# Impact Analysis of Topology Poisoning Attacks on Economic Operation of the Smart Power Grid

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

Rajesh Kavasseri
Department of Electrical and Computer Engineering
North Dakota State University, USA
Rajesh.Kavasseri@ndsu.edu

***Abstract*—The Optimal Power Flow (OPF) routine used in energy control centers allocates individual generator outputs by minimizing the overall cost of generation subject to system level operating constraints. The OPF relies on the outputs of two other modules, namely topology processor and state estimator. The topology processor maps the grid topology based on statuses received from the switches and circuit breakers across the system. The state estimator computes the system state, *i.e.*, voltage magnitudes with phase angles, transmission line flows, and system loads based on real-time meter measurements. However, topology statuses and meter measurements are vulnerable to false data injection attacks. Recent research has shown that such cyber attacks can be launched against state estimation where adversaries can corrupt the states but still remain undetected. In this paper, we show how the stealthy topology poisoning attacks can compromise the integrity of OPF, and thus undermine economic operation. We describe a formal verification based framework to systematically analyze the impact of such attacks on OPF. The proposed framework is illustrated with an example. We also evaluate the scalability of the framework with respect to time and memory requirements.**

***Keywords*—Power Grid, State Estimation, Optimal Power Flow, Impact of Stealthy Attacks, Formal Method.**

## I. Introduction

Cyber technologies are increasingly used in smart power grids with the promise of providing larger capacity, higher efficiency, and more reliability. While this integration helps energy providers to offer smarter services, real time demand responses, and economic advantages, power grids also become vulnerable to cyber attacks, particularly cyber intrusion and false data injection, which can cause improper controls leading to serious damages including power outages and destruction of critical equipment [1], [2].

In modern energy control centers, the Energy Management System (EMS) refers to a set of of computational tools which are employed for system wide monitoring, analysis, control, and operation. A schematic diagram of EMS and its modules are shown in Fig. 1. State Estimator (SE) is a core module in EMS that estimates the system state variables from a set of real-time telemetered measurements (from meters) and topology statuses (from breakers and switches). The term "state" denote bus voltages, from which transmission line power flows can be computed. As seen in Fig. 1, the output of state estimation is required by several other modules for economic dispatch calculations and security assessment.

Recent research has shown that state estimation is vulnerable to stealthy attacks, where adversaries can remain undetected despite injecting false data to corrupt the state estimator's solution [3]. Such attacks are termed as Undetected False Data Injection (UFDI) attacks. These attacks are based on the idea of corrupting measurements in a manner that is consistent with the measurement model. In state estimation, redundant measurements are used to detect and filter bad data (*i.e.*, erroneous meter measurements) by checking whether the measurement residual, which is the $l_2$-norm of the difference between observed and estimated measurements, is below a threshold [4], [5]. Therefore, an adversary who has perfect knowledge (*i.e.*, who knows the complete measurement model) can then manipulate measurements consistent with the measurement model to bypass the bad data detection process [3]. In [6], [7], it is shown that UFDI attacks by adversaries with perfect knowledge can be defended if a strategic set of measurements is secured (*i.e.*, data integrity protected).

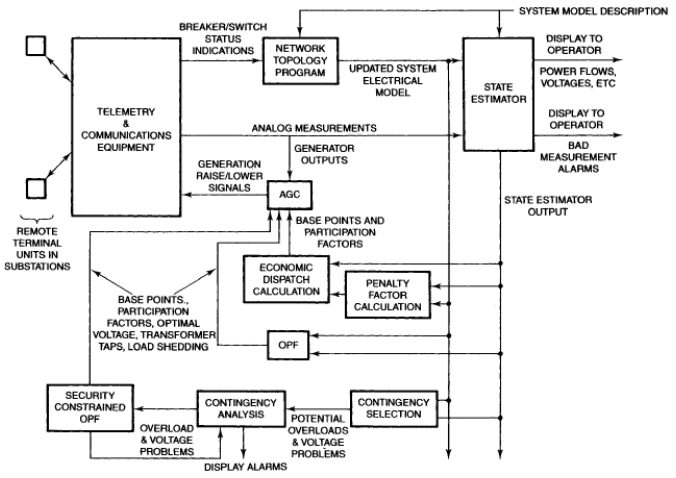



Fig. 1. Energy control center system security schematic (thanks to Allen J. Wood and Bruce F. Wollenberg, *Power Generation, Operation, and Control*, 2nd Edition)

The primary goal of this work to understand the impact of false data injection attacks on economic operation of power grids, more specifically on Optimal Power Flow (OPF). The OPF module determines the generator set-points required for Automatic Generation Control (AGC), as seen in Fig. 1. The OPF allocates optimal generator set-points to minimize the overall cost of generation while meeting system constraints. These set-points drive the power generation commands for the control loop of Automatic Generation Control (AGC), that regulates the generator's output. The OPF depends on

the state estimation result (*i.e.*, the states) and the topology. The topology processor maps the grid topology based on statuses received from the switches and circuit breakers across the system. As shown in Fig. 1, different modules in EMS, particularly state estimation and OPF are performed based on this topology. Therefore, corrupting the topology as well as the state estimation solution can result in an OPF result that is no longer optimal, *i.e.*, it can result in expensive generation dispatches. However, these attacks need to be stealthy enough to evade the bad data detection process. With this primary intuition, in this paper we develop a framework that can systematically analyze the impact of stealthy topology poisoning attacks on OPF. Specifically, our contributions are as follows:

- We define a formal framework for the impact analysis of topology attacks on OPF. The framework includes (i) modeling of stealthy topology attacks, (ii) modeling of OPF, and (iii) modeling of topology attacks' impact on OPF. In topology attacks, errors are introduced in the topology statuses which make the topology processor to exclude lines actually in service and include lines not in service. We also show that an adversary can strengthen the impact of topology attacks on OPF by infecting states, *i.e.*, incorporating UFDI attacks on state estimation.
- The proposed formal framework is modeled as a constraint satisfaction problem, which is implemented using an efficient SMT (Satisfiability Modulo Theories) solver [8]. We present an example in detail to illustrate how our framework verifies the potentiality of stealthy attacks with respect to an desired impact on OPF. We also evaluate the scalability of our proposed framework in terms of time and memory. Since our framework includes topology attacks and OPF together and these systems work mostly with real values, we apply a number of strategies to increase the scalability.

The rest of this paper is organized as follows: Section II presents background materials. Formalization of attacks and their impact on OPF are presented in Section III. Evaluation results are presented in Section IV. The related work is briefly discussed in Section V, which is followed by the conclusion.

## II. Background and Motivation

We first review the DC power-flow model, which has been widely used to analyze stealth attacks on state estimation (*e.g.*, [3], [9], [10]). Our analysis of OPF is also based on this model which is simplistic, yet useful in preliminary analytical power systems studies.

### A. DC Power Flow Model

The DC power flow model describes the power balance equations in a lossless power system [11]. With voltage magnitudes at all buses fixed at 1 per unit (p.u.), the only variables are phase angles. Therefore, the voltage phasor at bus $i$ is given 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: $P_{ij} = Y_{ij}(\theta_i - \theta_j)$ where $Y_{ij}$ is the reciprocal of the reactance. The model expresses the power-balance constraint which equates the algebraic sum of powers incident at every bus to zero. This yields a linear system of equations of the form: $[\mathbf{B}][\theta] = [\mathbf{P}]$. One of the buses is designated as the reference bus *i.e.*, slack bus, where $\theta_i = 0$. Assuming $n$ buses, $[\mathbf{B}]$ is a $n-1$ dimensional square matrix, and $\mathbf{P}$ is a $n-1$ dimensional column vector whose elements denote the net power demand at a bus and $[\theta]$ is a column vector of unknown phases corresponding to the bus voltage phasors. The model solves the unknown bus voltages, given the net power demands (*i.e.*, generation and/or load) at every bus and the line reactances. This linear model provides the basis for DC state estimation which is described next.

