Moving Target Defense for Hardening the Security of the Power System State Estimation

Mohammad Ashiqur Rahman and Ehab Al-Shaer
Dept. of Software and Information Systems
University of North Carolina at Charlotte, USA
{mrahman4, ealshaer}@uncc.edu

Rakesh B. Bobba
Information Trust Institute & ECE Dept.
University of Illinois at Urbana-Champaign, USA
rbobba@illinois.edu

ABSTRACT

State estimation plays a critically important role in ensuring the secure and reliable operation of the electric grid. Recent works have shown that the state estimation process is vulnerable to stealthy attacks where an adversary can alter certain measurements to corrupt the solution of the process, but evade the existing bad data detection algorithms and remain invisible to the system operator. Since the state estimation result is used to compute optimal power flow and perform contingency analysis, incorrect estimation can undermine economic and secure system operation. However, an adversary needs sufficient resources as well as necessary knowledge to achieve a desired attack outcome. The knowledge that is required to launch an attack mainly includes the measurements considered in state estimation, the connectivity among the buses, and the power line admittances. Uncertainty in information limits the potential attack space for an attacker. This advantage of uncertainty enables us to apply moving target defense (MTD) strategies for developing a proactive defense mechanism for state estimation.

In this paper, we propose an MTD mechanism for securing state estimation, which has several characteristics: (i) increase the knowledge uncertainty for attackers, (ii) reduce the window of attack opportunity, and (iii) increase the attack cost. In this mechanism, we apply controlled randomization on the power grid system properties, mainly on the set of measurements that are considered in state estimation, and the topology, especially the line admittances. We thoroughly analyze the performance of the proposed mechanism on the standard IEEE 14- and 30-bus test systems.

Categories and Subject Descriptors

J.m [**Computer Applications**]: Miscellaneous;
F.4.m [**Theory of Computation**]: Mathematical Logic and Formal LanguagesMiscellaneous

MTD'14, November 3, 2014, Scottsdale, Arizona, USA.

http://dx.doi.org/10.1145/2663474.2663482.

General Terms

Security

Keywords

Power Grid; State Estimation; False Data Injection Attack; Moving Target Defense.

1. INTRODUCTION

In the electric power grid, state estimation (SE) is the process of finding the best estimate for the system state in a weighted least square sense, given a measurement model and a set of measurements acquired through a Supervisory Control and Data Acquisition (SCADA) system. The 'state' corresponds to the vector of bus voltages, from which line currents and power-flows can be computed. State estimation solutions aid system operators in reliability assessment, initiating corrective control measures and enabling pricing calculations for real-time electricity markets. Hence, state estimation is a critical and inherent part of energy management system (EMS) applications for the power grid. However, critical infrastructures relying on SCADA based measurements are vulnerable to cyber-attacks [1]. It is worth mentioning that while phasor measurement units are gradually being deployed, the current grid still largely relies on extensive SCADA measurements for several EMS applications, including state estimation.

Recent work by [2] has revealed that state estimation is vulnerable to cyber-attacks, where adversaries can alter certain measurements by injecting false data to corrupt the estimation, but remain invisible to the system operator by evading the existing bad data detection algorithms. The key idea behind these attacks, called Undetected False Data Injection (UFDI) attacks, is as follows. State estimation uses high measurement redundancy to detect and filter bad or erroneous meter measurements by checking if the measurement residual (l_2-norm of the difference between observed and estimated measurements) is below a certain threshold [3, 4]. An adversary who knows the complete measurement model can then manipulate meter measurements to be consistent with the measurement model to bypass the bad data detection (BDD) process [2]. While the extent of model accuracy on attacks is analyzed in [5], it is shown in [6, 7] that UFDI attacks, when adversaries have perfect knowledge, can be defended if a strategically chosen set of measurements are secured. However, due to the resource constraint issues with legacy equipment, securing those selected measurements might not always be feasible. Moreover, if

one or more secured measurements become unavailable, the correctness of the state estimation is again in question.

An undetected attack on state estimation has several constraints, particularly in terms of an adversary's knowledge of the system and resources for achieving a desired attack outcome. The knowledge that is required to launch an attack mainly includes the measurements that are taken for state estimation, the grid topology (*i.e.*, connectivity among the buses), and the admittances of the power lines [2]. Though partial information might still be sufficient to launch some attacks [5], [8], information uncertainly limits the potential attack space. We take advantage of this uncertainty to apply moving target defense (MTD) strategies for developing a proactive defense mechanism for state estimation.

In this work, we propose an MTD mechanism with the following objectives: (i) increasing the complexity for attackers by introducing uncertainty, (ii) reducing the window of attack opportunity (*i.e.*, the attack space) for attackers, and (iii) increasing the attack cost (*e.g.*, the number of measurements to be compromised). In our MTD mechanism, we randomize the set of measurements that are considered in state estimation and the topology with respect to the line admittances. The choice of a measurement set for state estimation is not unconstrained. The chosen set of measurements should be able to observe the system, *i.e.*, all the unknown states of the system can be computed uniquely from the measurements. We perturb the admittances of a selected number of lines to perturb the topology. In this approach, we assume that a change in the admittance of a line can be performed if a Distributed Flexible AC Transmission System (D-FACTS) device is deployed there [9]. We thoroughly analyze the performance of our mechanism on the standard IEEE 14- and 30-bus test systems [10] using a UFDI attack verification model which we proposed in [11]. Our evaluation shows impressive results in securing state estimation from UFDI attacks by significantly reducing the number of potential attack vectors.

The rest of this paper is organized as follows: In Section 2, we provide the necessary background. We present the MTD mechanism in Section 3. The evaluation results of the MTD mechanism is presented in Section 4. We briefly discuss the related work in Section 5 and conclude in Section 6.

2. BACKGROUND

Stealthy attacks on state estimation (as shown in [2], [5]) were based on the DC (or linearized) power flow model. The DC model is simplistic but is popular as it is useful for preliminary analytical power system studies. We illustrate our techniques using the DC model but the strategies are equally applicable for the AC (non-linear) model. In fact, it is easier for an adversary to attack the DC model and so if we we can defend UFDI attacks against the DC state estimation, then we can expect to do better in the AC context.

2.1 DC Power Flow Model

In the DC power flow model, the power balance equations in a power system are expressed by assuming the impedance of a transmission line purely in terms of its reactance [12]. The voltage magnitudes at all buses are taken fixed at 1 per unit and only the phase angles are treated as the variables. Thus, the voltage phasor at bus i is expressed by $1\angle\theta_i$. Denoting the admittance of the line between buses i and j by Y_{ij}, the real power-flow (P_{ij}) across a transmission line is given by: $P_{ij} = Y_{ij}(\theta_i - \theta_j)$. Y_{ij} is the reciprocal of the reactance. The power-balance constraint that equates the algebraic sum of powers incident at every bus to zero creates a linear system of equations of the form: $[\mathbf{B}][\theta] = [\mathbf{P}]$.

