Impact of Stealthy Attacks on Optimal Power Flow: A Simulink-Driven Formal Analysis

Mohammad Ashiqur Rahman and Amarjit Datta
Department of Computer Science, Tennessee Tech University, Cookeville, USA
Emails: marahman@tntech.edu, adatta42@students.tntech.edu

Abstract—Optimal Power Flow (OPF) is a crucial part of the Energy Management System (EMS) as it determines individual generator outputs that minimize generation cost while satisfying transmission, generation, and system level operating constraints. OPF relies on a core EMS routine, namely state estimation, which computes system states, principally bus voltages/phase angles at the buses. However, state estimation is vulnerable to false data injection attacks in which an adversary can alter certain measurements to corrupt the estimators solution without being detected. It is also shown that such a stealthy attack on state estimation can increase the OPF cost. However, the impact of stealthy attacks on the economic and secure operation of the system cannot be comprehensively analyzed due to the very large size of the attack space. In this paper, we present a hybrid framework that combines formal analytics with Simulink-based system modeling to investigate the feasibility of stealthy attacks and their influence on OPF in a time-efficient manner. The proposed approach is illustrated on synthetic case studies demonstrating the impact of stealthy attacks in different attack scenarios. We also evaluate the impact analysis time by running experiments on standard IEEE test cases and the results show significant scalability of the framework.

Index Terms—Power Grid; Optimal Power Flow; Stealthy Attacks; Impact Analysis; Resiliency; Formal Verification.

1 Introduction

EMS refers to a set of computational routines employed for system-wide monitoring, analysis, control, and operation in electric power grids. A schematic diagram of EMS modules is shown in Fig. 1 (adapted from [1]). State estimation is the core routine or module in EMS that estimates the system state variables from a set of real-time telemetered measurements (from sensors/meters) and topology statuses (from circuit breakers and switches). The term "states" denotes bus voltages and phase angles, from which transmission line power flows can be computed. As seen in Fig. 1, the output of state estimation is required by OPF and contingency analysis for economic dispatch calculations and security assessment.

Cyber technologies are increasingly used in modern power grids with the promise of providing larger capacity, higher efficiency, and more reliability [2]. While this integration helps energy providers to offer smarter services, real-time demand-response actions, and economic advantages, power grids also become vulnerable to cyber attacks. Cyber intrusions and false data injections can be launched against power grids, which can cause improper controls and thereby economically inefficient as well as functionally insecure operations [3].

An attacker can compromise sensors/meters or communication media to introduce malicious measurements, which can lead to incorrect state estimation. Bad data detection algorithm [4], [5] can detect bad measurements, principally by comparing the mean-squared deviation between observed and estimated measurements with a threshold value. However, it has been shown that an attacker who possesses the knowledge of the grid can generate bad measurements, which can bypass this bad data detection mechanism [6]. These attacks are widely named in the literature as Undetected False Data Injection (UFDI) or simply "stealthy" attacks. As a result of these stealthy attacks, states are estimated incorrectly, which can easily lead the system to a non-optimal and vulnerable situation. Hence, it is crucial to develop an impact analytics framework that can identify potential stealthy attacks with respect to the interdependency among different EMS modules, different attack models, and possible impact on the system.

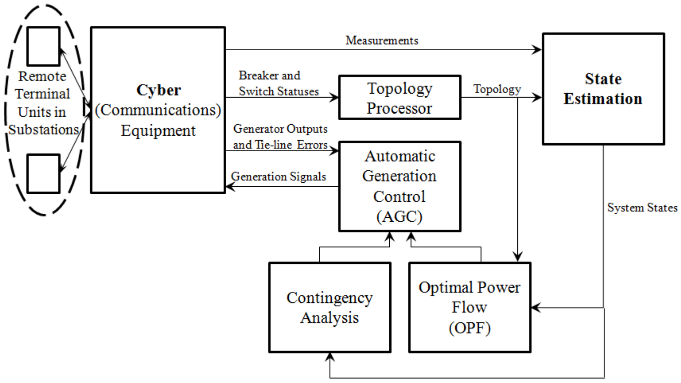

Remote Terminal Units in Substations
Cyber (Communications) Equipment
Measurements
Breaker and Switch Statuses
Topology Processor
Topology
State Estimation
Generator Outputs and Tie-line Errors
Generation Signals
Automatic Generation Control (AGC)
System States
Contingency Analysis
Optimal Power Flow (OPF)

Fig. 1. An schematic diagram of the EMS, which shows the interdependency among different modules on the state estimation routine.