### B. State Estimation and UFDI Attack

The state estimation problem based on the DC model is to estimate the bus voltages given several measurements of transmission line power flows. Specifically, one needs to estimate $n$ number of the state variables $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$ based on $m$ number of meter measurements $\mathbf{z} = (z_1, z_2, \cdots, z_m)^T$ [5]. Under the DC power-flow assumptions, the measurement model is linear (*i.e.*, the measured power-flows are linear functions of the bus voltages) and hence the measurement model reduces to:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \text{ where } \mathbf{H} = (h_{i,j})_{m \times n}$$

The measurement set is redundant, *i.e.*, $m > n$ which constitutes an over-determined set of linear equations. The redundancy enables detection, elimination, and smoothing the effect of unavoidable gross measurement errors. When the measurement error distribution is Gaussian with zero mean, the state estimate $\hat{\mathbf{x}}$ is given as:

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

Here, $\mathbf{W}$ is a diagonal "weighting" matrix whose elements are reciprocals of variances of the meter errors. Thus, estimated measurements are calculated as $\mathbf{H}\hat{\mathbf{x}}$. The measurement residual $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$ is used to determine bad data. If $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau$, a selected threshold, it indicates bad data.

The main idea in [3] is to generate a stealthy attack vector that can bypass the bad data detection process as follows. Consider an attacker who injects arbitrary false data $\mathbf{a}$ to the original measurements $\mathbf{z}$ such that $\mathbf{a} = \mathbf{H}\mathbf{c}$, *i.e.*, a linear combination of the column vectors of $\mathbf{H}$. Here, $\mathbf{c}$ is added to the original state estimate $\hat{\mathbf{x}}$ due to the injection of $\mathbf{a}$. Since $\mathbf{z}+\mathbf{a} = \mathbf{H}(\hat{\mathbf{x}}+\mathbf{c})$, the residual $||(\mathbf{z}+\mathbf{a})-\mathbf{H}(\hat{\mathbf{x}}+\mathbf{c})||$ still remains the same as $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$. Thus, the bad data detection is evaded. Since our work studies the stealthy attacks by corrupting the topology, we describe the associated module next.

### C. Topology Processor

EMS uses a *topology processor* (refer to Fig. 1) to map the grid topology. This processor receives telemetered statuses of various switches and circuit-breakers in the system to determine network connectivity. When the connectivity matrix $\mathbf{A}$ and the branch admittance matrix $\mathbf{D}$ are known, the measurement matrix $\mathbf{H}$ is computed as follows (as in [12]):

$$\mathbf{H} = \begin{bmatrix} \mathbf{DA} \\ -\mathbf{DA} \\ \mathbf{A}^T\mathbf{DA} \end{bmatrix} \quad (2)$$

Matrices $\mathbf{DA}$ (*i.e.*, multiplication of $\mathbf{D}$ and $\mathbf{A}$) and $-\mathbf{DA}$ represent the line power flows in forward and backward

directions, respectively. The matrix $\mathbf{A}^T\mathbf{DA}$ represents power consumption at the buses.

The state estimated solution (from Equation (1)) estimates bus voltages from which the system power-flows are computed. Summing up the net power flows incident on a bus then yields the estimated power (or load) at that bus. System conditions determined from state estimation are then used in the OPF module (see Fig 1) which is described next.

### D. Optimal Power Flow

The optimal power flow (OPF) problem aims to minimize the total cost of *generation* subject to the following constraints: (i) the total system load is served and (ii) honoring equipment ratings, transmission line limits and control variables, [11]. Denoting the cost of generation from generator $k$ by $C_k(P_k)$, where $C_k$ depends on the nature of plant (*e.g.*, fossil fired, combined cycle, etc.). the OPF problem (with the DC flow model) is described by:

$$min \sum_i C_k(P_k) \text{ s.t.} \tag{3}$$

$$[\mathbf{B}][\theta] = [\mathbf{P}] \tag{4}$$

$$|P_{ij}| \leq P_{ij}^{max} \tag{5}$$

$$P_k^{min} \leq P_k \leq P_k^{max} \tag{6}$$

Here, Equation (3) describes the objective function of minimizing the total cost of generation, subject to power-flow constraints in Equation (4), transmission line capacities in Equation (5) and generation capacities in Equation (6).

### E. Attack Model

Here, we characterize attacks in terms of attributes to assess their impact on the OPF. Our goal is to describe attacks in their most general form so that adversarial capabilities can be modeled. The attributes that represent the attack model includes mainly the attacker's accessibility, resources, and knowledge of the system.

Adversaries may only have restricted access to measurements, when physical or remote access to substations is restricted or when certain measurements are secured. Further, an adversary may be constrained in terms of cost or the efforts to mount attacks on vastly distributed measurements. In such cases, an adversary is limited to compromising only a limited subset of measurements. Also when the measurements targeted for corruption are distributed in many substations, *i.e.*, buses, then it is difficult to inject false data to those measurements compared to the case when the measurement set is distributed in a small number of substations. An attacker who has access to a substation (or to the corresponding remote terminal unit) can compromise measurements taken there [13].

State estimation of a power system is done based on the given topology (*i.e.*, connectivity among the buses) of the grid. For a successful UFDI attack, an attacker needs to know the grid topology and the electrical parameters of the transmission lines, which is not trivial [3]. In the case of partial knowledge, the attacker's capability becomes restricted. On the other side, as the topology is mapped by a topology processor by compiling the status of all switching devices, an adversary can manipulate the topology by injecting false status.

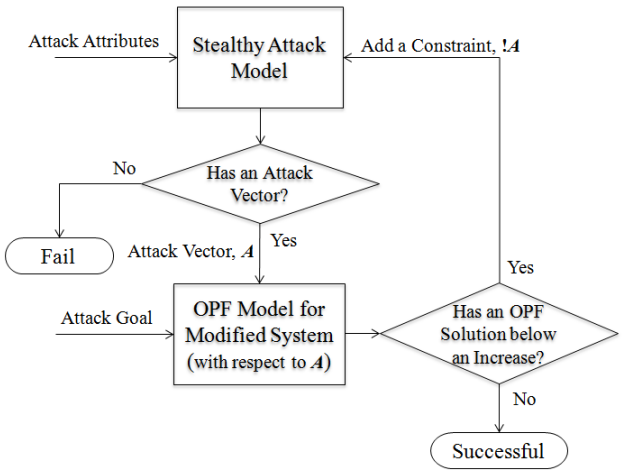



Fig. 2. The framework for finding the impact of UFDI attacks on OPF.

### F. Objective

Although the prior works (*e.g.*, [3], [9], [2], [14], [10]) addressed stealthy attacks in power grids, it is quite challenging to explore the impact of such stealthy attacks. Thus, we model the impact of stealthy topology attacks on OPF, whose solution will provide answers to queries such as: *Given an attack scenario, when is a UFDI attack possible that can make a desired impact on OPF?*. Answering this may allow grid operators to preemptively analyze and explore potential threats under changing attack scenarios.

It is worth mentioning that undetected attacks cannot increase total system loading; but can only change the loads of two or more buses (*i.e.*, some loads increase, while some loads decrease). This inference follows from two assumptions: (i) the measurements of the generated power are secure and (ii) the total generated power is equal to the total load. Therefore, the increase in the cost happens mainly due to the limitation of the transmission line capacities. Influencing the OPF cost even in a small amount is therefore challenging and our proposed approach attempts this by establishing a formal model.

## III. Formal Model of Analyzing Impact of Topology Poisoning Attacks on OPF

In this section, we first discuss briefly the framework of verifying the impact of stealthy attacks on OPF. Then, we discuss the associated formal models. We provide explanatory examples to demonstrate the formal framework.

