A Formal Model for Verifying the Impact of Stealthy Attacks on Optimal Power Flow in Power Grids

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

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

ABSTRACT

In modern energy control centers, the Optimal Power Flow (OPF) routine is used to determine individual generator outputs that minimize the overall cost of generation while meeting transmission, generation, and system level operating constraints. OPF relies on the output of another module, namely the state estimator, which computes all the system variables, principally the voltage magnitudes with phase angles, transmission line flows, and the bus (and total system) loads. However, recent works have shown that the widely used weighted least square based state estimation is vulnerable to stealthy attacks wherein an adversary can alter certain measurements to corrupt the estimator's solution, yet remain undetected by the estimator's bad data detection algorithm. Here, we show that an attack on state estimation can compromise the integrity of OPF and undermine the economic and secure system operation. We present a formal verification based framework to systematically investigate the feasibility of such stealthy attacks and their influence on OPF. The proposed approach is described with an illustrative example. We also develop a mechanism to increase the efficiency of executing our model, which is evaluated by running experiments on different IEEE test cases.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security

ICCPS 14, April 14—17, 2014, Berlin, Germany.

Keywords

Power Grid; State Estimation; Stealthy Attack; Optimal Power Flow; Formal Model

1. INTRODUCTION

Power system control centers employ a number of computational tools collectively referred to as the Energy Management System (EMS) for system wide monitoring, analysis, control, and operation. A schematic diagram of the various modules in EMS is shown in Figure 1 [1]. Within EMS, State Estimation (SE) is a critical module that estimates the system variables given a measurement model and a set of telemetered measurements. The term "state" corresponds to the vector of bus (or node) voltages, from which line (or branch) currents and power-flows can be computed. The output of state estimation is required for contingency analysis, economic dispatch calculation, and notably, for Optimal Power Flow (OPF) which determines the generator set-points required for Automatic Generation Control (AGC), as seen from Figure 1. However, critical infrastructures relying on SCADA based measurements are vulnerable to cyber-attacks [2]. Recent work has shown that state estimation is vulnerable to a stealthy type of cyber-attack, wherein an adversary injecting false data (to the measurement set) can corrupt the estimator's solution while remaining undetected [3]. The key idea behind such an attack, called an Undetected False Data Injection (UFDI) attack, 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 [4, 5]. An adversary with perfect knowledge (*i.e.*, who knows the complete measurement model) can then inject or manipulate meter measurements consistent with the measurement model to bypass the bad data detection (BDD) process [3]. While the extent of model accuracy on attacks is analyzed in [6], it is shown in [7, 8] that UFDI attacks launched by perfect

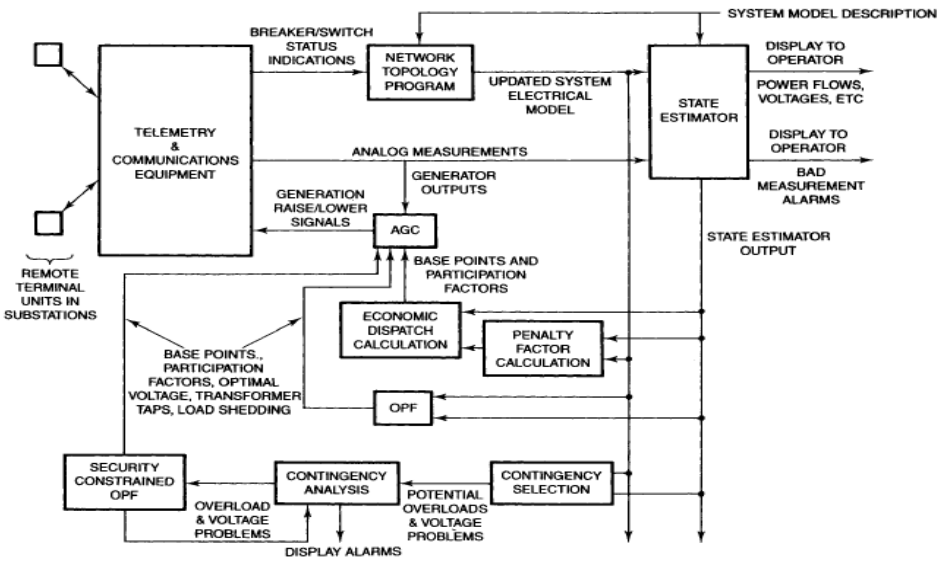

Figure 1: Energy control center system security schematic (thanks to Allen J. Wood and Bruce F. Wollenberg, *Power Generation, Operation, and Control*, 2nd Edition)

knowledge adversaries can be defended if a strategically chosen set of measurements are secured.

Since the state estimator is a very critical component of EMS, the primary goal of our work is to analyze the impact of UFDI attacks on the modules that are dependent upon or driven by the output of the estimator. Specifically, we focus on the OPF module which is responsible for determining the optimal generator set-points that minimize the overall cost of generation, while meeting transmission, generation, and system level operating constraints. These set-points provide the reference power generation commands for the AGC control loop that regulates the generator's output. An attack on the state estimator can result in an OPF solution that is no longer optimal, and the resulting generation dispatch will be economically disadvantageous. The paper is motivated from this stance leading to the following contributions:

- We present a formalism to model UFDI attacks in the broadest and most general form considering different attack attributes. An attack is defined in terms of these attributes which mainly represent an adversary's knowledge, resource, and target. The distinct advantage of this approach is the ability to systematically model different attack possibilities. A UFDI attack can easily have disadvantageous consequences on the OPF solution. Therefore, we formally model the OPF process and describe the UFDI attacks in terms of their impact on OPF.