2.2 State Estimation and UFDI Attack

The state estimation problem is to estimate n power system state variables in $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$ based on a set of m ($m > n$) measurements $\mathbf{z} = (z_1, z_2, \cdots, z_m)^T$ [4], according to the following relationship:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$$

Here, $\mathbf{h}(\mathbf{x}) = (h_1(x_1, \cdots, x_n), \cdots, h_m(x_1, \cdots, x_n))^T$ and $\mathbf{e}$ is the vector of measurement errors. In the case of the linearized estimation model (*i.e.*, the DC power flow model), $\mathbf{z} = \mathbf{Hx} + \mathbf{e}$, where $\mathbf{H} = (h_{i,j})_{m \times n}$. $\mathbf{H}$ is known as the Jacobian matrix.

When the measurement errors are zero mean and normally distributed, the state estimate $\hat{\mathbf{x}}$ is calculated as:

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}$$

Here, $\mathbf{W}$ is a diagonal matrix whose elements are reciprocals of variances of the meter errors. Thus, estimated measurements are calculated as $\mathbf{H}\hat{\mathbf{x}}$ and the residual $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$ is used to identify bad data. The condition $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau$ implies the presence of bad data [4], τ is set using a hypothesis test at a significance level. UFDI attacks [2] are based on the idea that if the attack vector $\mathbf{a}$ is taken equal to $\mathbf{Hc}$, then the residual remains unchanged, since $\mathbf{z}+\mathbf{a} = \mathbf{H}(\hat{\mathbf{x}}+\mathbf{c})$, the residual $||(\mathbf{z}+\mathbf{a}) - \mathbf{H}(\hat{\mathbf{x}}+\mathbf{c})|| = ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$. The implicit assumption here is that the adversary has full knowledge of the measurement model $\mathbf{H}$.

2.3 Attack Attributes

The UFDI attack model can be expressed with respect to a number of attributes of an attacker as follows:

- **Knowledge Limitation:** State estimation of a power system is done based on the topology of the grid and a number of power measurements taken on different lines and buses. For a successful UFDI attack, an attacker needs to know the connectivity among the buses and the electrical parameters (*i.e.*, admittances) of the transmission lines [2], which is not trivial. The attacker also needs to know the set of measurements considered in state estimation.

- **Accessibility and Resource Constraints**: An attacker usually does not have access to all of the measurements, when physical or remote access to substations is restricted or when certain measurements are already secured. Additionally, an adversary may be constrained with respect to the cost or effort to mount attacks on measurements vastly distributed. In such cases, an adversary is limited to compromising or altering only a limited subset of measurements or buses. The extent of access is limited by the attacker's resource limitations.

- **Attack Target:** An attacker may have a specific aim of corrupting the estimation of a certain set of state targeting a specific impact on the system.

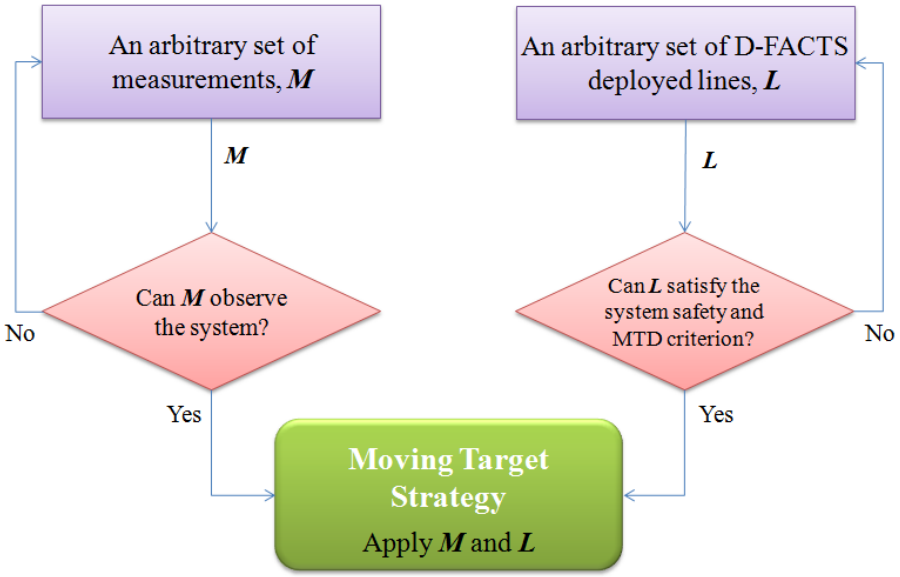

Figure 1: The architecture of moving target defense mechanism for hardening the security of state estimation.

2.4 Moving Target Defense

The idea of moving target defense (MTD) has been studied for a decade, especially in the field of cybersecurity [13]. Typical information technology systems operate in a static environment. Configuration parameters, such as IP addresses, DNS names, network topology, routing entries, security policies, software stacks, etc. remain mostly static over relatively long periods of time. When a system is static, attackers gets enough time to know the configuration and behavior of the system, to understand the vulnerabilities and corresponding attack vectors, and finally, to launch attacks on the system. The same is true for cyber-physical systems like power grids, where the physical and cyber system are highly static, the operations are fixed, and the protocols are known.

Moving target defense is the concept of controlled change across multiple system dimensions in order to (i) increase uncertainty and apparent complexity for attackers, (ii) reduce their opportunity space, and (iii) increase the costs of their probing and attack efforts [14]. Usually, MTD is not meant to provide perfect security. The aim of MTD is to enable the operations to be executed safely in a compromised environment, where the system is defensible rather than perfectly secure. The potential of moving target defense mechanisms lies in being able to randomize or perturb one or more of the UFDI attack attributes. In this work, we devise a moving target defense mechanism considering the knowledge attribute, where we add uncertainty in the information by changing the set of measurements and the topology properties (*i.e.*, line admittances). Even though, the attacker may still be successful in launching UFDI attacks, due to the uncertainty introduced by the MTD strategy, the attack space reduces.

3. MOVING TARGET DEFENSE AGAINST UFDI ATTACKS

In this section, we discuss the strategy of our MTD mechanism and the corresponding formal models.

3.1 Moving Target Defense Strategy

In order to increase the uncertainty of the attacker's knowledge about the power grid system related to state estimation, our MTD mechanism takes two properties of the system: (i) the set of measurements considered in state estimation and (ii) the admittances of a set of lines in the topology. In the following we describe the ideas behind randomizing these properties.