### A. Framework

We follow the framework as shown in Fig. 2 for verifying the impact of stealthy attacks on OPF. The framework includes two models: *stealthy attack model* that finds attack vectors corresponding to stealthy topology attacks, and *OPF model* that verifies whether there is an OPF solution within a threshold cost. Since the objective is to launch a stealthy attack such that the cost of power generation (according to the OPF solution) increases at least a specific amount, the idea of impact analysis is as follows: First, we look for an attack vector according to the attack model (*i.e.*, attack attributes). If the attack model gives an attack vector, we update the system with respect to the attack vector, *i.e.*, according to the changed loads and the modified topology. Then, we verify that whether there is an increase in the generation cost by executing the OPF model.

TABLE I. 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 $j$. |
| $\theta_j$ | The state value, *i.e.*, the voltage phase angle, at bus $j$. |
| $n$ | The number of states. |
| $m$ | The number of potential measurements. |
| $a_i$ | Whether measurement $i$ is required to be altered for the attack. |
| $c_j$ | Whether state $j$ is infected/affected due to false data injection. |
| $h_j$ | Whether any measurement residing at bus $j$ is required to be changed. |
| $t_i$ | Whether potential measurement $i$ is taken (*i.e.*, reported by a meter). |
| $r_i$ | Whether measurement $i$ is accessible to the attacker. |
| $s_i$ | Whether the measurement is secured or not. |
| $u_i$ | Whether line $i$ exists in the true (real) topology. |
| $v_i$ | Whether line $i$ is fixed in the topology. |
| $w_i$ | Whether the status information regarding line $i$ is secured. |
| $p_i$ | Whether line $i$ is excluded from the topology by an exclusion attack. |
| $q_i$ | Whether line $i$ is included in the topology by an inclusion attack. |
| $k_i$ | Whether line $i$ is considered (though it may not exist) in the topology. |

In order to verify this increase, we set the the threshold cost by adding the expected raise with the original (*i.e.*, in the no attack scenario) OPF solution and check whether there is still an OPF solution within this threshold value. If the result is no, then we are successful to find an attack vector that causes a minimum amount of increase in the generation cost. Otherwise, the same process will be executed for a new attack vector until either we find an attack vector satisfying the objective or there are no more attack vectors. It is worth mentioning that the objective is to increase the generation cost while ensuring convergence of OPF considering the power generation limit of each generator and the capacity of each transmission line. The framework combines the topology attack model and the OPF model into a single model, although they can be executed separately as shown in Fig. 2.

### B. Preliminaries

In order to model UFDI attack on state estimation we use a number of notations (see Table I) to denote different parameters, *i.e.*, system properties and attack attributes.

**Basic Power Model:**

Being 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. We denote the two end-buses of line $i$ using $f_i$ (*from-bus*) and $e_i$ (*to-bus*), where $1 \leq i \leq l$, $1 \leq f_i, e_i \leq b$, and $b$ is the number of buses. The admittance of the line is denoted by $d_i$. As, in the DC model, each state corresponds to a bus, the number of states $n$ is equal to $b$.

Each row of $\mathbf{H}$ corresponds to a power equation. The first $l$ rows correspond to the forward line power flow measurements. The second $l$ rows correspond to the backward line power flow measurements, which are the same as the first $l$, except the direction of the power flow is the opposite. The rest of the rows (*i.e.*, the last $b$ rows) of $\mathbf{H}$ correspond to the bus power consumptions. If $P_i^L$ denotes the power flow through line $i$ and $\theta_j$ denotes the state value, *i.e.*, the voltage phase angle at bus $j$, we have the following relation between the line power flow of line $i$ and the states at the connected buses ($f_i$ and $e_i$):

$$\forall_{1 \leq i \leq l} \quad P_i^L = d_i(\theta_{f_i} - \theta_{e_i}) \tag{7}$$

Equation (7) specifies that power flow $P_i^L$ depends on the difference between the connected buses' phase angles and $d_i$, the admittance of the line. $P_j^B$, the power consumption of a bus $j$, is simply the summation of the power flows of the lines connected to this bus. Let $\mathbb{L}_{j,in}$ and $\mathbb{L}_{j,out}$ be the sets of incoming lines and outgoing lines of bus $j$, respectively. The following equation shows the power consumption at bus $j$:

$$\forall_{1 \leq j \leq b} \quad P_j^B = \sum_{i \in \mathbb{L}_{j,in}} P_i^L \; - \sum_{i \in \mathbb{L}_{j,out}} P_i^L \tag{8}$$

The power consumption at a bus is also equal to the load power at this bus minus the power injected to the bus by the generators connected to this bus. If $P_j^D$ and $P_j^G$ denote the load power and generated power of bus $j$, respectively, the following equation holds:

$$\forall_{1 \leq j \leq b} \quad P_j^B = P_j^D \; - P_j^G \tag{9}$$

If bus $j$ does not connected with any generator, then $P_j^G = 0$. Similarly, if bus $j$ does not have any load, then $P_j^D = 0$.

Note that, state estimation in DC model is the process of finding the voltage phase angle ($\theta$) of each bus by solving the linear equations for all of the measurements ($P_i^L$s and $P_j^B$s) given the line admittances ($d_i$s).

**Attack Attributes:**

In the DC model, two measurements can be taken (*i.e.*, reported by meters) for each line: forward and backward line power flows. 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 $2l+b$ (*i.e.*, $m = 2l+b$) number of potential measurements at the maximum. 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 $i$ ($1 \leq i \leq m$) is taken. Note that measurement $i$ and $l+i$ correspond to the forward and backward power flows of line $i$, while measurement $2l+j$ correspond to the power consumption of bus $j$.

In stealthy topology attacks, one or more states of the system can be infected. We define $c_j$ to denote whether state $j$ is infected (*i.e.*, changed to an incorrect value). Parameter $a_i$ denotes whether measurement $i$ ($1 \leq i \leq m$) is required to be altered (by injecting false data) for the attack. If any measurement at bus $j$ is required to be changed, $b_j$ becomes true. 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 (*i.e.*, data integrity is protected) or not. An attacker often needs to know the admittance of the necessary transmission lines in order to inject the false data at the right amount, so that the attacker can remain undetected. We use $bd_i$ to denote whether the attacker knows the admittance of line $i$.

The topology of a power grid represents the connectivity among the grid buses. An attacker can inject false data in the topology information sent by various circuit breakers and switches in order to change the topology. Changes in the topology that we assume in this work include: (i) exclusion of a (closed) line from the topology (*exclusion attack*), and (ii) inclusion of a open line in the topology (*inclusion attack*).

Here, we also assume that the adversary can coordinate a topology error with other measurements to render the attack undetected. Therefore, a UFDI attack can be performed by leveraging the modified topology. However, there are different properties to be considered. Some of the lines in the topology are fixed (*i.e.*, they are never opened), which form the core part of the topology. The statuses of some lines might be secured, *i.e.*, their topology is always faithfully represented in the topology processor. Parameter $u_i$ denotes whether line $i$ exists in the true or real topology, while $v_i$ and $w_i$ denote whether the line is fixed and the associated line status is secured, respectively. In order to denote exclusion and inclusion attack, we use $p_i$ and $q_i$, respectively. Finally, $k_i$ represents whether line $i$ is considered (*i.e.*, mapped) in the topology.

### C. Topology Poisoning Attacks without Infecting States

In this work, we consider two kinds of topology poisoning attacks to assess impact on OPF. In the first kind, the attacker only changes the topology while the states remain unchanged. In the second kind, the attacker changes the topology and the states. In this subsection, we discuss the first type.

