Distributed Controller Role and Interaction Discovery

Shamina Hossain-McKenzie, Katherine Davis, Maryam Kazerooni, Sriharsha Etigowni*, Saman Zonouz*
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign, Rutgers University*
{shossai2, krogers6, kazeron2}@illinois.edu, {se260, saman.zonouz}@rutgers.edu*

***Abstract*—Distributed controllers have a ubiquitous presence in the electric power grid and play a prominent role in its daily operation. The failure or malfunction of distributed controllers is a serious threat whose mechanisms and consequences are not currently well understood and planned against. For example, if certain controllers are maliciously compromised by an adversary, they can be manipulated to drive the power system to an unsafe state. We seek to develop proactive strategies to protect the power grid from distributed controller compromise or failure. This research formalizes the roles that distributed controllers play in the grid, quantifies how their loss or compromise impacts the system, and develops effective strategies for maintaining or regaining system control. Specifically, an analytic method based on controllability analysis is derived using clustering and factorization techniques on controller sensitivities.**

***Index Terms*–controllability analysis, sensitivity analysis, distributed controllers, controller compromise**

I. Introduction

The smart grid initiative has driven the industry toward increasingly sophisticated systems of sensors, algorithms, and controllers that are involved in widespread communication and online decision-making. Distributed controllers play a prominent role in deploying this cohesive execution and are ubiquitous in their presence in the grid. As global information is shared and acted upon; if one distributed controller fails, the remaining set is quick to respond and ensure the overall control objective is maintained. However, multiple failures can cause detrimental, cascading effects (e.g., overloads leading to blackout) as the set struggles to automatically meet the control goal. Furthermore, if the controllers are maliciously compromised, they can be manipulated to drive the power system to an unsafe or unreliable operating state. Attack vectors for distributed controllers range from execution of malicious commands that can cause damage, to sensitive equipment, to forced system topology changes causing instability.

In this regard, distrusted control can be defined as when controller(s) are compromised and under the command of a sophisticated attacker. This adversary can craft these commands in a legitimate format and thus have them successfully executed in the system. Furthermore, these alterations could be masked to the operator or any security systems. Cyber attacks on the power grid are a serious issue, with about 40% of total critical infrastructure cyber incidents reported to the Department of Homeland Security from 2009 to 2014 occurring in the energy sector [1]. In fact, one of the first large-scale attacks on a power grid occurred in December 2015 in Ukraine, where cyber attacks led to the disconnection of 7 substations and power outage to 80,000 customers for several hours [2]. Additionally, the threat of physical consequences resulting from these cyber attacks has become a serious concern, as demonstrated by [3], [4].

With the modern power grid increasingly being outfitted with publicly available operating systems, network or Internet communication, and third-party software, there are many more access points for an attacker to gain entry. We no longer have the benefit of "security by obscurity" as historically achieved by proprietary control protocols that varied utility to utility – the adversary no longer needs to be deeply knowledgeable of the specific utility system to launch a successful attack [5]. In preventing and mitigating these attacks, specifically on distributed controllers, we must consider: the attack vectors, adversary capabilities, trusted entities, and impact on system controllability and stability.

In this paper, we focus on attacks which disrupt system control resulting from compromised or failed distributed controller(s). As mentioned, controller-based threats include execution of malicious control commands and changes to controller-level code and binaries which may drive the system to an unsafe or unreliable operating state. In particular, this paper provides an analytic solution to help restore the control capability of a system given a controller attack. By identifying the role of each controller, whether they are critical, essential, or redundant to system controllability, we can develop powerful techniques to improve control as well as protect the system. Furthermore, discovering the control support groups that indicate the interaction of the controllers with one another provides useful information. This insight can allow development of systematic method(s) to ensure or regain control of the system given compromise or failure.

II. Power System Controllability

In power systems, there are various components and behaviors we would like to control. We may seek to mitigate the impact of a disturbance or we would like to alter supply at various buses due to load change. Control systems and controllers allow us to enact these changes in system properties such as topology, equipment settings, and system behaviors.

The authors would like to thank the National Science Foundation (NSF): Award Numbers CNS 1446229 and CNS 1446471, ARPA-E: Award No. DE-AR0000233 with Smart Wire Grid, Inc., and PowerWorld Corporation for their support and sponsorship of this research.
978-1-5090-4000- 1/17/$31.00 ©2017 IEEE

However, the effectiveness of these controls, especially to influence behaviors, depends on the controllability of the system. This relies on the controllers (location, distribution, extent of abilities) and the power system itself (topology, constraints). Thus, the controllable region of the system.

