IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 2, 2020, accepted June 6, 2020, date of publication June 10, 2020, date of current version June 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001308

Cyber-Security Constrained Placement of FACTS Devices in Power Networks From a Novel Topological Perspective

HOSSEIN PARASTVAND[1], (Student Member, IEEE),
OCTAVIAN BASS[1], (Senior Member, IEEE),
MOHAMMAD A. S. MASOUM[2], (Senior Member, IEEE),
AIRLIE CHAPMAN[3], (Senior Member, IEEE), AND
STEFAN LACHOWICZ[1], (Senior Member, IEEE)

[1]Smart Energy Systems Research Group, School of Engineering, Edith Cowan University, Joondalup, WA 6027, Australia
[2]Department of Engineering, Utah Valley University, Orem, UT 84058, USA
[3]Department of Mechanical Engineering, School of Engineering, The University of Melbourne, Melbourne, VIC 3010, Australia

Corresponding author: Hossein Parastvand (h.parastvand@ecu.edu.au)

This work was supported by ECU Open Access Funding Support Scheme.

ABSTRACT Optimal placement of flexible AC transmission systems (FACTS) devices and the cyber-security of associated data exchange are crucial for the controllability of wide area power networks. The placement of FACTS devices is studied in this paper from a novel graph theoretic perspective, which unlike the existing approaches, purely relies on topological characteristics of the underlying physical graphs of power networks. To this end, the maximum matching principle (MMP) is used to find the set of required FACTS devices for the grid controllability. In addition, the cyber-security of the most critical data related to the FACTS controllers is guaranteed by introducing the concept of moderated-k-security where k is a measure of data obscurity from the adversary perspective. The idea of moderated-k-symmetry is proposed to facilitate the arrangement of the published cyber graph based on a permutation of nodes within the symmetry group of the grid, called generator of automorphism. It is then verified that the published cyber-graph can significantly obscure the data exchange over the cyber graph for adversaries. Finally, a similarity is observed and demonstrated between the set of critical nodes attained from the symmetry analysis and the solution of the FACTS devices placement that further highlights the importance of symmetry for the analysis and design of complex power networks. Detailed simulations are applied to three power networks and analyzed to demonstrate the performance and eligibility of the proposed methods and results.

INDEX TERMS Controllability, placement, FACTS devices, graph theory, power system security, cyber-security, cyber-physical system, shunt voltage sourced converter.

NOMENCLATURE

ABBREVIATIONS

CN	Complex network.
FACTS	Flexible AC transmission systems.
MMP	Maximum matching principle.
PID	proportional integrative derivative.
VSC	Voltage-source converter.
WAC	Wide area controlled.

PARAMETERS

α_{sh}	Angle of shunt VSC.
β	The bus voltage angles.
δ_i	The angle of voltage of node i.
γ_{sh}	Conversion ratio signal.
σ	An automorphism or a Permutation.
$\mathcal{A}$	Adjacency matrix.
$\mathcal{D}$	Degree matrix.
$\mathcal{E}$	The set of edges.
$\mathcal{E}_c$	The set of critical edges.
$\mathcal{F}$	The determining set attained from Gen($\mathcal{F}$).
$\mathcal{G}$	Graph.
$\mathcal{G}_k$	The released graph.

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Li.

$\mathcal{L}$	Laplacian matrix.
$\mathcal{V}$	The set of nodes.
$\mathcal{V}_c$	The set of critical nodes.
Aut($\mathcal{G}$)	Automorphism group.
Gen($\mathcal{G}$)	Generators of automorphism.
Gen$_{dis}$($\mathcal{G}$)	Set of disjoint generators.
Move(σ)	The set of moved nodes by permutation.
ε	Identity (or trivial) permutation.
φ	A generator of automorphism.
B	Input matrix.
C	Capacitor.
F_{vl}^{Gen}	The set of generators that fixes v_l.
I_{dc}	Capacitor current.
I_{sh}	Shunt reactive current setpoint.
I_{sh}^{*}	Reactive current of the outer loop.
k	The number of distinct mappings.
k_m	Conversion ration between the voltage of AC and DC sides.
M	A matching.
M_{vl}^{Gen}	The set of generators that moves v_l.
p	Multiplicity of critical node in Gen($\mathcal{G}$).
P_{ac}	Active power on AC side.
P_{ij}	Active power flow between nodes i and j.
q	The size of disjoint generators.
Q_{ij}	Reactive power flow between nodes i and j.
S	Determining set.
u	Control signal.
V	Voltage.
V_m	Voltage magnitude.
V_{dc}	Capacitor terminal voltage.
V_{ref}	Setpoint voltage.
Z	Line impedance.

I. INTRODUCTION

The imbalance between reactive power at the generating side and the network demand causes voltage instability. The wide area active compensation devices, collectively known as flexible AC transmission systems (FACTS) devices ([1]–[9]) are power electronic based equipment which play a vital role in enhancing the power system controllability and power flow capability. The importance of FACTS devices for the grid operation raises serious concerns about the cyber-security of data exchange over these controllers as the false data injection to one of the critical FACTS devices can lead to cascading failure in the grid [10]. In this paper, these two problems are addressed from a novel topological perspective.

A. STATE OF THE ART

The optimal placement of FACTS devices is a common yet important research topic in literature and has been investigated via various approaches. These include (1) conventional methods (such as indexing [11], controlling [12], residue analysis [13], numerical optimization [14], sensitivity [15], and eigenvalue [16]), (2) optimization methods (such as optimal power flow [17], linear programming [18], dynamic programming [19], mixed integer programming [20], stochastic load flow [21], and adaptive control law [22]), (3) artificial intelligence techniques (such as Monte Carlo simulation [23], artificial bee colony [24], artificial neural network [25], symbiotic organism search algorithm [26], fuzzy systems [27], and particle swarm optimization [28]), (4) hybrid techniques (such as hybrid of bee colony and neural networks [29], hybrid of genetic algorithm and fuzzy systems [16], mixed optimal power flow and particle swarm optimization [30], mixed bee colony and optimal power flow [31], and hybrid of fuzzy systems and Lyapunov theory [32]), and (5) other approaches (such as energy approach [33], active control [34], graph search algorithms [35], whale optimization [36], Gray Wolf optimizer [37], salp swarm optimizer [38], Grasshooper optimization [39], ant lion optimization [40], and spider monkey optimization [41]).

At the same time, cyber-security has been one of the hot topics related to the management, operation, and control of power systems [48]– [51]. The reliability of wide area controlled (WAC) power systems highly depends on the security of the underlying communication networks. Information exchange via cyber graph is one of the underpinning platforms of all networks including power networks and smart grids that has significant role in grid control and operation. The interplay between power systems and the underlying communication platforms raises various security concerns about attacks from adversary agents. Thus the important grid information such as the data associated with the critical transmission lines, generation units, and the locations of FACTS devices must be hidden or obscured for adversary agents.

Due to its significant impacts on various aspects of network, graph topology has drawn the attention of engineering communities including power system community during the last two decades. The role of network topology is investigated for a few power system problems such as synchronization [43], flexibility of transmission lines for day-ahead scheduling [44], and the patterns of attacks to power networks [45]. Recently, graph symmetry, described by automorphism groups, has been leveraged in literature to address important network behaviors such as its controllability [61], robustness [58], and synchronization [46]. It has been verified that symmetry is an obstruction to controllability [61] meaning that systems with larger number of automorphisms require more driver nodes to satisfy the network controllability. In contrast, network robustness can be improved by increasing the network symmetry (or the size of automorphism group) [58]. Also, power networks with high symmetry are more resilient towards desynchronization propagation [47].

Early applications of symmetry in security emerged in the computer science community targeting the cyber-security of social networks ([52]–[54]) by proposing the concepts of k-symmetry, k-isomorphic, and k-automorphic. In fact, these studies found that releasing a permuted graph by an automorphism or isomorphism instead of original cyber graph makes it difficult for adversary agents to distinguish their targets.

During the last decade, the applications of automorphisms in cyber-security, categorized under the concept of ''security via obscurity'', have been the main focus when implementing the symmetry characteristics for investigating the networks' cyber-security. However, the use of symmetry gives rise to some practical challenges. Computing and sweeping over all automorphisms to find the set of nodes with maximum multiplicities for a large network is a computationally challenging task. Moreover, important questions arise when identifying priorities for design and protection: Which cyber components, if compromised, can lead to significant power delivery disruption? What grid topologies are inherently robust to classes of cyber attack? Is the information available through advanced cyber infrastructure worth the increased security risk?

k-isomorphic graphs can be attained only by adding/deleting many edges through some modification algorithms (for example see [52]–[55]). Satisfying k-automorphism for a real world network imposes many modifications on the original network which compromises its cost efficiency. In k-symmetry it is enough that k distinct mappings exist where for each node the set of k automorphisms may be different. In practice, it is not computationally efficient to impose such modifications. Furthermore, for k automorphisms, the same set of k automorphisms have to be applied to all nodes. This makes k-automorphism an even more difficult property to satisfy. In k-isomorphism, in addition to the above issues, connections among sub-graphs are deleted in the released graph. This, in turn, causes the loss of data utility in the published graph.

B. RESEARCH GAPS AND CONTRIBUTIONS

Although the placement of FACTS controllers has been widely studied during the last decade, no study has considered the possible impacts of network topology on the solutions. Moreover, the majority of the existing approaches have computational issues such as intractable nature of optimization techniques [17]–[25] which is caused by the lack of an analytical, non-heuristic, or systematic approach for finding the solution. In addition, the cyber-security of FACTS devices have not been investigated in literature. In this paper, an analytical approach for the placement of FACTS controllers is proposed based on the topological characteristics of the network which does not suffer from the computational issues. To this end, the maximum matching principle is implemented which is a mechanism to find the set of unmatched nodes that are considered as the set of driver nodes which are able to drive the states of system from any initial state to any desired state in reasonable time (network controllability). The controllability of the complex networks (CNs) is then attributed to the number of required driver nodes for full state controllability [42].

In this paper, the placement of FACTS controllers is constrained to the controllability of the power grid. By realizing the power grid as a complex network, the grid controllability is attributed to the number of required driver nodes for full state controllability. The FACTS controllers act as these driver nodes which can be found by performing the maximum matching principle on the physical graph of power systems. To overcome the computational issues related to computing the whole set of automorphisms, we adapt a symmetry benchmark according to a set of elementary automorphisms, known as generators of automorphisms. It will be verified that all essential symmetry characteristics can be realized via this set which has a significantly smaller size than automorphism groups and it is computationally effective to calculate and sweep over them. In addition, the graph symmetry is implemented to find the most critical components of power system in terms of their impact on the network controllability. Nodes with bigger multiplicities in the automorphism group, or in generators of automorphisms, are considered as the most critical nodes. The computation of the symmetry groups and the associated computation complexity are discussed in details. Throughout simulation, it is observed that the set of critical nodes identified by symmetry analysis is a subset of unmatched nodes corresponding to the locations of FACTS controllers. This overlap further reveals the importance of symmetry in power network analysis and synthesis.

This study proposes an approach to secure the critical elements of power networks via obscuring the published graph of the grid and, in turn, reducing the chance of distinguishing and manipulating the critical data of FACTS devices by adversaries. This has been accomplished via introducing a new concept, namely moderated-k-security, which provides new necessary and sufficient conditions for obscuring the network critical data.

The rest of the paper is organized as follows. In Section II, a topology-based solution to the placement of FACTS controllers is presented using the maximum matching principle. The cyber-security of the critical data of the network including the data exchange between FACTS controllers is addressed in section III using the concept of symmetry groups. The simulation is carried out on the 49-bus, 274-bus, and 1, 176-bus systems in section IV and the effectiveness of the proposed approaches are verified.

