left(\frac{1}{2+2}\right) \tag{3}$$

Metric 2: Target Node Security Index

While min-cost target node security index helps identify critical nodes that have significant impact and low access costs for an attacker it doesn't provide the full picture. For example, consider two target nodes $T1, T2$ with the same physical impact score. Let us say that target node $T1$ has a lower minimum attack cost path than target node $T2$ but that $T2$ has multiple attacks paths. Presence of multiple attack paths increases the chances that an adversary is able to find one of them. This security metric tries to capture this increased chance for an adversary to find one of the multiple attack paths by considering all attack paths to a target node and is given by

$$T.N.S.I_t(i) = P.I_i * \sum_{j \in S} \frac{1}{C_{min_{ji}}} \tag{4}$$

Here $P.I_i$, and $C_{min_{ji}}$ are defined similar to those in equation 2. Note that $\sum_{j \in S} \frac{1}{C_{min_{ji}}}$ is also referred to as *reachability index* of a node later in the paper. The T.S.I for target $T1$ from Figure 1 which can be reached from the sources $S1$ and $S2$ is given by,

$$T.N.S.I_t(T1) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2} \right) \tag{5}$$

B. Stepping Stone Node Metrics

This set of metrics focuses on the intermediate nodes in the attack graph. Intermediate nodes acts as stepping stones to compromise the target nodes.

Metric 3: Intermediate Node Min-Cost Betweenness Security Index

This metric inspired by the *betweenness centrality* [] captures the importance of intermediate nodes as enablers of minimum cost attack paths between source and target nodes. Min-cost betweenness security index for an intermediate node k is defined as follows:

$$M.B.S.I_{in}(k) = \sum_{\{i,j | i \in T, j \in S, k \in j \rightarrow_{min} i\}} P.I_i * \frac{1}{C_{min_{ji}}} \tag{6}$$

Here $j \rightarrow_{min} i$ denotes the minimum cost attack path from j to i. For example, betweenness security index for the intermediate node In in Figure 1 is calculated based on its presence on the minimum cost attack paths between source nodes $S1, S2$ and target nodes $T1, T2$. As shown in the figure, using the intermediate node In, an attacker has the shortest path from source $S1$ and $S2$ to compromise the target $T1$. Similarly, to compromise the target $T2$, an attacker has the shortest path from source $S1$ using the intermediate node In. But, the shortest path to compromise the target $T2$ from source $S2$ doesn't include the intermediate node. Hence, min-cost betweenness security index for In is given by,

$$M.B.S.I_{in}(In) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2} \right) + 30 * \left(\frac{1}{2+2} \right) \tag{7}$$

Metric 4: Intermediate Node Betweenness Security Index

This metric, similar to T.N.S.I in equation 4, captures the importance of intermediate nodes across all attack paths and is given by

$$B.S.I_{in}(In) = \sum_{\{i,j | i \in T, j \in S, k \in j \rightarrow i\}} P.I_i * \frac{1}{C_{ji}} \tag{8}$$

The total betweenness security index for intermediate node In now considers all the attack paths possible from all sources $S1$ and $S2$ to all targets assets $T1$ and $T2$ that go through In. It is given by,

$$B.S.I_{in}(In) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2} \right) + 30 * \left(\frac{1}{2+2} + \frac{1}{3+2} \right) \tag{9}$$

C. Source Node Metrics

Metric 5: Min-Cost Source Node Security Index

This metric captures the importance of sources nodes by considering the target nodes in the system for which they act as the source of a minimum cost attack and is given by

$$M.S.S.I_s(j) = \sum_{\{i,j | i \in T, j \in S, j \in \min_S (j \rightarrow_{min} i)\}} P.I_i * \frac{1}{\min\limits_{j \in S}(C_{min_{ji}})} \tag{10}$$