The primary goal of our research is to efficiently analyze the impact of stealthy attacks on the modules that are dependent on state estimation. In this particular work, we focus on economic impact-based threat analysis considering the OPF module. OPF calculates the optimal production set-points for the power generators that meet the loads, satisfy transmission and generation-level operating constraints, and minimize the generation cost. An incorrect state estimation can result in an OPF solution that is no longer optimal, and the resulting generation dispatches will be economically disadvantageous. The stealthy attack capability allows an adversary to undermine a power system and create economic loss. Therefore, it is important to understand potential threats on a power system, with respect to an expected attack model and harden the security by mitigating the threats.

In our previous work [7], we proposed a formal approach (based on Satisfiability Modulo Theories (SMT) [8]) for assessing the impact of stealthy attacks on the economic operation of the system in different adversarial capacities. However, the attack space is often very large and a complete impact analysis of a decently large power system cannot be performed in a reasonable time frame because of the proposed solution approaches' limitations. Therefore, an efficient mechanism is required to perform a comprehensive impact analysis, and thus measure the system's dependability. The paper is motivated from this stance, leading to the following two key contributions:

- **Hybrid Framework:** We propose a hybrid framework to find critical threats by analyzing the economic impact of potential stealthy attacks with respect to a given system environment and expected attack model. We combine the SMT-based modeling with the Matlab Simulink-based system design [9]. We model the stealthy attack logically using SMT and solve the model using an efficient SMT solver to find attack vectors − the attack verification model. An attack vector represents a set of measurements that an attacker needs to alter, and thus the buses corresponding to these measurements that the attacker needs to access, to launch a stealthy false data injection attack that manipulates a particular set of states. We design a Simulink model for exploring the attack space for a particular attack vector and assess the impact on the OPF solution. Each attack vector is fed to this Simulink model, where possible alterations in the measurements are explored efficiently by modeling the attack vector. The resultant changes in the bus loads are fed to the OPF routine designed within the Simulink model, and it is verified whether there is a significant impact on the generation cost. The whole attack space can be studied to find all critical threats.
- **Efficient Execution of the Framework:** We further improve the efficiency of the framework for exploring the potential attack space by applying a two-level parallelism technique. First, we perform parallel execution of the SMT-based attack verification model and Simulink-based attack space exploration model. Then, within the latter process, we parallelly execute multiple instances of the exploration model. We devise necessary algorithms for this parallel execution. We evaluate the proposed framework by executing it on arbitrary attack scenarios according to different IEEE test cases [10] and observe that it can perform a comprehensive impact-based threat analysis of a system within a reasonable time period. This performance also depends on the available processing and parallelism capacity of the machine executing the framework.

The rest of this paper is organized as follows: Section 2 discusses the necessary background of stealthy attacks. We present the proposed framework in Section 3. Two case studies are demonstrated in the following section. We present the evaluation results of our model in Section 5. We perform the literature review in the context of our work in Section 7. We conclude the paper in Section 8.

2 Background and Motivation

This section includes necessary background knowledge and the research objective.

2.1 State Estimation and Optimal Power Flow

The DC power-flow model has been widely used to analyze stealth attacks on state estimation (*e.g.*, [6], [11], [12]). The DC model is a linearized estimation of the non-linear power system (AC model), but it is useful in preliminary analytical power systems studies [1]. In this work, we assume the DC power balance equations.