3.1.1 *Changing the set of measurements*

In regular practice, a fixed number of measurements are used in the state estimation process. According to the bad data detection algorithms, some of the measurements can be ignored in the process, if they are noisy enough (*i.e.*, bad) relative to rest of the measurements. An adversary needs to know the set of measurements used in state estimation and alter a group of measurements from the set that are required to launch a specific UFDI attack. If the attacker does not know the measurement set correctly, he may not be able to identify this group of required measurements perfectly, *i.e.*, one or more measurements can be missing in the group or included without necessity. Therefore, if we can randomize the measurement set used in state estimation by including a number of measurements from the unused (but possible) measurements, attackers knowledge about the measurement set becomes uncertain.

For an example, let us consider IEEE 14 bus test system [10], which has 14 buses and 20 lines. With respect to the DC power model, it is possible to have 54 measurements (considering forward and backward power flows through transmission lines and power consumptions at buses). Among these possible measurements, let us assume that a fixed set of 30 measurements are taken (recorded and reported using sensors/meters) for state estimation, while the rest (*i.e.*, remaining 24 potential measurements) are not. According to our MTD mechanism, we can take a set of 7 measurements from the unused measurements by deploying

measurement sensors there (if necessary). Then, from the total 37 measurements, we can select 30 measurements at random to be used in state estimation. However, the selected set must be capable of observe the system. Later in this section, we present a formal model of selecting a measurement set according to the observability requirement.

3.1.2 Perturbing line admittances

There are distributed flexible AC transmission system (D-FACTS) devices, which can be deployed on transmission lines and are capable of performing active impedance (*i.e.*, reactance) injection [15]. Leveraging this capability of D-FACTS devices, we consider the randomization of line admittances in our MTD mechanism. We assume that the admittance of a line can only be randomized if a D-FACTS device is deployed there. However, there are some limitations of using D-FACTS devices. Changes in impedance have impact on the power flows, which can easily impact the power system operations, *e.g.*, the optimal power flow of the system [3].

In order to obtain the effect on the power flows due to the deliberate changes in impedance of power lines with the help of D-FACTS devices, a sensitivity analysis related to D-FACTS devices is thoroughly explained in [9]. In our MTD mechanism, we consider a feasibility constraint in changing line admittances, which ensures that the secured optimal power flow solution [3] remains the same in spite of the changes in the admittances, although some of the power flows must change. We also need to ensure that the changes cannot be very trivial. Further, all the lines with D-FACTS devices will not be randomized always. A set of lines among them will be chosen every time (*i.e.*, with respect to each state estimation), and only admittances of these chosen lines will be changed. We assume that an adversary may know the actual admittance (*i.e.*, base admittance) of each of these lines, though he does not know the change amount, and thereby, the changed admittance is assumed to be unknown to the adversary. We also assume that when a set of line admittances are changed, the previously changed admittances are returned back to the base admittances. As a result, at a particular time admittances of only the selected set of lines are unknown to the adversary.

Arguably power system operations personnel may not be willing to perturb line impedances for the exclusive purpose of detecting attacks. However, D-FACTS based perturbation of line parameters has been considered for minimization of power system losses and voltage control applications [9]. In practice, such line parameter changes could be leveraged for detecting attacks. In the rest of the paper we illustrate the MTD through perturbation of line parameters as exclusively done for attack detection while keeping in mind that perturbation done for other optimization applications could be leveraged instead.

3.2 Formal Model for Strategy Selection

In Figure 1, we show the architecture of moving target defense mechanism. It is a combination of two modules, as shown in the figure: one for the arbitrary set of measurements selection for state estimation and another for the arbitrary set of lines selection for admittance randomization. In this section, we present the formal designs of these two modules. Different notations that we use in these models are shown in Table 1.

Table 1: Modeling Parameters

Notation	Definition
b	The number of buses in the grid.
l	The number of lines in the grid topology.
f_i	The *from-bus* of line i.
e_i	The *to-bus* of line i.
d_i	The admittance of line i.
g_i	Whether the admittance of line i is known.
P_i^L	The power flow through line i.
P_j^B	The power consumption at bus j.
θ_j	The state value: the voltage phase angle at bus j.
n	The number of states.
m	The number of potential measurements.
a_i	If measurement i needs to be altered for the attack.
t_i	Whether potential measurement i is taken.
h_i	Whether the admittance of line i is perturbed.

3.2.1 Basic Power Model

Consistent with the DC power flow model, the admittance of a branch (*i.e.*, line) is computed purely from its reactance. The direction of the line is assumed based on the current flow direction (*i.e.*, from a end-bus to another end-bus). We denote the two end-buses of line i using f_i (*from-bus*) and e_i (*to-bus*), where $1 \leq i \leq l$, $1 \leq f_i, e_i \leq b$, l is the number of lines, and b is the number of buses. The admittance of line i is denoted by d_i. Each row of $\mathbf{H}$ corresponds to a power equation. The first $2l$ rows correspond to the line power flow measurements, while the rest corresponds to the power consumption measurements. To represent a power equation, we define P_i^L to denote the power flow through line i, P_j^B to denote the power consumption by bus j, and θ_j to denote the state value, *i.e.*, the voltage phase angle at bus j. Parameter a_i denotes whether measurement i is required to be altered (by injecting false data) for the attack. We model incomplete information with respect to line admittance and use the variable g_i to denote whether the attacker knows the admittance of line i.

In the DC model, two measurements can be taken (*i.e.*, recorded and reported by meters) for each line: the forward and backward current flows. These measurements are equal in magnitude but the opposite in direction. For each bus, a measurement can be taken for the power consumption at the bus. Therefore, for a power system with l number of lines and b number of buses, there are maximally $2l+b$ (*i.e.*, $m = 2l + b$) number of potential measurements. Though a significantly smaller number of measurements are sufficient for state estimation, redundancy is provided to identify and filter bad data. We define t_i to denote whether potential measurement i is taken. Each row of $\mathbf{H}$ corresponds to a power equation. The first l rows correspond to the forward line power flows, while the second l rows correspond to the backward line power flows. The power flow of line i have the following relation with the states of the connected buses:

$$\forall_{1 \leq i \leq l} \quad P_i^L = d_i(\theta_{f_i} - \theta_{e_i}) \tag{1}$$

The last n rows of $\mathbf{H}$ correspond to the bus power consumptions. The power consumption at bus j is simply the summation of the power flows of the lines incident to this bus. If $\mathbb{L}_{j,in}$ and $\mathbb{L}_{j,out}$ are the sets of incoming and outgoing lines of bus j, respectively, then the consumption is:

$$\forall_{1 \leq j \leq b} \quad P_j^B = \sum_{i \in \mathbb{L}_{j,in}} P_i^L \; - \sum_{i \in \mathbb{L}_{j,out}} P_i^L \tag{2}$$

Basically, state estimation is to find the voltage phase angle (θ) of each bus by solving the equations for all of the measurements (P_i^Ls and P_j^Bs).