For example, in Figure 1, source $S1$ can launch a minimum cost attack path to asset $T1$ but not for asset $T2$. Because, asset $T2$ has a minimum cost attack path from source $S2$. Hence the security index of source $S1$ is given by,

$$M.S.S.I_s(S1) = 20 * \left(\frac{1}{2+3} \right) \tag{11}$$

Metric 6: Source Node Security Index

This metric captures the importance of source nodes considering all minimum cost attack paths originating from this node and is given by

$$S.S.I_s(j) = \sum_{i \in T} P.I_i * \frac{1}{C_{min_{ji}}} \tag{12}$$

To see the difference between M.S.S.I and S.S.I, for the example in Figure 1, the source security index of source $S1$ is given by all the minimum cost attacks that it can launch in order to compromise the assets $T1$ and $T2$. That is,

$$S.S.I_s(S1) = 20 * \left(\frac{1}{2+3} \right) + 30 * \left(\frac{1}{2+2} \right) \tag{13}$$

Note that in the case of M.S.S.I we only consider an attack path from a source j to target i if that is the minimum cost attack path to i among all attack paths to it. In contrast, in S.S.I we consider the minimum attack paths originating from a given source to all targets in the graph.

D. Overall Security Metric

Metric 7: Total Security Index

This metric aims to capture the overall security posture of the network. This can be helpful for tracking the progress of security efforts and also helping with prioritizing security controls. Total security index captures the overall risk of the system to cyber-induced outages and is defined as follows

TABLE II
PRIORITIZATION OF CONTINGENCIES BY SECURITY METRICS FOR 9-BUS

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	(M.T./M.B./M.S.) S.I.	Total Reach-ability Index	(T.N./B./S.) S.I.
10.37.1.101	Line (2-7)	Target	163(island, generator)	0.48828	79.5896	1.2501	203.7663
10.37.1.103	Line (5-7)	Target	31.5	0.4167	13.1261	0.4167	13.1261
10.37.1.102	Line (7-8)	Target	22.5	0.29411	6.6175	0.48828	10.9863
10.34.1.103	Line (4-6)	Target	22.5	0.2616	5.886	0.37037	8.333
10.36.1.102	Line (6-9)	Target	0	0.33298	0	0.33298	0
10.39.1.101	Line (8-9)	Target	0	0.4167	0	0.4167	0
10.37.1.250	Line (2-7),(5-7),(7-8)	Intermediate	217	n/a	86.2071	n/a	98.633
10.36.1.250	Line (6-9),(4-6)	Intermediate	22.5	n/a	0	n/a	5.698
10.40.1.22	Line (2-7),(4-6),(5-7),(6-9),(7-9),(8-9)	Source	239.5	n/a	105.2192	n/a	188.4623
72.36.82.194	Line (2-7)	Source	163	n/a	0	n/a	53.65

TABLE III
PRIORITIZATION OF CONTINGENCIES BY SECURITY METRICS FOR 39-BUS

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	(M.T./M.B./M.S.) S.I.	Total Reach-ability Index	(T.N./B./S.) S.I.
10.52.1.102	Line (21-22)	Target	1000*(does not converge)	0.4167	416.7	0.4167	416.7
10.61.1.102	Line (6-31)	Target	200*(2 islands, generator, load)	0.48828	97.656	1.2501	250.02
10.40.1.103	Line (10-32)	Target	316.1(2 islands, generator)	0.37037	117.063	0.37037	117.063
10.44.1.101	Line (13-14)	Target	82.12(cascade)	0.708616	58.1915	0.8265	67.8722
10.45.1.103	Line (15-16)	Target	82.12(cascade)	0.48828	40.0976	0.8265	67.8722
10.64.1.101	Line (20-34)	Target	0(2 islands, generator)	0.4167	0	0.4167	0
10.46.1.250	Line (16-21),(16-24),(15-16)	Intermediate	82.12	n/a	40.0976	n/a	40.0976
10.70.1.22	Line (21-22),(13-14)	Intermediate	1000*	n/a	58.1915	n/a	386.2
10.70.1.22	Line (21-22),(6-31),(10-32),(13-14),(15-16),(20-34)	Source	1000*	n/a	1128.42	n/a	1128.42
72.36.82.194	Line (21-22)	Source	1000*	n/a	416.7	n/a	580.34