2.1.1 Power Flow Model

A power grid system consists of a number of buses (or substations) and transmission lines. Each line connects two buses. A bus usually has a load to serve while it may be connected with one or more power generators. The DC power flow model describes the power balance equations in a lossless power system [1]. In this lossless model, the total power generation in a grid is equal to its overall load. The "state" of a bus is considered as the phase angle with respect to a reference bus (assuming that voltage magnitudes at all buses are fixed at one per unit). The power balance equations are formulated solely based on the reactance properties of the transmission lines. The model expresses the power-balance constraint that equates the algebraic sum of powers incident at every bus to zero. This yields a linear system of equations. EMS receives measurements from field devices and the state estimation routine calculates the (unknown) bus states from the power balance equations.

It is to be noted that the power flow can be measured at each end bus of a transmission line. A measurement can also be taken at a bus to realize its power consumption. Hence, at a bus, meters can be deployed to measure all or some of the power flow measurements (corresponding to all the incident lines to the bus) and the power consumption measurement. Typically, the possible measurements at all the buses are not metered and the state estimation routine is used to calculate the unknown (unmetered) measurements, which may include power consumption measurements (and so the loads) at different buses.

2.1.2 State Estimation

The state estimation problem, as formally defined, is estimating 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]. 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:

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

A significant number of redundant measurements are considered (*i.e.*, $m > n$) in creating an over-determined set of linear equations. The redundancy enables the detection, elimination, and smoothing of gross measurement errors. When the measurement error distribution is Gaussian with zero mean, the states are estimated ($\hat{\mathbf{x}}$) as follows:

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

Here, $\mathbf{W}$ is a diagonal "weighting" matrix whose elements are reciprocals of meter error variances. 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 $||\mathbf{z}-\mathbf{H}\hat{\mathbf{x}}||$ is greater than τ, a selected threshold value, it is bad data.

2.1.3 Optimal Power Flow

The OPF routine determines the optimal generation dispatches based on system properties and estimated loads at the buses. The aim of OPF is to minimize the total generation cost while serving the load at each bus and satisfying the following constraints [1]:

1) The power balance equations of the system.
2) Generation Limit: Each generator produces an amount of power within its maximum generation capability.
3) Transmission Capacity: The resultant power flow through each line must not cross its capacity.

2.2 Stealthy Attack and Adversary Model

2.2.1 Stealthy Attacks

The idea of stealthy attacks on state estimation was first mathematically shown by Liu et al. based on the DC power flow model [6]. These attacks are named as Undetected False Data Injection (UFDI) attacks. The concept of a UFDI attack is briefly discussed here. Let us consider an attacker who can inject 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 the change to the original estimation $\hat{\mathbf{x}}$ because of 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 because $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$. Thus, the bad data detection is evaded. To launch such a stealthy attack, an adversary requires knowledge of $\mathbf{H}$, more specifically the system topology, electrical properties of the transmission lines, and measurement configurations.

2.2.2 Attack Model

In this work, we consider false data injection- based cyber attacks that can potentially occur at the bus or substation level (Fig. 1). Measurement data can be altered by compromising the corresponding meter or sensor residing at the bus or the remote terminal unit (RTU), which is responsible for transmitting this measurement, as a man-in-the-middle attack. It is worth mentioning that measurements within a substation are often gathered at a single RTU. that an adversary can break into to access the measurement data.

2.2.3 Adversary Properties

An adversary's capability can be described by the following properties:

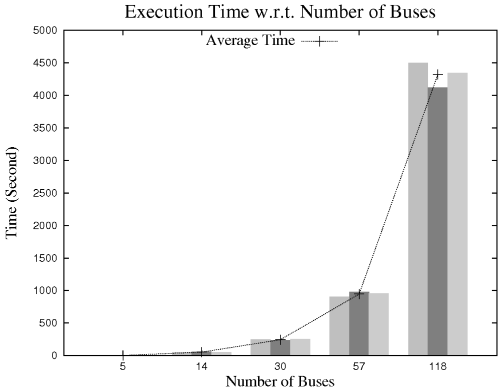


Fig. 2. The execution time to find a single threat vector that can increase the generation cost (2%) [7].