- Our proposed formal verification framework is modeled as a constraint satisfaction problem, which is implemented using an SMT (Satisfiability Modulo Theories) solver [9]. SMT is a powerful formal language to solve constraint satisfaction problems that arise in many diverse areas including software and hardware verification, test-case generation, scheduling, planning, etc. We also evaluate our approach by executing our model on different IEEE test cases [10]. In this regard, we develop a control mechanism in order to get better scalability in solving our model.

The rest of this paper is organized as follows: In Section 2, we describe the necessary background. We present our formal model for verifying the impact of UFDI attacks on OPF in Section 3. The evaluation results of our model are presented in Section 4. In Section 5, we discuss the related work in the context of our work. We conclude the paper in Section 6.

2. BACKGROUND AND MOTIVATION

The stealthy attacks on state estimation (as shown in [3, 6]) and the widely used OPF formulation are both based on the DC power-flow model. This DC model is simplistic but popular and widely used in preliminary analytical power systems studies.

2.1 DC Power-Flow Model

The DC power-flow model describes the power balance equations in a power system, assuming a transmission line described purely in terms of its reactance [1]. The voltage magnitudes at all buses are held fixed at 1 per unit (pu) and only the voltage phase angles are treated as the variables. Thus, 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: $P_{ij} = y_{ij}(\theta_i - \theta_j)$. Admittance is computed as the reciprocal of the reactance. The power-balance constraint equating the algebraic sum of powers incident at every bus to zero yields a linear system of equations of the form: $[\mathbf{B}][\theta] = [\mathbf{P}]$. Assuming that the system has n buses and considering one of these buses as the reference or slack bus ($\theta_i = 0$), $[\mathbf{P}]$ is a column vector of $n-1$ elements corresponding to the net power demand at every bus (except the slack bus), while $[\theta]$ is a column vector of (unknown) $n-1$ phases corresponding to the voltage phasors at those buses. $[\mathbf{B}]$ is an $n-1$ dimensional square matrix that makes the relation between $[\mathbf{P}]$ and $[\theta]$ with respect to the transmission line properties. The DC power-flow model solves the unknown bus voltages, given the net power demands (*i.e.*, generation and load) at every bus and the line admittances. This linear model provides the basis of DC state estimation which is described next.

2.2 State Estimation and UFDI Attack

The state estimation problem is to estimate n number of power system 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]. The following equation shows the relationship between x and z:

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

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. Under the DC power-flow assumptions, the measurement model is linear (*i.e.*, the measured power-flows are linear functions of the bus voltages). Thus, the measurement model reduces to:

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

Here, $\mathbf{H}$ is known as the Jacobian matrix. The number of measurements m is typically much larger than n, thus constituting an over-determined set of linear equations (unlike the DC power-flow). The redundancy is provided mainly to detect, eliminate and smoothen the effect of unavoidable gross measurement errors.

When the measurement errors are distributed 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 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 $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau$, it is assumed that bad data is present. Here, τ is a selected threshold value.

It has been proved that an attacker with perfect knowledge of the system can inject bad measurements and evade the bad data detection (BDD) process mentioned above [3]. The attacks which mislead the BDD process are undetectable false data injection attacks. If an attacker injects arbitrary false data $\mathbf{a}$ to the original measurements $\mathbf{z}$ following the relation $\mathbf{a} = \mathbf{H}\mathbf{c}$ (*i.e.*, a linear combination of the column vectors of $\mathbf{H}$), then bad data measurement can fail. Here, $\mathbf{c}$ is the added value 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 $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$.

The grid connectivity matrix $\mathbf{A}$ and the branch admittance matrix $\mathbf{D}$ are used to compute the measurement matrix $\mathbf{H}$ as shown in the following [11]:

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

Matrices $\mathbf{DA}$ (*i.e.*, the multiplication of $\mathbf{D}$ and $\mathbf{A}$) and $-\mathbf{DA}$ represent the line power flows in forward and backward directions, respectively. Matrix $\mathbf{A}^T\mathbf{DA}$ (*i.e.*, the multiplication of $\mathbf{A}^T$ and $\mathbf{DA}$) represents power consumption at the buses.

The state estimated solution (from Equation (1)) provides the estimate of bus voltages from which the system power-flows can be computed. Summing up the net power flows incident on a bus then yields the estimated power (or load) at that bus. The state estimated system conditions are then used in the OPF module (refer to Figure 1) which is described in the following:

2.3 Optimal Power Flow

In contrast to power flow or state estimation in which the voltage phasor is estimated from the system model and measurements, the optimal power flow problem aims to minimize the total cost of generation such that: (i) the total system load is served and (ii) the operating constraints, such as equipment ratings, transmission line limits and control variables (*e.g.*, transformer tap positions, capacitor bank settings, etc.) are satisfied [1]. Let the cost of generation from generator k be $C_k(P_k)$, where C_k depends on the nature of the plant (*e.g.*, fossil fired, combined cycle, etc.). The OPF problem (with the DC power-flow model) can then be described as:

$$min \sum_k C_k(P_k) \text{ s.t.} \quad (3)$$

$$[\mathbf{B}][\theta] = [\mathbf{P}] \quad (4)$$

$$|P_{ij}| \leq P_{ij}^{max} \quad (5)$$

$$P_k^{min} \leq P_k \leq P_k^{max} \quad (6)$$

Here, Equation (3) states the objective of minimizing the total cost of generation, subject to satisfying the following: power-flow constraints in Equation (4), transmission line capacities in Equation (5), and generation

capacities in Equation (6).