$$T.S.I = \sum_{i\in T} M.T.S.I_t(i) = \sum_{j\in S} M.S.S.I_s(j) \qquad (14)$$

An overall security metric that is expressed in terms of T.N.S.I or S.S.I may also be useful. Similarly, variations of B.S.I that take coordinated attacks into account can also be defined. Further we haven't explored metrics for coordinated attacks in this work. These and other variations will be considered in future work. We now proceed to illustrating the proposed metrics using cyber-physical models of test systems.

IV. Illustration of Proposed Security Metrics

A. Setup

In order to illustrate the proposed security metrics on a more realistic attack graph than the one from Figure 1, we use cyber-physical models for the WSCC 9-bus and IEEE 39-bus test models. Cyber-physical model for WSCC 9-bus system is derived from the model used in CyPSA [4], [5] Framework and described in [19]. Cyber-physical model for the IEEE 39-bus test system is created using the approach used in [4], [5]. In a nutshell, synthetic but realistic cyber-topologies are created including a list of services and software running on the hosts in the topology. Vulnerabilities associated with each service or software are queried from the national vulnerability database. The bus-branch electrical model is converted into a nod-breaker model using commonly used bus configurations (ring bus in this case) and associated protection schemes for which templates have been developed in [19]. For each case system, we simulated several line-outage and bus-outage combinations using the Cascading Outage Simulator with Multiprocess Integration Capabilities (COSMIC) [15] tool. Load shed is used a measure for physical impact of the outage. Number of faults and their locations in each combination are selected based on similarity of vulnerabilities present in the cyber infrastructure.

B. Security Metrics for Test Systems

1) WSCC 9-Bus: It is known as Western System Coordinating Council (WSCC) 9-bus testing system. There are three generation sets and three loads located on a loop structure. Based on the cyber attack graph generated we were able to identify 8 target nodes. Among those we have presented the indices for 6 target nodes[4] in Table II. As seen, contingency of line (4-6) and line(7-8) lead to load shed the same amount $22.5MW$ but they have different reachability numbers with the node controlling line (7-8) being slightly more reachable leading to a security index.

In addition the table also shows that node (10.37.1.250) that controls bus 7 is a crucial intermediate node as it can be leveraged to attack relays controlling three lines and can shutdown the whole bus leading to a large load shed as is reflected by both M.B.S.I. (86.2) and B.S.I. (98.63) for that node. Similarly we have identified two main attack source nodes, namely, FTP server and DMZ Jumphost. Among those DMZ Jumphost as expected has a higher security index as it is typically used to connect to many other nodes.

2) 39-Bus: It is known as New-England test system with 10 generations, 19 loads, and 46 lines. Using a setup similar to the one used for 9-bus test system, we have identified 19 target nodes in the attack graph. Table III shows indices for 6 of them. It is interesting to note that when considering only the physical impact, attack leading to outage of line (10-32) has higher priority than the one for line (6-31), but when all attack paths are taken into account line (6-31) that causes a lower amount of load shed comes out at the top. For cases where the power simulation do not converge or creates island, generator or load isolation were given big numbers to showcase their importance on physical impact side. In this case the relative ordering of intermediate and source nodes happens to line up along the lines of their physical impact.

C. Limitations

The illustration of metrics shows that for a given configuration the proposed metrics are able to identify critical cyber assets under different conditions and consequently can help prioritize limited cyber security resources. However, it is important to keep in mind that the synthetic cyber-physical models are used for illustration purposes and that the ranking of assets could be very different with a different model. Further, the absolute values for the security indexes themselves do not have any inherent meaning but can only provide relative ordering among assets. Further research is also needed to understand how to interpret the magnitude of differences between security indexes of different assets.