- *Accessibility*: It is very unlikely that an attacker has access to all measurements because physical or remote access to substations is restricted and some measurements may already be data integrity protected.
- *Resource*: The resource available to an adversary often limits (in terms of cost or effort) the injection of false data simultaneously to a large number of measurements, distributed over many substations.
- *Knowledge*: To launch a stealthy attack, an attacker needs to know the connectivity among the buses and the electrical parameters of the transmission lines [6]. If the attacker has only partial knowledge, the attack capability becomes restricted.
- *Attack Target*: A stealthy attack corrupts the state estimation and, thereby, impacts the EMS control decision, which is the ultimate objective of an adversary. Therefore, an adversary may like to assess the consequences of different possible stealthy attacks and launch the severe one. In the context of OPF, an attacker's target can be expressed in terms of the generation cost increase.

We specify these adversary properties as attack attributes that allow a grid operator to flexibly design different adversarial scenarios and assess the system's security.

2.3 Contribution

While many researchers, such as [6], [11], [13], addressed stealthy attacks by considering some adversarial properties in isolation, we verified the attack feasibility and assessed the impact on the OPF solution by formally modeling these attributes simultaneously [7]. However, this formal approach suffers from limited scalability (Fig. 2), where the execution time is significantly high and it grows exponentially with system size. While the negation of the OPF constraint is computationally expensive, as applied in [7], the performance is greatly impacted as the model deals with real values. While there is usually a large number of stealthy attack vectors possible in a particular attack scenario (as defined through the adversary properties), each attack vector is often associated with an infinitesimal number of changes for the real-valued states. This large space makes the impact analysis intractable. A thorough impact analysis, *e.g.*, to find the maximum possible impact or the set of all attack vectors that can cause a specific impact on OPF, is not feasible at all under such inefficient time requirements.

In this work, we address the challenge of developing an efficient impact analysis framework for comprehensively

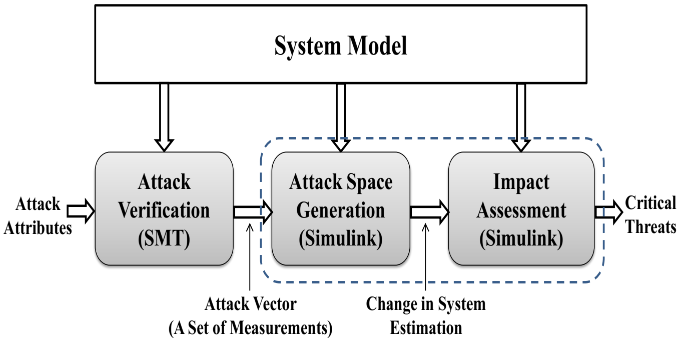

System Model
Attack Attributes
Attack Verification (SMT)
Attack Space Generation (Simulink)
Impact Assessment (Simulink)
Critical Threats
Attack Vector (A Set of Measurements)
Change in System Estimation

Fig. 3. The architectural design of the impact analytics framework.

assessing the system's security in terms of OPF, and thus reckoning the dependability of the system under attacks. To fulfill this need, we leverage the power of SMT for formal verification and that of Simulink for system modeling. SMT solvers can determine the satisfiability of formulas that contain thousands of variables and constraints [8]. Simulink is a powerful tool for simulating physical systems with complex mathematical properties [9]. It is being used successfully to model and evaluate the power system, especially with the help of SimPowerSystems [14], a component library for modeling/simulating power systems.

3 Impact Analysis Framework

In this section, we present the impact analysis framework.

3.1 Framework Architecture

The architecture of the impact analytics framework is presented in Fig. 3 and shows the process flow diagram that integrates formal (SMT) and Simulink models. The main idea is as follows: An SMT-based formalization is used to model the stealthy attacks based on the given attack attributes. This model is solved for generating all potential threat vectors that are fed into a Simulink model.