3.2.2 Selection of Measurement Set

The power system is observable, when the measurements, each of which represent a power equation, must solve the (unknown) states. Therefore, we consider Equations (1) and (2) as constraints. Now, if a measurement is taken, it's power flow or consumption measurement value assumed to be zero. That is:

$$\forall_{1\leq i\leq l} \quad (t_i \vee t_{l+i}) \rightarrow (P_i^L = 0)$$
$$\forall_{1\leq j\leq b} \quad t_{2l+j} \rightarrow (P_j^B = 0)$$

If the set of taken measurements can observe the system, when we consider each of them as zero, all of the states must be the same, *i.e.*, the difference between the states of each connecting pair of buses should be zero. Therefore, if the system is not observable with this set, then there exists at least a pair of buses which have different states with respect to each other (*i.e.*, nonzero difference). We find whether a set is observable using this contradiction. We take the following constraint that all of the states cannot be the same:

$$\exists_{1\leq j_1,j_2\leq b, j_1\neq j_2} \quad \theta_{j_1} \neq \theta_{j_2}$$

If there is no satisfiable solution to this model, then the set of measurements can observe the system.

3.2.3 Selection of Lines for Admittance Perturbation

In the selection of the lines and corresponding changes in admittances, the main constraint is that the changes need to be done such that the optimal power flow (OPF) cost does not increase. Specifically, our aim is to keep the generation dispatch as it is, *i.e.*, according to the existing OPF, so that there is a minimum impact on the system operation due to the topology change.

The main constraint for OPF is that the total generation must be equal to the total expected load. Since we are not changing the demands at different buses, the required total generation remains the same. Now, the existing OPF solution can remain optimal after the admittance changes, if and only if the changed power flows still remain within associated transmission limits. Since all the power flow and consumption equations must hold, we consider them (*i.e.*, Equations (1) and (2)) as constraints:

$$\forall_{1\leq i\leq l} \quad P_i^L = \hat{d}_i(\theta_{f_i} - \theta_{e_i})$$
$$\forall_{1\leq j\leq b} \quad P_j^B = \sum_{i\in\mathbb{L}_{j,in}} P_i^L - \sum_{i\in\mathbb{L}_{j,out}} P_i^L$$

Here, $\hat{d}_i$ is the changed admittance of line i, such that $\hat{d}_i = d_i + \Delta d_i$, where Δd_i is changes made on line i. The admittance of a line can be changed only if D-FACTS devices are deployed. Therefore, considering that a line will be chosen for admittance change when necessary D-FACTS facility is installed there, we define h_i for denoting whether the line is chosen for admittance change. Then, the following constraint holds on Δd_i:

$$\forall_{1\leq i\leq l} \quad \neg h_i \rightarrow (\Delta d_i = 0)$$

If there is a change in the line admittance, the change cannot be very small so that the change does not have any impact. If R is the ratio of the minimum change over the line admittance, then we can express this constraint as follows:

$$\forall_{1\leq i\leq l} \quad h_i \rightarrow (\Delta d_i \geq R \times d_i) \vee (\Delta d_i \leq -R \times d_i)$$

Each line has a capacity for the power flow, *i.e.*, the maximum power that can flow through that line. Let $P_{i,max}^L$ be the line capacity. Therefore:

$$\forall_{1\leq i\leq l} \quad P_i^L \leq P_{i,max}^L$$

The change of a line's admittance would be useful to hinder adversaries from launching an attack, if one or more measurements associated to this line are taken. It is worth mentioning that there are four measurements associated to a line: two (forward and backward) line flow measurements and two bus consumption measurements (at the end buses). Although the larger number of measurements is taken, the more benefit is supposed to be there, in this model, we consider the minimum case as a constraint, *i.e.*, at least one of the measurements associated to the line needs to be taken:

$$\forall_{1\leq i\leq l} \quad h_i \rightarrow m_i \vee m_{l+i} \vee m_{f_i} \vee m_{e_i}$$

The solution to this model verifies whether a given choice of admittance changes on a selected set of lines satisfy the constraints. This model can even synthesize all (or a number of) potential sets of lines for admittance randomization with changed admittance values.

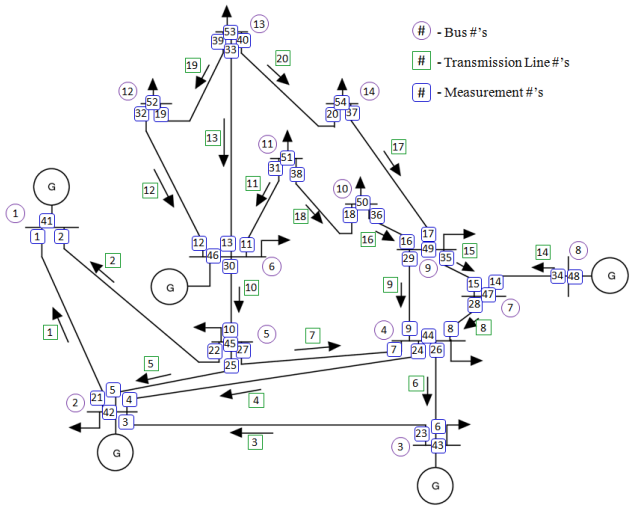

Figure 2: IEEE 14-bus test system.

3.2.4 Impact of MTD on Attack Attributes

The measurement set randomization: In order to launch a UFDI attack, *i.e.*, changing the states of a group of buses, power flows through some lines and power consumptions at some buses are impacted (*i.e.*, changed by ΔP_i^L and ΔP_j^B amounts, refer to the Appendix for the detailed formalization of UFDI attack constraints). The attacker needs to inject necessary false data to the measurements, *i.e.*, meter readings associated to those power flows and consumptions. However, the attacker only needs to inject necessary false