The controllable region is the subset of the state space on which the available controls can be used to steer the power system from one state to any other state [6]. In general, the power system dynamical equation can be written as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x}) u_i, \ \mathbf{x} \in \mathbf{\Xi} \tag{1}$$

where $\mathbf{x}$ is an n-vector of dynamic variables, $\mathbf{f}(\mathbf{x})$ is a vector consisting primarily of the power flow equations, and $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x}) u_i$ represents the effects of the controls on the system. The scalars $u_i, \ i = 1, ..., m$, are the system controls and are usually piece-wise constant in time, due to device physical characteristics. System state space, $\mathbf{\Xi}$, is an open subset of the n-dimensional Euclidean space. If we have $X(s_1, u, t) \in \mathbf{\Xi}$ representing the system movement with the initial state s_1, control u, and $0 \leq t \leq \infty$, the controllable region satisfies:

$$X(s_1, u, t) = s_2, \ u \in \mathbf{U} \text{ and } 0 \leq t \leq \infty \tag{2}$$

where every pair of states s_1 and $s_2 \in \mathbf{Z}$ satisfies (2). $\mathbf{Z}$ is the controllable region, a subset of $\mathbf{\Xi}$. Therefore, the system presented in (1) can be steered from a state to any other state within the controllable region. Further proofs and other references can be found in [6]. For this work, we will focus on decomposing the set of controls $\sum_{i=1}^{m} \mathbf{g_i}(\mathbf{x}) u_i$ into the controller role and control support group sets.

Classic linear methods developed for controllability and observability are the Popov, Belevitch, and Hautus (PBH) eigenvector tests using rank conditions [7]. Yet, these tests only provide answers in a "yes or no" fashion—e.g., yes the system is observable or no, the system is not observable. Although useful, more detailed measures of controllability are desired. Hamdan and Elabdalla [8] and Hamadan and Nayfeh [9] proposed using the cosine of the angle between appropriate subspaces to develop a quantified measure for controllability and observability of linear systems. In this manner, the measure is a continuous function of the distance between the two subspaces. Messina and Nayebzadeh [10] formulated a design procedure using modal analysis to derive quantitative controllability and observability measures to place multiple controllers. To check if the controllability or observability matrices are full rank, they examined the number of nonzero singular values and their magnitudes. In this work, we study the role and interaction of each of the controllers in the overall controllability. Similar to the work of Bobba et al. [11] that determined the sets of basic and redundant measurements, we seek to motivate and invoke the use of these and other observability-based methods to also study control.

III. Solution Overview

Using clustering and factorization techniques, the proposed work identifies the essential and critical controllers for maintaining controllability of the system as well as the redundant ones. With this classification, the compromise of controllers can be analyzed to determine how the remaining controllers should react to restore the system to its normative state.

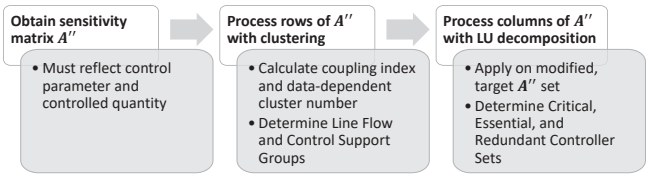

Fig. 1: Proposed methodology that applies clustering and factorization methods to process controller sensitivities.

- *Critical controllers* ($\mathbf{g_{C_i}}(\mathbf{x})\mathbf{u_{C_i}}$): devices that are irreplaceable and mandatory for system controllability
- *Essential controllers* ($\mathbf{g_{E_i}}(\mathbf{x})\mathbf{u_{E_i}}$): minimal set of devices required to maintain system controllability
- *Redundant controllers* ($\mathbf{g_{R_i}}(\mathbf{x})\mathbf{u_{R_i}}$): devices that can be removed without affecting system controllability