The Simulink model has two parts. For each threat vector, the first part generates the potential load changes at different buses. A threat vector specifies if (i) a measurement needs to be altered (or not), (ii) a state value will be affected (or not), and (iii) multiple states have the same change. According to these constraints, we use Simulink to model the relation between the states and measurements and generate possible load changes by exploring those affected states and altered measurements. These load changes are fed to the second part of the Simulink model, which is a Simulink block designed for OPF. This block runs the OPF process and verifies if the resultant generation cost is increased to the critical level. If the result is positive, this attack is specified as a critical threat. In this way, we identify the critical threats among all attack vectors for a given system and specified attack attributes, and analyze the depth (maximum possible increase in the generation cost) and breadth (the number of critical threats) of the threat space.

In the following, we first briefly present the formal modeling of the stealthy attack and the synthesis of all attack vectors. This model is driven from our previous work [7]. Then, we discuss the Simulink model design.

TABLE 1
Modeling Parameters

Notation	Type	Definition
b	Integer	The number of buses in the grid.
l	Integer	The number of lines in the grid topology.
f_i	Integer	The *from-bus* of line i.
e_i	Integer	The *to-bus* of line i.
d_i	Real	The admittance of line i.
g_i	Boolean	Whether the admittance of line i is known.
P_i^L	Real	The power flow through line i.
P_j^B	Real	The power consumption at bus j.
θ_j	Real	The state value, *i.e.*, the voltage phase angle, at bus j.
n	Integer	The number of states.
m	Integer	The number of potential measurements.
a_i	Boolean	Whether or not measurement i is required to be altered for the attack.
c_j	Boolean	Whether or not state j is affected due to false data injection.
u_j	Boolean	Whether or not any measurement residing at bus j is required to change.
t_i	Boolean	Whether or not measurement i is taken.
r_i	Boolean	Whether or not measurement i is accessible to the attacker.
s_i	Boolean	Whether or not measurement i is secured.

3.2 Formal Model for Stealthy Attack Verification

The formal model corresponding to the stealthy attack verification is presented in Table 2.

3.2.1 *Formal Modeling Parameters*

A number of parameters is used to denote different system properties and attack attributes. These parameters are summarized in Table 1. 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 and the direction of power flow is considered from f_i to e_i. In the DC power-flow model, two measurements can be taken (*i.e.*, recorded and reported by sensors/meters) for each line: the forward and backward current flows. These measurements are equal in magnitude but opposite in direction. A measurement can be taken to measure the power consumption at a bus. Therefore, for a power system with l number of lines and b number of buses, there are maximally $2l + b$ (*i.e.*, $m = 2l + b$) number of potential measurements ($1 \leq i \leq m$). We use t_i to denote whether measurement i is taken. 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). To denote the load power and generated power of bus j, P_j^D and P_j^G are used, respectively.

We use c_j to specify if state j ($1 \leq j \leq n$) is affected or corrupted due to a stealthy attack. In the DC power-flow model, each state corresponds to a bus: n is equal to b. We use a_i to denote whether measurement i ($1 \leq i \leq m$) is required to be altered for the attack. If a measurement at bus j is required to be changed, b_j becomes true, specifying whether the attacker needs to access bus j to compromise the measurement. An adversary's incomplete knowledge of the grid is modeled with respect to the line admittance. We use g_i to denote whether the attacker knows the admittance of line i. The attacker may not be able to alter a measurement due to inaccessibility or applied security. We use r_i to represent the accessibility of measurement i to the attacker and s_i to denote if the measurement is data integrity protected.

3.2.2 Physical Power Flow Properties

Power flow P_i^L depends on the difference of phase angles of the connected buses (f_i and e_i) and the admittance of line i (d_i). Equation 2 in Table 2 expresses this relation. The power consumption of bus j is simply the summation of the power flows of the lines connected to this bus. When $\mathbb{L}_{j,in}$ and $\mathbb{L}_{j,out}$ represent the sets of incoming lines and outgoing lines of bus j, respectively, then Equation 3 calculates the power consumption at bus j. The power consumption at a bus is the net power: the load at this bus minus the power injected to the bus (if one or more generators are connected to this bus). Equation 4 refers to this power component, where P_j^D and P_j^G denote the load power and the generated power at bus j, respectively. State estimation in the DC power-flow model involves finding the voltage phase angle (θ) of each bus by solving the linear equations for all the measurements (P_i^Ls and P_j^Bs) given the line admittances (d_is).

