Moving-Target Defense for Detecting Coordinated Cyber-Physical Attacks in Power Grids

Subhash Lakshminarayana*, E. Veronica Belmega† and H. Vincent Poor‡
* School of Engineering, University of Warwick, UK
† ETIS, Université Paris Seine, Université Cergy-Pontoise, ENSEA, CNRS, Cergy-Pontoise, France
‡ Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
Emails: *subhash.lakshminarayana@warwick.ac.uk, †belmega@ensea.fr ‡ poor@princeton.edu

***Abstract*—This work proposes a moving target defense (MTD) strategy to detect coordinated cyber-physical attacks (CCPAs) against power grids. A CCPA consists of a physical attack, such as disconnecting a transmission line, followed by a coordinated cyber attack that injects false data into the sensor measurements to mask the effects of the physical attack. Such attacks can lead to undetectable line outages and cause significant damage to the grid. The main idea of the proposed approach is to invalidate the knowledge that the attackers use to mask the effects of the physical attack by actively perturbing the grid's transmission line reactances using distributed flexible AC transmission system (D-FACTS) devices. We identify the MTD design criteria in this context to thwart CCPAs. The proposed MTD design consists of two parts. First, we identify the subset of links for D-FACTS device deployment that enables the defender to detect CCPAs against any link in the system. Then, in order to minimize the defense cost during the system's operational time, we use a game-theoretic approach to identify the best subset of links (within the D-FACTS deployment set) to perturb which will provide adequate protection. Extensive simulations performed using the MATPOWER simulator on IEEE bus systems verify the effectiveness of our approach in detecting CCPAs and reducing the operator's defense cost.**

I. Introduction

Cyber threats against power grids are of increasing concern due to the deep integration of information and communication technologies (ICT) into grid operation. A recent real-world example was the December 2015 cyber attack against the Ukraine's power grid which resulted in large-scale outages that lasted several hours [1]. The attack was carried out by opening several transmission line circuit breakers and simultaneously blocking the information lines (e.g., telephone lines) to cover up the attacks. Such attacks have alerted us to a general class of attacks called the coordinated cyber-physical attacks (CCPAs).

As the name suggests, a CCPA consists of two components, namely, a physical attack and a cyber attack. The physical attack involves disconnecting a transmission line, generator or transformer. On the other hand, a cyber attack involves manipulating the sensor measurements that are conveyed from the field devices to the control center, and has an effect of masking the physical attack. The attacker may readily launch such a cyber attack by exploiting the power grid's communication vulnerabilities [2]. CCPAs can have severe effects on the grid, since undetected line/generator outages may trigger cascading failures, and have received significant recent attention [3], [4], [5], [6].

To defend against CCPAs, recent studies [4] and [6] have proposed strategies based on securing a set of measurements (e.g., by encryption) or relying on measurements from known-secure phasor measurement units (PMU) deployed in the grid. However, power grids consist of many legacy devices whose life cycles can last several decades, and incorporating major security upgrades in these devices can be quite expensive. Moreover, extensive research has shown that PMUs themselves are vulnerable to false data injection (FDI) attacks, which can be launched by spoofing their GPS receivers [7].

In this work, we propose a novel defense strategy to detect CCPAs based on the technique of moving target defense (MTD). As in prior works [3], [4], [5], [6], we only consider physical attacks that disconnect the transmission lines. We note that to craft an undetectable CCPA, the attacker must obtain an accurate knowledge of certain line reactances [4], [6]. The main idea of the proposed MTD defense in this context is to invalidate the attacker's prior acquired knowledge by actively perturbing of the grid's line reactance settings. This can be accomplished using distributed flexible AC transmission system (D-FACTS) devices, which are capable of performing active impedance injection and are being increasingly deployed in power grids [8]. The proposed MTD defense strategy has the potential to make it extremely difficult for the attacker to track the system's dynamics and gather sufficient information to craft undetectable CCPA. The main contributions of this work are as follows:

- First, we formulate the MTD design problem to defend against CCPAs and identify the MTD design criteria in this context.
- We then propose a solution to the D-FACTS deployment problem using a graph-theoretic approach. Our proposed solution identifies the minimum-sized subset of links for D-FACTS deployment which enables the defender to detect CCPAs against any transmission line.
- However, an MTD solution that involves perturbing a large number the branch reactances can be expensive due to the MTD's operational cost [9]. To reduce the operator's cost of defense, during the system's operational

This work was supported in part by a startup grant at the University of Warwick and in part by the U.S. National Science Foundation under Grants DMS-1736417 and ECCS-1824710.

978-1-5386-8099-5/19/$31.00 ©2019 IEEE

time, we use a game-theoretic formulation to identify the best subset of links to perturb that will provide adequate protection.

Extensive simulations conducted using the MATPOWER simulator shows the effectiveness of our solution. Moreover, the results show that the game-theoretic approach significantly reduces the operator's defense cost.

II. Prior Work

Power grid security has received significant interest in the past few years. In particular, FDI attacks against power grid state estimation have been extensively studied [10], [11], [12]. While FDI attacks affect only the sensor measurements that are conveyed to the control center (and hence consist only of a cyber attack), recent research [3], [4], [5], [6] has studied CCPAs attacks, which as noted above consist of both cyber and physical components. CCPAs were first proposed in [3] based on disconnecting a set of transmission lines and blocking sensor measurements from the attacked area. However, the proposed cyber attack cannot completely mask the effects of the physical attack. Moreover, under some conditions, it was shown that the operator can recover the phase angles and detect the physical attack using information from outside the attacked zone [3]. On the other hand, [4], [5] and [6] proposed the design of cyber attacks that can completely mask the effects of the physical attack under different assumptions about the attacker's knowledge. Further, [4], [5] and [6] have also investigated defense against CCPAs relying on a subset of protected measurements, which however is vulnerable (see Section I).

