Multi-Component Risk Assessment Using Cyber-Physical Betweenness Centrality

1st Amarachi Umunnakwe
Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA
amarachi@tamu.edu

2nd Abhijeet Sahu
Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA
abhijeet_ntpc@tamu.edu

3rd Kate Davis
Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA
kate.davis@tamu.edu

2021 IEEE Madrid PowerTech | 978-1-6654-3597-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/PowerTech46648.2021.9494796

***Abstract*—Identifying important assets and evaluating the risk they pose to cyber-physical power systems, when compromised, is critical to maintaining the system security and resilience. The cyber-physical betweenness centrality (CPBC) index presents a suitable means for enhancing system resilience through vulnerability analysis and risk assessment. In this paper, we propose and demonstrate the CPBC for the multi-component risk assessment of the cyber-physical power grid. Specifically, the CPBC, based on the concept of betweenness centrality, traverses generated attack graphs to rank important components, while integrating the services, security cost of inter-component communication, and the likelihood of component exploitation as an adversary medium to the target relays. The CPBC index notably categorizes components in the same security caliber, hence simplifying computation for the system operator. The proposed model is implemented on the Cyber-Physical Situational Awareness 8-substation cyber-physical power system model and results demonstrate to the power system operator, the combinations of components to which security resources should be allocated.**

***Index Terms*—Cyber-physical betweenness centrality, multi-component ranking, risk assessment, attack graph**

I. Introduction

Power grids in modern societies are critical to national security and hence should be resilient to adversaries. Adversarial threats are increased by the integration of information technology, which although are essential and beneficial to smart grids, can introduce potential attack vulnerabilities [1]. These threats can exploit control assets in the power grid to cause data breaches, asset damage and outages. For instance, the 2015 Ukranian attack enabled the adversary to gain control of system circuit breakers, causing six hours of power outages for thousands of customers [2]. In order to be prepared for these anomalies, the system operator usually performs risk assessment to provide situational awareness of the power grid.

The power grid is a complex interdependent network consisting of physical devices for measurement, sensing and control, and cyber assets such as internet hosts for data acquisition, and communication services, where anomalies in the cyber layer can have repercussions in the physical layer and vice versa [3]. These increasing interdependencies also increase exploitable paths to critical devices, making monitoring intractable for operators and consequently, the grid becoming a "honey pot" for adversarial attacks [4].

Predominantly, the vulnerability of the cyber-physical power grid to adversarial threats has been assessed based on graph theory. Graph theory can be utilized to improve contingency analysis by modeling the system as a weighted graph, where priority is assigned to edges/vertices with the most connection paths passing through [5]. A graph can represent system topology, where vertices are components such as internet hosts and relays, while edges are communication links between vertices. Using this approach, [6] estimates cyber layer impacts on the physical system through cost-effect analysis. In [7], [8] contingency analysis is utilized to identify high-risk Markov Decision Processes [9], while quantifying physical system impact. In [10], centrality and electrical characteristics are utilized to identify critical vertices. In [5], parallel betweenness centrality is applied to power grid contingency selection in real-time, to aid operators to identify and mitigate potential widespread cascading failures. In [11], systematic investigation of topological and electrical characteristics is performed for power grid networks based on real and synthetic grid data, while in [12], the authors rank the importance of the grid vertices and lines based on centrality measures and other characteristics.

These topological methods also provide a variety of metrics toward identifying the most critical components in an electric grid [13]–[16]. In [17], effective graph resistance is utilized as a metric to assess the robustness of power grids against cascading failure, identifying the best pair of connectivity vertices toward optimizing the metric, while in [18], the group betweenness centrality approach is employed to identify multiple critical components with severe consequences on the power system when failed. Moreover, researchers have been extending test systems to emulate real cyber characteristics, featuring communication networks and cyber-physical interconnections that are salient in the control of power systems [7], [19], [20]. These communication networks could potentially be penetrated from multiple potential vectors, including through external connections and internal internet hosts.

Although there has been a great amount of research in regards to investigating the risk of the physical grid, less atten-

This work was supported by the US Department of Energy under award DE-OE0000895 and the National Science Foundation under Grant 1916142.