3.2.3 Stealthy Attack Properties

The attack on state j specifies that the voltage phase angle at bus j has changed (Equation 5). According to Equation 2, changes in the states must be reflected in the line power flow measurements. This is formalized in Equation 6. When $\Delta\theta_{f_i} \neq 0$ (or $\Delta\theta_{e_i} \neq 0$), then it is obvious that state f_i (or e_i) is changed (*i.e.*, attacked). The changes in power flow measurements are propagated to the power consumption measurements as shown in Equation 7.

To launch an attack, the attacker must inject required false data to a set of measurements corresponding to the power flows or consumptions that are impacted due to corrupting one or more states. 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 in Equation 8. Measurement i is altered only if it is taken and the corresponding power measurement is required to change (Equation 9).

3.2.4 Adversary Attribute Properties

If the admittance of a line is unknown, then the corresponding changes required in power flow measurements cannot be made. The constraint is formalized in Equation 10. An adversary's capability is considered in Equation 11. That is, if a measurement is data integrity protected (s_i), then though the attacker may be able to inject false data to the measurement, the false data injection will not be successful. Because of the resource limitation, an adversary can inject false data to no more than T_M number of measurements at a particular time. This constraint can be modeled based on the assumption that the adversary cannot inject false data to measurements distributed more than T_B number of buses at a time. Both forms of the resource constraint are formalized as in Equation 12 and Equation 14, respectively.

3.2.5 Generation of All Attack Vectors

When an attack vector (including c_js and a_is) is found by solving this formal model, a new constraint is added to the model so that the vector is removed from the search space. The idea is to assert the negation ($\neg$) of the attack vector, which is a conjunction ($\wedge$) of c_js and a_is, specifying the states that are affected and the measurements that are altered, respectively. This constraint is formalized as follows:

$$\neg(\bigwedge_j c_j \;\wedge\; \bigwedge_i a_i) \tag{15}$$

TABLE 2
Formalization of Attack Vector Verification

#1: Physical Power Flow Properties:

Power Flows and Topology:

$$\forall_{1\leq i\leq l}\;\; P_i^L = d_i(\theta_{f_i} - \theta_{e_i}) \tag{2}$$

Power Consumptions:

$$\forall_{1\leq j\leq b}\;\; P_j^B = \sum_{i\in\mathbb{L}_{j,in}} P_i^L - \sum_{i\in\mathbb{L}_{j,out}} P_i^L \tag{3}$$

$$\forall_{1\leq j\leq b}\;\; P_j^B = P_j^D - P_j^G \tag{4}$$

#2: Cyber-Physical Attack Properties:

Changes in States:

$$\forall_{1\leq j\leq n}\;\; c_j \rightarrow (\Delta\theta_j \neq 0) \tag{5}$$

Attack Evasion Properties:

$$\forall_{1\leq i\leq l}\;\; \Delta\bar{P}_i^L = d_i(\Delta\theta_{f_i} - \Delta\theta_{e_i}) \tag{6}$$

$$\forall_{1\leq j\leq b}\;\; \Delta P_j^B = \sum_{i\in\mathbb{L}_{j,in}} \Delta P_i^L - \sum_{i\in\mathbb{L}_{j,out}} \Delta P_i^L \tag{7}$$