Therefore, a stealthy attack on the state-estimator will influence the inputs used by OPF. The objective of this paper is to provide a systematic methodology to model and assess the impact of such attacks on OPF. We next characterize attacks by their attributes.

2.4 Attack Model

Our approach is to model a UFDI attack in its most generic form to study the feasibility of an attack under various scenarios. We define an attack in terms of its attributes as follows:

- **Accessibility and Resource Constraints**: An attacker may 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 vastly distributed measurements. In such cases, an adversary is limited to compromising or altering only a limited subset of measurements. However, if the measurements required for false data injection in an attack are distributed in many substations (*i.e.*, buses), then it would be harder for an attacker to inject false data to those measurements compared to the set of measurements 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 [12]. The extent of access is limited by the attacker's resource limitations.

- **Limited Knowledge**: For a successful UFDI attack, an attacker needs to know the grid topology (*i.e.*, the connectivity among the buses) and the electrical parameters of the transmission lines. However, gathering this knowledge is not trivial [3]. In the case of partial knowledge, the attacker's capability becomes restricted.

- **Attack Target**: Since a UFDI attack changes the estimation of one or more states and, thereby, impacts the EMS processes, an attacker may be interested in assessing the consequences of launching a certain attack. In the context of OPF, an attacker's target is expressed in terms of the increase in the generation cost by launching an attack.

2.5 Objective

While the prior works (*e.g.*, [3, 6, 13]) address UFDI attacks with these constraints considered in isolation, it is challenging to assess the attack feasibility when these attributes are considered simultaneously, in which case the interrelation between these attack variables becomes important. Thus being motivated, we model the UFDI attack on OPF as a constraint satisfaction problem. The solution will provide answers to queries, such as: *Given an attack scenario, whether or not a UFDI attack with a defined objective is feasible?* In answering this, the model allows a grid operator to preemptively analyze and explore potential threats under different attack scenarios. It is worth mentioning that a UFDI attack cannot increase the total load of the system; it only can change the loads of two or more buses (*i.e.*, some of the loads increase, while some other loads decrease). This is true due to the following two valid points that are considered in this work: First, the total generated power is equal to the total load. Second, the measurement regarding the power produced by each generator is known, *i.e.*, the power generation measurements cannot be compromised. The change in the OPF solution happens mainly due to the limitation of the power lines' transmission capabilities. Therefore, increasing the generation cost even in a small amount is challenging. Our proposed model gives a solution to this challenge.

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, *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 affected due to false data injection.
u_j	Whether any measurement residing at bus j is required to change.
t_i	Whether potential measurement i is taken.
r_i	Whether measurement i is accessible to the attacker.
s_i	Whether measurement i is secured.

3. FORMAL MODEL OF UFDI ATTACK IMPACT ON OPTIMAL POWER FLOW

3.1 Modeling Parameters

In order to model UFDI attacks on state estimation, we use a number of parameters (see Table 1) to denote different system properties and attack attributes.

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 an 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 $1 \leq i \leq l$, $1 \leq f_i, e_i \leq b$, and b is the number of buses. The ad-

mittance of the line is denoted by d_i.

There are two types of power measurements: the power flow through a line and the power consumption at a bus. We use P_i^L to denote the power flow through line i ($1 \leq i \leq l$), P_j^B to denote the power consumption by bus j ($1 \leq j \leq b$), and θ_j to denote the state value (*i.e.*, , the voltage phase angle at bus j). We also use P_j^D and P_j^G for denoting the load power and generated power of bus j, respectively.

We use c_j to denote whether state j ($1 \leq j \leq n$) is effected (*i.e.*, changed to an incorrect value) due to false data injection. Note that, in the DC power-flow model, each state corresponds to a bus. Thus, n is equal to b. 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 change, b_j becomes true.

Here, we model incomplete information only with respect to line admittance. We use the variable g_i to denote whether the attacker knows the admittance of line i. Note that if the end-buses of a line are unknown, the corresponding row in $\mathbf{A}$ is fully unknown to the attacker. In this case, there is no way for an adversary to launch UFDI attacks on the system. In the DC power-flow 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 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 $2l + b$ (*i.e.*, $m = 2l + b$) number of potential measurements ($1 \leq i \leq m$) 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 use t_i to denote whether potential measurement i is taken. Note that though m is often used to represent the taken measurements, in our formal model, m represents the maximum number of potential measurements.

The attacker may not be able to alter a measurement due to inaccessibility or existing security measures. We use r_i to represent whether measurement i is accessible to the attacker. We also use s_i to denote whether the measurement is secured.

3.2 Basic Power Model

Each row of $\mathbf{H}$ corresponds to a power measurement or equation. The first l rows correspond to the line power flow measurements. The second l measurements are the same as the first l, except the direction of the power flow is opposite. We have the following relation between the line power flow of line i (P_i^L) 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.

The last n rows of $\mathbf{H}$ correspond to the bus power consumptions. The power consumption, also known as the power injection, of a bus j is simply the summation of the power flows of the lines connected to this bus. If $\mathbb{L}_{j,in}$ and $\mathbb{L}_{j,out}$ represent the sets of incoming lines and outgoing lines of bus j, respectively, then 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 the net power at this bus, *i.e.*, the load power at this bus minus the power injected to the bus by its connected generators. If P_j^D and P_j^G denote the load power and the generated power at bus j, respectively, then the power consumption of bus j is represented by the following equation:

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

Basically, state estimation in the DC power-flow model is the process of finding the voltage phase angle (θ) of each bus by solving the linear equations for all of the measurements (P_i^Ls and P_j^Bs) given the line admittances (d_is).