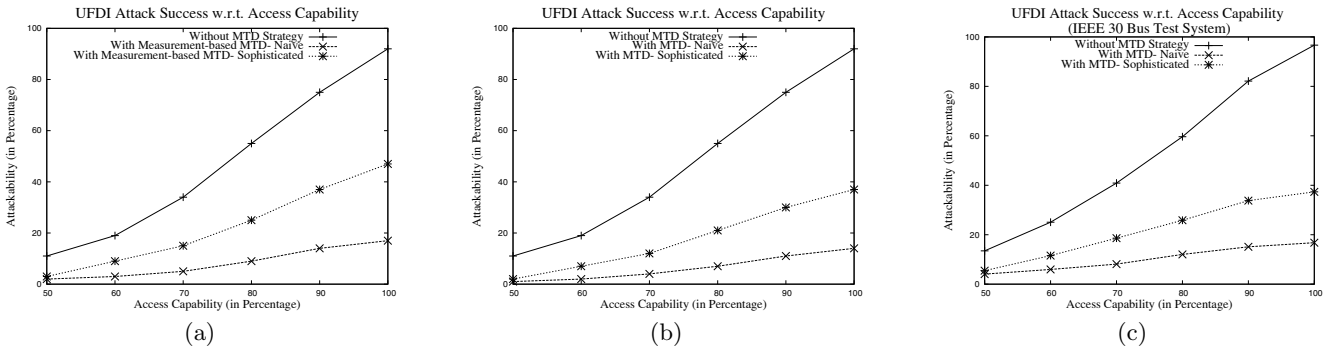

Figure 3: The probability of attack success in the cases of different access capabilities: (a) measurement based MTD strategy, (b) measurement and line admittance based MTD strategy (14-bus system), and (c) measurement and line admittance based MTD strategy (30-bus system).

data to a measurement i, when it is taken. That is:

$$\forall_{1\leq i\leq l}\ (\Delta P_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i})$$
$$\forall_{1\leq j\leq b}\ \ (\Delta P_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j})$$

The randomization of the set of measurements, considered in state estimation, make t_i uncertain for the adversary.

Perturbation of line admittances: If the admittance of a line is unknown to the attacker, he cannot determine the necessary changes that she needs to make in the power flow measurements of the line. The condition is formalized as:

$$\forall_{1\leq i\leq l}\ \ (\Delta P_i^L \neq 0) \rightarrow ((t_i \vee t_{l+i}) \rightarrow g_i)$$

Moreover, when the admittance of a line is perturbed (*i.e.*, randomized), we also consider that the admittance is (now) unknown to the adversary, although the actual admittance (we call it as base admittance) of the line may be known to the adversary. Therefore, we take the following constraint:

$$\forall_{1\leq i\leq l}\ \ h_i \rightarrow \neg g_i$$

4. PERFORMANCE EVALUATION

We evaluate the performance of our proposed MTD mechanism with respect to successful UFDI attacks on different bus states. We use *attackability*, defined as the number of states which can be attacked (*i.e.*, infected by UFDI attacks) over the total number of states, as the evaluation metric.

4.1 Implementation of Formal Models

In order to verify whether a successful UFDI attack can be launched against one or more targeted states, we encode the UFDI attack verification model [11] (see the Appendix for details) using satisfiability modulo theories (SMT) [16]. To execute the model, we use Z3, an efficient SMT solver [17]. By executing the model, we obtain the verification result as either satisfiable (*sat*) or unsatisfiable. When the result is *sat*, it specifies that there exists an attack vector satisfying the constraints regarding the attack attributes.

In order to implement a prototype of the proposed MTD mechanism, we again use SMT to encode the formal model of verifying whether a measurement set is observable (refer to Section 3.2.2). By solving this model using Z3, we generate a number of measurement sets to be used in state estimation. In our MTD mechanism, we randomly choose one among them following the uniform distribution. We also encode the formal model for the line admittance randomization that we present in Section 3.2.3. We first use the uniform distribution to select a subset of lines among the D-FACTS device deployed lines. Then, executing this model (in Z3) we figure out whether the admittances of these lines can be changed while satisfying all the necessary constraints.

4.2 Methodology

We evaluate the performance of our proposed moving target defense mechanism by analyzing the *attackability* under different scenarios considering access capabilities, knowledge limitations, and security measures. We evaluate the performance of our proposed MTD mechanism using IEEE 14-bus test system (Figure 2) [10]. It is consists of 14 buses, 20 transmission lines, and 54 possible measurements as shown in the figure. We also undertake evaluation using IEEE 30-bus test system for some scenarios to show the impact of the system size (*i.e.*, the number of buses) on the performance.

In our evaluation, we mainly consider two kinds of adversaries: (i) naive and (ii) sophisticated. The first type of adversary as the name indicates is unaware of the MTD scheme. He believes that a fixed set of measurements is used in state estimation. The second type of adversary knows that the MTD mechanism is running at the grid operator's side. As a result, in order to maximize his chances of a successful attack, he picks an attack vector that can cover as many potential sets of measurements as possible within his resource and access limits. For both kinds of adversaries, we consider the same resource constraints. An adversary can attack 13-15 measurements at a time, while these measurements cannot be distributed more than 7-8 buses of the system. We execute each evaluation experiment for at least 30 times and take the arithmetic average of them.

4.3 Evaluation Results and Discussion

4.3.1 Performance with respect to Accessibility

Figure 3(a) shows the attackability, *i.e.*, the number of states that can be attacked out of the total, in three different cases with respect to the application of the MTD (*i.e.*, defense based on our proposed MTD mechanism) and the adversary type. In the first case no MTD strategy is applied, while in the latter two cases the MTD is used but the

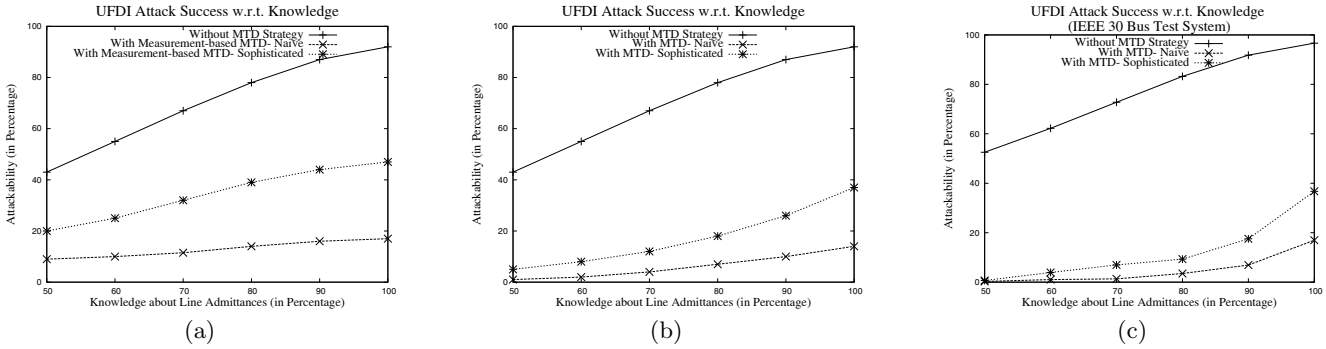

Figure 4: The attackability in the cases of different levels of knowledge about line admittances: (a) measurement based MTD strategy, (b) measurement and line admittance based MTD strategy (14-bus system), and (c) measurement and line admittance based MTD strategy (30-bus system).