**Change in Topology:**

In the case of an inclusion attack, the status information associated to an open line is compromised such a way that the topology processor considers the line as closed. Conversely, a closed line in service is omitted in an exclusion attack. Therefore, a line is mapped to the topology if the following condition holds:

$$\forall_{1\leq i\leq l} \quad k_i \rightarrow (u_i \wedge \neg p_i) \vee (\neg u_i \wedge q_i) \tag{10}$$

A line can be excluded from the topology only if the line exists in the real (or true) topology and it is not a fixed line and its status information is not secured. Similarly, a line can be included in the topology if the line is not in the true topology and its status information is not secured. These conditions are formalized as follows:

$$\forall_{1\leq i\leq l} \quad p_i \rightarrow u_i \wedge \neg v_i \wedge \neg w_i \tag{11}$$

$$\forall_{1\leq i\leq l} \quad q_i \rightarrow \neg u_i \wedge \neg w_i \tag{12}$$

In order to keep such an inclusion or exclusion attack (*i.e.*, an introduced topology error) undetected, it is necessary to alter certain measurements in necessary amounts. If a closed line is excluded from the topology, the corresponding line power flow measurement must be zero. As the states remain the same after the topology change, the corresponding connected buses' power consumption measurements need to be adjusted accordingly. Let $\Delta \bar{P}_i^L$ be the change amount in the power flow measurement of line $i$ in the case of a topology change. Then, the following constraint holds in the case of a exclusion attack:

$$\forall_{1\leq i\leq l} \quad p_i \rightarrow (\Delta P_i^L = -P_i^L) \tag{13}$$

On the other hand, when a open line is included in the topology, there should be a non-zero power flow through the line according to the phase difference between the connected buses. Therefore:

$$\forall_{1\leq i\leq l} \quad q_i \rightarrow (\Delta P_i^L = P_i^L) \tag{14}$$

If no exclusion or inclusion attack is done on line $i$, no change is required in line $i$'s power flow exclusively for the topology change:

$$\forall_{1\leq i\leq l} \quad \neg(p_i \vee q_i) \rightarrow (\Delta P_i^L = 0) \tag{15}$$

According to Equation (8), the change in the measurement of the power consumption ($\Delta P_j^B$) at bus $j$ depends on the changes done in the power flow measurements of the lines incident to this bus. Therefore:

$$\forall_{1\leq j\leq b} \; \Delta P_j^B = \sum_{i\in \mathbb{L}_{j,in}} \Delta P_i^L - \sum_{i\in \mathbb{L}_{j,out}} \Delta P_i^L \tag{16}$$

**False Data Injection to Measurements:**

When $\Delta P_i^L \neq 0$, it specifies that measurements $i$ and $l+i$ corresponding to line $i$, if they are taken (*i.e.*, $t_i$ and $t_{l+i}$), are required to be changed by $\Delta P_i^L$ amount. Similarly, the power consumption measurement at bus $j$ is required to change when $\Delta P_j^B \neq 0$ and it is taken. These are formalized as follows:

$$\begin{aligned} &\forall_{1\leq i\leq l} \; (\Delta P_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i}) \\ &\forall_{1\leq j\leq b} \quad (\Delta P_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j}) \end{aligned} \tag{17}$$

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

$$\begin{aligned} &\forall_{1\leq i\leq l} \quad a_i \rightarrow t_i \wedge (\Delta P_i^L \neq 0) \\ &\forall_{1\leq i\leq l} \quad a_{l+i} \rightarrow t_{l+i} \wedge (\Delta P_i^L \neq 0) \\ &\forall_{1\leq j\leq b} \quad a_{2l+j} \rightarrow t_{2l+j} \wedge (\Delta P_j^B \neq 0) \end{aligned} \tag{18}$$

Now, if line power flow measurement $i$ (or $l+i$) needs to change, according to Equations (13) and (14), we need to know $P_i^L$. In the case of exclusion attack, $P_i^L$ already exists (*i.e.*, the actual measurement) and the attacker must have the access to it. In the case of exclusion attack, $P_i^L$ needs to be estimated based on the difference between the states ($\theta_j$s) of the connecting buses. In order to approximate the states, the attacker needs to perform some sort of state estimation according to Equation (7) with respect to the power flow measurements taken at the connecting buses.

If the admittance of a line is unknown, the attacker cannot determine the necessary changes to make in the power flow measurements of the line (especially in the case of an line inclusion attack). We formalize this condition as follows:

$$\forall_{1\leq i\leq l} \quad (\Delta P_i^L \neq 0) \rightarrow ((t_i \vee t_{l+i}) \rightarrow g_i) \tag{19}$$

In order to inject false data to a measurement, the attacker must have the ability, with respect to the physical or remote access. If a measurement is secured (*i.e.*, data integrity protected), then though the attacker may have the accessibility 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:

$$\forall_{1\leq i\leq m} \quad a_i \rightarrow r_i \wedge \neg s_i \tag{20}$$

Due to limited resources, an attacker can only access or compromise a limited number of substations (*i.e.*, buses) at a particular time. A substation is required to be accessed or

compromised if a measurement residing at that substation is required to be altered. Therefore:

$$\begin{aligned} &\forall_{1\leq i\leq l} \;\; a_i \rightarrow h_{f_i} \\ &\forall_{1\leq i\leq l} \;\; a_{l+i} \rightarrow h_{e_i} \\ &\forall_{1\leq j\leq b} \;\; a_{2l+j} \rightarrow h_j \end{aligned} \tag{21}$$

Let $T_B$ be the maximum number of substations that an attacker can compromise. Then:

$$\sum_{1\leq j\leq b} h_j \;\; \leq T_B \tag{22}$$

### *D. Topology Poisoning Attacks including Infecting States*

In this case, the attacker strengthens the topology poisoning attacks incorporating the typical UFDI attacks on states. The formalization is the same as the previous subsection, except the additional formalization of UFDI attacks.

**Change in State Estimation:**

From Equation (7), it is obvious that a change of $P_i^L$ is required based on the changes on state $f_i$ ($\theta_{f_i}$) and/or state $e_i$ ($\theta_{e_i}$) or the vice versa. That is:

$$\Delta\bar{P}_i^L = d_i(\Delta\theta_{f_i} - \Delta\theta_{e_i}) \tag{23}$$

If $\Delta\theta_{f_i} \neq 0$ (or $\Delta\theta_{e_i} \neq 0$), then it is obvious that state $f_i$ (or $e_i$) is changed (*i.e.*, infected). However, if both of the states are changed in the same amount, $\Delta\bar{P}_i^L$ is still zero.

This above relation for line $i$ only holds if the line is considered in the topology (Equation 10). We formalize this constraint as follows.

$$\forall_{1\leq i\leq l} \;\; k_i \rightarrow (\Delta\bar{P}_i^L = d_i(\Delta\theta_{f_i} - \Delta\theta_{e_i})) \tag{24}$$

On the other side, if the line is not considered in the topology, there should be no measurement change for launching UFDI attacks:

$$\forall_{1\leq i\leq l} \;\; \neg k_i \rightarrow (\Delta\bar{P}_i^L = 0) \tag{25}$$

Now, when the voltage phase angle at bus $j$ is changed, state $j$ is changed (and the vice versa). That is:

$$\forall_{1\leq j\leq n} \;\; c_j \rightarrow (\Delta\theta_j \neq 0) \tag{26}$$

**False Data Injection to Measurements:**

As we consider the changes in the states (*i.e.*, UFDI attacks), the change for a power flow measurement is the summation of individual changes that are required for the topology change and the state change. Let $\Delta{P'}_i^L$ be the total change done on the power flow of line $i$. Then,

$$\forall_{1\leq i\leq l} \;\; \Delta{P'}_i^L = \Delta P_i^L + \Delta\bar{P}_i^L \tag{27}$$

Therefore, the total change in the measurement of the power consumption ($\Delta{P'}_j^B$) will be:

$$\forall_{1\leq j\leq b} \; \Delta{P'}_j^B = \sum_{i\in\mathbb{L}_{j,in}} \Delta{P'}_i^L - \sum_{i\in\mathbb{L}_{j,out}} \Delta{P'}_i^L \tag{28}$$

Now, the false data injection to a measurement is required with respect to $\Delta{P'}_i^L$ or $\Delta{P'}_j^B$. That is, Equation (17) turns into the following form:

$$\begin{aligned} &\forall_{1\leq i\leq l} \; (\Delta{P'}_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i}) \\ &\forall_{1\leq j\leq b} \;\; (\Delta{P'}_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j}) \end{aligned} \tag{29}$$

Equations (18) and (19) need the similar change.