Our method performs power system controllability analysis to provide an analytical solution to restore or maintain system control given a controller attack. Specifically, the controlled dynamical power system (1) can be described with each controller identified as critical, essential, or redundant:

$$\begin{aligned}\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) &+ \{\mathbf{g_{C_1}}(\mathbf{x})u_{C_1} + \mathbf{g_{C_2}}(\mathbf{x})u_{C_2} + ... + \mathbf{g_{C_{TC}}}(\mathbf{x})u_{C_{TC}}\} \\ &+ \{\mathbf{g_{E_1}}(\mathbf{x})u_{E_1} + \mathbf{g_{E_2}}(\mathbf{x})u_{E_2} + ... + \mathbf{g_{E_{TE}}}(\mathbf{x})u_{E_{TE}}\} \\ &+ \{\mathbf{g_{R_1}}(\mathbf{x})u_{R_1} + \mathbf{g_{R_2}}(\mathbf{x})u_{R_2} + ... + \mathbf{g_{R_{TR}}}(\mathbf{x})u_{R_{TR}}\}\end{aligned} \tag{3}$$

where $\mathbf{x} \in \mathbf{\Xi}$ and C_1 to C_{TC} represents the critical controllers where TC is the total number. Similarly, E_1 to E_{TE} represents the essential controllers where TE is the total number and R_1 to R_{TR} represents the redundant controllers where TR is the total number.

Fig. 1 shows the high-level proposed methodology. The algorithm uses clustering and factorization along with sensitivity analysis and provides a general power grid controllability analysis that can be applied to any control parameters and any deployed controller devices (only the appropriate sensitivities are required). In the following sections, we provide the details on the methodology using clustering and factorization techniques. The algorithms calculate and process the sensitivities to determine the control support groups.

- *Control support groups*: the controllers that are highly coupled for impact on both the control objective and each other

Controller coupling is discussed further in Section V. For example, given 8 controllers (one on each transmission line in an 8-line system), we can describe the system using the control support groups:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \overbrace{\mathbf{g_1}(\mathbf{x})u_1 + \mathbf{g_4}(\mathbf{x})u_4}^{\text{GROUP 1}} + \overbrace{\mathbf{g_3}(\mathbf{x})u_3 + \mathbf{g_6}(\mathbf{x})u_6 + \mathbf{g_8}(\mathbf{x})u_8}^{\text{GROUP 2}} + \overbrace{\mathbf{g_2}(\mathbf{x})u_2 + \mathbf{g_5}(\mathbf{x})u_5 + \mathbf{g_7}(\mathbf{x})u_7}^{\text{GROUP 3}} \tag{4}$$

Each of the labeled groups, $GROUP1 - GROUP3$, embodies a control support group—there are 3 in total. In this case, we achieve information on which controllers work most effec-

tively together on controlling a specific group of transmission lines. Further insight into the use of these results will be detailed throughout the paper, specifically Section VII. The novel contributions of this work are as follows: (1) Determining controllability-equivalence sets, the control support groups, via clustering, (2) Computing the number of equivalence sets (clusters) using a novel sensitivity-based method, and (3) Identifying the critical, essential, and redundant controller sets via factorization.

IV. Leveraging Sensitivities

A system's sensitivity matrix ($\mathbf{A}''$ in Fig. 1) is often used for robust control to ensure controller parameters are chosen in such a way that the closed loop system is not sensitive to variations in process dynamics [12]. With such sensitivity information, placement of the control devices to achieve various objectives is facilitated as well as details on the impact of compromised controllers on overall system controllability.

For our application, we require knowledge of the independently controllable lines as well as the controller role sets. The sets of those lines can be defined as:

- *Line flow groups*: the sets of transmission lines that can be controlled independently

The control support groups, as defined in Section III., provide the corresponding control. To obtain these groups, we cluster the rows of the sensitivity matrix and then investigate which lines are most affected by each other as well as those that are not and have no relation. Additionally, we decompose the transposed sensitivity matrix to determine the critical, essential, and redundant sets of controllers.

The appropriate sensitivities to be utilized depend on the control device and objective. To exemplify the framework, we use distributed flexible AC transmission system (D-FACTS) devices. The versatile array of D-FACTS devices for power flow control includes distributed series reactors (DSRs) and distributed static series compensators (DSSCs), and is currently deployed by SmartWires Inc. [13], [14]. We focus on DSSCs in this work, but are motivated by the flexibility of D-FACTS and the various sensitivities that can be derived. The results presented in this paper will be broadly useful and clearly indicate how any controller and control objective may be interchanged. This controller acts as a synchronous voltage source in series with the line, changing the line's effective impedance and thus its power flow [14]–[16]. Therefore, we concentrate on sensitivities considering power flows. Specifically, we use the total power flow to impedance sensitivity matrix. It reflects both direct (i.e., change in impedance of a line and its direct impact on that line's power flow) and indirect (i.e., change in impedance of a line and its indirect impact on all other lines' power flows) sensitivities. This sensitivity matrix is represented as $\mathbf{\Omega}$.

$$\Delta \mathbf{P_{flow.total}} = [\mathbf{\Omega}] \cdot \Delta \mathbf{x} \tag{5}$$

where $\Delta \mathbf{P_{flow.total}}$ are the changes in the line power flows and $\Delta \mathbf{x}$ are the impedances. Including the indirect power flow sensitivities in the calculation of $\mathbf{\Omega}$ allows the representation of the impact of lines on all other lines, which is very useful for our analysis in determining line flow groups. Nonetheless, other sensitivity matrices can be used depending on the desired application; further sensitivity formulations for D-FACTS devices and derivation of $\mathbf{\Omega}$ are developed in [17].