Recently, the concept of MTD has been applied to defend against FDI attacks [13], [14], [9], [15]. In comparison to these works, we are the first to apply MTD for defense against CCPAs. Our analysis shows that MTD for defending against CCPAs requires the formulation of novel design criteria both in terms of D-FACTS placement as well as D-FACTS perturbation selection in comparison to aforementioned works. Finally, we note that while game theory has been used in the context of defense against FDI attacks [16], [17], this work is the first to apply it in the context of MTD design in power grids.

III. System Model

Power Grid Model: We consider a power grid consisting of N buses and L transmission lines. The set of buses and transmission lines are denoted by $\mathcal{N} = \{1, \ldots, N\}$ and $\mathcal{L} = \{1, \ldots, L\}$ respectively. An example of the IEEE-4 bus system with 5 links is shown in Fig. 1. At bus i, we denote the amount of generation and load by G_i and L_i respectively. We let $l = \{i, j\}$ denote a transmission line $l \in \mathcal{L}$ that connects bus i and bus j and its reactance by x_l. The power flowing on the corresponding line l is denoted by F_l, which under the DC power flow model [18] is given by $F_l = \frac{1}{x_l}(\theta_i - \theta_j)$, where θ_i and θ_j are the voltage phase angles at buses $i, j \in \mathcal{N}$ respectively. In vector form, the power flow vector $\mathbf{f} = [F_1, \ldots, F_L]^T$ is related to the voltage phase angle vector $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_N]$ as $\mathbf{f} = \mathbf{D}\mathbf{A}^T\boldsymbol{\theta}$, where the matrix $\mathbf{A} \in \mathbb{R}^{N \times L}$ is the branch-bus incidence matrix [18] and $\mathbf{D} \in \mathbb{R}^{L \times L}$ is a diagonal matrix of the reciprocals of link reactances. We denote the set of links on which D-FACTS devices are deployed by $\mathcal{L}_D$ where $\mathcal{L}_D \subseteq \mathcal{L}$. D-FACTS devices enable the reactances of these lines to be varied within a pre-defined range $[\mathbf{x}^{\min}, \mathbf{x}^{\max}]$, where $\mathbf{x}^{\min}, \mathbf{x}^{\max}$ are the reactance limits achievable by the D-FACTS devices.

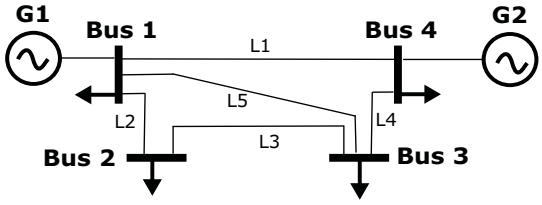

Fig. 1: An example of a 4 bus power grid.

Optimal Power Flow: For any given load condition $\mathbf{l} = [L_1, \ldots, L_N]$, the system operator sets the generation dispatch and line reactance settings by solving the optimal power flow (OPF) problem, stated as follows:

$$C_{\text{OPF}} = \min_{\mathbf{g}, \mathbf{x}} \sum_{i \in \mathcal{N}} C_i(G_i) \tag{1a}$$

$$s.t. \quad \mathbf{g} - \mathbf{l} = \mathbf{B}\boldsymbol{\theta}, \tag{1b}$$

$$\mathbf{f} \in \mathcal{F}, \mathbf{g} \in \mathcal{G}, \mathbf{x} \in \mathcal{X}, \tag{1c}$$

where $C_i(\cdot)$ is the generation cost at bus $i \in \mathcal{N}$. Equation (1a) is the nodal power balance constraint, where the matrix $\mathbf{B} = \mathbf{A}\mathbf{D}\mathbf{A}^T$. Constraints (1c) correspond to the branch power flows, generator limits, and D-FACTS limits, respectively, where $\mathcal{F} = [-\mathbf{f}^{\max}, \mathbf{f}^{\max}], \mathcal{G} = [\mathbf{g}^{\min}, \mathbf{g}^{\max}]$ and $\mathcal{X} = [\mathbf{x}^{\min}, \mathbf{x}^{\max}]$ and $\mathbf{f}^{\max}$ is the maximum permissible line power flow (i.e., the thermal limit) and $\mathbf{g}^{\min}, \mathbf{g}^{\max}$ are the generator limits. We note that in the absence of D-FACTS, OPF optimizes over the generator dispatch values only.

State Estimation & Bad Data Detection: The system state, i.e., the voltage phase angles $\boldsymbol{\theta}$, are estimated from the noisy sensor measurements using the state estimation (SE) technique. The sensor measurements, which we denote by $\mathbf{z} \in \mathbb{R}^M$, correspond to the nodal power injections, and the forward and reverse branch power flows, i.e. $\mathbf{z} = [\tilde{\mathbf{p}}, \tilde{\mathbf{f}}, -\tilde{\mathbf{f}}]^T$ and M is the total number of measurements, where $M = N + 2L$. We denote the sensor measurement noises by a vector $\mathbf{n} \in \mathbb{R}^M$, which is assumed to follow a Gaussian distribution. Under the DC power flow model, the relationship between $\boldsymbol{\theta}$ and $\mathbf{z}$ is given by $\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{n}$, where $\mathbf{H} \in \mathbb{R}^{M \times N}$ is the system's measurement matrix given by $\mathbf{H} = [\mathbf{D}\mathbf{A}^T; -\mathbf{D}\mathbf{A}^T; \mathbf{A}\mathbf{D}\mathbf{A}^T]$ ($[\mathbf{A}; \mathbf{B}]$ denotes the row concatenation of matrices $\mathbf{A}$ and $\mathbf{B}$). The maximum likelihood (ML) technique is used for system state estimation [18]. Under ML estimation, the estimate $\widehat{\boldsymbol{\theta}}$ is related to the measurements $\mathbf{z}$ as $\widehat{\boldsymbol{\theta}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}$, where $\mathbf{W}$ is a diagonal weighting matrix whose elements are reciprocals of the variances of the sensor measurement noise components.