### *E. Impact of UFDI Attacks on OPF*

In order to model the impact of stealthy attacks on OPF, we first model the OPF process as a problem of verifying whether there is a OPF solution within a threshold cost.

**Optimal Power Flow:**

The objective of the OPF is to optimally control the generation according to the load requirement. Let $\hat{P}_j^G$ be the changed power generated by the generator connected at $j$ after considering the state estimation result. The main constraint for OPF is that the total generation must be equal to the total expected load. Therefore:

$$\sum_{1\leq j\leq b} \hat{P}_j^G = \sum_{1\leq j\leq b} \hat{P}_j^D \tag{30}$$

Each generator has lower and upper bounds on power production. If $\hat{P}_{j,max}^G$ and $\hat{P}_{j,min}^G$ denote the maximum and minimum generation limits of the generator at bus $j$, then this constraint is formalized as follows:

$$\forall_{1\leq j\leq b} \; \hat{P}_{j,min}^G \leq \hat{P}_j^G \leq \hat{P}_{j,max}^G \tag{31}$$

Recall from Equation (4) (Section II) that the OPF considers the entire set of power-flow equations as constraints. In the case of OPF, let $\hat{\theta}$, $\hat{P}_i^L$, and $\hat{P}_j^B$ be the state of bus $j$, the power flow on line $i$ and the power consumption at bus $j$, respectively. Then, in the case of a power flow measurement, the following equation, similar to Equation (7) must hold, if and only if the line is considered in the topology:

$$\forall_{1\leq i\leq l} \;\; k_i \rightarrow (\hat{P}_i^L = d_i(\hat{\theta}_{f_i} - \hat{\theta}_{e_i})) \tag{32}$$

Similarly, the following equations, similar to Equations (8), and (9), must hold:

$$\begin{aligned} &\forall_{1\leq j\leq b} \;\; \hat{P}_j^B = \sum_{i\in\mathbb{L}_{j,in}} \hat{P}_i^L \; - \sum_{i\in\mathbb{L}_{j,out}} \hat{P}_i^L \\ &\forall_{1\leq j\leq b} \;\; \hat{P}_j^B = \hat{P}_j^D \; - \hat{P}_j^G \end{aligned} \tag{33}$$

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 upper bound for the line capacity. Therefore:

$$\forall_{1\leq i\leq l} \;\; \hat{P}_i^L \leq P_{i,max}^L \tag{34}$$

Let $\mathcal{C}_j(.)$ denote the cost function for the generator connected at bus $j$, which takes the total generated power as the parameter and returns the total cost to generate that power. Usually, $\mathcal{C}_j(.)$ is a strictly increasing convex function. Many electric utilities prefer to represent their generator cost functions as piecewise linear equations, *i.e.*, single or multiple segment linear cost functions [11]. Considering the viability of modeling the cost function, we consider the latter form for cost functions, given by $\mathcal{C}_j(\hat{P}_j^G) = \alpha + \beta\hat{P}_j^G$, where $\alpha$ and $\beta$ represent the cost-coefficients for that particular generator. In OPF, the objective is to minimize the total generation cost based on expected or estimated loads at different buses. With the loss of generality, we model this objective as the constraint that the cost must be less than a limit, $T_{OPF}$. This constraint is sufficient to understand the minimum impact of a UFDI attack. The constraint is formalized as follows:

$$\sum_{1\leq j\leq b} \mathcal{C}_j(\hat{P}_j^G) \ \leq T_{OPF} \tag{35}$$

We use notation $OPF$ to denote the conjunction of the OPF constraints, as we have described above, which we will use below to formalize the impact of stealthy attacks on OPF.

**Change in Loads due to Stealthy Attacks:**

In the case of a stealthy topology attack without infecting the states (refer to Section III-C), if $\Delta P_j^B \neq 0$, according to Equation (9), it specifies that there is a load and/or generation power change at the bus. In this work, we assume that a change in the measurement of a bus power consumption specifies a change exclusively in the load, which leads to $\Delta P_j^G = 0$. Because, the measurement of the power generated by a generator, *i.e.*, the power injected to the bus by a generator is pretty much well-defined, which is changed only if the grid operator finds that necessary. Typically, after the estimation of states, if any load change is found, the optimal power flow process (along with contingency analysis) is run, the result of which shows whether (and which) change in the generation is required for optimal efficiency. Therefore, the change in the power consumption of a bus specifies the change in the load at that bus. The following equation denotes this:

$$\forall_{1\leq j\leq b} \ \ \Delta P_j^D = \Delta P_j^B$$

Let $\hat{P}_j^D$ be the estimated load (according to the result of state estimation) at bus $j$, which is also the input to the OPF model. Therefore:

$$\forall_{1\leq j\leq b} \ \ \hat{P}_j^D = P_j^D + \Delta P_j^D$$

Similarly, in the case of a stealthy topology attack that infects the states as well (refer to Section III-D), $\hat{P}_j^D$ is estimated from $\Delta {P'}_j^B$.

At a particular bus $j$, there is usually an expected bound for the load. If $\hat{P}_{j,max}^D$ and $\hat{P}_{j,min}^D$ are the maximum and minimum loads at bus $j$, the following constraint holds:

$$\forall_{1\leq j\leq b} \ \hat{P}_{j,min}^D \leq \hat{P}_j^D \leq \hat{P}_{j,max}^D \tag{36}$$

**Attack Target- Impact on OPF:**

In order to define the increase in the generation cost (*i.e.*, the increase of $T_{OPF}$ in the OPF model), let $\mathcal{T}_{OPF}$ be the optimal cost of generation in the normal (*i.e.*, attack-free) situation. Now, if the attacker's objective is to increase the cost by $I\%$ of the optimal cost, then $T_{OPF} = \mathcal{T}_{OPF} I/100$. Therefore, the constraint to impose the desired impact by launching a UFDI attack is formalized as follows:

$$(T_{OPF} = \mathcal{T}_{OPF} I/100) \rightarrow \neg \ (\exists_{\hat{P}_1^G, \hat{P}_2^G, \cdots, \hat{P}_b^G} OPF) \tag{37}$$

The above constraint states that there is no possible allocation of generation that can cost less than $T_{OPF}$.

In addition, since the attacker's goal is not to fail the OPF solution to converge (possible when the line capacity constraints fail), it needs to ensure that there are OPF solutions for larger values:

$$(T_{OPF} >> \mathcal{T}_{OPF} I/100) \rightarrow \ \ OPF \tag{38}$$

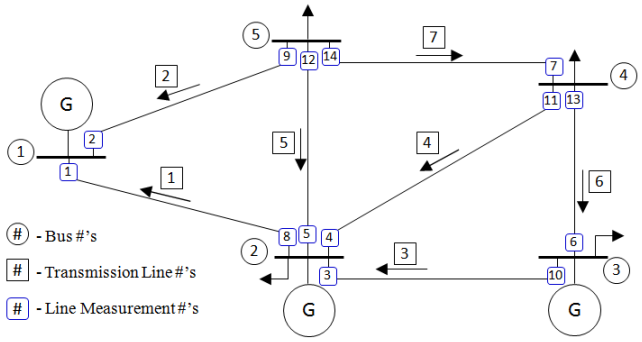



Fig. 3. A 5-bus test system topology. Bus numbers are in circles and line numbers are in squares.