3.3 Formalization of Changes in States and Corresponding Measurements

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

$$\forall_{1 \leq j \leq n} \quad c_j \rightarrow (\Delta\theta_j \neq 0) \tag{10}$$

From Equation (7), 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 (7) turns into the following:

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

The subtraction of Equation (7) from the above equation represents whether there are changes in the measurements and the states. The resulting equation will be as follows:

$$\Delta P_i^L = d_i(\Delta\theta_{f_i} - \Delta\theta_{e_i}) \tag{11}$$

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 $\Delta\theta_{f_i} \neq 0$ (or $\Delta\theta_{e_i} \neq 0$), then it is obvious that state f_i (or e_i) is changed (*i.e.*, attacked). Similarly, we have Equation (12) that

indicates whether a power consumption measurement is required to change:

$$\forall_{1\leq j\leq b} \;\; \Delta P_j^B = \sum_{i\in\mathbb{L}_{j,in}} \Delta P_i^L \; - \sum_{i\in\mathbb{L}_{j,out}} \Delta P_i^L \qquad (12)$$

The power generated (*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 it necessary. Typically, the OPF process is executed after the state estimation process to determine necessary changes in the generation dispatch. Therefore, in this model, we consider that a change in the power consumption measurement (as it is estimated by the state estimation process) specifies the change in the load, that is:

$$\forall_{1\leq j\leq b} \;\; \Delta P_j^G = 0 \qquad (13)$$

3.4 Formalization of False Data Injection to Measurements

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

$$\begin{aligned} &\forall_{1\leq i\leq l} \; (\Delta P_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i}) \\ &\forall_{1\leq j\leq b} \;\; (\Delta P_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j}) \end{aligned} \qquad (14)$$

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

$$\begin{aligned} &\forall_{1\leq i\leq l} \;\; a_i \rightarrow t_i \wedge (\Delta P_i^L \neq 0) \\ &\forall_{1\leq i\leq l} \;\; a_{l+i} \rightarrow t_{l+i} \wedge (\Delta P_i^L \neq 0) \\ &\forall_{1\leq j\leq b} \;\; a_{2l+j} \rightarrow t_{2l+j} \wedge (\Delta P_j^B \neq 0) \end{aligned} \qquad (15)$$

3.5 Formalization of Attack Attributes

Limited Information. If the admittance of a line is unknown, then the corresponding changes required in power flow measurements cannot be made. We formalize this condition as follows:

$$\forall_{1\leq i\leq l} \;\; (\Delta P_i^L \neq 0) \rightarrow ((t_i \vee t_{l+i}) \rightarrow g_i) \qquad (16)$$

The following equation shows an example of specifying the attacker's knowledge about the line admittances:

$$g_1 \wedge g_2 \wedge g_3 \wedge \neg g_4 \wedge \cdots \wedge g_l \qquad (17)$$

Limited Capabilities. The attacker usually cannot have the ability, with respect to physical or remote access, to inject false data to all the measurements. If a measurement is 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:

$$\forall_{1\leq i\leq m} \;\; a_i \rightarrow r_i \wedge \neg s_i \qquad (18)$$

The attacker's accessibility to the measurements are specified as follows:

$$r_1 \wedge \neg r_2 \wedge r_3 \wedge \neg r_4 \wedge \cdots \wedge r_m \qquad (19)$$

In the following equation, we show an example of specifying whether or not a measurement is secured:

$$\neg s_1 \wedge s_2 \wedge \neg s_3 \wedge \neg s_4 \wedge \cdots \wedge s_m \qquad (20)$$

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

$$\sum_{1\leq i\leq m} a_i \;\; \leq T_{CZ} \qquad (21)$$

Moreover, due to limited resources, an attacker can only access or compromise a limited number of substations (*i.e.*, buses) simultaneously. A substation is required to be accessed if one ore more measurements taken at that substation need to be altered. Therefore:

$$\begin{aligned} &\forall_{1\leq i\leq l} \;\; a_i \rightarrow u_{f_i} \\ &\forall_{1\leq i\leq l} \;\; a_{l+i} \rightarrow u_{e_i} \\ &\forall_{1\leq j\leq b} \;\; a_{2l+j} \rightarrow u_j \end{aligned} \qquad (22)$$

If T_{CB} is the maximum number of substations that the attacker can compromise, then:

$$\sum_{1\leq j\leq b} u_j \;\; \leq T_{CB} \qquad (23)$$

3.6 Formalization of Optimal Power Flow

The objective of OPF is to optimally control the generation according to the (changed) load requirement. Let us assume that $\hat{P}_j^G$ is the (modified) power produced by the generator connected to bus j after considering the (changed) load requirement (as seen from the state estimation result). The main constraint that the OPF solution must satisfy is that the total generation must be equal to the total load requirement. Therefore:

$$OPF_1: \quad \sum_{1\leq j\leq b} \hat{P}_j^G = \sum_{1\leq j\leq b} \hat{P}_j^D$$

Each generator has lower and upper bounds on the production of power, as follows:

$$OPF_2: \;\; \forall_{1\leq j\leq b} \; \hat{P}_{j,min}^G \leq \hat{P}_j^G \leq \hat{P}_{j,max}^G$$

In the above formulation, $\hat{P}_{j,max}^G$ and $\hat{P}_{j,min}^G$ are the maximum and minimum production limits of the generator at bus j.