Attack Plan Properties:

$$\begin{array}{ll} \forall_{1\leq i\leq l} & (\Delta P_i^L \neq 0) \rightarrow (t_i \rightarrow a_i) \wedge (t_{l+i} \rightarrow a_{l+i}) \\ \forall_{1\leq j\leq b} & (\Delta P_j^B \neq 0) \rightarrow (t_{2l+j} \rightarrow a_{2l+j}) \end{array} \tag{8}$$

$$\begin{array}{ll} \forall_{1\leq i\leq l} & a_i \rightarrow t_i \wedge (\Delta P_i^L \neq 0) \\ \forall_{1\leq i\leq l} & a_{l+i} \rightarrow t_{l+i} \wedge (\Delta P_i^L \neq 0) \\ \forall_{1\leq j\leq b} & a_{2l+j} \rightarrow t_{2l+j} \wedge (\Delta P_j^B \neq 0) \end{array} \tag{9}$$

#3: Adversary Attribute Properties:

Attacker's Knowledge:

$$\forall_{1\leq i\leq l}\;\; (\Delta P_i^L \neq 0) \rightarrow ((t_i \vee t_{l+i}) \rightarrow g_i) \tag{10}$$

Attacker's Access Capability:

$$\forall_{1\leq i\leq m}\;\; a_i \rightarrow r_i \wedge \neg s_i \tag{11}$$

Attacker's Resource:

$$\sum_{1\leq i\leq m} a_i \;\leq T_M \tag{12}$$

$$\begin{array}{ll} \forall_{1\leq i\leq l} & (a_i \rightarrow h_{f_i}) \wedge (a_{l+i} \rightarrow h_{e_i}) \\ \forall_{1\leq j\leq b} & a_{2l+j} \rightarrow h_j \end{array} \tag{13}$$

$$\sum_{1\leq j\leq b} h_j \;\leq T_B \tag{14}$$

3.3 Simulink Model for Impact Analysis

In this subsection, we present the Simulink model that explore the stealthy attack space and perform verification for the desired impact.

3.3.1 Identification of Load Changes

The change in the loads at the buses due to an stealthy attack is realized from Equation 4. The power produced by a generator is fairly well-defined and it is changed only if it is driven by the OPF results when it is executed. Typically, the OPF process is executed after the state estimation to determine necessary changes in the generation dispatch. Therefore, the following is assumed in this model:

$$\forall_{1\leq j\leq b}\ \Delta P_j^G = 0 \tag{16}$$

Therefore, the change performed in the power consumption measurement specifies the change in the load at the corresponding bus. Since this change is made by following the stealthy attack properties, the state estimation process complies. According to Equation (16), the change in the load at bus j is formalized as:

$$\forall_{1\leq j\leq b}\ \Delta P_j^B = \Delta P_j^D \tag{17}$$

If $\hat{P}_j^D$ denotes the estimated load (according to the state estimation result) at bus j, Equation 18 specifies this estimation:

$$\forall_{1\leq j\leq b}\ \hat{P}_j^D = P_j^D + \Delta P_j^D \tag{18}$$

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

$$\forall_{1\leq j\leq b}\ \hat{P}_{j,min}^D \leq \hat{P}_j^D \leq \hat{P}_{j,max}^D \tag{19}$$

Using Simulink modeling, we calculate all valid changes of the loads corresponding to the attack vector (including ΔP_i^Ls and ΔP_j^Bs) fed from the SMT-model. The steps are briefly discussed below:

Valuation of $\Delta\theta$s: We classified the states (θs) into two sets: ($\mathcal{A}$) states that are affected (true c_js) by the stealthy attacks and ($\mathcal{B}$) states that remains unchanged. Set $\mathcal{A}$ is further classified into subsets $\mathcal{A}_k \leq |\mathcal{A}|$ based on the following constraints:

$$\forall_{1\leq i\leq l}\ (\Delta P_i^L = 0) \wedge (\neq c_{f_i}) \wedge (\neq c_{e_i})\ \rightarrow (\theta_{f_i} = \theta_{e_i})$$