After state estimation, a bad data detector (BDD) computes a quantity referred to as the residual, which we denote by r

as $r = ||\mathbf{z} - \mathbf{H}\widehat{\boldsymbol{\theta}}||$. A bad data alarm is flagged if the residual exceeds a predefined threshold τ. The threshold is adjusted to ensure that the false positive (FP) rate does not exceed α, where $\alpha > 0$ (usually a small value close to zero).

Undetectable False Data Injection Attacks: We denote the FDI attack vector by $\mathbf{a} \in \mathbb{R}^M$, which the attacker injects into the sensor measurements and the measurement vector with the FDI attack by $\mathbf{z}^a$, given by $\mathbf{z}^a = \mathbf{z} + \mathbf{a}$. It has been shown [10] that an FDI attack of the form $\mathbf{a} = \mathbf{H}\mathbf{c}$, where $\mathbf{c} \in \mathbb{R}^N$, remains undetected by the BDD. Specifically, the probability of detection for such attacks is equal to the FP rate α. We call these attacks undetectable FDI attacks.

Coordinated Cyber and Physical Attack: While an FDI attack only modifies the sensor measurements, a CCPA attacks the grid physically followed by a coordinated FDI attack on the sensor measurements, as noted above. In particular, we consider physical attacks that disconnect a set of transmission lines, e.g., by opening the line circuit breakers. The physical attack will alter the power grid's topology and power flow, and the mismatch between the pre-attack (i.e., line disconnections) and post-attack measurements can generally be detected by the BDD. However, it has been shown that if the attacker injects a carefully-constructed coordinated FDI attack on the sensor measurements, then the effect of the physical attack on the BDD residual can be completely masked [6]. Hence, the attack remains undetected by the BDD.

Denote the set of links disconnected by the attacker under a physical attack by $\mathcal{L}_A$. We use the subscript "p" to denote the power grid parameters following the physical attack. It can be shown that the grid measurements post the physical attack are related to the pre-attack measurements by $\mathbf{z}_p = \mathbf{z} + \mathbf{a}_p$, where $\mathbf{a}_p = \mathbf{H}\Delta\theta + \Delta\mathbf{H}\boldsymbol{\theta}_p$, where $\Delta\mathbf{H}$ is the change in the measurement matrix before and after the physical attack, given by, $\Delta\mathbf{H} = \mathbf{H} - \mathbf{H}_p$. Reference [6] showed that in order to mask the effect of the physical attack and remain undetected by the BDD, the attacker must inject a coordinated FDI attack of the form $\mathbf{a} = \Delta\mathbf{H}\boldsymbol{\theta}_p$.

Knowledge Required to Launch a CCPA: Next, we enlist the knowledge required by the attacker to construct an FDI attack of the form $\mathbf{a} = \Delta\mathbf{H}\boldsymbol{\theta}_p$. Assume that the attacker disconnects a single branch $\mathcal{L}_A = \{l\}$ that connects buses i and j. It can be easily verified that $\Delta\mathbf{H}$ depends on the tripped branch reactance x_l only. Therefore, to construct the attack $\mathbf{a} = \Delta\mathbf{H}\boldsymbol{\theta}_p$, the attacker must obtain knowledge of the branch reactance x_l and the difference in phase angles of the buses i and j following the physical attack, i.e., $\theta_{i,p} - \theta_{j,p}$ [6]. The knowledge of $\theta_{i,p} - \theta_{j,p}$ can be obtained by monitoring the line power flows following the physical attack as follows:

$$\theta_{i,p} - \theta_{j,p} = -\sum_{m \in p_l^k} x_{l_m} F_{l_m,p}, \tag{2}$$

where p_l^k is any alternative path between nodes i and j in the residual power network following the physical disconnections, i.e., $\mathcal{L} \setminus \mathcal{L}_A$. Each path p_l^k in turn is a collection of links $p_l^k = \{l_{k_1}, l_{k_2}, \ldots, l_{k_M}\}$ such that $src(l_{k_1}) = i$ and $dst(l_{k_M}) = j$, and k_M is the number of links in the path p_l^k. We denote by $\mathcal{P}_l = \{p_l^1, p_l^2, \ldots, p_l^{K_l}\}$ a collection of all alternative paths between buses i and j, where K_l is the number of such alternative paths. Note that the subscript l denotes the disconnected link.

In the IEEE-4 bus example, assume that the attcker disconnects link 1. After the disconnection, there are two alternative paths between buses 1 and 4, and hence, $K_1 = 2$. These paths are given by $p_l^1 = \{2, 3, 4\}$ with $k_1 = 3$ and $p_l^2 = \{5, 4\}$ with $k_2 = 2$. The attacker can compute the phase angle difference between nodes 1 and 2 using (2) as $\theta_{1,p} - \theta_{j2p} = -(x_2 F_{2,p} + x_3 F_{3,p} + x_4 F_{4,p})$ or, $\theta_{1,p} - \theta_{j2p} = -(x_5 F_{5,p} + x_4 F_{4,p})$.

In (2), the attacker can obtain the knowledge of power flows $F_{l_m,p}$ by monitoring the line flow sensor measurements. On the other hand, the line reactances x_{l_m} can be learned by monitoring the grid power flows over a period of time using existing techniques [19], [20]. The attacker can also learn the reactance of the disconnected branch x_l similarly.