978-1-6654-3597-0/21/$31.00 ©2021 IEEE

tion has been accorded the interdependent cyber-physical risk of the power system. Hence, cyber-physical risk assessment as a fundamental power system monitoring tool would allow the operator knowledge of expected system performance in the case of an adversary threat, and can thus aid in preparing the system operators for possible scenarios by ranking equipment according to access, vulnerability, and impact.

This paper investigates the effects and mitigation of the vulnerability of multiple components on the adversary impact (number of exploitable power system paths). More specifically, in this paper we present a multi-component cyber-physical operation model, m-CRSA, that ranks cyber and physical components in order of importance toward minimizing the interdependencies that the adversary can exploit. From a physical perspective, the cyber-physical betweenness centrality (CPBC) index of the m-CRSA offers flexible cyber vulnerability integration, security-oriented risk awareness and management in power system risk sensitivity analysis. In particular, it efficiently ranks components based on cyber network configuration, whereas from a cyber perspective, control network's common vulnerability exposure (CVE) scores are also integrated according to the underlying power system topology, and the result is components ranked in security tiers. The model effectively investigates attack and defense from adversary and system operator perspectives simultaneously, as an algorithm is presented that protects critical components in order to demonstrate the efficiency of the proposed model.

The rest of this paper is organized as follows. Section II presents the cyber-physical model for integrating cyber vulnerability into the power system, while the proposed ranking and multi-component risk assessment is furnished in Section III. The simulation results on an 8-bus test system are presented in Section IV, and conclusions are drawn in Section V.

II. Cyber-Physical Power System Vulnerability Modeling

Although it is quite improbable that an adversary accesses all information required to attack, but as with high impact low probability events, the probability $\rightarrow 0$ until event occurs and the probability is 1. Therefore, we assume the adversary has access to the grid topology information and can carry out an attack based on component vulnerability and graph theory [21]. In this section, we explain how the system information is used to determine the state of the cyber-physical network.

The attack graph provides information on the potential paths an adversary could take to reach target components given the possible points of intrusion. It is generated [1] from system connectivity and topology information. The connectivity file is generated based on the access control list configured in each firewall [22], while the cyber topology is generated by NP-View [24]. Given the connectivity matrix, the security state of the system is evaluated by assigning scores, referred to as cyber costs, to communication links between connected components. Component connectivity is stored in three elements:

[1]Based on our work in security assessment [7], [22], available online [23].

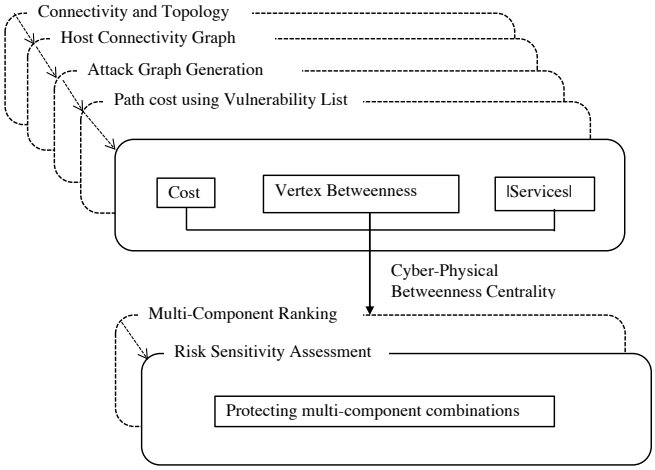

Fig. 1: Multi-Component Ranking and Risk Sensitivity Assessment Model (m-CRSA).

1) source object; 2) sink object; and 3) their security cyber cost (CC).

The security state of the system can be evaluated, as we assume that the adversary gains access into the network and can reach the target relays through internet hosts. For instance, an attack source vertex may leverage knowledge of required username and password to remotely access another sink vertex with hard-coded SSH credentials by exploiting the vulnerability `CVE-xxxx-xxxx` with a score, hence the path between the two vertices will be weighted on the cyber costs (CC) which are computed based on the Common Vulnerability Scoring System (CVSS) scores obtained from the National Vulnerability Database (NVD) [25]. Further details on system vulnerability modeling and attack graph generation using the system connectivity matrix, cyber topology and host connectivity can be found in our work [26].