II. A TOPOLOGICAL APPROACH TO THE PLACEMENT AND CONTROL OF FACTS DEVICES IN POWER NETWORKS

In this section, we look at the placement of FACTS devices from a controllability perspective. To this end, the problem of FACTS placement is transformed to the problem of finding the number and locations of the required FACTS devices that can structurally control the system. First, some preliminaries on graph theory and symmetry are reviewed and then the main result of this section is presented.

A. PRELIMINARIES ON GRAPH THEORY AND SYMMETRY GROUPS

A graph $\mathcal{G}$ is a composition of a set of nodes $\mathcal{V}$ and edges $\mathcal{E}$ denoted by $\mathcal{G}(\mathcal{V}, \mathcal{E})$. Two nodes are *adjacent* if there is an edge between them. The size and order of $\mathcal{G}$ are denoted

by $|\mathcal{V}|$ and $|\mathcal{E}|$, respectively. An *adjacency matrix* $\mathcal{A}$ is a square $|\mathcal{V}| \times |\mathcal{V}|$ whose elements a_{ij} indicate the connection between every pair of nodes within the graph. $a_{ij} = 1$ if there is an edge between nodes i and j, otherwise $a_{ij} = 0$. The *degree matrix* $\mathcal{D}$ is a diagonal matrix whose diagonal elements d_{ii} is equal to the number of nodes connected via an edge to node i. The *Laplacican matrix* $\mathcal{L}$ is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A}$. A *permutation* σ of a set of ordered nodes $\mathcal{V}$ is a rearrangement of its members into a sequence. The order of σ is the smallest positive integer m such that $\sigma^m = \varepsilon$ where ε is the identity (also known as trivial) permutation. The composition of two permutations σ_1 and σ_2, denoted by $\sigma_1 \circ \sigma_2$ is the point-wise product of them. If a node is rearranged by a permutation it is called a *moved* node by that permutation, otherwise it is a *fixed* node. The set of all permutations that rearrange a node v_l is denoted by Mov_{v_l}. Two permutations σ_1 and σ_2 are *disjoint* if each moved node by σ_1 is fixed by σ_2, or equivalently, every moved node by σ_2 is fixed by σ_1, otherwise, σ_1 and σ_2 are *joint* permutations.

Proposition 1: If a node is rearranged by a permutation σ on $\mathcal{G}$, it can not be fixed by the composition of σ and its disjoint permutations on $\mathcal{G}$.

Proposition 2: If a node is fixed by a set of disjoint permutations, it can not be moved by the compositions of these disjoint permutations.

Automorphism group is a quantified notion of symmetry. Under the act of an automorphism, a graph can be mapped to itself without changing the graph adjacency or Laplacian matrices. It can be mathematically described as a permutation σ for which $\{i, j\} \in \mathcal{E}(\mathcal{G})$ if and only if $\sigma(i), \sigma(j) \in \mathcal{E}(\mathcal{G})$. The set of all automorphisms of $\mathcal{G}$ and its size are denoted by $\text{Aut}(\mathcal{G})$ and $|\text{Aut}(\mathcal{G})|$. Automorphism groups can be built up from a set of elementary automorphisms called generators of automorphisms $\text{Gen}(\mathcal{G})$ (See Appendix A). Once the whole set of generators are determined, the automorphism group can be constructed from the compositions of all generators and automorphisms of order m up to generating unique permutations. Throughout this paper, σ and φ are used to indicate an automorphism and a generator of automorphism, respectively. The symmetry elements, including $\text{Aut}(\mathcal{G})$ and $\text{Gen}(\mathcal{G})$, are computed in Sage (System for Algebra and Geometry Experimentation).

B. CN CONTROLLABILITY IMPLICATIONS FOR PLACEMENT OF FACTS DEVICES

The above preliminaries on graph theory and symmetry will be used later in this paper. Now, the necessary conditions for controllablity by means of a set of FACTS devices are presented using the maximum matching principle which can be implemented for finding the number of required FACTS devices in the next section. The necessary conditions for uncontrollability of a pair of system matrices $(\mathcal{A}, B)$ is related to a the determining set [57] which can be attained from the symmetry group.

Definition 3: A subset S of the vertices of a graph $\mathcal{G}$ is called a determining set if whenever $g, h \in Aut(\mathcal{G})$ so that $g(s) = h(s)$ for all $s \in S$, then $g = h$. Equivalently, a subset of nodes of a graph $\mathcal{G}$ is called a determining set $\mathcal{S}$ if every automorphism of $\mathcal{G}$ can be uniquely determined by its action on the nodes of $\mathcal{S}$.

Corollary 4 [61]: A necessary condition for controllability of the pair $(\mathcal{A}(\mathcal{G}), B(S))$ is that S is a determining set.

Lemma 5 adapts the necessary conditions for controllability attained in [61] to the context of power networks where the FACTS controllers act as the so called driver nodes.

Lemma 5 [57]: Assume that the adjacency matrix $\mathcal{A}$ of the graph of power network $\mathcal{G}$ is diagonalizable and symmetry preserving. Then the pair of system matrices $(\mathcal{A}, \mathcal{S})$, where $\mathcal{S}$ and $|S|$ are the associated determining set and its size, respectively, is uncontrollable if $\mathcal{G}$ admits a nontrivial automorphism σ which fixes the input set $\mathcal{S}$, i.e., $\sigma(i) = i$ for all $i \in \mathcal{S}$.

A straightforward result of the Lemma 5 is stated in the proposition 6.

Proposition 6: The necessary condition for controllability of $(\mathcal{A}, \mathcal{S})$ is that for all $\sigma_i \in Aut(\mathcal{G})$ there is at least one node v_l where $v_l \in Mov(Aut(\mathcal{G}))$.

The above proposition simply means that at least one moved node of each automorphism must belong to the determining set $\mathcal{S}$ in order to satisfy the controllability of $(\mathcal{A}, \mathcal{S})$. Although Lemma 5 or Proposition 6 can theoretically be used to examine the controllability of power networks, in practice, checking the whole set of automorphisms for medium and large networks is not computationally effective. In [58], the size of automorphism group of US power grid is computed which is equal to 5.1851×10^{152}. Clearly, this is a big computation burden to calculate the determining set S by computing all automorphisms and sweeping over them. In contrast, if we attain the determining set from the generators of automorphisms, which is significantly a smaller set than automorphism group, then the determining set can be effectively computed using the conventional processing tools.

Lemma 7: Assume that $\mathcal{A}$ is diagonalizable and symmetry preserving, $\mathcal{F}$ is a determining set (for which if the generators of automorphisms $\varphi_1, \varphi_2 \in Gen(\mathcal{G})$ so that $\varphi_1(f) = \varphi_2(f)$ for all $f \in \mathcal{F}$ then $\varphi_1 = \varphi_2$), and $\mathcal{J}$ is the set of all possible unique compositions of generators of order m with at least one joint node. The pair of system matrices $(\mathcal{A}, \mathcal{F})$ is uncontrollable if there exists at least one generator of automorphism φ_j, where $\varphi_j \neq \varepsilon$, for which $\varphi_j(i) = i$ for all $i \in \mathcal{S}$. Moreover, the necessary conditions for controllability of the power system using the FACTS devices corresponding to the nodes in $\mathcal{F}$ are

1) *$\forall \mathcal{J}_J$, $J = 1, \ldots, |\mathcal{J}|$, $i = 1, \ldots, |\mathcal{F}|$, $\mathcal{F}(i) \neq j$ where j is a joint node of $\mathcal{J}_J$,*
2) *If $\forall v_l \in \varphi_g \Rightarrow v_l$ is a joint node, then $\mathcal{F}(v_l) \neq v_l$,*
3) *$\forall i \in \mathcal{F} \Rightarrow \varphi_g(i) \neq i$ where $g = 1, \ldots, h$ and $h = |Gen(\mathcal{G})|$.*

Proof: Using the proof by contradiction, we assume that if there is a generator φ_j for which $\varphi_g(i) = i$ for all $i \in \mathcal{S}$ then the pair $(\mathcal{A}, \mathcal{F})$ is controllable. This means

$$\exists \sigma,\ \sigma \in \text{Aut}(\mathcal{G})\ \&\ \sigma(i) = i$$

since all $\varphi \in \text{Aut}(\mathcal{G})$. This contradicts the condition of Lemma 5. For the second part of the proof, we have to verify that the determining set or the locations of FACTS devices attained in $\mathcal{F}$ must satisfy the conditions 1-3. The composition of joint generators may fix an unfixed node by one or some of them. Condition 1 thus excludes the joint nodes from $\mathcal{F}$ as it might be fixed in a composition and does not emerge in the resulted automorphisms. Hence, another node in those generators containing joint nodes must be included in $\mathcal{F}$. On the other hand, if all moved nodes of a generator are joint nodes, then all nodes must be included in $\mathcal{F}$, i.e., $\forall v_l \in \varphi_g$, $\mathcal{F}(v_l) \neq v_l$, as some of these nodes might be fixed by the composition (condition 2). Condition 3 considers the case where the composition is a product of disjoint generators. In this case, selecting one node from each generator will generate a set of nodes that necessarily satisfies the condition of being a determining set for the corresponding set of automorphisms. This is because the composition of disjoint generators does not fix a moved node by each of generators. This verifies that $\mathcal{S} \subset \mathcal{F}$ which means the determining set attained from generator set contains all moved nodes by $\mathcal{S}$. □

Lemma 7 facilitates using generators of automorphisms instead of automorphism group in order to find the determining set. According to Lemma 7, the whole set of FACTS devices can be attained effectively from the set of generators of automorphisms. However, Lemma 7 only provides the necessary conditions for controllability. To attain the sufficient condition for controllability of power systems, we use the maximum matching principle.

Definition 8: A matching, M, of $\mathcal{G}$ is a subset of edges of E such that no node in V is adjacent to more than one edge in M, or intuitively, no two edges in M share a common node. A matching M is called maximum matching if for any other matching M', $|M| \geq |M'|$.

In [56], the CN controllability is addressed by maximum matching principle where the set of all unmatched nodes are considered as driver nodes. In our problem setup, the set of FACTS devices can be considered as the set of required driver nodes for full controllability of power network. Once the maximum matching algorithm is implemented, all unmatched nodes must be considered as the locations of FACTS devices.

Using the maximum matching principle, the set of required FACTS devices for full controllability of power network can be attained. The simulation results on 49-bus and 274-bus systems in section IV confirm the effectiveness of using maximum matching principle for the placement of FACTS devices. Lemma 7 is also assessed in the simulations where it is observed that the number and locations of FACTS devices attained from MMP and Lemma 7 are very similar.

C. MODELING OF THE SHUNT FACTS DEVICES IN POWER NETWORKS

Once the number and locations of the required FACTS devices are determined, a dynamic control strategy can be implemented to improve the power flow capabilities. Note

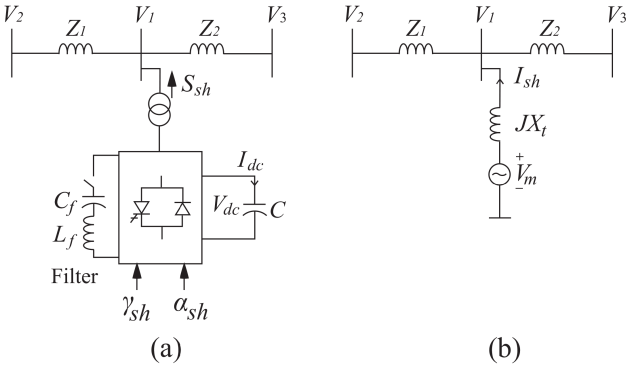


FIGURE 1. Shunt VSC converter. (a) The schematic diagram, (b) The balanced positive-sequence model.

that there are various types of FACTS devices which we do not intend to explore as the main focus of this paper is on the proposed approaches for placement of FACTS devices (Section II) and securing them (Section III) from the novel topological perspectives.