Recall from Equation (4) in Section 2 that OPF considers the entire set of power-flow equations as constraints. In the case of OPF, if $\hat{\theta}$, $\hat{P}_i^L$ and $\hat{P}_j^B$ are the state of bus j, the power flow on line i, and the power consumption at bus j, respectively, the following equations, similar to Equations (7), (8), and (9), must hold:

$$\begin{aligned} OPF_3: \quad & \forall_{1\leq i\leq l} \;\; \hat{P}_i^L = d_i(\hat{\theta}_{f_i} - \hat{\theta}_{e_i}) \\ & \forall_{1\leq j\leq b} \;\; \hat{P}_j^B = \sum_{i\in\mathbb{L}_{j,in}} \hat{P}_i^L \; - \sum_{i\in\mathbb{L}_{j,out}} \hat{P}_i^L \\ & \forall_{1\leq j\leq b} \;\; \hat{P}_j^B = \hat{P}_j^D \; - \hat{P}_j^G \end{aligned}$$

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

$$OPF_4: \quad \forall_{1\leq i\leq l} \;\; \hat{P}_i^L \leq P_{i,max}^L$$

Let us assume that $\mathcal{C}_j(.)$ 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 [1]. Considering the viability of modeling the cost function, we consider the latter form for cost functions, given by:

$$\mathcal{C}_j(P_j^G) = \alpha + \beta P_j^G$$

Here α and β 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. Without 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 an UFDI attack. The constraint is formalized as follows:

$$OPF_5: \quad \sum_{1\leq j\leq b} \mathcal{C}_j(\hat{P}_j^G) \; < T_{OPF}$$

We denote the OPF model (OPF) as the conjunction of OPF_1, OPF_2, and so on, as follows:

$$OPF = \bigwedge_{1\leq k\leq 5} OPF_k$$

3.7 Formalization of Impact of UFDI Attacks on OPF

We have formalized the optimal power flow (OPF) in the previous subsection, the negation of which will be used as a constraint in the UFDI attack model. This constraint represents the expected attack impact, which specifically represents whether an attack is possible which will increase the generation cost (according to the OPF solution) at least to an expected value.

According to Equation (13), the change in the power consumption of a bus specifies the change in the load at that bus. The following equation formalizes this:

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

Let $\hat{P}_j^D$ be the estimated load (according to the state estimation result) at bus j. Therefore:

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

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 load at bus j, then:

$$\forall_{1\leq j\leq b} \; \hat{P}_{j,min}^D \leq \hat{P}_j^D \leq \hat{P}_{j,max}^D \tag{24}$$

Impact-based Attack Target. The constraint on the expected impact by launching a UFDI attack is formalized as follows:

$$\neg \left(\exists_{\hat{P}_1^G, \hat{P}_2^G, \cdots, \hat{P}_b^G} OPF\right) \tag{25}$$

The above constraint states that there is no possible generation distribution that can cost less than T_{OPF}. In order define the increase in the cost properly, 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:

$$T_{OPF} = \mathcal{T}_{OPF} I/100$$

In addition, since the attacker's goal is not to fail the OPF solution to converge, he needs to ensure that there is an OPF solution for an arbitrarily higher value, $\bar{T}_{OPF}$, which is $\mathcal{T}_{OPF}\bar{I}/100$ and $\bar{I} > I$. Let $\overline{OPF}$ be this OPF solution, which is the same as that of OPF (Equation (24)), except the following constraint:

$$\overline{OPF}_6: \quad \sum_{1\leq j\leq b} \mathcal{C}_j(\hat{P}_j^G) \; < \bar{T}_{OPF}$$

The formalization of $\overline{OPF}$ has to be satisfied.

3.8 Implementation

We encode the system configuration and the constraints into SMT [14]. We write a program leveraging the *Z3 .Net API* [9] 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

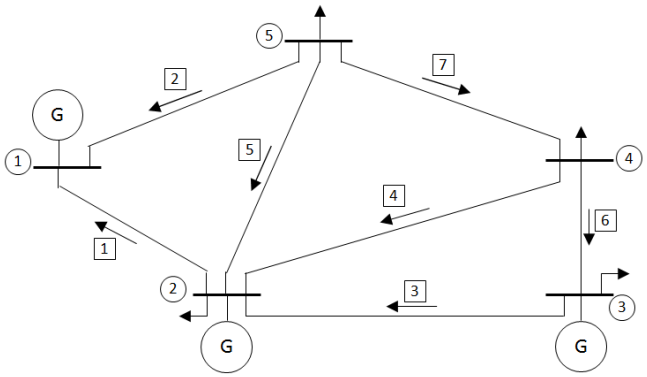

Figure 2: A 5-bus test system. Bus numbers are in circles and line numbers are in squares.

Table 2: Line Information of the Example in Section 3.9

Line #	From	To	Admittance	Capacity	Knowledge Status
1	1	2	16.90	0.15	1 [a]
2	1	5	4.48	0.15	1
3	2	3	5.05	0.10	0 [b]
4	2	4	5.67	0.20	1
5	2	5	5.75	0.15	0
6	3	4	5.85	0.10	1
7	4	5	23.75	0.15	0

[a]The attacker knows the impedance of this line.
[b]The attacker does not know the impedance of this line.

from the assignments of the variables, a_is, 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).

3.9 An Example Case Study

Here, we present an example in order to delineate our model and its execution. In this example, we consider a 5-bus sub-system taken from the *IEEE 14-bus test system* [10]. The 5-bus system is shown in Figure 2. The input regarding the line information are shown in Table 2. 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) and the knowledge status (*i.e.*, the line admittance of a line is known to the attacker). According to the input, the admittance of line 5 is unknown.