IV. Moving-Target Defense for CCPAs

In this work, we propose a solution to defend the system against CCPAs based on the MTD technique. The main idea behind this approach is to periodically perturb the branch reactances of certain transmission lines to invalidate the attacker's acquired knowledge. Hence, an attack constructed using outdated knowledge of the system can be detected by the BDD. (The reader can refer to [20] for practical guidance on how frequently the branch reactances must be perturbed.) In this section, we first formalize the MTD design problem to defend against CCPAs. The solution to the MTD design problem is presented in Section V. The details are presented next.

Recall from (2) that to construct an undetectable CCPA, the attacker must acquire the following: (i) knowledge of the reactance of the tripped branch, x_l, and (ii) knowledge of branch reactances in at-least one alternate paths p_l^k between the nodes i and j. Therefore, under MTD, the defender can thwart the CCPA by invalidating one of the two:

C1. Invalidate the attacker's knowledge of the tripped branch's reactance x_l.
C2. Invalidate the attacker's knowledge of at-least one of the branches in the path p_l^k between nodes i and j.

Note that the defender however cannot have prior knowledge of which link the attacker chooses to disconnect. Moreover, for a disconnected link l, the defender has no way of knowing which path $p_l^k \in \mathcal{P}_l$ the attacker may have used to compute the phase angle difference $\theta_{i,p} - \theta_{j,p}$ as in (2). Thus, the defender must invalidate the attacker's knowledge of the reactance of at-least one branch in every path $p_l^k \in \mathcal{P}_l$. The defender must do so for every link $l \in \mathcal{L}$ (such that the attacker cannot launch a CCPA by disconnecting any link in the grid). Based on the arguments above, the MTD perturbation selection problem can be stated as follows:

Problem 1 (MTD problem)**.** *For each branch $l \in \mathcal{L}$, invalidate the knowledge of at-least one of the branches in $\{l\} \cup p_l^k,\ k = 1, \ldots, K_l$.*

The MTD perturbation problem poses constraints on the D-FACTS deployment set $\mathcal{L}_D$, since a preliminary requirement to invalidate the attacker's knowledge of a branch reactance is the presence of a D-FACTS device on that link. Thus, $\mathcal{L}_D$ must be chosen in a way that it gives the defender the ability to protect every link $l \in \mathcal{L}$. A trivial solution is to deploy a D-FACTS device on every link of the power grid. However, a system operator may wish to minimize the number of D-FACTS devices installed in order to minimize the device deployment cost.

On the other hand, MTD perturbations incur an opeartional cost for the defender. Reference [9] characterized this cost in terms of the increase in OPF cost of the grid due to the MTD perturbations[1]. Perturbing the reactances of a large number of links may be expensive. Thus, at the system's operational time, the defender may wish to perturb the reactances of only a subset of links, which we denote by $\mathcal{L}_{D_w}$, where $\mathcal{L}_{D_w} \subseteq \mathcal{L}_D$, such that the attacker cannot launch CCPAs against some specific links that are perceived to be important and vulnerable to attack.

In what follows, we provide solutions to both the aforementioned aspects of MTD design problem. Specifically, we first present an algorithm to find the D-FACTS deployment set $\mathcal{L}_D$ that satisfies the MTD design problem with a minimum number of devices based on a graph-theoretic approach. Subsequently, we present a solution to the problem of selecting a subset of links $\mathcal{L}_{D_w}$ for reactance perturbation at the operational time based on a game-theoretic approach.

V. Solution to the MTD Design Problem

In this section, we solve the MTD design problem formalized in Section IV. We first address the problem of finding the D-FACTS deployment set.

A. D-FACTS Deployment

Our key observation to solve the D-FACTS deployment set problem is that each set of links $\{l\} \cup p_l^k, k = 1, \ldots, k_M$, forms a loop in the graph $\mathcal{G}$. For example, in the 4-bus example in Figure 1, assuming that the attacker disconnects link 1, the links $\{1\} \cup \{2, 3, 4\}$ and $\{1\} \cup \{4, 5\}$ form loops in the corresponding graph. If a DFACTS device is installed on a subset of links in the graph such that every loop in the network has at least one link with a D-FACTS device installed, then the attacker cannot launch an undetectable CCPA.

In graph-theoretic terms, the problem is equivalent to removing a subset of links in the network such that the residual graph has no loops. For optimized deployment, $\mathcal{L}_D$ must be the minimum number of such links. If each link is assigned a weight of 1, then $\mathcal{L}_D$ must be a subset of links with minimum weight.

[1]Note that in the absence of MTD, the D-FACTS settings are adjusted to minimize the OPF cost as in (1a). Thus, the MTD perturbations will increase the OPF cost, and the MTD operational cost in non-negative.

The set $\mathcal{L}_D$ can be found by solving the *minimum weight feedback edge set problem in an undirected graph* [21]. The solution proceeds by finding the *maximum weight spanning tree* (MWST). Specifically, let $\mathcal{L}_{\text{sptr}}$ be the MWST of the graph $\mathcal{G}$. If D-FACTS devices are installed on the links $\mathcal{L} \backslash \mathcal{L}_{\text{sptr}}$, then the attacker cannot find a loop within the graph whose branches do not have a D-FACTS device installed. Equivalently, the attacker cannot launch an undetectable CCPA. Further, since the links in $\mathcal{L}_{\text{sptr}}$ form a maximum-weighted spanning tree, $\mathcal{L} \setminus \mathcal{L}_{\text{sptr}}$ are the links with minimum weight which can be disconnected. Equivalently, the links $\mathcal{L} \backslash \mathcal{L}_{\text{sptr}}$ are the minimum number of links that satisfy the D-FACTS desgin problem described in Section IV. Thus, the D-FACTS deployment set $\mathcal{L}_D = \mathcal{L} \setminus \mathcal{L}_{\text{sptr}}$.