The power flow equations can be written as

$$P_{ij} = \frac{V_i V_j}{X_{ij}} sin(\delta_i - \delta_j) \tag{1}$$

$$Q_{ij} = \frac{1}{X_{ij}}(V_i^2 - V_i V_j cos(\delta_i - \delta_j)) \tag{2}$$

where V_i and V_j are the voltage magnitudes at buses i and j, X_{ij} is the reactance of the line between buses i and j, and $\delta_i - \delta_j$ is the angle difference between phasor voltages V_i and V_j. We have used the shunt voltage-source converter (VSC) FACTS devices in two control modes: voltage magnitude control mode and var control mode. The dynamic model of a shunt VSC FACTS devices is shown in Figure 1.a and its balanced positive sequence model is shown in Figure 1.b where V_i, $i = 1, 2, 3$ is the bus voltage, and Z_1 and Z_2 are the line impedances. Also, γ_{sh} and α_{sh} are conversion ratio signal to control the shunt converter voltage magnitude and the angle of the shunt VSC measured with respect to β of the shunt bus voltage phasor V. The dynamic model of shunt VSC with PID (proportional integrative derivative) controller in voltage magnitude mode and VAR control mode are shown in Figure 2.a and 2.b, respectively. The voltage magnitude V_m and the angle of the VSC voltage are determined from the control signal generated by a PID controller. In voltage magnitude control mode, by fixing k_{dc} to a constant, the VSC voltage magnitude changes in response to changing the capacitor voltage. The bus voltage V_1 is regulated compared to setpoint voltage V_{ref} using outer control loop consisting an integrator with a gain which results in a droop α. The outer loop generates a reactive current I_{sh}^* which acts as the setpoint for the inner control loop. Finally, the shunt reactive current I_{sh}^* is compared to real I_{sh} via the inner PID loop and a low-pass filter. The VSC voltage angle α can then be computed from the bus voltage angle β. In VAR control mode, the shunt reactive current setpoint I_{sh} is directly

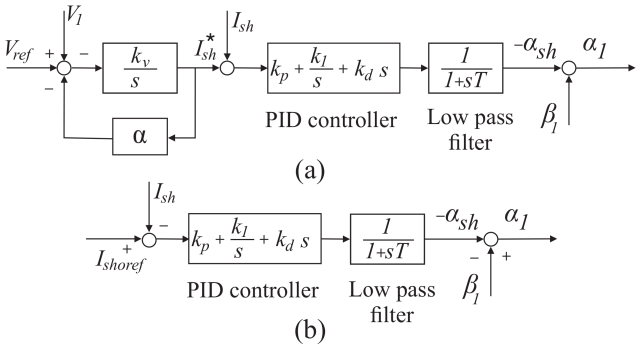


FIGURE 2. Schematic control diagram of a shunt VSC in (a) voltage control mode, (b) VAR control mode.

determined (without an outer loop) and compared with real I_{sh} to trigger the PID controller.

The inserted voltage by VSCs can be approximated as

$$V_m = k_m V_{dc} e^{j(\alpha_{sh}+\beta)} \tag{3}$$

where V_{dc} and k_m are the capacitor terminal voltage and the conversion ratio between the dc-side and ac-side voltages, respectively. From Figure 1.b, the line current I_s can be written as

$$I_{sh} = \frac{V_m - V_1}{jX_t} \tag{4}$$

and the active power that can be injected to the system is

$$P_{sh} = -\frac{V_1 V_m sin(\beta - \alpha_{sh})}{X_t} \tag{5}$$

and the reactive power injected to the system is equal to

$$Q_{sh} = \frac{V_1(V_m cos(\beta - \alpha_{sh}) - V_1)}{X_t}. \tag{6}$$

When the system is oscillating, the control signal is not zero and the capacitor C will exchange reactive power with the power system which results in increasing or decreasing the capacitor voltage V_{dc} following the equation

$$C\frac{dV_{dc}}{dt} = I_{dc} \tag{7}$$

where I_{dc} is the capacitor current. After transition time, the control signal converges to zero and, as a result, the energy exchange between the capacitor and power system converges to zero. With an ideal VSC model, the active power on its ac and dc sides are equal ($P_{ac} = V_{dc}I_{dc}$). Thus we can write

$$\frac{dV_{dc}}{dt} = \frac{1}{CV_{dc}}P_{ac}. \tag{8}$$

The dynamic model of power system can then be constructed by interfacing the dynamic model of FACTS device with other network components attained from the Kirchhoff electrical equations in order to analyze the power flow.

III. THE MODERATED k-SECURITY APPROACH FOR OBSCURING THE CRITICAL NETWORK DATA FOR ADVERSARIES

In this section, the cyber-security of critical elements of power grid is addressed using a graph theoretic property, i.e., graph symmetry. In discrete algebra, the graph symmetry is quantified using the automorphism group. It is verified that graph symmetry has a significant role in determining the controllability of the underlying network [61]. In fact, symmetry is an obstruction to controllability. The higher the number of automorphisms, the more symmetric is the network and, in turn, more driver nodes are required for full state controllability. These driver nodes, in the context of power networks, are the well known FACTS devices ([8], [9], [16], and [18]) or wide area controllers ([64], [65]).

A. DEFINITIONS AND PROPOSED THEOREMS

A notion of symmetry, k-symmetry, is leveraged here to make the critical nodes/edges indistinguishable by adversary agents. Necessary and sufficient conditions for security are attained and a novel algorithm is proposed for cyber-security constrained placement of FACTS devices. The bigger the symmetry group, the more symmetric the underlying graph is. On the other hand, symmetry is an obstruction to controllability [61] meaning a bigger number of FACTS devices are required when the network is more symmetric. We compute the symmetry index (Aut($\mathcal{G}$) or Gen($\mathcal{G}$)) before and after removing a node possessing a FACTS device as a measure of how critical is this node. This index is computed in simulation section for 49-bus and 1, 176-bus systems.

Now, we leverage on the concept of k-security to obscure the identification of critical elements of power grid.

Definition 9 [55]: Let $\mathcal{G}_k$ be the released version of $\mathcal{G}$. The set of critical nodes $\mathcal{V}_c$ of $\mathcal{G}$ is k-secure if the adversary cannot distinguish it from $\mathcal{G}_k$ with a probability greater than $1/k$. The set of critical edges $\mathcal{E}_c$ of $\mathcal{G}$ is k-secure if the adversary cannot distinguish them from $\mathcal{G}_k$ with a probability greater than $1/k$.

Now, we introduce the concept of moderated-k-symmetry which will be used in Theorem 11 to adapt an approach for securing the most critical elements of the power grid.

Definition 10: A graph $\mathcal{G}$ satisfies moderated-k-symmetry if for the finite set of nodes v_l there exists $k-1$ distinct automorphisms $\sigma_{i,1}(v_l), \sigma_{i,2}(v_l), \ldots, \sigma_{i,k}(v_l)$ that satisfy

(i) $\sigma_{i,m}(v_l) \neq \sigma_{i,n}(v_l)$ if $m \neq n$, and

(ii) $\sigma_i(v_l) \neq v_l$ for $l = 1, \ldots, n$.

Theorem 11: The critical nodes/edges of $\mathcal{G}$ are k-secure if $\mathcal{G}$ satisfies moderated-k-security for the finite set of nodes $v_c = \{v_1, \ldots, v_i\}$.

Proof: If $\mathcal{G}$ is moderated-k-symmetric, then for every critical node v_c there are $k-l$ distinct mappings that preserve the network structure after permuting v_c. For any accessible structural information $\mathcal{G}_k$ for the adversary targeting node v_c there are at least k distinct nodes that act the same structural role as v_c. Hence, the adversary cannot distinguish v_c with a probability greater than $1/k$. Subsequently, for a successful

attack on an edge, the adversary needs to identify the end nodes of the targeted edge. Hence the probability of identifying an edge is equal to $1/k \times 1/k = 1/k^2$. □

Theorem 11 can be used to secure the cyber graph of the power network by releasing a permuted graph to the public. However, the approach is not optimal as usually not all critical nodes are permuted by the k number of automorphisms in Aut($\mathcal{G}$). We have improved this approach by relating the concept of moderated-k-security to the case where only the critical nodes are needed to be secured. Moreover, the automorphism groups typically have a gigantic size for medium and large networks [58] and it is not possible to compute and sweep over all of them. Theorem 12 resolves these issues by leveraging on the symmetric characteristics of generators of automorphisms.

Theorem 12: Assume that the adjacency matrix of $\mathcal{G}$ is diagonalizable and symmetry preserving, b is the indicator vector associated to the set $\mathcal{F}$ containing $|\mathcal{F}|$ number of FACTS devices, and $\mathcal{G}_P$ is the published network to the public. Having access to $\mathcal{G}_P$, the adversary cannot distinguish the critical nodes and edges of the network with the probabilities greater than $1/(p(1+q)-1)$ and $1/(p(1+q)-1)^2$, respectively, where p and q are the multiplicities of the critical node/s in Gen($\mathcal{G}$) and the size of disjoint generators denoted by $|Gen_{dis}(\mathcal{G})|$.

Proof: Assume $\mathcal{A}'$ is the adjacency matrix associated with $\mathcal{G}_P$. Since $\mathcal{G}_P$ is the permuted graph of $\mathcal{G}$ under an automorphism σ_l, and $\sigma_l \in$ Aut($\mathcal{G}$), we can write $\mathcal{A}' = \mathcal{A}$ which simply means that the adjacency matrix of the published graph is preserved under mapping that generates $\mathcal{G}$. Given $F_{v_l}^{Gen}$, $M_{v_l}^{Gen}$, and $F_{\cdot} \circ M$ as the set of generators that fixes v_l, the set of generators that moves v_l, and the pointwise composition of $F_{v_l}^{Gen}$ and $M_{v_l}^{Gen}$, respectively, we can write

$$|M_{v_l}^{Aut}| \geq |M_{v_l}^{Gen}| + |M_{v_l}^{F_{\cdot}\circ M}|. \tag{9}$$

The above equation can be written as

$$|M_{v_l}^{Aut}| \geq p + p.q. \tag{10}$$

Therefore the multiplicity of critical nodes in Gen($\mathcal{G}_P$) is at least $p(1+q)$. Then the immediate result, according to Theorem 11, is that the network is moderated-k-secure where $k = p(1+q)-1$. □

B. PROPOSED ALGORITHM FOR LOCATING AND SECURING CRITICAL FACTS DEVICES

Associating the cyber-security to p and q in Theorem 12 guarantees conservative bounds on the probabilities of recognizing the critical elements. The reason for this is that conditions of Theorem 12 are derived assuming that all compositions of automorphisms moving a critical node with joint generators and mediators will fix the joint nodes, which, in practice, is a very rare possibility. In fact, since the size of automorphism group is very big compared with generator set, the probabilities of recognizing the critical nodes and edges are far less than $1/(p(1+q)-1)$ and $1/(p(1+q)-1)^2$, respectively. This means that the probability of recognizing the critical elements is lower than the bounds guaranteed by Theorem 12. The proposed symmetry-based approach for identifying and protecting the critical data of the cyber networks is summarized in the Algorithm 1.