The input about the measurements is shown in Table 3. Since this bus system has 5 buses and 7 lines, the maximum number of potential measurements is (5 + 2×7) or 19. Each row of Table 3 includes (i) whether the measurement is taken for state estimation (all of the potential measurements are taken except measurements 8 and 9), (ii) whether the measurement is secured (measurements 1, 2, and 15 are secured) and (iii) whether the attacker has the accessibility to alter the measurement (the attacker does not have the ability to alter measurements 1, 2, 8, 9, and 15). The rest of the input is shown in Table 4. 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. Note that a single generator at the maximum is connected to a bus. The generation cost of power is followed from the simple linear function as shown in Section 3.6. The values of coefficient a and b for each generator are given in the input (see Table 4). 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). The cost constraint in the attack-free condition is $1580.

Table 3: Measurement Information of the Example in Section 3.9

Measurement #	Is Recorded?	Secured	Can Alter?
Forward Line Flows:			
1	1 [a]	1 [b]	0
2	1	1	0
3	1	0	1 [c]
4	1	0	1
5	1	0	1
6	1	0	1
7	1	0	1
Backward Line Flows:			
8	0	0	0
9	0	0	0
10	1	0	1
11	1	0	1
12	1	0	1
13	1	0	1
14	1	0	1
Bus Power Consumptions:			
15	1	1	0
16	1	0	1
17	1	0	1
18	1	0	1
19	1	0	1

[a]The measurement is taken or recorded for state estimation.
[b]The measurement is secured (mainly in terms of integrity).
[c]The attacker has the accessibility to alter the measurement.

In this example, the attacker's objective is to attack the states, to induce a 2.5% increase in the generation cost from the base-case OPF solution. It is important to note that the attacker's objective is *not* to prevent convergence of OPF, but to subtly lead OPF towards a costlier solution. The attacker's resource limitation limits alteration to utmost 12 measurements at a time distributed in no more than 4 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 assignments, we find that the objective can be successful by attacking states 3 and 4. In order to attack these states, measurements 3, 4, 6, 7, 10, 11, 13, 14, 17, 18, and 19 are required to be altered. These measurements are distributed in buses 2, 3, 4, and 5. If the attacker's resources are very limited

Table 4: Input of the Example in Section 3.9

```
# Topology (Line) Information
# (line no, from bus, to bus, admittance, knowledge?)
1 1 2 16.90 0.15 1
. . . . . .

# Measurement Information
# (Measurement No, measurement Taken?, secured?, can attacker
alter?)
1 1 1 0
. . . . . .

# Maximum Number of States for Estimation Attack
4

# Attacker's Resource Limitation
# (In terms of measurements and buses, respectively)
12 4

# 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, maximum generation, minimum generation, cost coeffi-
cient a and b)
1 0.50 0.10 60 1800
2 0.40 0.10 50 2200
3 0.60 0.10 60 1200

# Load Information
# (bus no, existing load, maximum load, minimum 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 %)
1580 2.5
```

(*e.g.*, 8 measurements or 2 buses only), then there is no feasible attack vector satisfying the objective.

From the assignments, we see that due to the UFDI attack on the state estimation, the loads of buses 3, 4, and 5 are changed to approximately 0.2, 0.273, and 0.147 units, respectively (while the actual loads are 0.24, 0.18, and 0.2 units). As a result, because of the limited capacity of the lines, the cost is increased almost to \$1620, which is around 2.5% more than the optimal value in the case of attack-free scenario. In the attacked scenario, the power generated at buses 1, 2 and 3 are 0.26, 0.295, and 0.275 units, respectively, while in the without attack scenario, the generated power at these buses are 0.24, 0.265, and 0.325 units. If the attacker likes to increase the generation cost up to 5%, there is no attack vector in this attack scenario.

4. EVALUATION

In this section, we present the evaluation results of the proposed model for scalability in terms of time and memory requirements.

4.1 Methodology

We evaluate the scalability of our proposed 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, although the number of generation buses is also crucial for the OPF calculation. We evaluated the scalability of our model based on different sizes of IEEE test systems, *i.e.*, 14-bus, 30-bus, 57-bus, and 118-bus [10], along with our 5-bus test-case system. In these test systems of 14, 30, 57, and 118 buses, we consider 5, 6, 7, and 23 generators. We consider the same cost function, *i.e.*, a linear segment based cost function, as we have have discussed in Section 3.6. We run our experiments on an Intel Core i5 Processor with 4 GB memory. The proposed model is coded using Z3 Managed API and execute the program using an associated SMT solver [9]. We also apply the following ideas to increase the scalability of the analysis:

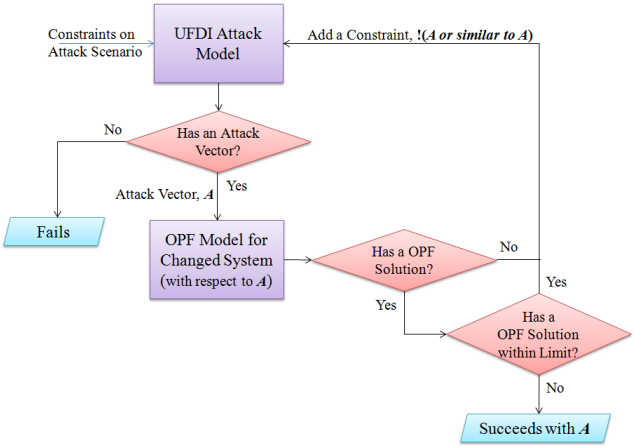

Figure 3: The flow diagram of finding the impact of UFDI attacks on OPF.