Consider the D-FACTS deployment set $\mathcal{L}_D$ chosen according to the above arguments. Assume that the defender perturbs the reactances of the set of links $\mathcal{L}_{D_w} \subseteq \mathcal{L}_D$. Then, we have the following:

- A physical attack against a link l can be detected by the BDD if the links in $\mathcal{L}_{D_w}$ ensure that the conditions listed in Problem 1 are satisfied for that link. We will henceforth refer to such a link to being "protected" under the MTD link perturbation set $\mathcal{L}_{D_w}$.
- Naturally, based on the arguments stated in this section, if $\mathcal{L}_{D_w} = \mathcal{L}_D$, then all the links $l \in \mathcal{L}$ are protected from the physical attacks.

B. MTD Perturbation Selection Using Game Theory

MTD perturbations incur an operational cost, and perturbing the reactances of a large set of links may not be cost effective. In this section, we answer the question of how to select the appropriate perturbation set $\mathcal{L}_{D_w}$. The main idea is to protect only a subset of links from physical attacks depending on the operational state of the system, as well as the perceived threat to those links. This is approached using a game-theoretic formulation. The details are presented next.

1) Game Formulation: We define the strategic interactions between the attacker and the defender as a two-player non-cooperative game. To formalize this, we define the game as a triplet $\mathcal{G} \triangleq (\{D, A\}, \{\mathcal{S}_D, \mathcal{S}_A\}, \{u_D, u_A\})$ in which the components are: (i) the set of players $\{D, A\}$; (ii) $\mathcal{S}_D$ and $\mathcal{S}_A$, the sets of actions that defender and attacker can take respectively; and (iii) the payoffs of the players $u_k : \mathcal{S}_D \times \mathcal{S}_A \to \mathbb{R}$ for $k \in \{D, A\}$, where $u_k(s_D, s_A)$ measures the benefit obtained by player k when the action profile that has been played is $s = (s_D, s_A)$.

We denote the attacker's and the defender's action sets by $\mathcal{S}_A = \{a_0, a_1, \ldots, a_{N_A - 1}\}$ and $\mathcal{S}_D = \{d_0, d_1, \ldots, d_{N_D - 1}\}$ respectively, where N_A and N_D are the cardinality of the sets $\mathcal{S}_A$ and $\mathcal{S}_D$ respectively. The attacker's action set is the subset of links it disconnects physically. We denote the set of links disconnected by the attacker under action a_i by $\mathcal{L}_{a_i}$, where, $\mathcal{L}_{a_i} \subseteq \mathcal{L},\ i = 0, 1, \ldots, N_A - 1$. The action a_0 corresponds to the case when the attacker does not attack any link. The defender's action is to select a subset of links within $\mathcal{L}_D$ whose reactances will be perturbed. We denote the set of links chosen

by the defender under action d_i by $\mathcal{L}_{d_i}$, where, $\mathcal{L}_{d_i} \subseteq \mathcal{L}_D$, $i = 1, \ldots, N_D - 1$. The action d_0 corresponds to the case when the defender does not perturb the reactance of any link.

Next, we characterize the attacker's and the defener's payoffs. The cost of damage due to the attack can be characterized as follows. If the attacker disconnects a link l that is protected by the defender (due to the MTD perturbations), then the CCPA will be detected by the BDD, and the system operator can quickly restore the link to ensure that the attack does not result in any further damage. For instance, the defender can quickly restore the circuit breaker of the disconnected link to a closed position. On the other hand, if the attacker disconnects a link that is not protected by the defender, then the CCPA will go undetected. The link disconnection will result in redistribution of power flows. Consequently, all the links on which the power flows exceeds the corresponding thermal limits will experience physical damage, and will get disconnected from the grid. In this case, the system operator will have to initiate load shedding in order to ensure that the attack does not result in further damage. (Herein, we assume that the BDD will detect the attack once additional links are disconnected, since the attacker's data injection will only mask the effect of disconnection of the first link.) We denote the cost of load shedding at bus i by $C_{i,s}(L_i^s)$, where $L_i^s (\leq L_i)$ is the quantity of load that is shed. We denote $\mathbf{l}_s = [L_1^s, \ldots, L_N^s]$.

Let $C_{\text{OPF}}(a_m, d_n)$ denote the OPF cost when the attacker takes an action a_m and the defender takes an action d_n. It can be computed as follows:

$$C_{\text{OPF}}(a_m, d_n) = \min_{\mathbf{g}, \mathbf{l}_s} \sum_{i \in \mathcal{N}} C_{i,g}(G_i) + C_{i,s}(L_i^s) \quad (3)$$
$$s.t. \quad \mathbf{g} - \mathbf{l} + \mathbf{l}_s = \mathbf{B}_{a_m,d_n} \boldsymbol{\theta},$$
$$\mathbf{f} \in \mathcal{F}, \mathbf{g} \in \mathcal{G},$$

where $\mathbf{B}_{a_m,d_n}$ is given by $\mathbf{B}_{a_m,d_n} = \mathbf{A}_{a_m,d_n} \mathbf{D}_{a_m,d_n} \mathbf{A}_{a_m,d_n}^T$. Here, $\mathbf{A}_{a_m,d_n}$ is the bus-branch connectivity matrix when the attacker and the defender choose actions a_m and d_n respectively. These quantities are computed as in Algorithm 1.