### F. Implementation

We encode the system configuration and the constraints into SMT [15]. We write a program leveraging the *Z3 .Net API* [8] for encoding the formalization of our proposed false data injection model. We encode our formalizations mainly using Boolean (*i.e.*, for logical constraints) and real (*e.g.*, for the relation between power flows or consumptions with states) terms. The system configurations and the constraints are given in a text file (*input* file). By executing the model (in Z3), we obtain the verification result as either satisfiable (*sat*) or unsatisfiable (*unsat*). If the result is *unsat*, it means that the problem has no attack vector that satisfies the constraints. In the case of *sat*, we get the attack vector from the assignments of the variables, $a_i$s, which represent the measurements required to alter for the attack. The results corresponding to our model are also printed in a text file (*output* file).

### G. Example Case Studies

Here, we present two example case studies: first with the stealthy topology attacks without infecting the states, while second with the stealthy topology attacks including infecting the states. In these examples, we consider a 5-bus sub-system as shown in Fig. 3.

**Case Study 1:**

The complete input regarding the example is shown in Table II. The line information includes a set of data for each line: line number, end buses (from-bus and to-bus) of the line, a value indicating the line admittance, the line capacity (*i.e.*, the maximum possible power flow through this line), the knowledge status (*i.e.*, the line admittance of a line is known to the attacker), and the line status properties. There are four line status properties: (i) whether this line is included in the true topology, (ii) whether its existence is fixed in the topology, (iii) whether the topology information regarding this line is secured, and (iv) whether the attacker has the ability to alter the data. According to the input, all of the 7 lines are included in the true topology, while lines 5 and 6 are not included in the core topology (*i.e.*, these lines can be kept open in some situations). The topology mapping information regarding lines 1, 2, and 6 are not secured, while the attacker has the capability to change the topology information regarding all of the lines, except 1 and 2.

Since the example bus system has 5 buses and 7 lines, the maximum number of potential measurements is (5 + 2×7)

TABLE II. INPUT OF THE EXAMPLE AT CASE STUDY 1

```
# Topology (Line) Information
# (line no, from bus, to bus, admittance, line capacity, knowledge?, in true topology?, in core?, secured?, can alter?)
1 1 2 16.90 0.15 1 1 1 0 0
2 1 5 4.48 0.15 1 1 1 0 0
3 2 3 5.05 0.05 1 1 1 1 1
4 2 4 5.67 0.20 1 1 1 1 1
5 2 5 5.75 0.10 1 1 0 1 1
6 3 4 5.85 0.20 1 1 0 0 1
7 4 5 23.75 0.15 1 1 1 1 1

# Measurement Information
# (measurement no, measurement taken?, secured?, can attacker alter?)
1 1 1 0
2 1 1 0
3 1 1 0
4 0 1 0
5 1 1 0
6 1 0 1
7 1 0 1
8 0 1 0
9 0 1 0
10 1 0 1
11 0 0 0
12 1 1 1
13 1 0 1
14 1 1 1
15 1 1 0
16 1 1 0
17 1 0 1
18 1 0 1
19 1 1 1

# Attacker's Resource Limitation (measurements, buses)
8 3

# Bus Types (bus no, is generator?, is load?)
1 1 0
2 1 1
3 1 1
4 0 1
5 0 1

# Generator Information (bus no, max generation, min generation, cost coefficient)
1 0.80 0.10 60 1800
2 0.60 0.10 50 2200
3 0.50 0.10 60 1200

# Load Information (bus no, existing load, max load, min load)
2 0.21 0.30 0.10
3 0.24 0.25 0.15
4 0.18 0.30 0.10
5 0.20 0.25 0.10

# Cost Constraint, Minimum Cost Increase by Attack (in percentage)
1580 3
```

or 19. Each row of the measurement information includes (i) whether the measurement is taken for state estimation (All of the potential measurements are taken except measurements 4, 8, 9, and 11), (ii) whether the measurement is secured (all measurements taken at buses 1, 2, and 5 are secured) and (iii) whether the attacker has the accessibility to alter the measurement (the attacker has the accessibility to alter measurements 6, 7, 10, 12, 13, 14, 17, 18, and 19). The information about the buses in terms of load and generation is shown in the table. The generation capability, *i.e.*, the maximum and minimum generation, of the generators corresponding to the buses are given. We assume that a generation bus only has a single generator connected. The generation cost of power is followed from the simple linear function as shown in Section III-E. The values of coefficient $\alpha$ and $\beta$ for each generator are given in the input. Note that these coefficients are taken arbitrarily, which do not correspond to the real costs. The total load of the system is 0.83 per unit, *i.e.*, 83 MW (considering a 100 MVA base) and the individual loads at the buses are 0, 0.21, 0.24, 0.18, and 0.20, respectively in order. The cost constraint in the attack-free condition is \$1520 (*i.e.*, there is a satisfied OPF solution in this cost).

In this example, the attacker's objective is to launch a stealthy topology attack without infecting the states (refer to Section III-C), such that he can create at least 3% of increase in the generation cost. In this example, the attacker's resource limitation limits alteration of utmost 8 measurements at a time, distributed in no more than 3 buses. The execution of the model corresponding to this example returns *sat* along with the assignments to different variables of the model. From the assignments, we find that:

- An exclusion attack on the topology is launched, such that line 6 is unmapped in the topology.
- In order to keep this attack undetected, measurements 6, 13, 17, and 18 need to be altered only. These measurements are distributed in buses 3 and 4.

The increase in the generation cost is almost \$1650 which is around 4% more than the optimal value in the case of actual (*i.e.*, without attack) scenario. Note that in this scenario, *i.e.*, according to the given constraints, the attacker cannot launch a UFDI attack to any state. Hence, it has been interesting to see from this example that still the attacker has succeeded in increasing the cost of generation by launching an exclusion attack on the topology mapping without changing any state of the system.

**Case Study 2:**

The input of the example 2 is shown in Table III. The line information is the same as the previous example. The measurement related input shows that all of the potential measurements are taken. The measurements taken at bus 1 (*i.e.*, measurements 1, 2, and 15) are secured. The attacker has the accessibility to alter all measurements except 1, 2, and 15. The input about the generation and load buses is the same as the previous case study.

In this example, the attacker's objective is launch a stealthy topology poisoning attack including UFDI attacks (refer to Section III-D), to induce at least a 6% increase in the generation cost based on the base-case OPF solution. The attacker's resource limitation limits alteration to at most 12 measurements at a time, while these measurements can be distributed in no more than 3 substations (*i.e.*, buses). The execution of the model corresponding to this example returns *sat* along with the assignments to different variables of the model. From the execution of our formalizations according to this example, we find a satisfiable solution. According to this solution, we see the following results:

- An exclusion attack on the topology needs to be launched, so that line 6 is unmapped in the topology.
- It is also required to execute UFDI attack on state 3.
- In order to keep this attack undetected, it is required to alter measurements 3, 6, 10, 13, 16, and 18. These measurements are distributed in buses 2, 3, and 4.
- From the assignments, we also see that by attacking the states, the loads of buses 3 and 5 are changed from 0.21 and 0.18 unit to 0.29 and 0.1 unit, respectively.