4.1.1 Limiting the number of attack vectors:

As we are considering real values, there is usually a very large number of UFDI attack vectors possible in an attack scenario. Moreover, 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 10). In order to keep the computation cost tractable, we follow the mechanism as shown in Figure 3 to find the impact. 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 tractable execution time. In our experiments, we consider the precision of 2 digits to take two attack vectors as the same one.

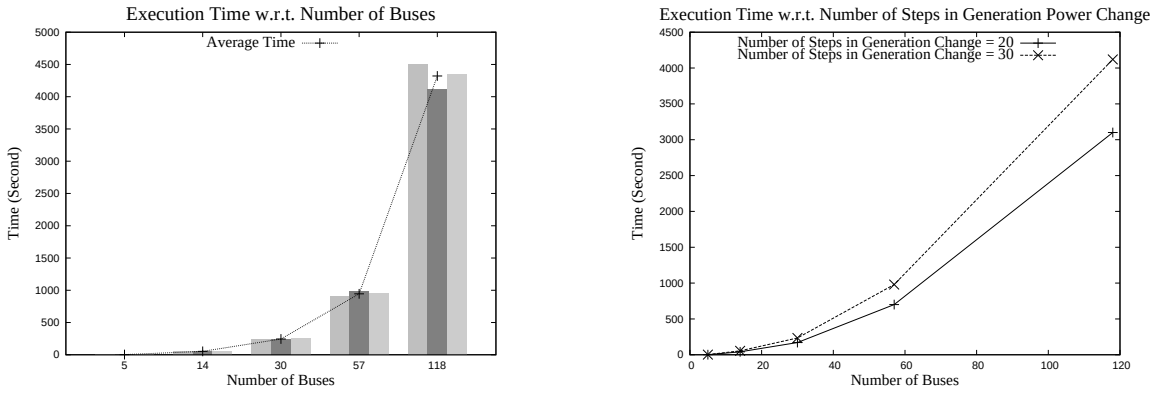

Figure 4: (a) The execution time of OPF Impact model with respect to the number of buses, and (b) the impact of the number of steps of the generation power change on the model execution time.

4.1.2 *Limiting the number of possible values of generator dispatches:*

The generated power at a bus can be any value between the minimum and maximum boundaries. Since we are working with real values, there is a infinitesimal number of possible generation dispatch values. In order to keep this number a finite and limited one, we consider a fixed number of possible values of the generation by taking a specific number of steps in changing generation starting from minimum value till the maximum value. In our experiments, we mostly consider 30 steps.

4.1.3 *Using generation and load distribution factors for the OPF calculation:*

The OPF model presented in Section 3.6 takes a very long time for 57, 118 or larger bus systems, which makes the impact verification infeasible as we need to run the OPF model once or twice at each iteration of our impact verification mechanism, as illustrated in Figure 3. In order to reduce the OPF model execution time, we adopt the idea of generation and load shift factors (or generation-to-load distribution factors) for calculating the line power flows in the OPF model [4, 15]. The use of shift factors replaces the voltage phase angle based line power flow calculation (as in Equation (7)).

4.2 Evaluation Results and Discussion

4.2.1 *Time Complexity*

Figure 4(a) shows the execution time of our proposed model for finding the impact of UFDI attacks on the OPF solution. The evaluation is executed with respect to the problem size. We vary the problem size by considering different IEEE test systems. We perform three experiments taking different random scenarios, especially in terms of the attacker's resource limitation. We consider an amount of 2% increase in the generation cost. The execution time of each case is shown in Figure 4(a) using a bar chart. A graph is also drawn using the average execution time for each bus system. We observe that with respect to the bus size the increase in the execution time follows almost the quadratic order. A SMT program's execution time depends on the number of variables and the complexity of the theories applied in the model. This number of variables increases with the increase of the problem size. For a specific bus size, we also observe that the execution time differs, though in small amounts, for different scenarios. In the case of the 118-bus system, the time is comparatively very high, mostly due to a larger number of generators compared to that of the other systems. It is worth mentioning that the execution time in a scenario, in which no attack is possible satisfying the given impact target, can be very high when the number of attack vectors generated by the UFDI attack model is very large (refer to Section 4.1.1). Because, for each of this large number of attack vectors, it is required to verify whether that particular attack can cause the expected impact.

Figure 4(b) shows impact of the number of possible values of the generated power (*i.e.*, the number of steps between the minimum and maximum values) at a bus on the execution time. We observe that the execution time decreases with the decrease of the number of steps. Because, when the number of possible values of the generated power at each generation bus reduces, the search space for the OPF solution becomes smaller.