Algorithm 1 An Algorithm for Finding and Securing the Critical FACTS Devices

Input: The graph $\mathcal{G}$ of the power network

Output: The number and locations of FACTS devices and the cyber-secured topology of the power network

1: Perform the maximum matching procedure on the graph of power network to attain the set of unmatched nodes.
2: Assign a FACTS device to each unmatched node.
3: Compute the adjacency matrix $\mathcal{A}$ of the network
4: Compute Gen($\mathcal{G}$) from $\mathcal{A}$ using Sage.
5: Find the set of FACTS devices $\mathcal{F}$ with maximum multiplicity in Gen($\mathcal{G}$).
6: **for** i=1:$|\mathcal{F}|$ **do**
7: Remove the FACTS device number i.
8: Compute the symmetry index (Aut(G) or Gen($\mathcal{G}$)) after removing the FACTS device number i.
9: **end for**
10: Sort all values of |Aut(G)| or |Gen($\mathcal{G}$)| attained in steps 6-9 from the highest to the lowest value in a vector z which will be correspondent to the critical FACTS devices from highest to the lowest critical device.
11: The lowest amount of |Aut(G)| or |Gen($\mathcal{G}$)| corresponds to the most critical node identified in Step 1.
12: Order the critical elements in a vector e_r from maximum critical to the minimum critical element.
13: Determine the generator φ that moves the most critical nodes.
14: Attain the cyber-secured graph under the act of φ attained in Step 13.

C. DISCUSSIONS

In this paper, the placement of FACTS devices is pursued using the network topology. The physical parameters of the power systems are then used to analysis the power flow with fixed FACTS controllers. As the network size increases, the proposed approach is more effective since the typical network symmetry group is bigger and the nodes with maximum multiplicities in generators of automorphisms are more effective in determining the number of required FACTS devices. Furthermore, for large symmetry sizes, the associated vast obscurity can be realized by further reducing the probability of distinguishing the most critical nodes of the grid. In a similar manner, the proposed approach for identifying the critical nodes can be used to identify the critical edges. We do this by (a) removing the edges with at least one end connected to a FACTS controller with maximum multiplicity in Gen($\mathcal{G}$), and (b) following steps 3-12 for edges instead of FACTS devices.

TABLE 1. Parameters of the modified 49-bus system [66] for power flow analysis: Bus number, bus voltage magnitude $|V|$ in volts, angle of bus θ, net active power of the bus P_n in MW, and the net reactive power of the bus Q_n in MVar.

Bus	|V| (V)	θ (deg)	P_n (MW)	Q_n (MVar)	Bus	|V| (V)	θ (deg)	P_n (MW)	Q_n (MVar)
1	380	0	-35	-12	26	347	-12	-33	-17
2	366	-10	45	12	27	338	-11	127	45
3	372	-5	-39	45	28	358	-9	212	67
4	361	2	-73	-27	29	349	4	-37	-17
5	353	0	-87	-42	30	376	-14	-22	-15
6	383	-1	-63	-28	31	359	-1	-39	-13
7	345	-4	-22	-9	32	366	-10	-47	-19
8	347	-8	-52	-24	33	330	6	237	121
9	369	5	-45	-19	34	369	-9	-78	-33
10	346	-7	-39	-21	35	354	7	-49	-18
11	338	5	-27	-11	36	357	-11	256	79
12	339	-8	-56	-21	37	347	-12	-56	-26
13	339	-5	-37	-14	38	327	-10	-67	-17
14	349	-7	-68	-34	39	337	-12	-44	-15
15	353	-11	-65	-13	40	347	-13	-32	-14
16	345	-8	277	101	41	369	-9	255	98
17	349	6	-55	-23	42	350	-7	-43	-19
18	350	8	284	121	43	352	2	-61	-27
19	354	3	-45	-22	44	357	-7	-27	-13
20	351	-12	-37	-17	45	352	-3	-83	-36
21	334	-11	189	82	46	323	-6	302	143
22	336	-5	-64	-34	47	341	-9	-45	-21
23	354	3	-12	8	48	339	-6	-74	-31
24	337	-11	-43	-19	49	350	-5	-64	-25
25	355	-12	-32	-8					

A novel advantage of the proposed methodology is that the symmetry concept is inherent in the graph of the network; therefore, no manipulation is required as we only leverage on an intrinsic property of the network. The impacts of symmetry on the number and locations of FACTS devices and their roles in the security of the underlying cyber graph motivate the consideration of symmetry characteristics of the grid in developing the existing networks or constructing new networks. Embedding the asymmetrical structures makes the system more controllable which, in turn, reduces the number of required FACTS devices which leads to more security realization.

The critical elements of the grid can be identified using the proposed symmetry analysis. It will be observed in simulations of section IV that these critical nodes are usually the same nodes that are selected as the locations of FACTS controllers. This is quite interesting as the locations of FACTS controllers are at the unmatched nodes attained from the maximum matching principle while the critical nodes are attained from a totally different technique, i.e. nodes with maximum multiplicities in the symmetry groups are identified as critical nodes. This re-emphasizes the role of symmetry for explaining the emergent behavior of a complex power network.

The proposed cyber-security approach is implemented after placement of the FACTS devices. It obscures identifying the data associated to FACTS devices by leveraging on the symmetry characteristics of the grid. In fact, the proposed security approach only deals with the cyber graph and has no compromising implication for the physical graph of power network. Thus the approach does not compromise the original functionalities of the FACTS devices. However, the placement result can, to some extent, impact on the level of cyber-security. This is because the symmetry characteristics of the set of FACTS devices might be slightly different for different configurations of FACTS devices in the grid. This difference is not significant since the majority of FACTS devices are placed at the locations of driver nodes identified from symmetry analysis.

IV. IMPLEMENTATION OF THE PROPOSED CYBER CONSTRAINED PLACEMENT OF FACTS CONTROLLERS ON THREE POWER NETWORKS

The proposed topology-based approach for placement, control, and securing FACTS devices is implemented for the small 49-bus, moderate 274-bus, and a large 1,176-bus systems of references [66], [67], and [68], respectively. For the 274-bus and 1,176 bus systems, the emphasis is on the effectiveness of the proposed approach for obscuring the critical data for moderate/large networks.

A. SIMULATIONS AND ANALYSES OF 49-BUS SYSTEM

The physical graph of the 49-bus system with 59 transmission lines is shown in Figure 3. There are 9 generation buses where all of them are load buses as well. The rest of buses are considered as load buses. The physical parameters of 49-bus system including the voltage magnitude and angle, active, and reactive power of all 49 busses are presented in Table 1. The line parameters for each of 59 transmission lines are presented in Tables 2 where $|V|, \theta, R, X$ and B are the bus voltage magnitude in volts, angle of bus voltage in degree, line resistance in ohms (Ω), line reactance in ohms (Ω), and capacitive susceptance in siemens (s), respectively. The conductance is

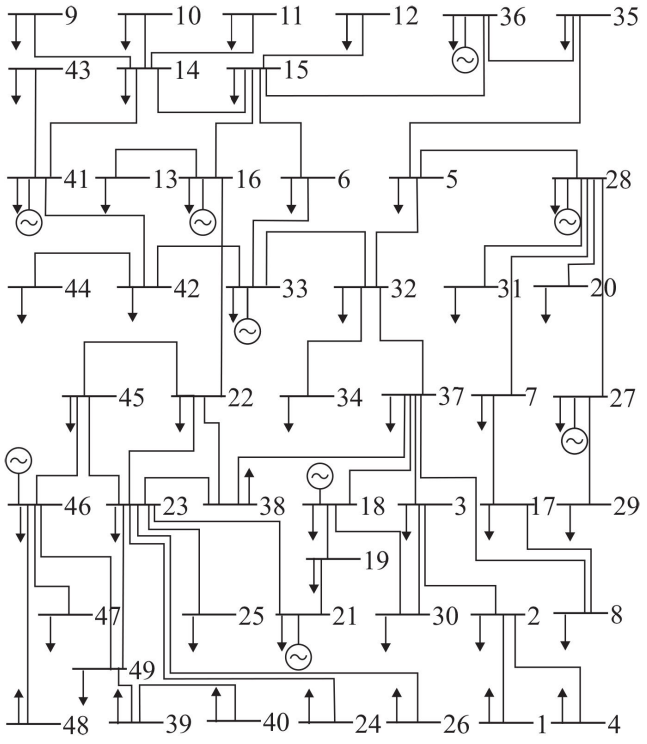


FIGURE 3. The schematic diagram of the modified 49-bus system [66].

considered zero at all lines. The maximum matching principle is implemented on the graph of the 49-bus system and the matched edges are illustrated with red lines in Figure 4. Implementing the MMP has resulted in 7 unmatched nodes at locations 4, 9, 10, 24, 25, 47 and 48 which, according to the maximum matching principle adapted in Section III, can be considered as the locations of FACTS devices. Therefore, seven series VSC FACTS controllers with 100-MVA rating at a voltage of 1 p.u. are located at the determined locations (Figure 4). The power flow transmission is analysed in MATLAB using Newton Raphson algorithm to solve for a vector of bus voltage magnitudes and angles. The parameters of PID controller are selected after trial and error. The proportional coefficient is $k_p = 0.3$, the integrator coefficient is $k_i = 0.5$, and the derivative parameter is $k_d = 0.05$. The power flow analysis of 49-bus system is performed in MATLAB by interfacing the 7 shunt VSC-FACTS devices with the network. The network parameters including the line/bus voltage, angle, and apparent power before and after adding the FACTS controllers are presented in Figure 5. The Newton Raphson algorithm has reached the solution after 28 iterations. The bus voltage magnitudes of all busses before and after using the FACTS controllers are illustrated in Figure 5.a. The voltage drop from the voltage base of 1 p.u. has significantly reduced after using the FACTS controllers. The average magnitude voltage of all 49 buses before and after using FACTS devices are 0.9233 p.u. and 0.9947 p.u., respectively, that means over %7.7 increase in the average of bus voltage magnitudes. The active power flow transfer of all 59 lines are compared and demonstrated in Figures 5.b. The sums of active power flow

TABLE 2. Parameters of the modified 49-bus system [66] for power flow analysis: line number as "$l : i - j$" where l is the line number and i and j are the the nodes at two ends of the line number l, line resistance R in ohms (Ω), reactance X in ohms (Ω), and capacitive susceptance B in siemens (s).

line	R (Ω)	X (Ω)	B (s)	line	R (Ω)	X (Ω)	B (s)
1:1-2	0.40	0.23	0.213	31:6-33	0.23	0.15	0.034
2:2-3	0.10	0.04	0.124	32:32-33	0.35	0.31	0.042
3:2-4	0.12	0.03	0.154	33:7-34	0.54	0.24	0.635
4:9-14	0.40	0.33	0.163	34:32-34	0.51	0.34	0.122
5:10-14	0.05	0.23	0.017	35:28-35	0.5	0.38	0.210
6:11-14	0.39	0.06	0.213	36:15-36	0.23	0.34	0.045
7:6-15	0.43	0.28	0.143	37:35-36	0.34	0.04	0.030
8:12-15	0.10	0.36	0.013	38:3-37	0.04	0.09	0.027
9:14-15	0.23	0.33	0.123	39:8-37	0.45	0.41	0.037
10:13-16	0.25	0.29	0.114	40:18-37	0.03	0.08	0.028
11:15-16	0.32	0.35	0.026	41:32-37	0.12	0.25	0.033
12:7-17	0.23	0.14	0.118	42:22-38	0.34	0.33	0.015
13:8-17	0.24	0.18	0.216	43:23-38	0.04	0.13	0.035
14:18-19	0.03	0.07	0.028	44:37-38	0.45	0.04	0.035
15:7-20	0.32	0.04	0.238	45:39-40	0.03	0.08	0.043
16:19-21	0.24	0.03	0.018	46:41-14	0.12	0.01	0.123
17:16-22	0.09	0.04	0.118	47:42-33	0.34	0.03	0.145
18:22-23	0.10	0.24	0.219	48:41-42	0.43	0.03	0.136
19:23-24	0.03	0.32	0.173	49:43-41	0.45	0.04	0.120
20:23-25	0.05	0.07	0.133	50:44-42	0.43	0.02	0.040
21:23-26	0.23	0.04	0.115	51:45-21	0.02	0.05	0.179
22:5-28	0.34	0.03	0.266	52:45-22	0.04	0.13	0.220
23:20-28	0.10	0.23	0.326	53:46-45	0.06	0.08	0.040
24:27-28	0.03	0.05	0.246	54:47-46	0.04	0.24	0.254
25:27-29	0.05	0.28	0.166	55:48-46	0.34	0.04	0.074
26:3-30	0.23	0.01	0.226	56:49-23	0.33	0.03	0.135
27:18-30	0.13	0.08	0.216	57:49-39	0.43	0.11	0.255
28:20-31	0.04	0.09	0.173	58:49-45	0.45	0.13	0.130
29:5-32	0.03	0.05	0.046	59:49-46	0.05	0.03	0.220
30:44-28	0.05	0.24					

before and after using FACTS controllers are 3, 052 MW and 3, 153 MW, respectively. Equivalently, there is 101 MW power flow increase with using FACTS controllers. Also the line power losses for all 59 transmission lines before and after placing the FACTS controllers are shown in Figure 5.c. The sum of power losses has been reduced from 8.65 MW to 7.08 MW indicating an overall improvement of over %18.