III. Component Ranking and Risk Assessment

If data flows from object v_i to v_j, then object v_j is dependent on v_i and the dependency is represented by the network edge $e_{ij} = v_i \rightarrow v_j$. We represent G as a pair of vertex and edge sets (V, E), with $V = \{v_1, v_2, v_3, ..., v_n\}$, and $E = \{e_1, e_2, e_3, ..., e_m\}$ with individual weights $CC(e) \rightarrow \mathbf{R}^+$. From one cyber vertex to another, the interdependency is the data flow or service, while from a cyber to physical vertex the interdependency is the commands (control) to the relay.

The goal is to discover effective operator strategies to reduce overall system vulnerability (number of attack paths exploitable by adversary). Thus, we obtain possible attack scenarios towards component ranking, using the CPBC index [26]. In particular, the CPBC incorporates the CC in (1), representing severity(operator-side)/vulnerability(adversary-side) of compromising services between vertices,

$$CC(e) = \sum_{e \in E} \min V_e \tag{1}$$

where V_e are vulnerability scores from the NVD, and the cost metric associated with realizing an attack edge is obtained

from the CVSS with a script that extracts exploitability subscores using access complexity and authentication scores [9].

The goal of the system operator remains mitigating system threats. Toward this, the m-CRSA utilizes the CPBC to rank components given possible cyber-originated intrusions that target physical power system control components. The CPBC, as in (2), utilizes computed shortest paths (important vertices have a greater chance to lie on multiple vulnerability-weighted shortest paths to target relays), the cardinality of services, and CC of communication links, to calculate a unified cyber-physical ranking for the entire network. Hence for the system operator, the higher the number and cost of services running on a vertex, the more important (highly critical node).

$$CPBC(v) = \sum_{s \neq v \neq t \in V} \sigma_{st}(v) \times \varepsilon \times \frac{1}{\sum^{e_v} \left(\frac{1}{CC(e)} \right)}, \qquad (2)$$

where $\sigma_{st}(v)$ is the number of shortest paths, as in Algorithm 1, from source vertex s to target vertex t that pass through the vertex v with edges weighted on the communication link cyber costs, and e_v is the set of all edges to/from v, with cardinality of ε which proportional to the vertex density in the network. We use the reciprocal of the CC to weigh the vertices in the cyber-physical topology graph to make computation consistent with the cyber vulnerability concept discussed. Another important advantage of this setup is that it allows for the grouping of vertices in the same security tier as further illustrated in the result section.

Next, the risk sensitivity assessment proceeds with prioritized protection of ranked components while the impact of protection towards reducing the system's vulnerability is measured. The aim here is to provide the system operator enough information about the combination of components she chooses to protect in order to make monitoring tractable during threats. As illustrated in Algorithm 2, protecting critical vertices follows with the removal of y% of vulnerabilities of components in $S*$ in the attack graph G, generating a new attack graph, H, subgraph of G, with attack paths $\leq G$.

Algorithm 1 Obtaining Node Importance

```
Select IP of targeted relays, Physical_vertices
Select IP of Internet vertices, Cyber_vertices
function node_importance(vertices)          ▷ vertices: Generated Attack graph unique vertices
    for relay in Physical_vertices do
        for host in Cyber_vertices do
            weighted shortest paths  ▷ Get list of shortest paths, SPL, unless host=relay  ▷ Pass exception if no path
            for short_path S in SPL do
                for node in vertices do
                    if vertex in short_path then
                        unique_node_importance += 1
                    end if
                end for
            end for
        end for
    end for
return node_importance, σ_st(v), (for the ranking index)
end function
```