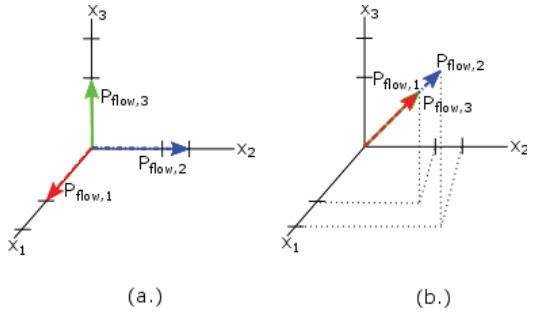

Fig. 2: Completely decoupled line flows (a.) and completely coupled line flows (b.) [17].

With the calculated sensitivity matrix, we can apply clustering to determine the control support and line flow groups. The matrix is represented as $\mathbf{A}''$ in Fig. 1. It is important to note that the algorithms presented in this paper are applicable to any controller and control objective; only the appropriate sensitivity matrix needs to be selected, or more precisely, one that reflects the controlled quantities and the control objective.

V. Controllability-Equivalence Sets

By obtaining sets of line flows that can be independently controlled with respect to other sets in a system, we can gain valuable insight on the influence of various controllers and the control support groups. Identifying these line flow groups is a key step in achieving comprehensive power flow control. Within each set, it only makes sense to control one line flow, as they are all highly coupled given the power system topology; controlling one line flow will always strongly impact the others in a predictable way.

A. Control Support Groups

To provide the most complete and effective control for the entire system, it is necessary to identify how the control of line flows are related to each other by determining the control support groups [17]. We can study a trivial example as shown below, with three power flows (the controlled quantity) and three impedances (the control).

$$a.\ \begin{matrix} \\ P_{flow,1} \\ P_{flow,2} \\ P_{flow,3} \end{matrix} \begin{matrix} \begin{matrix} x_1 & x_2 & x_3 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{matrix} \qquad b.\ \begin{matrix} \\ P_{flow,1} \\ P_{flow,2} \\ P_{flow,3} \end{matrix} \begin{matrix} \begin{matrix} x_1 & x_2 & x_3 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix} \end{matrix} \tag{6}$$

These vectors are illustrated in Fig. 2 where line flow vectors are illustrated as completely coupled or decoupled. When the vectors are orthogonal, the line flows are completely decoupled as shown in Fig. 2(a.), and can be controlled independently. Conversely, in the completely coupled case in Fig. 2(b.), the row vectors are aligned and the angle between them is 0°. When line flows are highly coupled, only one needs to be controlled, as the others will respond as well. Independent control of those lines cannot be achieved. When the row

vectors are exactly aligned but point in opposite directions (angle of 180°), the lines are still completely coupled [17].

The ability of certain lines to exhibit this independently controllable property is discernible from the relationships in the sensitivities. We can compare the cosine of the angles between vectors and determine the coupling sets. Subsequently, grouping of line flows can be determined using any appropriate clustering algorithm.

B. Coupling Index

We leverage the line flow vector angle relationships, to determine the controllability-equivalence sets by comparing the angles between row vectors of the sensitivity matrix to find the coupled and decoupled sets of lines flows. To calculate and compare these angles, we utilize the coupling index (CI) and measure the cosine similarity [18]. The CI is equal to the cosine of the angle between two row vectors, $\mathbf{v_1}$ and $\mathbf{v_2}$, of the sensitivity matrix $\mathbf{A}''$ as in (7).

$$cos\theta_{\mathbf{v_1 v_2}} = \frac{\mathbf{v_1} \cdot \mathbf{v_2}}{\|\mathbf{v_1}\|\|\mathbf{v_2}\|} \tag{7}$$

The clusters identified using the CI are approximately orthogonal to each other. The CI has values between -1 and 1. By clustering the rows of the sensitivity matrix using CI, the coupled and decoupled sets of line flows can be determined. Thus, each cluster will be independent and decoupled from the other sets. Within the cluster, the line flows are coupled and dependent on one another.