To secure the data exchange between FACTS controllers using the proposed topological approach, first the cyber graph of the 49-bus system is adapted from its physical graph as shown in Figure 4. The size of Aut($\mathcal{G}$) for this network is computed in Sage and is equal to 144 (More explanation about computing the symmetry characteristics of the graph is presented in Appendix A). Although this is not a significantly large number and we can effectively compute the determining set by sweeping over all automorphisms, but we proceed with Gen($\mathcal{G}$) instead to adhere to the proposed approach of this paper. Later, for larger networks (274-bus and 1, 176-bus systems), it will be shown that we can not sweep over the corresponding automorphism groups due to their gigantic sizes. The generators of automorphisms Gen($\mathcal{G}$) of 49-bus system are computed in Sage as

$$\text{Gen}(\mathcal{G}) = \{\varepsilon, (1, 4), (9, 10), (10, 11), (24, 25), (47, 48)\}$$

and illustrated inside the dashed loops in Figure 4 (See Appendix A for calculating Gen($\mathcal{G}$)). The necessary

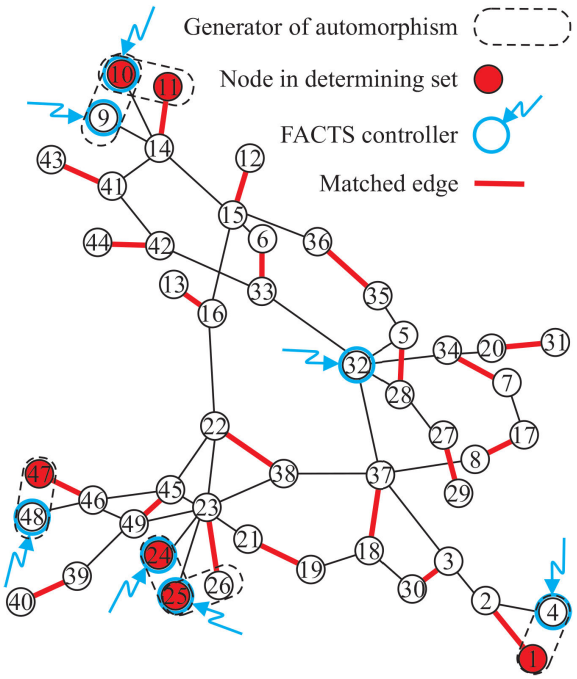


FIGURE 4. The duplicated topology of the network shown in Figure 3 generated in Sage. Red nodes are the set of nodes in determining set, red transmission lines are the matched edges attained from MMP, nodes inside the dashed loops are the set of nodes in Gen($\mathcal{G}$), and the blue rings with arrows represent the FACTS controllers which are positioned at the unmatched nodes attained from MMP.

conditions of controllability in Lemma 7 are tested and the determining set over Gen($\mathcal{G}$) is determined as $\mathcal{F} = \{1, 10, 11, 24, 25, 47\}$. Interestingly, it can be observed that the set of determined locations for FACTS devices attained from MMP is a subset of locations of generators of automorphisms. This verifies the importance of symmetry in controllability of power networks.

To investigate the cyber-security of FACTS devices, we first construct the cyber-graph of the network based on the available physical graph. The cyber graph is illustrated in Figure 4. The cyber-security of the most critical nodes of 49-bus system can be investigated using Theorem 12. The maximum multiplicity of the critical nodes in Gen($\mathcal{G}$) is 2, i.e., $p = 2$, and the number of disjoint generators is 4. Therefore, by publishing a permuted network instead of the original network, the probability of the critical nodes and edges being recognized by an adversary is not greater than 1/9 and 1/81, respectively. It should be noted that under this permutation, the actual obscurity for adversary agent is even more than these values. This is because the maximum multiplicities of nodes in Aut($\mathcal{G}$) is 96 and the number of disjoint automorphisms is 4. Thus the actual probability of distinguishing the FACTS devices is less than 1/385. However, for networks with bigger sizes, it is not feasible to compute the whole set of automorphisms and we have to rely on generators of automorphisms. This is verified via the simulation results on the next two networks, 274-bus and 1, 176-bus systems.

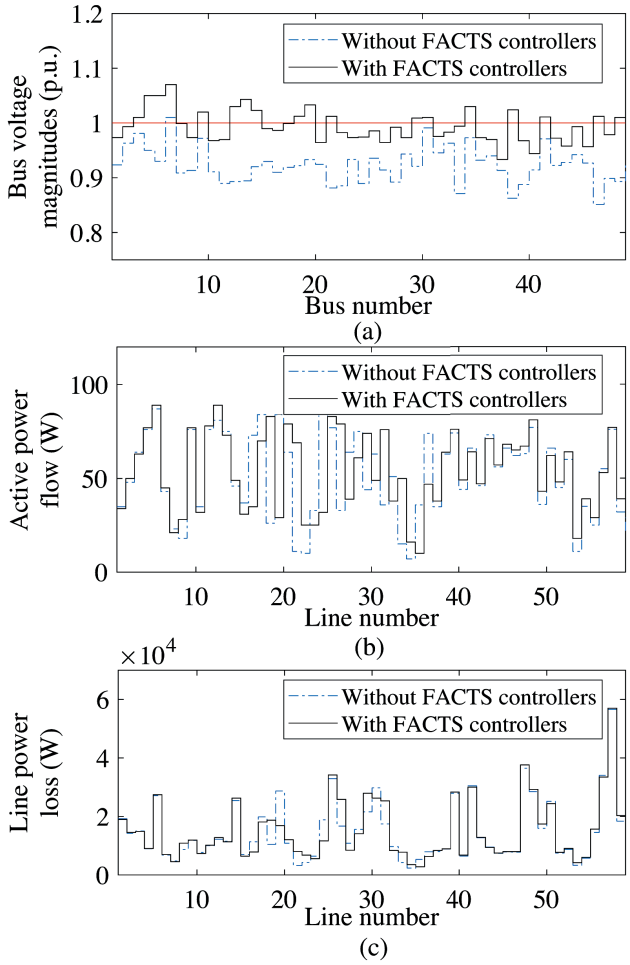


FIGURE 5. The power flow analysis of 49-bus system before and after using FACTS controllers. (a) The average of bus voltage magnitude has increased from 0.9233 p.u. to 0.9947 p.u. that means %0.0774 p.u. increase. (b) The active power flow, which shows the overall 101 MW (or %3) addition of active power transfer throughout the transmission lines. (c) The line power loss, which indicates %18 reduction in power loss in the 59 transmission lines after using FACTS controllers.

B. SIMULATIONS AND ANALYSES OF 274-BUS SYSTEM

We perform simulations for the 274-bus system to better clarify the advantages of the proposed approaches for larger networks. Since the networks' parameters such as the impedances of the lines are not available for these two networks, we have not investigated the impacts of the proposed FACTS placement. We only determine the locations of FACTS controllers, the cyber-security, and the symmetry analysis for these networks. The FACTS placement impacts can be investigated in the same way as performed on the 49-bus system.

The 274-buss system is the equivalenced representation of US power grid [67] which has 274 nodes and 1, 338 edges as illustrated in Figure 6. The number of automorphisms of this network is 28, 311, 552. Therefore, it is not computationally effective to sweep over this huge number of automorphisms. However, the size of Gen($\mathcal{G}$) for this network is very small compared to automorphism group and is equal to 23. The maximum matching principle is implemented on this network

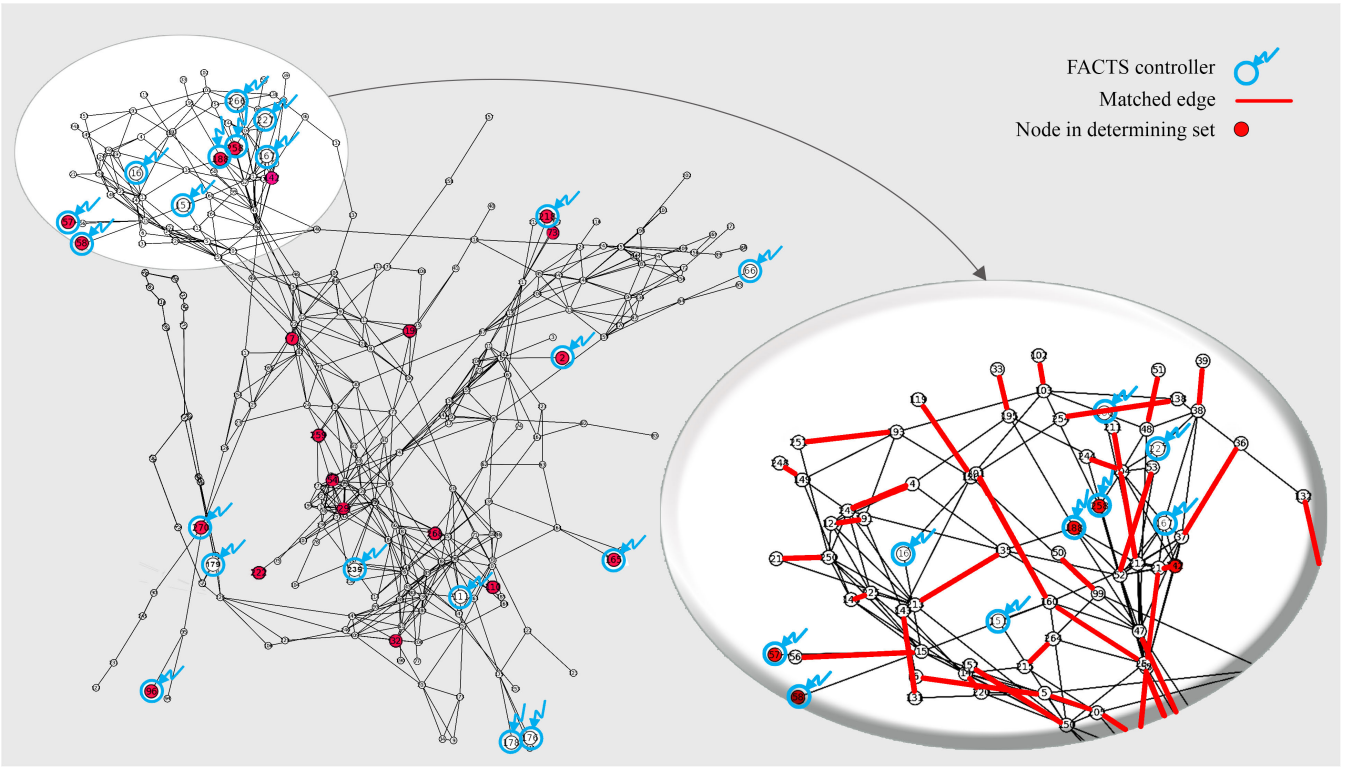


FIGURE 6. The MMP performed on the graph of 274-bus system. The unmatched nodes are considered as the locations of FACTS controllers. For clarification, a portion of matched edges is magnified on the right side of the figure. In total, 253 out of all 1338 edges are matched edges.