Algorithm 2 Protecting Important Vertices

```
function Generate_Attack_Graph, H(G, L, sel_t)
    Create empty attackGraph, H
    Get set, S*, of components to be protected
    Get CC(e) (vuln_list) of x ranked components in S*.
    for component in S* do
        v_list = Get(vuln_list - y% of vuln_list)
        new_path = get_path(G, v_list)
        for adversary a in L do
            d,p = djikstra_shortest_path(a,G)
            for target t in d do
                if t in L then
                    path = G(t)      ▷ get the path from G
                    Add path to attackGraph, H
                end if
            end for
        end for
    end for
return new_attackGraph, H
end function
```

The formulation of the protection algorithm is as follows. Let E_1 be the set of edges with links to a unique vertex v_1, in the set [v_1,v_2,..., v_m], in the attack graph G, and E_1^c be the set of edges with links to critical vertex v_1^c in the attack graph H. Then, the list of edges E_1^c is defined as unique row entries with all but y% of the edges of the original set E_1, where $E_1^c \in E_1 \in E$. Hence, for multi-components, the set of edges E^*, from set V^*, not in H is:

$$E^* = \sum_{1}^{|V^*|} \frac{y}{100} \quad of \quad E_i \quad \text{for } i = 1, 2, \ldots, m. \qquad (3)$$

where y is a 100% to remove any bias in analysis. Hence the total number of exploitable paths in the new attack graph H, is reduced by paths formed by E^*, which is the improvement, i.e., reduction in paths accessible to adversary, that increased protection of critical vertices provides the system operator.

IV. Study Results

The proposed model for multi-component risk assessment is implemented on an 8-substation test case [19] including components such as hosts, routers, remote terminal units, with details available in [23]. Results are obtained with an i7 1.80 GHz processor and 16 GB of RAM computer. The results presented are threefold: first, is the ranking of the power system cyber-physical components. Secondly, we demonstrate the important characteristic of the CPBC, which is the grouping of the components in security tiers for multi-component risk assessment. Thirdly, we present the multi-component assessment risk tables that would be provided to the power system operator for optimal protection strategy and

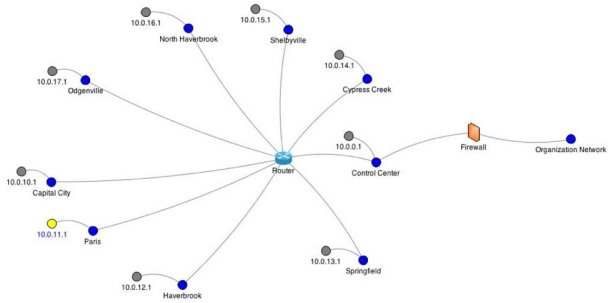

Fig. 2: The cyber topology of the 8 substation model [19].

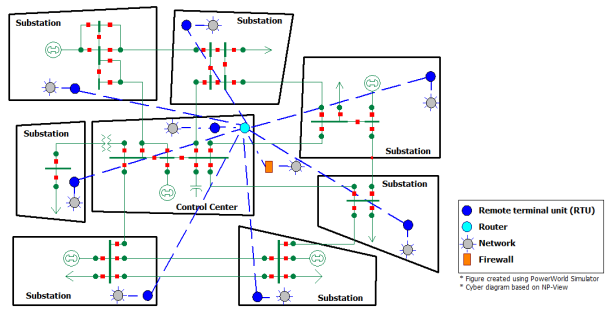

Fig. 3: The cyber-physical topology of the 8 substation model [19].

assess the model accuracy. Lastly, we furnish an illustration of the power system operator strategy.

In the first case, we implement the ranking model on the test cases with results in Table I which furnishes the component ranks, calculated CPBC value, unique component ID and types, respectively. For instance, Host PC with ID 1896 and rank 1, reduces adversary security impact on the system by 12.95% when protected, as observed from Table II. Furthermore, a unique characteristic of the CPBC ranking which is important to the power system operator is the capacity to rank components in security tiers. For example, there are 4 components in the security rank 2, which means that protecting any of these components will reduce system attack paths by an equal percentage. In Table II, we illustrate the functionality of the multi-component security tiers. We observe that combinatorially protecting any members of unique groups reduces attack paths by the same amount. For instance, protecting components (1896,2018) or (1896,2004) will produce similar results as they are from tiers 1 and 2, respectively. This is important for the system operator to gain on computational and time complexity, and improve her system security knowledge.