C. Number of Clusters

For our application, it is difficult to arbitrarily select k as it will change on a system by system basis. We want to find very cohesive clusters that most accurately reflect how we can effectively control lines that are either highly dependent on or independent of each other. We choose to use hierarchical agglomerative clustering as it groups data by creating a cluster tree or dendogram and applying a maximum threshold value k_m for the number of clusters to form (cutting the tree) rather than a strict rule [19]. Though, any other suitable clustering method may be used.

To leverage the sensitivity matrix and its inherent groupings, singular values are studied and are computed using singular value decomposition (SVD), for which details are provided in [20], [21]. SVD is applied to obtain a rank reduced approximation of a data set to generalize some properties or structure. One interpretation of the singular values is information on the largest contributions to the matrix and its general structure. Therefore, the most significant or largest singular values represent the most significant groups present in the data, which in our case is the sensitivity matrix. To determine these significant singular values, we calculate an *optimal hard threshold* using the techniques detailed by Gavish and Donoho [22] and obtain an initial estimate for the number of clusters, i.e., k_m. The final result is not a fixed threshold chosen *a-priori* but a data-dependent threshold. Since we seek high cohesiveness within our clusters for effective control, we then iterate on k_{in} by evaluating the coefficient of variance and the average of the resultant cluster's silhouette values for k_{in} [23]. Satisfying these conditions ensures the objects within the clusters are well-matched and cohesive. Ultimately, we obtain k_f to input as the final maximum number of clusters k_m for the hierarchical clustering or as k for other methods.

VI. Critical, Essential, and Redundant Controller Sets

With the resultant control support and line flow groups, the power grid operators and security administrators can specify the number of controllers to consider as well as an objective for each group of interest. The devices can be placed for maximum controllability such that the most independent controllability of groups is achieved. A target set of lines can be derived, as only one line from each independent group needs to be controlled. Hence, the target set is analyzed to discover the critical, essential, and redundant sets of controllers.

Consequently, the protection of critical controllers would be necessary in maintaining system controllability. If a controller from any set is compromised, we can determine how to recover controllability using controllers from its support group. This requires examining the coupling of the columns of the sensitivity matrix (of the target set), consistently labeled as $\mathbf{A}''$, or the rows of $[\mathbf{A}'']^\mathbf{T}$, to identify candidate lines with the best spread (linearly independent) to meet the objective.

Critical measurement identification in regards to observability analysis has been investigated, as demonstrated by the works of Bobba et al. [11] and Chen and Abur [24] A similar methodology can be applied to identify critical controllers as well. We apply the analysis on our sensitivity matrix to study controllability, the dual of observability. The idea is to perform a change of basis to obtain a mapping from measurements to equivalent states. Instead of using this decomposition to examine the redundancy of measurements for estimating states, we use it to examine the set of control devices needed to control equivalent line flows. Define $[\mathbf{A}'']^\mathbf{T}$, where the rows correspond to control devices and columns correspond to the variable being controlled. For simplicity, we continue to use the example of D-FACTS devices with columns corresponding to the real power flows to be controlled. Again, we only consider the real power flows of the target set of lines, as determined from the clustering results.

LU factorization is applied to obtain the change of basis, decomposing the transposed sensitivity matrix to lower and upper triangular factors; [25] describes the LU factorization method. The following decomposition of $[\mathbf{A}'']^\mathbf{T}$ is obtained as:

$$[\mathbf{A}'']^\mathbf{T} = \mathbf{P^{-1}} \mathbf{L_F} \mathbf{U_F} \tag{8}$$

$$\mathbf{L_F} = \begin{bmatrix} \mathbf{L_b} \\ \mathbf{M} \end{bmatrix} \tag{9}$$

Using the Peters-Wilkinson [25] method, we are able to decompose $[\mathbf{A}'']^\mathbf{T}$ into its factors, where $\mathbf{P}$ is the permutation matrix and $\mathbf{L_F}$ and $\mathbf{U_F}$ are the lower and upper triangular factors of dimension n, respectively. M is a sparse, rectangular matrix with rows corresponding to redundant controllers. The new basis has the structure:

$$\mathbf{L_{CER}} = \mathbf{L_F} \mathbf{L_b^{-1}} = \begin{bmatrix} \mathbf{I_n} \\ \mathbf{R} \end{bmatrix} \tag{10}$$

TABLE I: Singular Values y_i of $\mathbf{\Omega}$

y_1	y_2	y_3	y_4	y_5	y_6	y_7	...
4.13	3.24	1.14	1.06	0.41	0.02	0.01	...