TABLE 3. The results of FACTS placement and cyber-security of critical data using moderated-k-security indicating the number of nodes $|\mathcal{V}|$, edges $|\mathcal{E}|$, matched edges $\mathcal{M}$, number of required facts controllers $|\mathcal{F}|$, the average voltage of all buses in p.u. without FACTS controller $|\mathcal{V}_0|$ and with FACTS controllers $|\mathcal{V}^*|$, the total power flow in lines without FACTS controllers $|\mathcal{P}_0|$ and with FACTS controllers $|\mathcal{P}^*|$, the total line power losses without FACTS controllers $\mathcal{P}_{L0}$ and with FACTS controllers $\mathcal{P}_L^*$, the size of automorphism group |Aut| and generators of automorphism |Gen|, the size of determining set $|\mathcal{S}|$, maximum multiplicity of nodes in generators of automorphisms p, the number of disjoint generators q, the probability of distinguishing the data associated to the critical nodes $\mathcal{P}_\mathcal{V}$ and edges $\mathcal{P}_\mathcal{E}$ by adversary. The results of FACTS placement on the voltage and power flow and power loss of 274-bus and 1, 176-bus systems are not computed since these networks' information are not available. "NC" stands for "Not computed".

Simulation task			MMP		FACTS placement on the physical graph						Symmetry results			Cyber-security of critical data			
System	$\|\mathcal{V}\|$	$\|\mathcal{E}\|$	$\mathcal{M}$	$\|\mathcal{F}\|$	$\|\mathcal{V}\|_0$	$\|\mathcal{V}\|^*$	$\mathcal{P}_0$	$\mathcal{P}^*$	$\mathcal{P}_{L0}$	$\mathcal{P}_L^*$	|Aut|	|Gen|	$\|\mathcal{S}\|$	p_A	q_G	$\mathcal{P}_\mathcal{V}$	$\mathcal{P}_\mathcal{E}$
49-bus [68]	49	59	21	7	0.92	0.99	3052	3153	8.65	7.08	144	6	4	2	6	0.11	0.01
274-bus [69]	274	1338	253	20	NC	NC	NC	NC	NC	NC	28311552	23	21	1	21	0.047	0.002
1,176-bus [70]	1176	18552	1121	53	NC	NC	NC	NC	NC	NC	$10E259$	377	33	4	237	0.001	$10E-6$

and matched edges are identified (A portion of these matched edges are denoted by red lines in Figure 6). This has resulted in 20 unmatched nodes that are selected as the locations of FACTS devices. Since it is not possible to compute the maximum multiplicities of nodes in Aut($\mathcal{G}$) we compute the multiplicities of nodes in Gen($\mathcal{G}$). The maximum multiplicity of nodes in Gen($\mathcal{G}$) for 274-bus system is 1 and the size of disjoint generators is 21. It follows from Theorem 12 that $p = 1$ and $q = 21$. Correspondingly, the probabilities of the critical nodes being recognized when the adversary has access only to a permuted version of 274-bus network is no greater than $1/(1.(1+21)-1) \simeq 0.047$. Similarly, the probability of identifying the critical edges, assuming one end at the critical node, is not greater than $1/(1.(1+21)-1)^2 \simeq 0.002$.

C. SIMULATIONS AND ANALYSES OF LARGE 1,176-BUS SYSTEM

We also examine the security of the 1, 176-bus system [68] which has 1, 176 nodes and 18, 552 edges. The number of automorphisms of this network is approximately 10^{259}. Clearly, it is computationally prohibitive to generate the whole set of automorphisms and then compute the maximum multiplicities of nodes within the set. However, the size of Gen($\mathcal{G}$) for this graph is 377. We performed the MMP on this network and identified 437 unmatched nodes which are then considered as the locations of FACTS devices. The maximum multiplicity of the most repeated nodes in Gen($\mathcal{G}$) is 4 and the size of disjoint generators is 237. Following the conditions of Theorem 12, the probability of recognizing the

TABLE 4. The determining set attained from symmetry analysis and the locations of FACTS controllers attained from MMP. The overlap between the set of FACTS locations attained from MMP and the determining set underscores an important impact of symmetry on networked systems. The number of 4 out of 6 nodes of determining set of 49-bus system, 8 out of 21 nodes of the determining set of 274-bus system, and 14 out of 33 nodes of determining set of 1, 176-bus are also selected as the locations of facts controllers by MMP.

System	Determining set $\mathcal{S}$ attained from symmetry analysis	The locations of FACTS controllers $\mathcal{F}$ attained from MMP
49-bus [68]	$\{1, 10, 11, 24, 25, 47\}$	$4, 9, 10, 24, 25, 47, 48$
274-bus [69]	{2, 16, 17, 18, 28, 30, 32, 54, 57, 65, 73, 95, 111, 142, 166, 178, 219, 222, 259, 268, 271}	3, 7, 58, 59, 67, 97, 112, 142, 166, 168, 177, 179, 180, 189, 219, 222, 236, 259, 267, 271
1,176-bus [70]	{5, 25, 55, 76, 129, 131, 188, 241, 276, 288, 308 , 366, 376, 455, 465, 475, 516, 547, 627, 668, 670, 695, 712, 734, 746, 765, 777, 805, 824, 849, 852, 931, 948}	5, 24, 40, 54, 70, 73, 92, 107, 112, 129, 132, 147, 152, 154, 172, 189, 212, 241, 276, 286, 296, 306, 307, 331, 346, 356, 366, 376, 386 , 396, 426, 455, 465, 476, 515, 549, 627, 668, 680, 694, 711, 732, 746, 765, 771, 787, 803, 824, 835, 851, 937, 948, 1031

data associated to the FACTS devices and the critical edges in 1, 176-bus system are 10^{-3} and 10^{-6}, respectively. Due to space limitations, it is not possible to illustrate the graph of 1, 176-bus system.

The simulation results are summarized in Tables 3-4. As can be observed in Table 4, there is an overlap between the nodes in determining set and the set of nodes that are considered as the locations of FACTS controllers by MMP. For the 49-bus, 274-bus, and 1, 176-bus systems, these overlaps are %66, %38, and %42, respectively. Although all nodes in determining set are not selected as the locations of FACTS controllers, yet it is inline with Lemma 7 since for every node in determining set which is not selected as a FACTS controller there is an alternative node belonging to $\mathcal{F}$ and within the same generator of automorphism which plays a same structural role in the network and, as such, can be alternatively selected as the location of FACTS controllers. For example, in 49-buss system, node 1 is in determining set but is not in $\mathcal{F}$. As demonstrated in Figure 4, nodes 1 and 4 belong to a same generator of automorphism and, according to Lemma 7, a necessary condition for controllability is that only one of these nodes must be included in the set of FACTS controllers. This further highlights the importance of symmetry in explaining some aspects of the network behavior.

V. CONCLUSION

The placement of FACTS devices in power systems with the consideration of cyber-security of associated data exchange is addressed from a CN controllability perspective based on advanced topological techniques which, unlike the conventional methods, has no computational impediments. The proposed solution is attained using: i) the concepts of MMP and moderated-k-security to guarantee the cyber-security of the most critical data related to the FACTS controllers., ii) the idea of moderated-k-symmetry to arrange the published cyber graph based on generators of automorphisms that will significantly obscure the data exchange over the cyber graph for adversaries, and iii) the similarity between the set of critical nodes attained from the symmetry analysis to enhance the FACTS placement solution. The proposed solution procedure is implemented on the modified small 49-bus, moderate 274-bus, and large 1,176-bus systems. The power flow analysis of 49-bus system shows that the voltage magnitudes of all buses have increased by reaching to near 1 p.u. and the active power flow over the transmission lines has increased by %3 while the total power losses has decreased by %18 due to reactive compensation by FACTS controllers. In addition, the most critical data of the cyber graph is attributed to data exchange between FACTS controllers. This is in line with the verified importance of these controllers for the whole network performance. The cyber-security of these controllers are then addressed by obscuring the data exchange throughout the nodes assigned as the locations of these controllers. To this end, the network symmetry is leveraged to identify the set of permutations within the symmetry group for which the most critical nodes corresponding to the locations of FACTS controllers are permuted. It is verified in the paper that publishing any of the graphs associated to the network structure mapped by one of these permutations can significantly obscure the source of critical data for adversaries.

Throughout the simulations, an overlap is observed between the set of nodes in determining set and the set of nodes assigned as the locations of FACTS controllers by MMP. This further reveals the importance of symmetry in power network analysis. Therefore, another novel contribution of this paper is that finding the set of driver nodes for a power system can be translated to finding the set of nodes with highest repetitions in the symmetry group. Potential forthcoming research directions may be on: i) considering the network topology while addressing future expansions of the existing networks or constructing a new network, and ii) expanding the proposed approach to also address sizing of FACTS devices.

APPENDIX A
COMPUTATIONAL CLARIFICATION

In this appendix, the computation process of the proposed approaches are explained. First, we clarify how to compute MMP in MATLAB and then the symmetry analysis is discussed in Sage.

A. COMPUTING THE MATCHED EDGES AND UNMATCHED NODES OF MMP

The required data for performing MMP is the adjacency matrix of the network. Once the adjacency matrix of the

underlying graph of the network is constructed in MATLAB, we can attain the full set of matched edges using the command

$$\gg maximal\_matching(A)$$

which uses a matching function in MATLAB. In all our case studies, MATLAB was able to compute the whole set of matched edges and unmatched nodes in a few seconds. Thus finding the locations of FACTS devices (or unmatched nodes) does not impose a big computation burden.

B. CALCULATING THE SYMMETRY GROUPS

The previous studies (for example [61]) rely on computing the automorphism group to identify the determining set (which can be used to find the set of driver nodes) while the proposed approach of this paper is based on computing the generators of automorphisms. The computational advantage of the proposed approach can be distinguished simply by comparing the size of automorphism groups with the size of generators of automorphisms. For the small grid of 49-bus system, it is shown in section IV.A that there are only 144 automorphissms and it is possible to compute and sweep over this range. However, for the moderate 274-bus system, and the large 1, 176-bus system, it is shown that the sizes of the corresponding automophism groups are 28, 311, 552 and 10^{259}, respectively. Therefore, it is not computationally effective to compute these sets and sweep over them. In addition, the large number of automorphisms makes it very difficult, if not impossible, to find the critical nodes as it needs to compute all automorphisms and then sweep over them to find the set of nodes with maximum multiplicities in Aut($\mathcal{G}$). However, the novel approach of this paper addresses these computational issues by adapting generators of automorphisms instead of automorphism groups. As indicated in sections IV.B and IV.C, the number of generators of automorphisms for 274-bus is 23, and for 1, 176-bus systems it is equal to 381. Clearly sweeping over these small sets of generators is more computationally effective than sweeping over the very large number of automorphisms associated with theses systems. There are effective algorithms, such as those in [63] for computing the automorphism group but, in general, the algorithms for calculating automorphism group and elementary automorphisms are well-known and rather trivial. These algorithms are built in some commands in SageMath or similar computing tools. Once the underlying graph is constructed in Sage, computing the automorphism group and the elementary automorphisms can be easily done using the following commands:

$$> \mathcal{G}.automorphismgroup().list()\#Computing\ \mathrm{Aut}(\mathcal{G})$$
$$> \mathcal{G}.gens()\quad \#Computing\ \mathrm{Gen}(\mathcal{G}).$$

However, for moderate/large scale networks, the first command will not result in the list of automorphisms. Only the cardinality of automorphism group can be computed using the following commands:

$$> \mathcal{A} = \mathcal{G}.automorphismgroup()$$
$$> \mathcal{A}.cardinality().$$

REFERENCES

[1] J. Bhukya and V. Mahajan, "Optimization of controllers parameters for damping local area oscillation to enhance the stability of an interconnected system with wind farm," *Int. J. Elect. Power Energy Syst.*, vol. 119, Jul. 2020, Art. no. 105877, doi: 10.1016/j.ijepes.2020.105877.