Next, the proposed model is implemented to evaluate the multi-component risk assessment aiding strategy (Fig. 4). After component ranking, the vertices are protected as in Algorithm 2, by reducing the vulnerabilities associated with that vertex by 100% (to eliminate bias), hence deterministically patching the vulnerabilities and producing new attack graph H as illustrated in (3) with decrease in attack paths as furnished in Table III. Column 2 presents the rank/security tier to which components belong, column 3 represents the total number of attack paths present in H, while column 4 furnishes the percentage decrease in attack paths from G to H. As expected and observed from the tables, there is a

TABLE I: Component ranking: 8 substation test case

Rank	CPBC	Vertex ID	Component Type
1	0.0652	1896	Host PC
2	0.0583	[2018,2020,2004,2006]	[Overcurrent relay x2, Distance relay x2]
3	0.0528	[2014,2016,1998,2000,2002,2008,1996]	[Overcurrent relay x2, Distance relay x4, Host PC]
4	0.0476	2012	Overcurrent relay
5	0.0304	1930	Overcurrent relay
6	0.0282	[1920,1922,1924,1926,1928]	[Overcurrent relay x5]
7	0.0175	2024	Distance relay
8	0.0105	[1938,1940,1942,1934,1936,1932]	[Overcurrent relay x3, Distance relay x2, Host PC]
9	0.0067	2022	Host PC
10	0.0061	[2010,1877]	[Distance relay, Router/Switch]
11	0.0015	[1916,1918,1910,1912,1914,1870]	[Overcurrent relay x2, Distance relay x3, Router/Switch]
12	0.0013	1871	[Router/Switch]
13	0.0007	1878	[Router/Switch]
14	0.0005	1894	Host PC
15	0.0003	[1898,1900,1902,2030]	[Host PC x3, Router/Switch]

decreasing trend in attack paths given different combinations of components according to their declining security tiers. This trend of reduction in attack paths as visualized in Fig. 5, illustrates the accuracy of the ranking model. For example, protecting two components ranked in groups 1 and 2, will decrease the number of exploitable attack paths by a higher percentage than protecting two components ranked in groups 1 and 3. The accuracy of the proposed model over one-to-five component protection, as in Table III, is assessed in Fig. 6, showing that the model performance is high with 84% accuracy and a few mispredicted ranks, given the decrease

TABLE II: Illustrating the security categories of the components as ranked by the CPBC index

Protecting any member of the first group by CPBC		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896	68398	12.960
[2018, 2020, 2004, 2006]	70469	10.324
[2014, 2016, 1998, 2000, 2002, 2008, 1996]	70860	9.827
2012	71256	9.323
1930	75097	4.435
[1920, 1922, 1924, 1926, 1928]	75063	4.478
2024	74991	4.570
[1938, 1940, 1942, 1934, 1936, 1932]	75267	4.219
2022	76080	3.184
[2010, 1894, 1875, 1892, 1877, 1870, 1871, 1916, 1910, ...]	78582	0.000
Protecting members of the first and second groups by CPBC		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896, 2018	60646	22.8
1896, 2020	60646	22.8
1896, 2004	60646	22.8
1896, 2006	60646	22.8
Protecting members of the first and third groups by CPBC		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896, 2014	61018	22.3
1896, 2016	61018	22.3
1896, 1998	61018	22.3
1896, 2000	61018	22.3
1896, 2002	61018	22.3
1896, 2008	61018	22.3
1896, 1996	61018	22.3
Protecting members of the first, second, and third groups by CPBC		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896, 2018, 2014	53950	31.3
1896, 2020, 2016	53950	31.3
1896, 2004, 1998	53950	31.3
1896, 2006, 2000	53950	31.3
1896, 2018, 2002	53950	31.3
1896, 2020, 2008	53950	31.3
1896, 2004, 1996	53950	31.3
Protecting members of the first, second, third, and fourth groups by CPBC		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896, 2018, 2014, 2012	48204	38.66
1896, 2020, 2016, 2012	48204	38.66
1896, 2004, 1998, 2012	48204	38.66
1896, 2006, 2000, 2012	48204	38.66
1896, 2018, 2002, 2012	48204	38.66
1896, 2020, 2008, 2012	48204	38.66
1896, 2004, 1996, 2012	48204	38.66