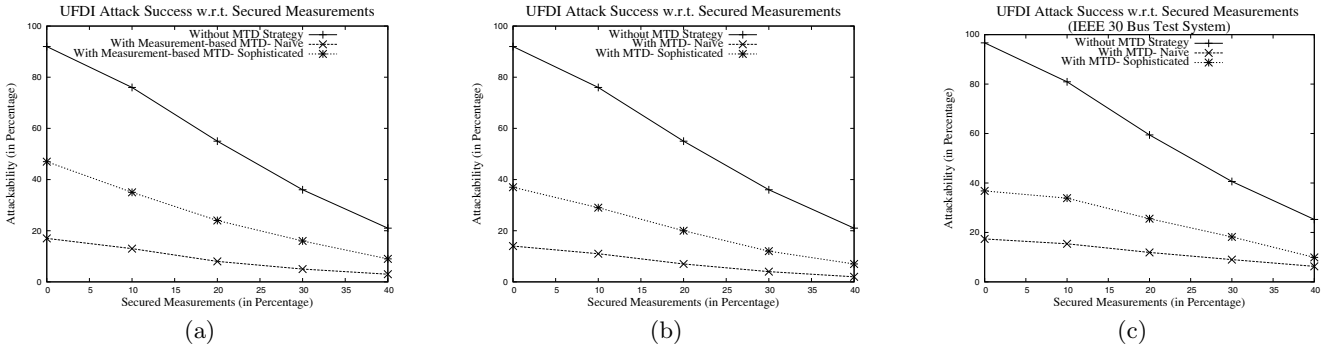

Figure 5: The attackability in the cases of different numbers of secured measurements in different scenarios: (a) measurement based MTD strategy, (b) measurement and line admittance based MTD strategy (14-bus system), and (c) measurement and line admittance based MTD strategy (30-bus system).

type of adversary is different. In the second case the adversary is naive, while in the third case he is sophisticated. In this set of experiments, only the MTD strategy of randomizing the set of measurements used for state estimation is applied. Here, we consider the 14-bus test system. We take 100 sets of 30 measurements arbitrarily chosen from 37 (taken) measurements. We vary the accessibility, *i.e.*, access capability, of the adversary in the experiments from 50% to 100%. According to the experiment results, we observe that the attack success probability is always high when there is no MTD. In both of the cases of naive and sophisticated adversaries, the attackability reduces significantly. In the case of a sophisticated adversary, as would be expected, the attackability reduces less compared to a naive adversary. This is because the sophisticated adversary uses all of his resources to cover as many potential sets of measurements as possible, while the naive adversary only believes one particular set of measurements to be used in the state estimation process. The graphs in Figure 3(a) also show the impact of access capability of the adversary on the atatckability. The results are obvious, *i.e.*, the lower the attacker's access capability, the better the performance of MTD strategy, which is able reduce attackability down to 5% when the access capability is no more than 60%.

Figure 3(b) shows the attackability under different attack capabilities of the adversary as well. However, in this set of experiments, the MTD strategy of perturbing line admittances is applied along with the randomization of the set of measurements used for state estimation. We assume that D-FACTS devices are deployed on an arbitrary set of 5 lines, while only 2 lines are chosen among them for admittance perturbation at each time. According to the graphs in Figure 3(b), we can see that the MTD mechanism shows improved performance when we apply both of the MTD strategies. This performance improvement is nearly more than 10% with respect to the measurement set randomization based MTD alone.

In Figure 3(c), we present the performance of our proposed MTD mechanism in the case of the 30-bus test system by varying the attacker's access capability. We observe the similar behavior in this case as well. Note that we have 30 states associated to 30 buses and we consider 100 sets of 65 measurements. Each of these sets are arbitrarily chosen from 80 (taken) measurements.

4.3.2 *Performance with respect to Knowledge:*

We evaluate the impact of the adversary's knowledge limitation on the performance of the MTD. Again we consider

the same three cases, *i.e.*, without MTD, MTD with naive adversary, and MTD with sophisticated adversary. Figure 4(a) shows the impact of knowledge limitation when only measurement based MTD strategy is applied (in the 14-bus system). We observe that when the adversary has limited knowledge, MTD strategies perform better. However, the impact of knowledge limitation is significant in the case of the sophisticated adversary. Since a sophisticated adversary leverages knowledge about the system and the MTD strategy in order to increase his attack success, when the knowledge is limited to less than 80%, his attack success drops significantly.

In the case of the MTD considering both randomization of the measurement set and perturbation of line admittances, we see similar behavior (see Figure 4(b) and Figure 4(c) for the 14- and 30-bus systems, respectively). The only difference is that the impact of limited knowledge is higher in this case. That is, the performance of the MTD increases with the decrease of the adversary's knowledge and this increase is more significant when both MTD strategies are applied.

4.3.3 Performance with respect to Existing Security:

Figure 5(a) and Figure 5(b) show the impact of secured (*i.e.*, data integrity protected) measurements on the performance of MTD in the case of the 14-bus system. Figure 5(a) shows the case when only measurement set randomization strategy is used and, and Figure 5(b) shows the case when both measurement set randomization and line admittance perturbation strategies are used. The more secured measurements the better is the performance of MTD strategies. Note that the measurements are secured arbitrarily, *i.e.*, they are not secured optimally to achieve the best performance. Clearly the performance is better when both of the MTD strategies are applied, as evidenced by the graphs in the figures. We observe the similar behavior in the case of the 30-bus system (see Figure 5(c)).

5. RELATED WORK

The concept of undetected false data injection attack was presented in [2] for the first time, and was extended in [18]. The authors discussed UFDI attacks considering different scenarios, such as limited access to meters and limited resources to compromise meters, under random and specific targets, assuming that the adversary has complete information about the grid. In the general case, the attack vector computation problem is NP-complete. Therefore, the authors presented few heuristic approaches that can find attack vectors. UFDI attacks with incomplete or partial information are discussed in [5, 8]. These works mathematically showed the impact of incomplete knowledge on the potentiality of UFDI attacks. Several security metrics are proposed in [19] to quantify the importance of individual buses and the cost of attacking individual measurements considering the vulnerability of the communication infrastructure. In [20], authors claimed that an l_1 relaxation-based technique provides an exact optimal solution of the data attack construction problem.