[2] A. H. Elmetwaly, A. A. Eldesouky, and A. A. Sallam, "An adaptive D-FACTS for power quality enhancement in an isolated microgrid," *IEEE Access*, vol. 8, pp. 57923–57942, 2020, doi: 10.1109/ACCESS.2020.2981444.

[3] A. AL Ahmad and R. Sirjani, "Optimal placement and sizing of multi-type FACTS devices in power systems using metaheuristic optimisation techniques: An updated review," *Ain Shams Eng. J.*, Dec. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2090447919301510, doi: 10.1016/j.asej.2019.10.013.

[4] A. M. S. Yunus, A. Abu-Siada, M. A. S. Masoum, M. F. El-Naggar, and J. X. Jin, "Enhancement of DFIG LVRT capability during extreme short-wind gust events using SMES technology," *IEEE Access*, vol. 8, pp. 47264–47271, 2020, doi: 10.1109/ACCESS.2020.2978909.

[5] M. Moghbel, M. A. S. Masoum, A. Fereidouni, and S. Deilami, "Optimal sizing, siting and operation of custom power devices with STATCOM and APLC functions for real-time reactive power and network voltage quality control of smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5564–5575, Nov. 2018, doi: 10.1109/TSG.2017.2690681.

[6] A. M. S. Yunus, M. A. S. Masoum, and A. Abu-Siada, "Application of SMES to enhance the dynamic performance of DFIG during voltage sag and swell," *IEEE Trans. Appl. Supercond.*, vol. 22, no. 4, Aug. 2012, Art. no. 5702009, doi: 10.1109/TASC.2012.2191769.

[7] A. M. Shiddiq Yunus, A. Abu-Siada, and M. A. S. Masoum, "Sag and flicker reduction using hysteresis-fuzzy control based SMES Unit," *Can. J. Electr. Comput. Eng. Meas.*, vol. 42, no. 1, pp. 52–57, Nov. 2019. [Online]. Available: https://www.semanticscholar.org/paper/Sag-and-Flicker-Reduction-Using-Hysteresis-Fuzzy-Yunus-Habriansyah/600645-7b32c099a4dc039042f8433fcfb1b4a65b, doi: 10.1109/CJECE.2019.2891272.

[8] E. Naderi, M. Pourakhbari-Kasmaei, and H. Abdi, "An efficient particle swarm optimization algorithm to solve optimal power flow problem integrated with FACTS devices," *Appl. Soft Comput.*, vol. 80, pp. 243–262, Jul. 2019, doi: 10.1016/j.asoc.2019.04.012.

[9] M. Ghiasi, "Technical and economic evaluation of power quality performance using FACTS devices considering renewable generations," *Renew. Energy Focus*, vol. 29, pp. 49–62, Jun. 2019, doi: 10.1016/j.ref.2019.02.006.

[10] M. M. Eladany, A. A. Eldesouky, and A. A. Sallam, "Power system transient stability: An algorithm for assessment and enhancement based on catastrophe theory and FACTS devices," *IEEE Access*, vol. 6, pp. 26424–26437, 2018, doi: 10.1109/ACCESS.2018.2834906.

[11] G. Carpinelli, P. Caramia, A. Russo, and P. Varilone, "Voltage stability in unbalanced power systems: A new complementarity constraints-based approach," *IET Gener., Transmiss. Distrib.*, vol. 9, no. 14, pp. 2014–2023, Nov. 2015, doi: 10.1049/iet-gtd.2014.0990.

[12] J. Zhu, K. Cheung, D. Hwang, and A. Sadjadpour, "Operation strategy for improving voltage profile and reducing system loss," *IEEE Trans. Power Del.*, vol. 25, no. 1, pp. 390–397, Jan. 2010, doi: 10.1109/TPWRD.2009.2033968.

[13] M. Adnan, M. Tariq, Z. Zhou, and H. V. Poor, "Load flow balancing and transient stability analysis in renewable integrated power grids," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 744–771, Jan. 2019, doi: 10.1016/j.ijepes.2018.06.037.

[14] S. W. Mohod and M. V. Aware, "A STATCOM-control scheme for grid connected wind energy system for power quality improvement," *IEEE Syst. J.*, vol. 4, no. 3, pp. 346–352, Sep. 2010, doi: 10.1109/JSYST.2010.2052943.

[15] N. A. Bakar and K. M. Mohd, "Optimal placement of TCSC in transmission network using sensitivity based method for multi objective optimization," in *Proc. IEEE Sys. Conf. Energy Convers.*, Kuala Lumpur, Malaysia, Oct. 2017, pp. 321–329, doi: 10.1109/CENCON.2017.8262484.

[16] Y. Li, C. Rehtanz, S. Ruberg, L. Luo, and Y. Cao, "Assessment and choice of input signals for multiple HVDC and FACTS wide-area damping controllers," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 1969–1977, Nov. 2012, doi: 10.1109/TPWRS.2012.2189865.

[17] F. Hu, K. Sun, A. Del Rosso, E. Farantatos, and N. Bhatt, "Measurement-based real-time voltage stability monitoring for load areas," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2787–2798, Jul. 2016, doi: 10.1109/TPWRS.2015.2477080.

[18] A. Lashkar Ara, A. Kazemi, and S. A. N. Niaki, "Multiobjective optimal location of FACTS shunt-series controllers for power system operation planning," *IEEE Trans. Power Del.*, vol. 27, no. 2, pp. 481–490, Apr. 2012, doi: 10.1109/TPWRD.2011.2176559.

[19] N. Khalesi, N. Rezaei, and M. R. Haghifam, "DG allocation with application of dynamic programming for loss reduction and reliability improvement," *Int. J. Elec. Pow. Energy Sys.*, vol. 33, no. 2, pp. 243–262, Feb. 2011, doi: 10.1016/j.ijepes.2010.08.024.

[20] M. Nojavan, H. Seyedi, and B. Mohammadi-Ivatloo, "Voltage stability margin improvement using hybrid non-linear programming and modified binary particle swarm optimisation algorithm considering optimal transmission line switching," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 4, pp. 815–823, Feb. 2018, doi: 10.1049/iet-gtd.2016.1895.

[21] M. Jadidbonab, M. J. Vahid-Pakdel, H. Seyedi, and B. Mohammadi-ivatloo, "Stochastic assessment and enhancement of voltage stability in multi carrier energy systems considering wind power," *Int. J. Electr. Power Energy Syst.*, vol. 106, pp. 572–584, Mar. 2019, doi: 10.1016/j.ijepes.2018.10.028.

[22] R. Muzzammel, M. Ahsan, and W. Ahmad, "Non-linear analytic approaches of power flow analysis and voltage profile improvement," in *Proc. Power Gener. Syst. Renew. Energy Technol. (PGSRET)*, Jun. 2015, pp. 1–7, doi: 10.1109/PGSRET.2015.7312232.

[23] G. Blanco, F. Olsina, F. Garces, and C. Rehtanz, "Real option valuation of FACTS investments based on the least square Monte Carlo method," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1389–1398, Aug. 2011, doi: 10.1109/TPWRS.2010.2094211.

[24] S.-J. Huang and X.-Z. Liu, "Application of artificial bee colony-based optimization for fault section estimation in power systems," *Int. J. Electr. Power Energy Syst.*, vol. 44, no. 1, pp. 210–218, Jan. 2013, doi: 10.1016/j.ijepes.2012.07.012.

[25] B. Mozhgan, "Using neural network to control STATCOM for improving transient stability," *J. Artif. Intell. Elect. Eng.*, vol. 1, no. 1, pp. 26–31, 2012.

[26] R. K. Pandey and D. K. Gupta, "Integrated multi-stage LQR power oscillation damping FACTS controller," *CSEE J Pow. Energy Sys.*, vol. 4, no. 1, pp. 83–92, Mar. 2018, doi: 10.17775/CSEEJPES.2016.00510.

[27] L. J. Cai and I. Erlich, "Fuzzy coordination of FACTS controllers for damping power system oscillations," in *Proc. MEPS Conf.*, 2002. [Online]. Available: https://www.semanticscholar.org/paper/Fuzzy-Coordination-of-FACTS-Controllers-for-Damping-Cai-Erlich/83124e7e6eddc20b2f77114e78e2d5f34983daa9

[28] H. Shayeghi, H. A. Shayanfar, S. Jalilzadeh, and A. Safari, "Design of output feedback UPFC controller for damping of electromechanical oscillations using PSO," *Energy Convers. Manage.*, vol. 50, no. 10, pp. 2554–2561, Oct. 2009, doi: 10.1016/j.enconman.2009.06.005.

[29] A. Satheesh and T. Manigandann, "Maintaining power system stability with FACTS controllers using artificial bee algorithm and ANN," *J. Theo. Appl. Inf. Tech.*, vol. 49, no. 1, pp. 38–47, Mar. 2013.

[30] T. Niknam, M. R. Narimani, J. Aghaei, and A. R. Azizipanah, "Improved PSO for multi- objective OPF considering the cost, loss, emission and voltage stability index," *IET Gen. Trans. Dist.*, vol. 6, no. 6, pp. 515–527, Jun. 2012, doi: 10.1049/iet-gtd.2011.0851.

[31] M. Rezaei Adaryani and A. Karami, "Artificial bee colony algorithm for solving multi-objective optimal power flow problem," *Int. J. Electr. Power Energy Syst.*, vol. 53, pp. 219–230, Dec. 2013, doi: 10.1016/j.ijepes.2013.04.021.

[32] P. Kumkratug, "Application of Lyapunov theory and fuzzy logic to control shunt FACTS devices for enhancing transient stability in multimachine system," *J. Electr. Eng. Technol.*, vol. 7, no. 5, pp. 672–680, Sep. 2012, doi: 10.5370/JEET.2012.7.5.672.

[33] J. Aghaei, A. Heidari, M. Asban, M. Zarei, V. G. Agelidis, and S. Ghavidel, "Determining potential stability enhancements of flexible AC transmission system devices using corrected transient energy function," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 2, pp. 470–476, Feb. 2016, doi: 10.1049/iet-gtd.2015.0849.

[34] C. Guo, W. Jiang, and C. Zhao, "Small-signal instability and supplementary coordinated damping-control of LCC-HVDC system with STATCOM under weak AC grid conditions," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 246–254, Jan. 2019, doi: 10.1016/j.ijepes.2018.06.055.

[35] C. Madtharad, S. Premrudeepreechacharn, N. R. Watson, and R. Saeng-Udom, "An optimal measurement placement method for power system harmonic state estimation," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 1514–1521, Apr. 2005, doi: 10.1109/TPWRD.2004.841309.

[36] P. R. Sahu, P. K. Hota, and S. Panda, "Whale optimization algorithm for fuzzy lead-lag structure SSSC damping controller design," in *Proc. 14th IEEE India Council Int. Conf. (INDICON)*, Dec. 2017, pp. 1–5.

[37] D. P. Ladumor, I. N. Trivedi, R. H. Bhesdadiya, and P. Jangir, "Optimal power flow with shunt flexible AC transmission system (FACTS) device using grey wolf optimizer," in *Proc. 3rd Int. Conf. Adv. Electr., Electron., Inf., Commun. Bio-Inform. (AEEICB)*, Feb. 2017, pp. 387–391, doi: 10.1109/AEEICB.2017.7972338.