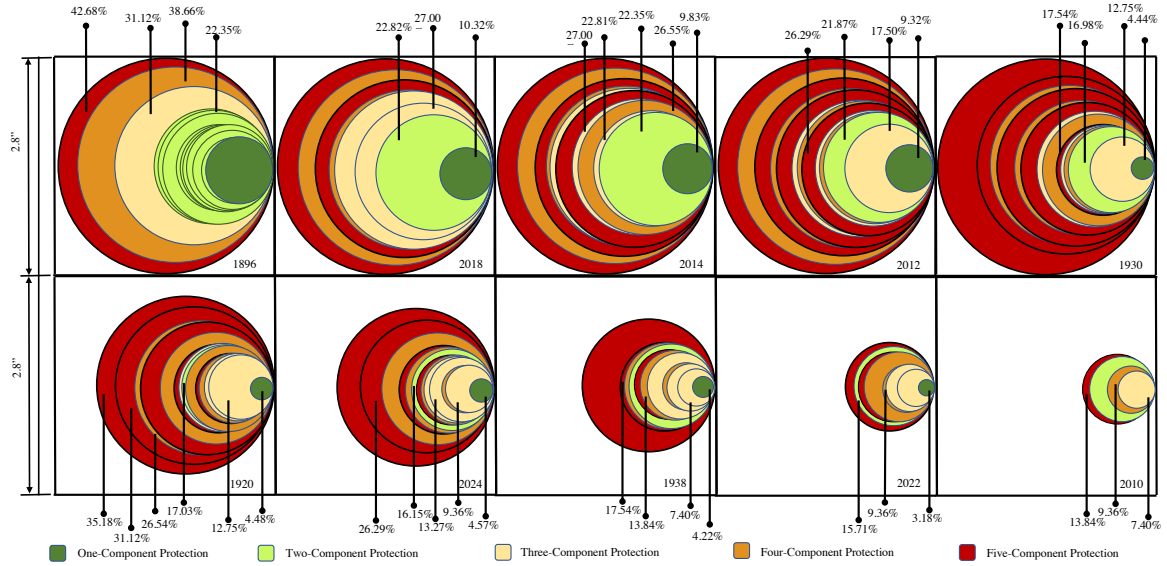

Fig. 4: Demonstrating the multi-component protection strategy (from the risk attack tables) enhancing Economics, Security, and Resilience: Colors from green to red represent low to high economic commitment. Number and size of circles in unique squares is proportional to resilience improvement and security enhancement, respectively, attainable by that component's protection