In our proposed model for impact of UFDI attacks on the OPF solution, we have two main parts: (i) OPF model, and (ii) UFDI model. In order to understand their individual effects on the time complexity, we also evaluate them. The results are shown in Figure 5(a) and Figure 5(b). We can see that the execution time is much larger in the case of OPF model compared to that of the UFDI model. We also see the increase in the time

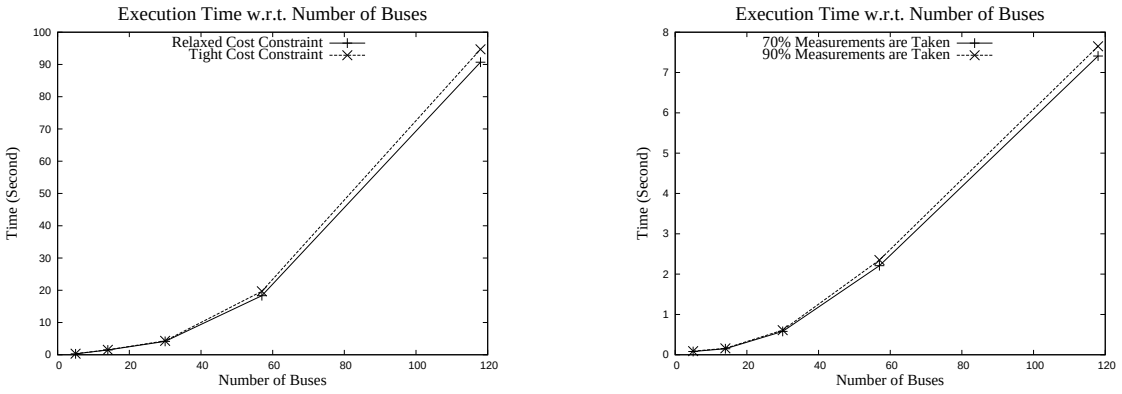

Figure 5: These graphs shows the model execution time with respect to the number of buses: (a) the execution time of OPF model alone, and (b) the execution time of UFDI model alone.

Table 5: The Required Memory Space (in MB) for UFDI and OPF

# of Buses	UFDI Model	OPF Model
5	0.59	1.56
14	1.32	2.85
30	2.60	5.10
57	4.56	10.16
118	9.69	22.36

is linear for individual cases, although their combined effect is almost quadratic, as we need to execute a *exists* quantification for OPF (refer to Equation (24)).

4.2.2 Memory Complexity

The memory required by the SMT solver [9] for executing our proposed model is evaluated in different IEEE test systems. We evaluate the memory requirement for different parts of our model individually also. The memory requirement for an execution of the 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 UFDI attack model and OPF model, individually, in Table 5. We can see that the memory requirement of our models increases almost linearly with the increase in the number of buses.

5. RELATED WORK

In this section, we limit our discussion to cyber-attacks discussed in recent literature, which however, are mainly centered on state estimation. The concept of stealthy attacks, which was presented by Liu et al. in [3] for the first time, has attracted a lot of attention in recent literature. In [16], the authors extended 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.

Bobba et al. showed that for detecting UFDI attacks it is necessary and sufficient to protect a set of basic measurements, which corresponds to the minimum set of measurements ensuring observability [7]. Kim and Poor 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 attacksin [8].

Vukovic et al. proposed a number of security metrics to quantify the importance of individual buses and the cost of attacking individual measurements considering the vulnerability of the communication infrastructure [12]. Kin Sou et al. claimed that an l_1 relaxation-based technique provides an exact optimal solution of the data attack construction problem [17]. UFDI attacks with incomplete or partial information are discussed by the works presented in [6, 13]. These works mathematically showed the impact of incomplete knowledge on the potentiality of UFDI attacks, only in the context of state estimation. In our previous work, we presented a formal model for the comprehensive verification of the power system state estimation security with respect to different constraints and requirements [18].

In contrast, our work in this paper considers the OPF module, a critical component of EMS, which relies on the output of the state estimator. While it is intuitive that an attack on the state estimator can impact OPF, we provide a systematic modeling framework to analyze such cyber-attacks considering several attributes. It is worth mentioning that, to our best knowledge, our work is the first of its kind in modeling and analyzing cyber-vulnerabilities through a formal satisfiability

framework, particularly on critical modules that rely on the state-estimator.

6. CONCLUSION

Given that the electric grid is a critical infrastructure, it is crucial to first understand its vulnerabilities before developing defensive strategies. In this context, we focus on the Optimal Power Flow - a module responsible for economic and secure operation of the electric grid in power system control centers. Our work shows how a cyber-attack can be mounted on OPF via a stealthy attack. Formulating such an attack in its most general form and encoding the problem constraints from a Boolean satisfiability viewpoint, we show how the framework can be used to systematically model and query the implications of several attack scenarios. The resulting model is solved with an SMT solver and the proposed method is illustrated on a small (5 bus) test system. For the test example, we compute feasible attack configurations that increase the base-case (*i.e.*, attack free) cost of operation, e.g., up to about 2%. More generally, our results show that a clever adversary can subtly manipulate carefully chosen measurements not to brazenly disable OPF, but to induce an increase in overall cost of generation. The proposed framework is thus useful in understanding the impact of cyber-attacks, and thus provides the first step in developing suitable tools to keep the electric grid secure. In our future work, we would like to extend our model by incorporating other kinds of attacks, *e.g.*, topology attacks, with respect to the impact on OPF.

7. REFERENCES

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

[2] 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*, October 2010.

[3] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *the 16th 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] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. S. Sastry. Cyber security analysis of state estimators in electric power systems. In *the 49th IEEE Conference on Decision and Control (CDC)*, pages 5991–5998, 2010.

[7] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. Detecting false data injection attacks on dc state estimation. In *the 1st IEEE Workshop on Secure Control Systems, CPS Week*, Apr 2010.

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

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

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

[11] K. C. Sou, H. Sandberg, and K. Johansson. Electric power network security analysis via minimum cut relaxation. In *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, pages 4054–4059, 2011.

[12] O. Vukovic, K. C. 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*, October 2011.

[13] 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.

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

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

[16] 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.

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

[18] 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*, October 2013.