Note that, in this example scenario, the actual increase in the cost is almost 7% and we cannot increase the cost more than 8% (*i.e.*, if the objective is to at least 9% increase more than the base-cost, then there is no solution in this scenario). Most interestingly, without topology attacks, UFDI attacks

TABLE III. INPUT OF THE EXAMPLE IN CASE STUDY 2

```
# Topology (Line) Information
# (line no, from bus, to bus, admittance, line capacity, knowledge?, in true topology?, in core?, secured?, can alter?)
1 1 2 16.90 0.15 1 1 1 0 0
2 1 5 4.48 0.15 1 1 1 0 0
3 2 3 5.05 0.05 1 1 1 1 1
4 2 4 5.67 0.20 1 1 1 1 1
5 2 5 5.75 0.10 1 1 0 1 1
6 3 4 5.85 0.20 1 1 0 0 1
7 4 5 23.75 0.15 1 1 1 1 1

# Measurement Information
# (measurement no, measurement taken?, secured?, can attacker alter?)
1 1 1 0
2 1 1 0
3 1 0 1
4 1 0 1
5 1 0 1
6 1 0 1
7 1 0 1
8 1 0 1
9 1 0 1
10 1 0 1
11 1 0 1
12 1 0 1
13 1 0 1
14 1 0 1
15 1 1 0
16 1 0 1
17 1 0 1
18 1 0 1
19 1 0 1

# Attacker's Resource Limitation (measurements, buses)
12 3

# Bus Types (bus no, is generator?, is load?)
1 1 0
2 1 1
3 1 1
4 0 1
5 0 1

# Generator Information (bus no, max generation, min generation, cost coefficient)
1 0.80 0.10 60 1800
2 0.60 0.10 50 2200
3 0.50 0.10 60 1200

# Load Information (bus no, existing load, max load, min load)
2 0.21 0.30 0.10
3 0.24 0.25 0.15
4 0.18 0.30 0.10
5 0.20 0.25 0.10

# Cost Constraint, Minimum Cost Increase by Attack (in percentage)
1580 6
```

alone cannot satisfy the attack objective. In that case (*e.g.*, when all the line statuses are either secured or fixed), the maximum increase in the generation cost is less than 3%.

## IV. EVALUATION

In this section, we present the results of the scalability evaluation of our proposed model.

### A. Methodology

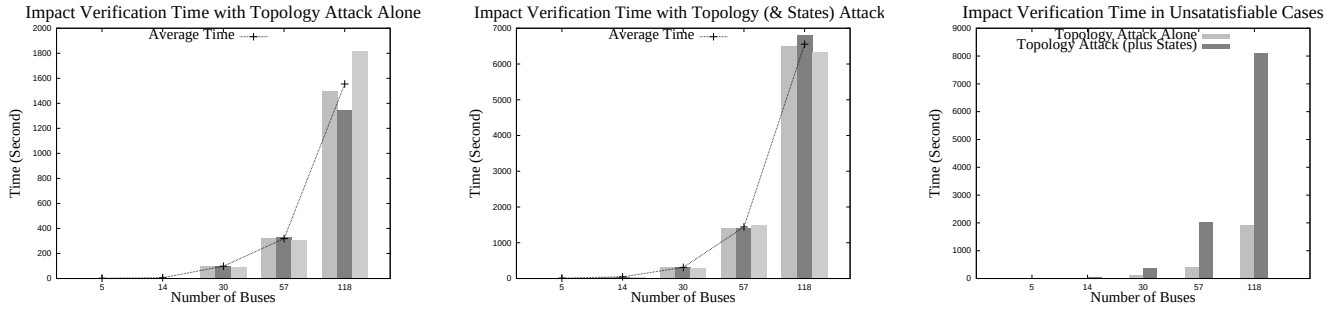
We evaluate the scalability of our proposed framework model by analyzing the time and memory requirements for executing the model in different problem sizes. Problem size depends mainly on the number of buses. We evaluate the scalability of our model based on different sizes of IEEE test systems, *i.e.*, 14-bus, 30-bus, 57-bus, and 118-bus [16] (along with our 5-bus test-case system), where we consider 5, 6, 7, and 23 generators, respectively. We take a linear segment based cost function as we have illustrated in Section III-E. We run our experiments on an Intel Core i5 Processor with 4 GB memory. The proposed model is coded using Z3 Managed API and executed using the Z3 SMT solver [8].

**Ideas to Improve the Scalability of Impact Analysis:** As we are considering real values, there is usually a very large number of stealthy topology attack vectors possible in an attack scenario, especially when we consider infecting the states as well. We observed that finding the impact on OPF considering such a large number of attack vectors become very costly (even intractable) when the number of buses becomes large (more than 14). In order to keep the computation cost tractable, we enhance the proposed framework with the following ideas:

- The intuition behind this mechanism is as follows: Though there can be a larger number of attack vectors, many attack vectors are very close to each other, *i.e.*, the difference between them is very insignificant with respect to the potential impact on OPF. Therefore, it is enough to consider one of these similar attack vectors to see the impact for each of them. According to this idea, the number of attack vectors considered for finding the impact becomes limited, which leads to a reduced execution time. In our experiments, we take the precision of 2 digits to consider two attack vectors as the same one.
- The typical OPF model, as we have presented in Section III-E, takes a very long time for 57, 118 or larger bus systems, which makes the impact verification often infeasible. In order to reduce the OPF model execution time, we adopt the idea of using generation-to-load distribution factors for calculating the line power flows in the OPF model [4], [17]. The use of shift factors alone cannot replaces the voltage phase angle based line power flow calculation as in Equation (32), because it is conditioned with the existence of the line in the topology. Therefore, we use the line outage or line closure distribution factors (LODF/LCDF) to work with any line exclusion or inclusion attacks [18]. However, since these LODF/LCDF are usually calculated for single line breakage or closure, in our evaluations, we only consider single line inclusion or exclusion based topology attacks.

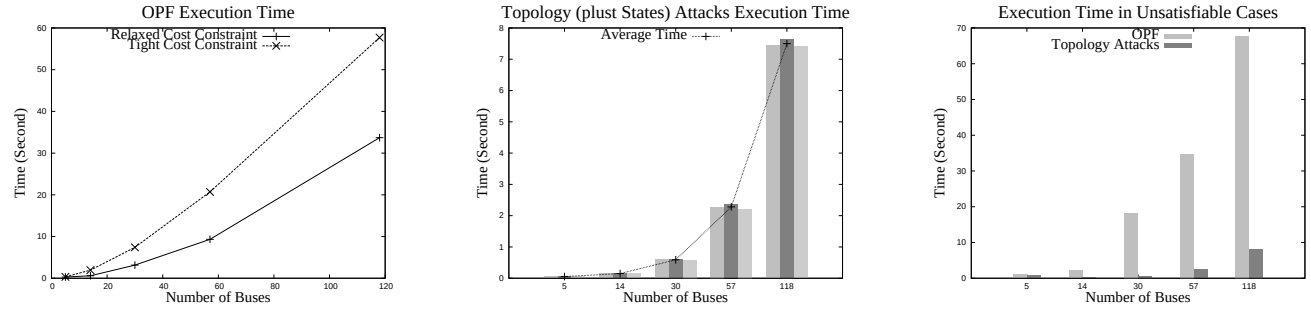
### B. Evaluation of Time Complexity

Fig. 4(a) and Fig. 4(b) show the execution times of the proposed model, *i.e.*, with and without infecting the states, respectively, of analyzing the impact of UFDI attacks on the OPF solution. The graphs show the impact of the problem size on the execution time. We vary the problem size by considering different IEEE test systems. At each problem size, we perform three experiments taking different random scenarios, especially in terms of the attacker's resource limitation. We consider a 1-2% of increase in the generation cost. The execution time of each of these experiments is shown using a bar chart. A graph is also drawn using the average execution time for each bus system. We see that, with respect to the bus size, the increase in the execution time follows almost the quadratic order. The execution time of an SMT model depends on the number of variables and the complexity of the theories applied in the model. The number of variables increases with the problem size, particularly in this model due to the number of generators and lines. However, we observe that the execution time is much higher in the scenario when infection to the states are also performed (Fig. 4(b)). Because, it is possible to launch multiple attacks on one or more states with respect to a single topology (*i.e.*, line inclusion or exclusion) attack, which




(a) (b) (c)

Fig. 4. The execution time of Impact verification on OPF with respect to the number of buses in (a) topology attacks without infecting states, (b) topology attacks including infecting states, and (c) unsatisfiable cases.




(a) (b) (c)

Fig. 5. These graphs shows the model execution time of individual models with respect to the problem size: (a) the OPF model, (b) the topology attack model, and (c) both of the individual models in the unsatisfiable cases.

increases the attack space, *i.e.*, search space, significantly. It is worth mentioning that due to this larger attack space, the second scenario can make larger (and various) impact on OPF compared to the first.