Some work has been done to defend state estimation from UFDI attacks. For example, Kosut et al. in [21] proposed a mechanism based on the generalized likelihood ratio test to detect UFDI attacks. Similar approach is found in [22] with the help of adaptive cumulative sum control chart test. Few other works proposed mechanisms to identify the optimal set of measurements to be secured to make UFDI attacks detectable. Bobba et al. in [6] showed that for detecting UFDI attacks it is necessary and sufficient to protect a set of basic measurements, which is actually a minimum set of measurements ensuring observability. Kim and Poor in [7] proposed a greedy suboptimal algorithm, which selects a subset of measurements that can be made immune from false data injection for the protection against UFDI attacks. In our recent work, we have addressed the problem of verifying stealthy attacks on state estimation by providing a comprehensive model of the attack attributes along with the impact of such attacks on the economic operation of the system [11, 23, 24]. In addition, in [24], we have devised a security architecture synthesis mechanism with respect to a given attack model and the grid operator's resource constraints. Since the number of measurements to be secured is not so small, applying the group of security measures incurs substantial cost, especially due to the existing legacy hybrid system. Therefore, a cheaper and useful defense strategy like moving target defense (MTD) seems to be attractive.

MTD techniques have been presented for traditional enterprise networks in recent literature. Antonatos et al. proposed a network address space randomization scheme to offer an IP hopping approach that can defend against hitlist worms [25]. Duan et al. presented a proactive random route mutation technique in [26], which enables the random and simultaneous changes of the routes of the multiple flows in a network. However, to our knowledge, moving target based defenses haven't received as much attention in SCADA and other control networks. In [27], Mo and Sinopoli proposed perturbing the input signal to a control system in order to detect replay attacks. Controlled perturbation of line admittances to detect UFDI was proposed in [28, 29]. Line admittance perturbation along with parameter estimation was shown to enhance the detectability of UFDI attacks on nonlinear state estimation in [30]. In this work, we go beyond line admittance perturbation and propose a multipronged, comprehensive MTD strategy where the measurements used in state estimation are changed along with the line admittances in a controlled fashion. The proposed approach is novel in this domain.

6. CONCLUSION

Securing state estimation against cyber-attacks is of paramount importance to maintain the integrity of the electric power grid. One way to secure state estimation from stealthy attacks like undetected false data injection attack is by securing a strategically selected number of measurements, which can be beyond the capability of the stakeholders. Therefore, a less expensive security solution like MTD mechanism that we have proposed in this paper is interesting. In this mechanism, we have applied randomization on the power grid system properties, particularly the set of measurements that is used in state estimation and the admittances of a set of lines. We have presented formal models to find the observable sets of measurements and the lines to randomize admittances. We have evaluated the performance of our mechanism on the standard IEEE test systems and have presented the results. We have found that our proposed MTD mechanism can reduce the attackability by 50%-60% compared to the situation when this mechanism is not applied. While a linear power system model with no losses was used here, a future direction of this work would be to extend

the current solution to account for losses and eventually deal with the inherent nonlinearity in power systems.

7. ACKNOWLEDGMENTS

This research was supported in part by National Science Foundation under Grant No. CNS-1352238. Any opinions, findings, conclusions or recommendations stated in this material are those of the authors and do not necessarily reflect the views of the funding sources.

8. REFERENCES

[1] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry. Towards a framework for cyber attack impact analysis of the electric smart grid. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010.

[2] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *ACM Conference on Computer and Communications Security (CCS)*, pages 21–32, 2009.

[3] A. Monticelli. *State estimation in electric power systems: a generalized approach*. Kluwer Academic Publishers, Norwell, MA, 1999.

[4] A. Abur and A. G. Exposito. *Power System State Estimation : Theory and Implementation*. CRC Press, New York, NY, 2004.

[5] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cyber security analysis of state estimators in electric power systems. In *IEEE Conference on Decision and Control (CDC)*, 2010.

[6] R. B. Bobba et al. Detecting false data injection attacks on dc state estimation. In *IEEE Workshop on Secure Control Systems, CPS Week*, Apr 2010.

[7] T.T. Kim and H.V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326 –333, Jun 2011.

[8] M. Ashfaqur Rahman and Hamed Mohsenian-Rad. False data injection attacks with incomplete information against smart power grids. In *IEEE Conference on Global Communications (GLOBECOM)*, Dec 2012.

[9] K.M. Rogers and T.J. Overbye. Some applications of distributed flexible ac transmission system (d-facts) devices in power systems. In *North American Power Symposium (NAPS)*, pages 1–8, 2008.

[10] Power systems test case archive. `http://www.ee.washington.edu/research/pstca/`.

[11] Mohammad Ashiqur Rahman, Ehab Al-Shaer, and M. Ashfaqur Rahman. A formal model for verifying stealthy attacks on state estimation in power grids. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2013.

[12] Allen J. Wood and Bruce F. Wollenberg. *Power Generation, Operation, and Control, 2nd Edition*. Wiley, 1996.

[13] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and Xiaoyang Sean Wang, editors. *Moving target defense- creating asymmetric uncertainty for cyber threats*, volume 54 of *Advances in Information Security*. Springer, 2011.

[14] Moving target defense (mtd). Cyber Security, R & D Center, U.S. Homeland Security, 2011. `http://www.cyber.st.dhs.gov/moving-target-defense/`.

[15] D. Divan and H. Johal. Distributed facts - a new concept for realizing grid power flow control. In *Power Electronics Specialists Conference, 2005. PESC '05. IEEE 36th*, pages 8–14, June 2005.

[16] L. de Moura and N. Bjorner. Z3: An efficient smt solver. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340, 2008.

[17] Z3: An efficient smt solver. In *Microsoft Research*. http://research.microsoft.com/en-us/um/redmond/projects/z3/.

[18] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 14(1):13:1–13:33, Jun 2011.

[19] O. Vukovic, Kin Cheong Sou, G. Dan, and H. Sandberg. Network-layer protection schemes against stealth attacks on state estimators in power systems. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2011.

[20] Kin Cheong Sou, H. Sandberg, and K.H. Johansson. On the exact solution to a smart grid cyber-security analysis problem. *IEEE Transactions on Smart Grid*, 4(2):856–865, 2013.

[21] O. Kosut, L. Jia, R. J. Thomas, and L. Tong. On malicious data attacks on power system state estimation. In *International Universities Power Engineering Conference*, August 2010.

[22] Yi Huang, Husheng Li, K.A. Campbell, and Zhu Han. Defending false data injection attack on smart grid network using adaptive cusum test. In *Annual Conference on Information Sciences and Systems (CISS)*, March 2011.

[23] M. Ashiqur Rahman, E. Al-Shaer, and R. Kavasseri. A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids. In *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), CPS Week,*, April 2014.

[24] M. Ashiqur Rahman, E. Al-Shaer, and R. Kavasseri. Security threat analytics and countermeasure synthesis for state estimation in smart power grids. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2014.

[25] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis. Defending against hitlist worms using network address space randomization. *Journal of Computer and Telecommunications Networking*, 51(12):3471–3490, August 2007.