TABLE III: Multi-Component Risk Attack Tables

Two-Component Protection			
Protected vertex ID	Component Rank (group)	Final No of Attack paths	% Decrease attack paths
1896, 2018	1, 2	60646	22.82456542
1896, 2014	1, 3	61018	22.35117457
1896, 2012	1, 4	61394	21.87269349
1896, 1930	1, 5	65237	16.98226057
1896, 1920	1, 6	65202	17.02680003
1896, 2024	1, 7	65890	16.15128146
1896, 1938	1, 8	65406	16.7671986
1896, 2022	1, 9	66238	15.70843196
1896, 2010	1, 10	68398	12.95971088
Three-Component Protection			
Protected vertex ID	Component Rank (group)	Final No of Attack paths	% Decrease attack paths
1896, 2018, 2014	1, 2, 3	53950	31.34560077
2018, 2014, 2012	2, 3, 4	57362	27.00363951
2014, 2012, 1930	3, 4, 5	60660	22.80674964
2012, 1930, 1920	4, 5, 6	64829	17.50146344
1930, 1920, 2024	5, 6, 7	68565	12.74719401
1920, 2024, 1938	6, 7, 8	68157	13.26639688
2024, 1938, 2022	7, 8, 9	71226	9.360922349
1938, 2022, 2010	8, 9, 10	72765	7.402458578
Four-Component Protection			
Protected vertex ID	Component Rank (group)	Final No of Attack paths	% Decrease attack paths
1896, 2018, 2014, 2012	1, 2, 3, 4	48204	38.65770787
2018, 2014, 2012, 1930	2, 3, 4, 5	53877	31.43849737
2014, 2012, 1930, 1920	3, 4, 5, 6	57719	26.549337
2012, 1930, 1920, 2024	4, 5, 6, 7	61238	22.07121224
1930, 1920, 2024, 1938	5, 6, 7, 8	65250	16.96571734
1920, 2024, 1938, 2022	6, 7, 8, 9	67707	13.83904711
2024, 1938, 2022, 2010	7, 8, 9, 10	71226	9.360922349
Five-Component Protection			
Protected vertex ID	Component Rank (group)	Final No of Attack paths	% Decrease attack paths
1896, 2018, 2014, 2012, 1930	1, 2, 3, 4, 5	45042	42.68153012
2018, 2014, 2012, 1930, 1920	2, 3, 4, 5, 6	50936	35.18108473
2014, 2012, 1930, 1920, 2024	3, 4, 5, 6, 7	54128	31.1190858
2012, 1930, 1920, 2024, 1938	4, 5, 6, 7, 8	57923	26.28973556
1930, 1920, 2024, 1938, 2022	5, 6, 7, 8, 9	64800	17.53836757
1920, 2024, 1938, 2022, 2010	6, 7, 8, 9, 10	67707	13.83904711

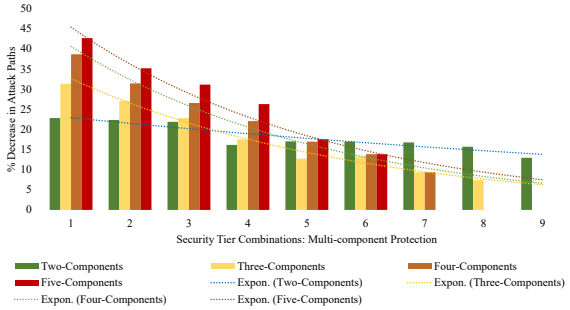

Fig. 5: Decreasing trend in attack paths illustrated in Table I

in attack paths, between IDs 2024 and 1930.

Finally, the system operator (OP) aims for a balance between system resilience, economics and security as in Fig. 7.

Actual Rank \ Predicted Rank	1896	2018	2014	2012	2024	1920	1930	1938	2022	2010
1896	5									
2018		5								
2014			5							
2012				5						
2024					2		1	2		
1920						4	1			
1930					1	1	3			
1938					2			3		
2022									5	
2010										5

Fig. 6: Accuracy: Confusion Matrix

Toward this objective, the m-CRSA provides the strategy demonstrated in Fig. 4, where colors from green-to-red represents budgetary increase (protecting two or more components is ideally more expensive than protecting one component), the number of circles present in unique component squares is proportional to system resilience (reduction in attack paths attained by protecting unique components improves robustness

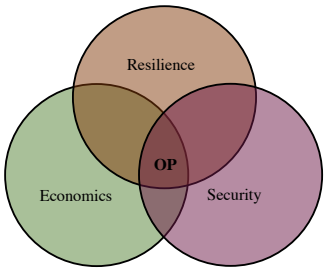

Fig. 7: System operator decision strategy.

against attacks by reducing attacker reachability), and sizes of the circles (% decrease in attack paths) represents improvements in system security by eliminating certain vulnerabilities. Generally, resilience and security improves by protecting more components but economics suffers i.e., ideally assuming costs increase as more components are protected. In particular, some components (e.g., routers) may have higher protection costs than others (e.g., host computers which may just require software downloads), however, it is out of this paper's scope to model these costs. The OP can observe that protecting 1896 improves security and resilience with limited budget, while resilience and security improvements taper towards 2010 even with higher budgets. Table IV shows OP strategy, where ✓ is strong correlation, ✓ implies some correlation, ✗ is negative correlation, and *o* is no correlation.