[38] Y. C. Kuyu and F. Vatansever, "Real loss minimization in power systems via recent optimization techniques," in *Proc. 2nd Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2018, pp. 1–4.

[39] H. Hamour, S. Kamel, H. Abdel-mawgoud, A. Korashy, and F. Jurado, "Distribution network reconfiguration using grasshopper optimization algorithm for power loss minimization," in *Proc. Int. Conf. Smart Energy Syst. Technol. (SEST)*, Sep. 2018, pp. 1–5, doi: 10.1109/SEST.2018.8495659.

[40] T. George, A.-R. Youssef, M. Ebeed, and S. Kamel, "Ant lion optimization technique for optimal capacitor placement based on total cost and power loss minimization," in *Proc. Int. Conf. Innov. Trends Comput. Eng. (ITCE)*, Feb. 2018, pp. 350–356, doi: 10.1109/ITCE.2018.8316649.

[41] T. K. Behera, M. K. Behera, and N. Nayak, "Spider monkey based improve P&O MPPT controller for photovoltaic generation system," in *Proc. Technol. Smart-City Energy Secur. Power (ICSESP)*, Mar. 2018, pp. 1–6, doi: 10.1109/ICSESP.2018.8376735.

[42] F. Pasqualetti, S. Zampieri, and F. Bullo, "Controllability metrics, limitations and algorithms for complex networks," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 1, pp. 40–52, Mar. 2014.

[43] A. B. Siddique, L. Pecora, J. D. Hart, and F. Sorrentino, "Symmetry- and input-cluster synchronization in networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 97, no. 4, Apr. 2018, Art. no. 042217, doi: 10.1103/PhysRevE.97.042217.

[44] Y. Li, B. Hu, K. Xie, L. Wang, Y. Xiang, R. Xiao, and D. Kong, "Day-ahead scheduling of power system incorporating network topology optimization and dynamic thermal rating," *IEEE Access*, vol. 7, pp. 35287–35301, 2019, doi: 10.1109/ACCESS.2019.2904877.

[45] L. Wang, Z. Qu, Y. Li, K. Hu, J. Sun, K. Xue, and M. Cui, "Method for extracting patterns of coordinated network attacks on electric power CPS based on temporal–topological correlation," *IEEE Access*, vol. 8, pp. 57260–57272, 2020, doi: 10.1109/ACCESS.2020.2982057.

[46] F. Sorrentino and L. Pecora, "Approximate cluster synchronization in networks with symmetries and parameter mismatches," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 26, no. 9, Sep. 2016, Art. no. 094823, doi: 10.1063/1.4961967.

[47] L. M. Pecora, F. Sorrentino, A. M. Hagerstrom, T. E. Murphy, and R. Roy, "Cluster synchronization and isolated desynchronization in complex networks with symmetries," *Nature Commun.*, vol. 5, no. 1, pp. 1–8, Jun. 2014.

[48] B. Li, Y. Chen, S. Huang, R. Yao, Y. Xia, and S. Mei, "Graphical evolutionary game model of virus-based intrusion to power system for long-term cyber-security risk evaluation," *IEEE Access*, vol. 7, pp. 178605–178617, 2019, doi: 10.1109/ACCESS.2019.2958856.

[49] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018, doi: 10.1016/j.ijepes.2017.12.020.

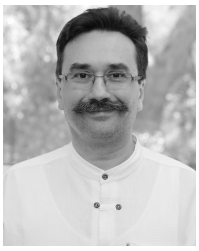
[50] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control," *Int. J. Electr. Power Energy Syst.*, vol. 90, pp. 124–133, Sep. 2017, doi: 10.1016/j.ijepes.2017.01.016.

[51] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094, doi: 10.1016/j.comnet.2019.107094.

[52] L. Zou, L. Chen, and M. T. Özsu, "K-automorphism: A general framework for privacy preserving network publication," *Proc. VLDB Endowment*, vol. 2, no. 1, pp. 946–957, Aug. 2009, doi: 10.14778/1687627.1687734.

[53] J. Yang, B. Wang, X. Yang, H. Zhang, and G. Xiang, "A secure K-automorphism privacy preserving approach with high data utility in social networks," *Secur. Commun. Netw.*, vol. 7, no. 9, pp. 1399–1411, Sep. 2013, doi: 10.1002/sec.840.
[54] Z. Lin, "From isomorphism-based security for graphs to semantics-preserving security for the resource description framework (RDF)," M.S. thesis, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2016.
[55] J. Cheng, A. W.-C. Fu, and J. Liu, "K-isomorphism: Privacy preserving network publication against structural attacks," in *Proc. Int. Conf. Manage. Data SIGMOD*, 2010, pp. 459–470, doi: 10.1145/1807167.1807218.
[56] Y. Liu, J. J. Slotine, and A. L. Barabasi, "Controllability of complex networks," *Nature*, vol. 437, pp. 167–173, May 2011.
[57] A. Chapman, M. Nabi-Abdolyousefi, and M. Mesbahi, "Controllability and observability of Network-of-Networks via Cartesian products," *IEEE Trans. Autom. Control*, vol. 59, no. 10, pp. 2668–2679, Oct. 2014, doi: 10.1109/TAC.2014.2328757.
[58] B. D. MacArthur, R. J. Sánchez-García, and J. W. Anderson, "Symmetry in complex networks," *Discrete Appl. Math.*, vol. 156, no. 18, pp. 3525–3531, Nov. 2008, doi: 10.1016/j.dam.2008.04.008.
[59] W. Wu, Y. Xiao, W. Wang, Z. He, and Z. Wang, "K-symmetry model for identity anonymization in social networks," in *Proc. 13th Int. Conf. Extending Database Technol. EDBT*, 2010, pp. 111–122, doi: 10.1145/1739041.1739058.
[60] H. Parastvand, A. Chapman, O. Bass, and S. Lachowicz, "Graph automorphic approaches to robustness of complex power networks," submitted for publication, *Control Eng. Pract.*, 2020.
[61] A. Chapman and M. Mesbahi, "On symmetry and controllability of multi-agent systems," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 625–630, doi: 10.1109/CDC.2014.7039451.
[62] A. Farrugia and I. Sciriha, "Controllability of undirected graphs," *Linear Algebra Appl.*, vol. 454, pp. 138–157, Aug. 2014, doi: 10.1016/j.laa.2014.04.022.
[63] J. J. Cannon and D. F. Holt, "Automorphism group computation and isomorphism testing in finite groups," *J. Symb. Comp.*, vol. 35, no. 3, pp. 241–267, Mar. 2003, doi: 10.1016/S0747-7171(02)00133-5.
[64] M. Maherani, I. Erlich, and G. Krost, "Robust centralized fixed order wide area damping controller for wind integrated power system," *IFAC-PapersOnLine*, vol. 52, no. 4, pp. 170–175, 2019.
[65] A. Noori, M. Jafari Shahbazadeh, and M. Eslami, "Designing of wide-area damping controller for stability improvement in a large-scale power system in presence of wind farms and SMES compensator," *Int. J. Electr. Power Energy Syst.*, vol. 119, Jul. 2020, Art. no. 105936.
[66] S. Aziz, H. Wang, Y. Liu, J. Peng, and H. Jiang, "Variable universe fuzzy logic-based hybrid LFC control with real-time implementation," *IEEE Access*, vol. 7, pp. 25535–25546, 2019.
[67] B. Dembart and J. Lewis. *Symmetric Structure Equivalenced Presentation of US Power Network*. SuitSparse Matrix Collection. Accessed: May 2020. [Online]. Available: https://sparse.tamu.edu/HB/bcspwr04
[68] A. Erisman. *Symmetric Pattern of Erisman, Summer 1973*. SuitSparse Matrix Collection. Accessed: May 2020. [Online]. Available: https://sparse.tamu.edu/HB/eris1176

HOSSEIN PARASTVAND (Student Member, IEEE) received the B.S. degree in instrumentation and control from the Shiraz University of Technology, Shiraz, Iran, in 2008, and the M.S. degree in control engineering from the Sahand University of Technology, Tabriz, Iran, in 2010. He is currently pursuing the Ph.D. degree with the Smart Energy Systems Group, Edith Cowan University, Joondalup, WA, Australia. From 2010 to 2017, he was a Senior Automation and Control Engineer at MegaTrans Corporation, Iran. His main research interest focuses on the applications of control theories in complex power networks.



OCTAVIAN BASS (Senior Member, IEEE) received the master's and Ph.D. degrees from the Politehnica University Timisoara, Romania, in 1995 and 2001, respectively. His employment history includes research positions at the Budapest University of Technology and Economics, Hungary, The Hong Kong Polytechnic University, Hull University, U.K., and Utsunomiya University, Japan. He was a Lecturer at James Cook University, Australia, from 2006 to 2009, and is currently a Senior Lecturer with the School of Engineering, Edith Cowan University, Perth, Australia. He has coauthored 90 professional publications. His fields of interests include smart grid technologies, renewable energy resources, and non-linear dynamics in power electronics.

MOHAMMAD A. S. MASOUM (Senior Member, IEEE) received the B.S. and M.S. degrees from the University of Colorado Denver, Denver, CO, USA, in 1983 and 1985, respectively, and the Ph.D. degree from the University of Colorado Boulder, Boulder, CO, USA, in 1991, all in electrical and computer engineering. He was an Associate Professor with the Iran University of Science and Technology, Tehran, Iran, from 1993 to 2003, and a Professor with Curtin University, Perth, Australia, from 2004 to 2018. He is currently an Associate Professor with the Department of Engineering, Utah Valley University, Orem, UT, USA. He has coauthored *Power Quality in Power Systems and Electrical Machines* (Elsevier, 2008 and 2015) and *Power Conversion of Renewable Energy Systems* (Springer, from 2011 to 2012). He is an Editor of the IEEE TRANSACTIONS ON SMART GRID and the IEEE POWER ENGINEERING LETTERS.

AIRLIE CHAPMAN (Senior Member, IEEE) received the B.S. degree in aeronautical engineering and the M.S. degree in engineering research from The University of Sydney, Australia, in 2006 and 2008, respectively, and the M.S. degree in mathematics and the Ph.D. degree in aeronautics and astronautics from the University of Washington, Seattle, in 2013. She is currently a Senior Lecturer with the Department of Mechanical Engineering, The University of Melbourne. Her research interests are multi-agent dynamics, networked dynamic systems, data-driven control, and graph theory with applications to robotics and aerospace systems.

STEFAN LACHOWICZ (Senior Member, IEEE) received the M.Eng.Sc. and Ph.D. degrees in electronics engineering from the Lodz University of Technology, Lodz, Poland, in 1981 and 1986, respectively. From 1994 to 1992, he was a Research Assistant and an Assistant Professor with the Institute of Electronics, Lodz University of Technology. Since 1993, he has been a Lecturer with the School of Engineering, Edith Cowan University, Perth, WA, Australia, where he has been a Senior Lecturer, since 2001. He has authored or coauthored about 110 research articles. His current research interests include modern power systems, smart energy systems, electric vehicles, and power electronics.

Author/s:
Parastvand, H; Bass, O; Masoum, MAS; Chapman, A; Lachowicz, S

Title:
Cyber-Security Constrained Placement of FACTS Devices in Power Networks from a Novel Topological Perspective

Date:
2020-06-10

Citation:
Parastvand, H., Bass, O., Masoum, M. A. S., Chapman, A. & Lachowicz, S. (2020). Cyber-Security Constrained Placement of FACTS Devices in Power Networks from a Novel Topological Perspective. IEEE Access, 8, pp.108201-108215. https://doi.org/10.1109/ACCESS.2020.3001308.

Persistent Link:
http://hdl.handle.net/11343/241672

File Description:
Published version