V. Conclusion

Good Security metrics can be a very useful tool to prioritize security efforts and to track progress. However, good security metrics are hard to design and validate given the uncertainty introduced by unknown and continuously evolving quantities such as unknown vulnerabilities, attacker capabilities etc. In this work we take a first step towards defining multiple cyber-physical security metrics for electrical grid infrastructures and illustrating their value in relatively ranking critical assets. However, further research is needed to validate these metrics in the real world and understanding how to interpret the differences in their absolute values.

Acknowledgement

The authors would like to thank the CyPSA team and Jiajia Song for their help during the work. The material presented in this paper is based upon work supported in part by the Department of Energy under Award Numbers DE-AR0000342 and DE-OE0000780. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] Common vulnerability scoring system. [online]. available: https://nvd.nist.gov/cvss.cfm.

[2] National vulnerability database. [online]. available: http:// nvd.nist.gov/.

[3] B. Chen, Z. Kalbarczyk, D. M. Nicol, W. H. Sanders, R. Tan, W. G. Temple, N. O. Tippenhauer, A. H. Vu, and D. K. Yau. Go with the flow: Toward workflow-oriented security assessment. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 65–76. ACM, 2013.

[4] K. Davis, R. Berthier, S. Zonouz, G. A. Weaver, R. B. Bobba, E. J. Rogers, P. W. Sauer, and N. D. M. CCyber-Physical Security Assessment (CyPSA) for Electric Power Systems, 2016.

[5] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer. A cyber-physical modeling and assessment framework for power grid infrastructures. *Smart Grid, IEEE Transactions on*, 6(5):2464–2475, 2015.

[6] L. C. Freeman. A set of measures of centrality based on betweenness. *Sociometry*, pages 35–41, 1977.

[7] M. Halappanavar, Y. Chen, R. Adolf, D. Haglin, Z. Huang, and M. Rice. Towards efficient nx contingency selection using group betweenness centrality. In *High Performance Computing, Networking, Storage and Analysis (SCC), 2012 SC Companion:*, pages 273–282. IEEE, 2012.

[8] P. Hines and S. Blumsack. A centrality measure for electrical networks. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, pages 185–185. IEEE, 2008.

[9] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke. Model-based security metrics using adversary view security evaluation (advise). In *Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on*, pages 191–200. IEEE, 2011.

[10] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W. H. Sanders. Adversary-driven state-based system security evaluation. In *Proceedings of the 6th International Workshop on Security Measurements and Metrics*, page 5. ACM, 2010.

[11] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham. Validating and restoring defense in depth using attack graphs. In *MILCOM 2006-2006 IEEE Military Communications conference*, pages 1–10. IEEE, 2006.

[12] M. A. McQueen, T. A. McQueen, W. F. Boyer, and M. R. Chaffin. Empirical estimates and observations of 0day vulnerabilities. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–12. IEEE, 2009.

[13] S. Noel and S. Jajodia. Metrics suite for network attack graph analytics. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, pages 5–8. ACM, 2014.

[14] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest-adversary security metric for network configuration security analysis. In *Proceedings of the 2nd ACM workshop on Quality of protection*, pages 31–38. ACM, 2006.

[4] All indices will be presented in the full version of the paper.

[15] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. Hines. Dynamic modeling of cascading failure in power systems. *IEEE Transactions on Power Systems*, 31(3):2085–2095, 2016.

[16] V. Verendel. Quantified security is a weak hypothesis: A critical survey of results and assumptions. pages 37–50, 2009.

[17] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. An attack graph-based probabilistic security metric. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 283–296. Springer, 2008.

[18] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel. k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, 11(1):30–44, 2014.

[19] G. A. Weaver, K. Davis, M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and N. D. M. Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case. In *International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016.

[20] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders. SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures. *IEEE Transactions on Smart Grid*, 5(1):3–13, 2014.