TABLE II: Line Flow Grouping Clusters

Clus1	Clus2	Clus3	Clus4	Clus5	Clus6
L1, L2, L6, L8	L3, L4	L5	L7	L9	L10, L11

The transformed basis, shown in (10), must be full rank for a controllable system and this requires the $m \times (n-1)$ matrix to have a column rank of $(n-1)$ to be a controllable n-bus system with m-measurements. Since $\mathbf{L_F}$ and $\mathbf{U_F}$ will be nonsingular for a controllable system, the rank of $[\mathbf{A}'']^{\mathbf{T}}$ can be confirmed by checking the rank of the transformed factor $\mathbf{L_{CER}}$. Also, $\mathbf{L_b}$ has full rank and with $\mathbf{L_F}$ multiplied by $\mathbf{L_b^{-1}}$ from the right, the row identities will be preserved in the transformed matrix $\mathbf{L_{CER}}$. Each row of the matrix will, therefore, correspond to the respective controllers [24].

Rows of $\mathbf{I_n}$ correspond to essential controls that are sufficient to assure independent controllability of the equivalent line flows. If the essential controller is the only non-zero entry of an equivalent line flow column, it is the *only* controller that can control it and is irreplaceable. There is only one entry for that line flow and it is in $\mathbf{I_n}$. Thus, the control corresponding to that row in $\mathbf{I_n}$ is critical, since that equivalent line flow cannot be independently controlled by any of the other devices. Rows of $\mathbf{R}$ correspond to redundant controls. These roles were defined in Section III. Columns correspond to the equivalent flows which can easily be mapped back to the original flows using the permutation matrix $\mathbf{P}$ obtained from the LU decomposition step.

VII. Evaluations

The proposed methodology to discover the distributed controller role and interaction (controllability-equivalence sets) was tested on a PowerWorld 7-bus system and is detailed next. The system has 5 generators and 11 lines that are modeled in PowerWorld as the *B7_DFACTS_DEMO* case [26]. For this study, we assume the controllers are D-FACTS devices whose control objective is to change line flows by changing the effective impedance of lines. We first perform an *a-priori* grouping of parallel lines. In this case, there are two parallel lines, lines 10 and 11. Whichever line flow group and critical, essential, or redundant set line 10 is placed in, line 11 is also in. We also exclude the transformers as D-FACTS controller placement options. Lastly, we posit there is a controller on every allowable line for simplicity, but this can be easily altered as well.

Using the total power flow to impedance sensitivity matrix $\mathbf{\Omega}$, discussed in Section IV., we compute the CI matrix to measure the cosine similarity between row elements of $\mathbf{\Omega}$. Next, we perform SVD on $\mathbf{\Omega}$ and obtain the singular values, y_i, shown in Table I where $y_8 - y_{10}$ are near zero.

With the calculated hard threshold $\hat{\tau}^* = 0.503$ for the $n \times n$ sensitivity matrix $\mathbf{\Omega}$, we find that 4 singular values satisfy this threshold. Therefore, we set $k_{in} = 4$ and then iterate on it by evaluating the coefficient of variance and average silhouette values. In this manner, the number of clusters is increased to 6 so we set $k_m = 6$ and achieve our line flow groups. The resultant line flow groups, labeled Clus1-Clus6, are provided in Table II. Note that line 11 (parallel with line 10) is also included in the final results. The clusters are visually represented in Fig. 3. The lines are colored according to cluster membership, a black line indicates only that line was in the cluster – not grouped with any other line.

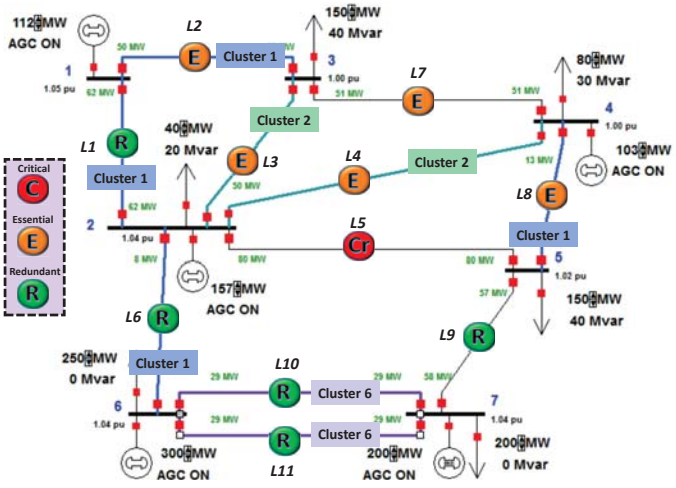

Fig. 3: 7-bus case with lines colored according to cluster group and labeled with critical, essential, and redundant controllers.