[26] Qi Duan, Ehab Al-Shaer, and Jafar Haadi Jafarian. Efficient random route mutation considering flow and network constraints. In *IEEE Conference on Communications and Network Security*, October 2013.

[27] Yilin Mo and Bruno Sinopoli. Secure control against replay attacks. *Annual Allerton Conf. on Communication Control and Computing*, pages 911–918, 2009.

[28] Kate L Morrow et al. Topology perturbation for detecting malicious data injection. In *System Science*

(HICSS), 2012 45th Hawaii International Conference on, 2012.

[29] Katherine R Davis et al. Power flow cyber attacks and perturbation-based defense. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2012.

[30] William Niemira et al. Malicious data detection in state estimation leveraging system losses & estimation of perturbed parameters. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013.

APPENDIX

A. FORMAL MODEL OF UFDI ATTACKS

We utilize the formal model of verifying UFDI attacks, as described in our previous work [11, 24], for evaluating the efficacy of our proposed MTD mechanism. Here, we briefly describe this verification model for readers' convenience.

We define c_j to denote whether state j ($1 \leq j \leq n$) is affected (*i.e.*, changed to an incorrect value) due to false data injection. Note that, in the DC model, each state corresponds to a bus. Thus, n is equal to b. The attacker may not be able to alter a measurement due to inaccessibility or existing security measures. We define r_i to denote whether measurement i is accessible to the attacker. We also define s_i to denote whether the measurement is secured or not.

A.1 Formalization of Attacks on States

The attack on state j specifies that the voltage phase angle at bus j is changed. This condition is formalized as follows:

$$\forall_{1\leq j\leq n} \;\; c_j \rightarrow (\Delta\theta_j \neq 0)$$

From Equation (1), it is obvious that a change of P_i^L is required based on the changes on state f_i (θ_{f_i}) and/or state e_i (θ_{e_i}). If in the case of false data injection, P_i^L, θ_{f_i}, and θ_{e_i} are changed to ${P'}_i^L$, ${\theta'}_{f_i}$, and ${\theta'}_{e_i}$, then Equation (1) turns into the following:

$${P'}_i^L = d_i({\theta'}_{f_i} - {\theta'}_{e_i})$$

The subtraction of Equation (1) from the above equation represents whether there are changes in the measurements and the states. The resultant equation will be as follows:

$$\Delta P_i^L = d_i(\Delta\theta_{f_i} - \Delta\theta_{e_i})$$

In this equation, $\Delta P_i^L = {P'}_i^L - P_i^L$, $\Delta\theta_{f_i} = {\theta'}_{f_i} - \theta_{f_i}$, and $\Delta\theta_{e_i} = {\theta'}_{e_i} - \theta_{e_i}$. If $\Delta\theta_{f_i} \neq 0$ ($\Delta\theta_{e_i} \neq 0$), then it is obvious that state x_{f_i} (x_{e_i}) is changed (i.e., attacked). Similarly, we have the following equation that indicates whether a bus power consumption measurement is required to change:

$$\forall_{1\leq j\leq b} \;\; \Delta P_j^B = \sum_{i\in\mathbb{L}_{j,in}} \Delta P_i^L \; - \sum_{i\in\mathbb{L}_{j,out}} \Delta P_i^L$$

A.2 Formalization of False Data Injection

In order to launch an attack, the attacker must alter a set of measurements, which depends on the changes that are required to made on different power flows or consumptions. When $\Delta P_i^L \neq 0$, then it specifies that measurements i and $l+i$ (*i.e.*, forward and backward power flow measurements corresponding to line i), when they are taken (*i.e.*, t_i and t_{l+i}), are required to be changed. Similarly, the power consumption measurement at bus j is required to change when $\Delta P_j^B \neq 0$. These are formalized as follows:

$$\forall_{1\leq i\leq l} \; (\Delta P_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i})$$
$$\forall_{1\leq j\leq b} \;\; (\Delta P_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j})$$

Conversely, measurement i is altered, only if it is taken and corresponding power measurement is changed. The constraint is formalized as follows:

$$\forall_{1\leq i\leq l} \;\; a_i \rightarrow t_i \wedge (\Delta P_i^L \neq 0)$$
$$\forall_{1\leq i\leq l} \;\; a_{l+i} \rightarrow t_{l+i} \wedge (\Delta P_i^L \neq 0)$$
$$\forall_{1\leq j\leq b} \;\; a_{2l+j} \rightarrow t_{2l+j} \wedge (\Delta P_j^B \neq 0)$$

A.3 Formalization of Attack Attributes

Limited Information. If the admittance of a line is unknown to the attacker, then she cannot determine the necessary changes that she needs to make in the measurements associated to the line. We formalize this condition as follows:

$$\forall_{1\leq i\leq l} \;\; (\Delta P_i^L \neq 0) \rightarrow ((t_i \vee t_{l+i} \vee t_{f_i} \vee t_{e_i}) \rightarrow g_i)$$

Moreover, when the admittance of a line is perturbed (*i.e.*, randomized), we consider that the admittance is unknown to the adversary, although the actual admittance (we call it as the base admittance) of the line may be known to the adversary. The reason is that the changed amount is not known to the adversary. The following constraint addresses this point:

$$\forall_{1\leq i\leq l} \;\; h_i \rightarrow \neg g_i$$

Limited Capabilities. If a measurement is data integrity secured, then though the attacker may have the ability to inject false data to the measurement, the false data injection will not be successful. Hence, the attacker will only be able to change measurement i in order to attack, if the following condition holds:

$$\forall_{1\leq i\leq m} \;\; a_i \rightarrow r_i \wedge \neg s_i$$

Limited Resources. The typical resource limitation specifies that, at a particular time, the attacker can inject false data to T_{CZ} number of measurements, at the maximum:

$$\sum_{1\leq i\leq m} a_i \;\; \leq T_{CZ}$$

There can be a similar resource constraint with respect to the number of buses that need to be accessed in order to inject false data to the measurements residing at those buses. The following conditions identify the buses which need to be accessed:

$$\forall_{1\leq i\leq l} \;\; (a_i \rightarrow u_{f_i}) \wedge (a_{l+i} \rightarrow u_{e_i})$$
$$\forall_{1\leq j\leq b} \;\; a_{2l+j} \rightarrow u_j$$

Let T_{CB} be the maximum number of substations that the attacker can compromise simultaneously. Then:

$$\sum_{1\leq j\leq b} u_j \;\; \leq T_{CB}$$

Specific Targets. The attacker most often has a target of attacking a selected set of states. However, the attacker usually has no specification on the rest of the states. That is, an unspecified state might be attacked or not. If the target is to attack states 3, 5, and 6, then it is specified as follows:

$$c_3 \wedge c_5 \wedge c_6$$