Fig. 4(c) shows the execution time in the unsatisfiable cases. If we compare the graphs in this figure with those in Fig. 4(a) and Fig. 4(b), we can see that the execution time in unsatisfiable cases is higher than the time in the satisfiable cases. The reason is obvious, *i.e.*, , the SMT solver requires verifying of all the potential attack vectors to conclude that there is no attack that can create the desired impact.

In our proposed model for analyzing the impact of stealthy topology attacks on the OPF solution, we have two main parts: (i) OPF model, and (ii) topology attack verification (or generation) model. In order to understand their individual effects on the time complexity, we also evaluate them in isolation. The execution time of the OPF model is shown in Fig. 5(a) with respect to the problem size (*i.e.*, the number of buses), where we observe that the execution time depends on the tightness of the (cost) constraint. The more close is the cost constraint to the optimal, the larger time is required to get a solution, because the solver needs to search more as the potential satisfiable solutions becomes smaller. The execution time of the topology attack model is shown Fig. 5(b) in three arbitrary cases (with respect to the attacker's resource limitation) for each bus system. Here, we observe that the time increases almost linearly with respect to the problem size. From these two figures, we can see that the execution time is much larger in the case of OPF model compared to that of the topology attack model. We also see that the increase in the time is linear for each individual model, although their combined effect is almost quadratic. Because, in simple words, the combined model needs to run these two individual models many times until an attack vector is found with the desired impact. In Fig. 5(c), we present the execution time in the unsatisfiable cases for both of the OPF model and the topology attack model. The figure shows that the execution time in the unsatisfiable cases is often larger than that in the satisfiable cases. The reason is the same as we have discussed in the last paragraph, *i.e.*, the solver needs to go through the whole search space to conclude with the unsatisfiable result.

TABLE IV. REQUIREMENT OF THE MEMORY (IN MB) BY THE SOLVER

| # of Buses | Topology Attack Model (in MB) | OPF Model (in MB) |
|---|---|---|
| 5 | 0.90 | 1.55 |
| 14 | 1.60 | 2.85 |
| 30 | 3.10 | 5.10 |
| 57 | 5.90 | 10.15 |
| 118 | 12.20 | 22.35 |

### C. Evaluation of Memory Complexity

The memory requirements of the SMT solver [8] for executing our individual models are evaluated in different IEEE test systems. The memory requirement for the execution of an SMT model depends mainly on the number of variables defined in the model and the number of intermediate variables generated by the solver to implement the satisfiability modulo theories used in the model. We show the memory requirements for the topology attack model (with infecting the states) and OPF model, individually, in Table IV. We can see that the memory requirement of our models increases almost linearly with the increase in the number of buses.

## V. RELATED WORK

We restrict our discussion to cyber-attacks which have mainly focused on state estimation. The idea of stealthy attacks, *i.e.*, UFDI attacks, was first reported by Liu et al. in [3]. The work in [19], extends the scope of UFDI attacks considering an adversary's limited access to meters, limited resources to compromise meters, with specific or random goals,

under assumptions that adversaries have perfect knowledge, *i.e.*, complete information about the grid. In general, computing the attack is an NP-complete problem and hence, the authors considered heuristics. Vukovic et al. proposed security metrics to quantify the importance of individual buses and the cost of attacking individual measurements accounting for communication vulnerabilities [13]. Bobba et al., in [6], showed that protecting a set of measurements that ensure observability is a necessary and sufficient condition to detect UFDI attacks. Kim and Poor in [7] proposed a greedy suboptimal algorithm to determine measurement subset that can be made immune from false data injection for the protection against UFDI attacksin. Kin Sou et al. in [20] show that an $l_1$ relaxation-based technique can provide an exact solution of the data attack construction problem. The works in [9], [14] consider UFDI attacks with incomplete or partial information. Very recently, in [21] Kim and Tong presented algebraic conditions of undetected topology attacks in power grids. However, all of these prior works focused on the attacks against state estimation from an individual attack stand point. In our recent works, we have addressed the problem of verifying stealthy attacks on state estimation by providing a comprehensive model of the attack attributes. In [10] we have presented a formal framework for verifying typical UFDI attacks, while in [22] we have introduced stealthy attacks with the novel idea of strengthening UFDI attacks by incorporating topology poisoning. In addition, in [22], we have devised a security architecture synthesis mechanism with respect to a given attack model and the grid operator's resource constraints.

Being motivated from the success of providing formal models for verifying stealthy attacks in our previous works, we have proposed a formal mechanism of verifying the impact of typical UFDI attacks on the OPF module first in [23]. In contrast, this paper shows how topology poisoning attacks can mount subtle attacks on the OPF module by changing the topology (plus states). While it appears intuitive that an attack on the state estimator can compromise the OPF, we provide a systematic modeling framework to analyze such cyber-attacks.

## VI. Conclusion

In this work, we have shown that topology poisoning attacks (*i.e.*, deliberate introduction of topology errors) can induce vulnerabilities to the Optimal Power Flow (OPF) module. We have further shown that topology poisoning attacks being combined with stealthy attacks on state estimation can create stronger impact on OPF. We have proposed a verification based formal framework solved with an SMT solver that allows us to model attributes of such an attack, analyze its feasibility, and quantify consequences in terms of increases in overall generation costs. We have demonstrated the framework on a small illustrative 5 bus test system. For the test system, we have determined attack configurations that increase cost of operation at least 6%, compared to the attack-free scenario. We have also evaluated the scalability of the proposed framework on the IEEE test systems. Our framework would be useful in systematically identifying and analyzing cyber-vulnerabilities, thus assist in developing suitable defense strategies. In future, we would like to investigate the impact of stealthy attacks on the power system's security.

## References


[1] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security Privacy*, 7(3):75–77, 2009.

[2] D. Kundur, X. Feng, Shan Liu, T. Zourntos, and K. L. Butler-Purry. Towards a framework for cyber attack impact analysis of the electric smart grid. In *IEEE International Conference on Smart Grid Communications*, Oct 2010.

[3] 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.

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

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

[6] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye. 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] Z3: An efficient smt solver. In *Microsoft Research*. http://research.microsoft.com/en-us/um/redmond/projects/z3/.

[9] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry. Cyber security analysis of state estimators in electric power systems. In *IEEE Conference on Decision and Control*, pages 5991–5998, 2010.

[10] M. Ashiqur Rahman, Ehab Al-Shaer, and Md. Ashfaqur Rahman. A formal model for verifying stealthy attacks on state estimation in power grids. In *IEEE International Conference on Smart Grid Communications*, Oct 2013.

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

[12] K. Sou, H. Sandberg, and K.H. Johansson. Electric power network security analysis via minimum cut relaxation. In *IEEE Conference on Decision and Control and European Control Conference*, pages 4054–4059, 2011.

[13] O. Vukovic, K. 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*, Oct 2011.

[14] Md. Rahman and H. Mohsenian-Rad. False data injection attacks with incomplete information against smart power grids. In *IEEE Conference on Global Communications*, Dec 2012.

[15] Leonardo de Moura and Nikolaj Bjørner. Satisfiability modulo theories: An appetizer. In *Brazilian Symposium on Formal Methods*, 2009.

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

[17] R. Treinen. Shift factors: Methodology and example. http://www.caiso.com/docs/2004/02/13/200402131609438684.pdf, 2005. CRR Educational Class, CAISO Market Operations.

[18] P.W. Sauer, K.E. Reinhard, and T.J. Overbye. Extended factors for linear contingency analysis. In *Annual Hawaii International Conference on System Sciences*, pages 697–703, Jan 2001.

[19] 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.

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

[21] Jinsub Kim and Lang Tong. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE Journal on Selected Areas in Communications*, 31(7):1294–1305, Jul 2013.

[22] 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)*, Jun 2014.

[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*, Apr 2014.