Now that we have the line flow groups, we can determine the the critical, essential, and redundant sets of controllers. In fact, the cluster results can be used to determine the target set of lines. Only one line in each line flow group needs to be controlled, so one line from each cluster can be selected to be analyzed with the controller sets. For example, a target set of lines that encompasses control of the entire system can be $L1$, $L3$, $L5$, $L7$, $L9$, and $L10$. By applying the decomposition method on the transposed sensitivity matrix, $[\mathbf{A}'']^{\mathbf{T}}$, comprised of the targeted lines and all possible controllers, we achieve the transformed basis $\mathbf{L_F}^{\mathbf{T}}$ shown in Table III and results provided in Table IV.

By examining Table III, we can determine the critical, essential, and redundant controllers. An equivalent line flow column with only one non-zero entry, as highlighted for **EQ.L3**, has only one device that can control it and thus is a critical controller corresponding to row 3. The essential controllers are discovered by examining the first 6 rows ($\mathbf{I_n}$) and the remaining 4 rows ($\mathbf{R}$) correspond to redundant controls. We can, therefore, deduce that if there are controllers on every line, the critical and essential controllers on lines 2, 3, 4, 5, 7, and 8 would provide full system controllability. The locations of the critical, essential, and redundant controllers for the 7-bus system are also illustrated in Fig. 3.

1) Insights for Regaining Control: With these valuable results about the flexibility and redundancy of the control, we can effectively strategize regaining control of a given system after a controller attack. The following situations could arise and, with our insights from this analysis, we can respond in the corresponding manners:

TABLE III: Transformed Basis

EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6
1.0000	0	0	0	0	0
0	1.0000	0	0	0	0
0	0	1.0000	0	0	0
0	0	0	1.0000	0	0
0	0	0.0000	0	1.0000	0
0	0	0	0	0	1.0000
-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000
-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000
0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466
-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000

TABLE IV: Critical, Essential, and Redundant Controller Sets

	Lines with Controllers
Critical Set	L5
Essential Set	L2, L3, L4, L7, L8
Redundant Set	L1, L6, L9, L10, L11

#1 **Redundant Controller(s) Compromised**
If the controllers on $L1$ and $L9$ are compromised, we know from the clustered line flow groupings that for $L1$ controller, we can most effectively use the essential controllers in $GR1$ to best mitigate any adverse actions from $L1$ controller. The redundant controller on $L6$ can be used, additionally. Since no critical or essential controllers have been compromised, we still maintain full system control. We see that $L9$ controller is independently controlled (no other members in cluster), so perhaps we need the efforts of multiple, uncompromised controls to counter any malicious actions.

#2 **Critical or Essential Controller(s) Compromised**
If $L2$, $L5$, and $L8$ controllers are compromised, we know that $L1$ and $L6$ redundant controllers will be most effective in mitigating any actions of $L2$ or $L6$ essential controllers. However, since the critical controller on $L5$ is compromised, we do not have full system control. All other "safe" controller actions are necessary in trying to regain control of the system. This is true for $L5$ controller as well, especially since it has no other controls in its support group. If combination of critical, essential, and redundant controllers compromised, a similar response of utilizing all uncompromised system controls and/or defense mechanisms to regain system control is needed.

VIII. Conclusion

The presented methodology provides significant insight on how to best regain or maintain control given controller compromise or failure. We gain information on 1) the control support groups, the controllers that are highly coupled for both impact on the control objective and each other, 2) which controllers are critical and essential in maintaining system controllability, and 3) which controllers are redundant and can be managed more readily if compromised. Thus, if a given controller in a redundant set is compromised, a set of essential and critical controllers can be used to restore the system and mitigate any adverse consequences. Conversely, if an essential or critical controller is compromised, immediate remedial actions are necessary as full system controllability is no longer maintained, especially for critical controller compromise. These insights can allow for strategic protection schemes, as well as a prioritization of cyber (and physical) defense mechanisms surrounding critical and essential sets of controllers. System restoration strategies and further security measures on critical control points are aided significantly with the results of this analysis.