ALGORITHM 1: Cost Computation

Data: a_m, d_n
Result: $C_{\text{OPF}}(a_m, d_n)$
Set branch reactances to $\mathbf{x}_{d_n}$.
Set $\mathbf{A}_{a_m,d_n} = \mathbf{A}_{a_0,d_0}$.
Solve (3) to obtain $C_{\text{OPF}}(a_0, d_n)$.
if *attack is successful* **then**
  Recompute power flows after removing the branches in $\mathcal{L}_{a_m}$.
  Monitor the branches for which the power flow exceeds the line capacity. Denote such links by $\mathcal{L}_{a_m}^c$.
  Set $\mathbf{A}_{a_m,d_n}$, $\mathbf{D}_{a_m,d_n}$ by removing the branches $\mathcal{L}_{a_m}$ and $\mathcal{L}_{a_m}^c$. Solve (3) to compute $C_{\text{OPF}}(a_m, d_n)$.
else
  Set $C_{\text{OPF}}(a_m, d_n) = C_{\text{OPF}}(a_0, d_n)$.
end

Based on the formulation above, the defender's payoff is given by

$$u_D(s_D, s_A) = \begin{cases} C_{\text{OPF}}(d_0, a_0) - C_{\text{OPF}}(s_D, a_0), & \text{if } \mathcal{I}_S = 0 \\ C_{\text{OPF}}(d_0, a_0) - C_{\text{OPF}}(s_D, s_A), & \text{if } \mathcal{I}_S = 1, \end{cases}$$

and the attacker's payoff is

$$u_A(s_D, s_A) = \begin{cases} 0, & \text{if } \mathcal{I}_S = 0 \\ C_{\text{OPF}}(s_D, s_A) - C_{\text{OPF}}(d_0, a_0), & \text{if } \mathcal{I}_S = 1, \end{cases}$$

where $\mathcal{I}_S$ is an indicator variable to represent the success ($\mathcal{I}_S = 1$) or failure of an attack ($\mathcal{I}_S = 0$). Both players aim to choose their actions such that their own payoff is maximized and although the game is not a zero-sum game, we can see that the two players have contradictory objectives. The above payoffs can be explained as follows. First, $C_{\text{OPF}}(d_0, a_0)$ denotes the benchmark operating cost of the defender when none of the players takes an action to either disrupt or defend the system. The term $C_{\text{OPF}}(s_D, s_A) - C_{\text{OPF}}(d_0, a_0)$ denotes the the additional cost incurred by the defender and caused by a successful attack, when the attacker chooses s_A and the defender chooses s_D; the defender's aim is to minimize this cost whereas the attacker wants to maximize it. The term $C_{\text{OPF}}(s_D, a_0) - C_{\text{OPF}}(d_0, a_0)$ represents the additional cost incurred by the defender for choosing an action s_D against an unsuccessful attack s_A; the defender will seek to minimize this cost while neutralizing the attack. Of course, the benefit of the attacker if its attack fails is equal to zero.

2) Solving the Game Formulation: The game described above is discrete and finite. In such an interactive situation, a natural solution is the Nash equilibrium (NE), which is a stable state to unilateral deviation. Mathematically this is defined as:

Definition 1. *A strategy profile (s_D^*, s_A^*) is an NE for the game $\mathcal{G}$ if the following conditions are met: $u_D(s_D^*, s_A^*) \geq u_D(s_D, s_A^*),\ \forall s_D \in \mathcal{S}_D, u_A(s_D^*, s_A^*) \geq u_A(s_D^*, s_A),\ \forall s_A \in \mathcal{S}_A$.*

This means that neither player has any incentive to unilaterally deviate and will lose in terms of utility otherwise. This type of game may not have a pure NE solution but it always has at least one mixed-strategy NE [22], which is the NE of the extension of the game $\mathcal{G}$ to mixed strategies. It is defined as follows: $\widetilde{\mathcal{G}} \triangleq (\{D, A\}, \{\Delta_D, \Delta_A\}, \{\tilde{u}_D, \tilde{u}_A\})$. The action sets of the extended game $\widetilde{\mathcal{G}}$ are the probability simplices of dimension N_k, $k \in \{D, A\}$: $\Delta_k = \left\{ p_k \in \mathbb{R}_+^{N_k} \,\middle|\, \sum_{j=0}^{N_k} p_{k,j} = 1 \right\}$ where $p_k = (p_{k,0}, \ldots, p_{k,N_k-1})$ is the discrete probability vector of player k such that $p_{D,j}$ and $p_{A,j}$ represent the probability of choosing the action d_j by the defender and the probability of choosing the action a_j by the attacker, respectively. The modified payoffs are simply the resulting expected payoffs following the randomization of play:

$$\tilde{u}_k(p_D, p_A) = \sum_{j=0}^{N_D-1} \sum_{i=0}^{N_A-1} u_k(d_j, a_i)\ p_{D,j}\ p_{A,i}. \quad (4)$$

The mixed NE can be defined similarly to the pure strategy NE.

Definition 2. *A mixed strategy profile (p_D^*, p_A^*) is a mixed an NE for the game $\mathcal{G}$ if it is a NE for the extended game $\widetilde{\mathcal{G}}$ and the following conditions are met:* $\tilde{u}_D(p_D^*, p_A^*) \geq \tilde{u}_D(p_D, p_A^*),\ \forall p_D \in \Delta_D$, *and* $\tilde{u}_A(p_D^*, p_A^*) \geq \tilde{u}_A(p_D^*, p_A),\ \forall p_A \in \Delta_A$.

The mixed NE can be computed by using the Von-Neumann indifference principle [22], which basically says that: i) player k is rendered indifferent (in terms of its expected payoff) between its pure actions that are played at the NE with strictly positive probability, by the choice of the other's mixed action p_{-k}, for any $k \in \{D, A\}$; and ii) the actions that are not played at the NE (their probability equals 0 at the NE) give strictly lower payoffs than the ones that are played (see i)), for both players. Formally, this is stated in the following.