TABLE IV: Visualizing Results for Operator Strategy

	No. of Circles		Size of Circle		Color of Circle	
	↑	↓	↑	↓	Green	Red
Resilience	✓	✗	✓	✗	*o*	*o*
Security	✓	✗	✓	✗	*o*	*o*
Economics	✓	✗	*o*	*o*	✓	✗

V. Conclusion

This paper proposes a model, m-CRSA, for critically ranking multiple components, which integrates industry standard vulnerabilities into risk assessment of the cyber-physical power system. The model ranks components in security tiers with high accuracy, providing protection prioritization strategy to the system operator. The m-CRSA is implemented on an 8 substation cyber-physical power system. The simulation results show that the system operator will benefit from enhanced knowledge of her system's security, while computational complexities will be reduced due to the attribute of the model to rank components in security tiers, in addition to providing the operator different system protection strategies.

References

[1] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.
[2] J. E. Sullivan and D. Kamensky, "How cyber-attacks in ukraine show the vulnerability of the us power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.
[3] S. M. Amin, "Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems," in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–5.
[4] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.
[5] S. Jin, Z. Huang, Y. Chen, D. Chavarría-Miranda, J. Feo, and P. C. Wong, "A novel application of parallel betweenness centrality to power grid contingency analysis," in *2010 IEEE International Symposium on Parallel & Distributed Processing (IPDPS)*. IEEE, 2010, pp. 1–7.
[6] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.
[7] 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*, vol. 5, no. 1, pp. 3–13, 2013.
[8] 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," *IEEE Transactions on smart grid*, vol. 6, no. 5, pp. 2464–2475, 2015.
[9] K. Davis, R. Berthier, S. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. Sauer, and D. Nicol, "Cyber-physical security assessment (cypsa) for electric power systems," *IEEE-HKN: THE BRIDGE*, 2016.
[10] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 3, pp. 346–350, 2017.
[11] Z. Wang, A. Scaglione, and R. J. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE transactions on Smart Grid*, vol. 1, no. 1, pp. 28–39, 2010.
[12] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *49th IEEE conference on decision and control (CDC)*. IEEE, 2010, pp. 5792–5797.
[13] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, 2014.
[14] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, 2012.
[15] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET generation, transmission & distribution*, vol. 4, no. 6, pp. 716–724, 2010.
[16] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.
[17] X. Wang, Y. Koç, R. E. Kooij, and P. Van Mieghem, "A network approach for power grid robustness against cascading failures," in *2015 7th international workshop on reliable networks design and modeling (RNDM)*. IEEE, 2015, pp. 208–214.
[18] M. R. Narimani, H. Huang, A. Umunnakwe, Z. Mao, A. Sahu, S. Zonouz, and K. Davis, "Generalized contingency analysis based on graph theory and line outage distribution factor," *arXiv preprint arXiv:2007.07009*, 2020.
[19] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 140–146.
[20] P. Wlazlo, K. Price, C. Veloz, A. Sahu, H. Huang, A. Goulart, K. Davis, and S. Zounouz, "A cyber topology model for the texas 2000 synthetic electric power grid," in *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2019, pp. 1–8.
[21] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *PES T&D 2012*. IEEE, 2012, pp. 1–6.
[22] A. Sahu, H. Huang, K. Davis, and S. Zonouz, "A framework for cyber-physical model creation and evaluation," in *2019 20th International Conference on Intelligent System Application to Power Systems (ISAP)*, 2019, pp. 1–8.
[23] [Online]. Available: https://cypres.engr.tamu.edu/test-cases/
[24] "NP-View," [Online]. Available from: https://www.network-perception.com/np-view/.
[25] [Online]. Available: https://nvd.nist.gov/vuln
[26] A. Umunnakwe, A. Sahu, R. Narimani, Mohammad, D. Katherine, and S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," *IET Cyber-Physical Systems: Theory & Applications*, in press.