References

[1] J. Wirfs-Brock, "The realities of cybersecurity at a rural utility," *Inside Energy*, Sept. 2015. [Online]. Available: http://grid.insideenergy.org/cybersecurity/

[2] M. J. Assante, "Confirmation of a coordinated attack on the ukrainian power grid," *SANS Industrial Control Systems*, Jan. 2016. [Online]. Available: ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[3] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[4] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantic Security Response, Tech. Rep., Oct. 2010.

[5] E. Hayden, M. Assante, and T. Conway, "An abbreviated history of automation & industrial controls systems and cybersecurity," *SANS analyst white papers*, 2014.

[6] M. Hong and C.-C. Liu, "Complete controllability of power system dynamics," in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 4, 2000, pp. 241–244 vol.4.

[7] T. Kailath, *Linear Systems*. Prentice-Hall Englewood Cliffs, NJ, 1980, vol. 156.

[8] A. Hamdan and A. Elabdalla, "Geometric measures of modal controllability and observability of power system models," *Electric Power Systems Research*, vol. 15, no. 2, pp. 147–155, 1988.

[9] A. Hamdan and A. Nayfeh, "Measures of modal controllability and observability for first-and second-order linear systems," *Journal of Guidance, Control, and Dynamics*, vol. 12, no. 3, pp. 421–428, 1989.

[10] A. Messina and M. Nayebzadeh, "An efficient placement algorithm of multiple controllers for damping power system oscillations," in *Power Engineering Society Summer Meeting, 1999. IEEE*, vol. 2. IEEE, 1999, pp. 1280–1285.

[11] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[12] M. Dahleh and I. Diaz-Bobillo, *Control of Uncertain Systems: A Linear Programming Approach*. Prentice Hall, 1995.

[13] SmartWireGrid. (2016, September) Minnesota power deploys smart wires to optimize its grid and save customers money. Online. SmartWires Incorporated. [Online]. Available: http://www.smartwires.com/category/press-release/

[14] D. Divan, "Improving power line utilization and performance with D-FACTS devices," in *Power Engineering Society General Meeting, 2005. IEEE*. IEEE, 2005, pp. 2419–2424.

[15] D. M. Divan, W. E. Brumsickle, R. S. Schneider, B. Kranz, R. W. Gascoigne, D. T. Bradshaw, M. R. Ingram, and I. S. Grant, "A distributed static series compensator system for realizing active power flow control on existing power lines," *IEEE Transactions on Power Delivery*, vol. 22, no. 1, pp. 642–649, Jan 2007.

[16] H. Johal and D. Divan, "Design considerations for series-connected distributed FACTS converters," *IEEE Transactions on Industry Applications*, vol. 43, no. 6, pp. 1609–1618, Nov 2007.

[17] K. Rogers, "Power system control with distributed flexible ac transmission system devices," Master's thesis, University of Illinois at Urbana-Champaign, 2009.

[18] K. Rogers, R. Klump, H. Khurana, and T. Overbye, "Smart-grid -enabled load and distributed generation as a reactive resource," in *Innovative Smart Grid Technologies (ISGT), 2010*, Jan 2010, pp. 1–8.

[19] (2015) PowerWorld Simulator. PowerWorld Corporation. [Online]. Available: http://www.powerworld.com/products/simulator/overview

[20] M. T. Heath, *Scientific Computing*. McGraw-Hill New York, 2002.

[21] J. M. Lim and C. L. DeMarco, "Model-free voltage stability assessments via singular value analysis of PMU data," in *Bulk Power System Dynamics and Control - IX Optimization, Security and Control of the Emerging Power Grid (IREP), 2013 IREP Symposium*, Aug 2013, pp. 1–10.

[22] M. Gavish and D. Donoho, "The optimal hard threshold for singular values is $\frac{4}{\sqrt{3}}$," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 5040–5053, Aug 2014.

[23] P. J. Rousseeuw, "Silhouettes: a graphical aid to the interpretation and validation of cluster analysis," *Journal of Computational and Applied Mathematics*, vol. 20, pp. 53–65, 1987.

[24] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *Power Systems, IEEE Transactions on*, vol. 21, no. 4, pp. 1608–1615, Nov 2006.

[25] G. Peters and J. H. Wilkinson, "The least squares problem and pseudo-inverses," *The Computer Journal*, vol. 13, no. 3, pp. 309–316, 1970.

[26] PowerWorld Corporation. (2016) D-FACTS Quick-Start Tutorial. http://www.powerworld.com/knowledge-base/d-facts-quick-start-tutorial.