Definition 3. *A mixed strategy profile (p_D^*, p_A^*) is a mixed NE for the game $\mathcal{G}$ if it is an NE for the extended game $\widetilde{\mathcal{G}}$ and the following conditions are met:*

1) *both players are indifferent among their own pure actions that are played with positive probability at the NE*

$$\begin{aligned} \tilde{u}_D(d_j, p_A^*) &= \tilde{u}_D(d_i, p_A^*),\ \forall d_j, d_i \in \mathcal{I}_D^*, \\ \tilde{u}_A(p_D^*, a_j) &= \tilde{u}_A(p_D^*, a_i),\ \forall a_j, a_i \in \mathcal{I}_A^*. \end{aligned}$$

2) *the pure actions that result in strictly smaller payoffs are played with zero probability at the NE*

$$\begin{aligned} \tilde{u}_D(d_j, p_A^*) &< \tilde{u}_D(d_i, p_A^*),\ \forall d_j \notin \mathcal{I}_D^*, d_i \in \mathcal{I}_D^*, \\ \tilde{u}_A(p_D^*, a_j) &< \tilde{u}_A(p_D^*, a_i),\ \forall a_j \notin \mathcal{I}_A^*, a_i \in \mathcal{I}_A^* \end{aligned}$$

where the sets $\mathcal{I}_k^* \subseteq \mathcal{S}_k, \forall k$ denote the actions that are played with strictly positive probability at the NE: $\mathcal{I}_D^* = \{d_j \in \mathcal{S}_D : p_{D,j}^* > 0\}$ and $\mathcal{I}_A^* = \{a_j \in \mathcal{S}_A : p_{A,j}^* > 0\}$.

All defender's actions that are not in the set $d_j \notin \mathcal{I}_D^*$ have zero probability at the NE $p_{D,j}^* = 0$ (they are not played at all at the NE) and the same goes for the attaker, all actions $a_j \notin \mathcal{I}_A^*$ have zero probability $p_{A,j}^* = 0$ at the NE. Definition 3 provides a simple way to compute the mixed NEs by solving a system of linear equations and checking some conditions, which we adopt in this work.

VI. Simulation Results

In this section, we perform simulations to show the effectiveness of the proposed defense. All the simulations are carried out using the MATPOWER simulator.

First, we examine the D-FACTS deployment set problem. We perform simulations using the IEEE-14 bus system. As proposed in Section V-A, we solve the minimum weight feedback edge set problem for the graph corresponding to the IEEE-14 bus system. Following this approach, the D-FACTS deployment set is given by $\mathcal{L}_D = \{1, 3, 5, 8, 9, 18, 19\}$. We then perturb the reactances of all the links in the set $\mathcal{L}_D$. We simulate physical attacks against the three most important links in the system, i.e., Links 1, 2 and 3 (which have the maximum power flow among all the links in the bus system) by disconnecting the links (one at a time), and injecting a corresponding CCPA of the form $\mathbf{a} = \Delta\mathbf{H}\boldsymbol{\theta}_p$, where both

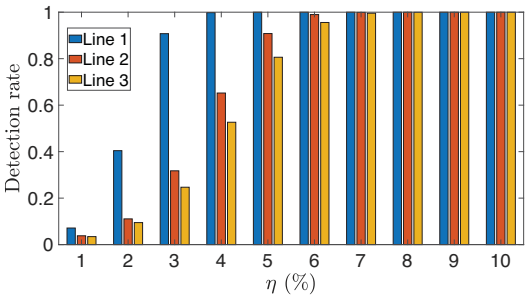

Fig. 2: Attack detection probability as a function of the percentage change (η) in the link reactance.

Bus system	$\lvert\mathcal{L}\rvert$	$\lvert\mathcal{L}_D\rvert$
IEEE 9-bus system	9	1
IEEE 14-bus system	20	7
IEEE 24-bus system	38	15
IEEE 39-bus system	36	8

TABLE I: Size of the D-FACTS deployment set $|\mathcal{L}_D|$ for different IEEE bus systems.

$\Delta\mathbf{H}$ and $\boldsymbol{\theta}_p$ are computed using outdated knowledge of the system. We plot the BDD's attack detection probability for each case in Fig. 2 as a function of the percentage change in line reactances. It can be observed that the CCPAs can be detected with a high probability following the MTD approach. Moreover, about $5 - 6\%$ perturbation in the line reactances is sufficient to achieve a high detection rate. We also enlist the size of the D-FACTS deployment set for different IEEE bus systems in Table I. It can be observed that the proposed algorithm enables the defender to protect all the links in the system with only a few D-FACTS devices. Moreover, this is also the minimum-sized D-FACTS deployment set that can detect any CCPA against the grid. From the table, we can also conclude that $|\mathcal{L}_D|$ depends on not just the size of the bus system, but also its actual topology (e.g., $|\mathcal{L}_D| = 15$ for the 24 bus system, where as $|\mathcal{L}_D| = 9$ for the 39-bus system).

Finally, we show the effectiveness of the game-theoretic approach in reducing the operator's defense cost. The simulations are done on a IEEE-14 bus system. The generation cost is assumed to be linear, i.e., $C_i(G_{i,t}) = c_i G_{i,t}$. The generators' capacities at buses $1, 2, 3, 6, 8$ are $G_{\max} = 300, 50, 30, 50, 20$ MWs and $c_i = 20, 30, 40, 50, 35$ \$/MWh respectively. $\mathbf{f}_{\max}$ is chosen to be 160 MWs for link 1, and 60 MWs for all other links. We consider two load conditions: (i) a heavily loaded system, scenario 1 with the load values at Bus 1 to 14 given by $0, 21.7, 94.2, 47.8, 7.6, 11.2, 0, 0, 29.5, 9, 3.5, 6.1, 13.5, 14.9$ MWs respectively, and (ii) a lightly loaded system, scenario 2 with the load values at Bus 1 to 14 given by $0, 100, 94.2, 47.8, 30, 11.2, 0, 0, 0; 0, 0, 0, 0, 0$ MWs respectively. We consider five MTD perturbation strategies for the defender, i.e., $d_1 = \{1\}, d_2 = \{1, 3\}, d_3 = \{1, 3, 5\}, d_4 = \{1, 3, 5, 8\}, d_5 = \{1, 3, 5, 8, 9, 18, 19\}$. We note that $d_5 = \mathcal{L}_D$, which protects all the links of the system from CCPA. The

Load scenario	NE D-FACTS perturbation set	Defense cost
Scenario 1	{1,3,5,8,9,18,19}	11.62 %
Scenario 2	{1,3,5,8}	2.86 %

TABLE II: D-FACTS perturbation set and the defense cost (the percentage increase in OPF cost) computed using the game-theoretic approach for different load scenarios.

attacker in turn launches a CCPA by disconnecting one of the links at a time. Under this set-up, we compute the NE solution in each of two scenarios according to Definition 3 and the results are listed in Table II. It can be observed that the D-FACTS perturbation sets in the two scenarios are different. While, in the heavily loaded scenario (scenario 1), all the links in $\mathcal{L}_D$ need to be perturbed, in the lightly loaded scenario (scenario 2), it is sufficient to perturb only a subset of links. The rationale is that in the lightly loaded scenario, only a subset of links need to be protected from physical attacks, since the attacker is unlikely to target the unimportant links (i.e., the links that have very little power flow). We also list the defense cost, which is the percentage increase in the OPF cost. The NE solution of scenario 2 incurs much lower defense cost, since only a subset of links are perturbed. The above experiments show that the MTD perturbation set depends on the operational state of the system. By following the proposed game-theoretic approach, the operator can reduce its defense cost.

VII. Conclusions and Future Work

In this work, we have proposed a novel strategy to detect CCPAs based on MTD and presented MTD design criteria in this context. We have identified the subset of links for D-FACTS device deployment that enables the defender to detect physical attacks against any link in the system. Further, to reduce the operator's defense cost, we have identified the set of links whose reactances must be perturbed at the operational time based on a game-theoretic approach.

There are still many open problems. First, D-FACTS devices are traditionally deployed in the grid with an objective of minimizing the transmission losses [23]. On the other hand, in this work, we discuss the D-FACTS device deployment problem from a security point of view only. These considerations suggest that the D-FACTS deployment problem will generally involve a trade-off between minimizing the transmission power losses and the security application. Another important problem arises in the game-theoretic formulation. Definition 3 provides a simple way to compute the mixed NEs by solving a system of linear equations and checking some conditions. Still, in order to use it, one would have to know in advance the faces of the simplex $\Delta_D \times \Delta_A$ on which the NE (p_D^*, p_A^*) lies, i.e., one would have to know the sets $\mathcal{I}_D^*$ and $\mathcal{I}_A^*$ for all NEs in advance. An exhaustive search has exponential complexity: the $(N_D + N_A)$-dimesional simplex has $2^{N_D+N_A}$ faces and all possibilities will have to be considered. Thus, a low-complexity algorithm must be found to compute the NE. We plan to investigate these issues in our future work.

References

[1] "Analysis of the cyber attack on the Ukrainian power grid," http://bit.ly/2ohNwJ1.

[2] "Hackers infiltrated power grids in U.S., Spain," https://bit.ly/2WxFxoj.

[3] S. Soltan, M. Yannakakis, and G. Zussman, "Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery," in *Proc. ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS)*, 2015, pp. 361–374.

[4] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[5] ——, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[6] R. Deng, P. Zhuang, and H. Liang, "CCPA :Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sept. 2017.

[7] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection (IJCIP)*, vol. 5, pp. 146–153, 2012.

[8] D. Divan and H. Johal, "Distributed FACTS; A new concept for realizing grid power flow control," *IEEE Trans. Power Syst.*, vol. 22, no. 6, pp. 2253–2260, Nov 2007.

[9] S. Lakshminarayana and D. K. Y. Yau, "Cost-Benefit analysis of moving-target defense in power grids," in *Proc. IEEE/IFIP Dependable Systems and Networks (DSN)*, June 2018, pp. 139–150.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 21–32.

[11] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[12] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.

[13] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. International Conference on System Sciences*, Jan 2012, pp. 2104–2113.

[14] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. First ACM Workshop on Moving Target Defense*, 2014, pp. 59–68.

[15] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying fdi attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, Aug 2018.

[16] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, March 2013.

[17] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, July 2016.

[18] A. Wood and B. Wollenberg, *Power Generation, Operation, and Control*. A Wiley-Interscience, 1996.

[19] X. Li, H. V. Poor, and A. Scaglione, "Blind topology identification for power systems," in *Proc. IEEE International Conference on SmartGrid Communications (SmartGridComm)*, Oct 2013, pp. 91–96.

[20] S. Lakshminarayana, F. Wen, and D. K. Y. Yau, "Trade-offs in data-driven false data injection attacks against the power grid," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Apr. 2018, pp. 2022–2026.

[21] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*. London : Macmillan, 1976.

[22] D. Fudenberg and J. Tirole, *Game theory*. MIT Press, 1991.

[23] K. M. Rogers and T. J. Overbye, "Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems," in *Proc. North American Power Symposium (NAPS)*, Sept 2008, pp. 1–8.