Each subgroup $\mathcal{A}_k$ consists of the states that are the same. We associate a value generator ($\Delta\Theta_k$) for each subset. Then, the following is true: $\forall_{\theta_j\in\mathcal{A}_k}\Delta\theta_j = \Delta\Theta_k$. However, there is an exception that depends on whether $\Delta P_j^B = 0$. According to Equation 7, $\Delta P_j^B = 0$ holds if either of the following two conditions is true:

$$\text{(i) } \forall_{(i\in\mathbb{L}_{j,in})\vee(i\in\mathbb{L}_{j,out})}\ \Delta P_i^L = 0, \text{Or}$$
$$\text{(ii) } \sum_{i\in\mathbb{L}_{j,in}} \Delta P_i^L - \sum_{i\in\mathbb{L}_{j,out}} P_i^L = 0$$

If condition (i) is not true, we calculate one of the $\Delta\theta$s (associated with the lines) from the rest of the $\Delta\theta$s, following Equations 6 and 7, such that $\Delta P_j^B = 0$. If $\mathcal{S}_i$ is the set of $\Delta\theta$s corresponding to P_i^Ls $((i \in \mathbb{L}_{j,in}) \vee (i \in \mathbb{L}_{j,out}))$, one of them, let $\Delta\theta_j \in \mathcal{S}_i$, is computed as $\Delta\theta_j = f(\Delta\theta_{-j} \in \mathcal{S}_i)$.

Valuation of ΔP_j^Bs: We calculate each ΔP_i^Ls from $\Delta\theta_{f_i}$ and $\Delta\theta_{e_i}$ (Equation 6). Then, each ΔP_j^B is calculated summing the ΔP_i^Ls corresponding to this bus. $\Delta\theta$s are controlled in such a way, as shown above, that only those line power flows and bus power consumptions receive nonzero values that are indicated as $\Delta P_i^L \neq 0$ and $\Delta P_j^B \neq 0$ in the attack vector.

3.3.2 Optimal Power Flow and Impact Assessment

The OPF block in the Simulink model implements the OPF routine (refer to Section 2.1.3). The objective of OPF is to control optimally the generation according to the load requirement. The OPF process is briefly explained below.

Operating Constraints: If P_j^G is the power produced by the generator connected to bus j (assuming a single generator at each bus), the total generation must match the total load:

$$\sum_{1\leq j\leq b} P_j^G = \sum_{1\leq j\leq b} P_j^D \tag{20}$$

Each generator has a production capacity ($P_{j,max}^G$). Thus:

$$\forall_{1\leq j\leq b}\ P_j^G \leq \hat{P}_{j,max}^G \tag{21}$$

The power balance equations (*i.e.*, Equations 2, 3, and 4) must hold. Each line has a power transmission capacity. If $P_{i,max}^L$ is the maximum line capacity, then:

$$OPF_4:\ \forall_{1\leq i\leq l}\ \hat{P}_i^L \leq P_{i,max}^L \tag{22}$$

Cost Minimization: If $\mathcal{C}_j(.)$ denotes the cost function for the generator connected at bus j, the total generated $\mathcal{C}_j(.)$ is a strictly increasing convex function. OPF minimizes the following function subject to satisfying the operating constraints mentioned above:

$$min \sum_{1\leq j\leq b} \mathcal{C}_j(P_j^G)$$

Impact-Assessment: Let C be the actual generation cost, *i.e.*, the minimum cost in the normal (no attack) scenario. If $\hat{C}$ is the minimum generation cost in the attacked scenario and the criticality threshold is T% increase in the cost, then a critical threat satisfies the following:

$$(\hat{C} - C) * 100/C \geq T \tag{23}$$

3.4 Implementation

The implementation of the proposed framework, *i.e.*, the formal model and the Simulink model, is discussed briefly in this section. We also present an example Simulink model.

3.4.1 Implementation of Formal Model

The formal model for attack vector generation is encoded into SMT logics using the Microsoft Z3 .NET framework [15]. The bus system's configurations, attack attributes, and associated constraints are provided in a text file (*input* file). The execution of the Z3 program gives the verification result as either satisfiable (*sat*) or unsatisfiable (*unsat*). The *unsat* result means that the problem has no attack vector that satisfies the constraints. In the case of *sat*, the result includes the attack vector, which is the values assigned to the variables (*e.g.*, c_js, a_is, etc.). This attack vector specifies the affected states, the changes to be done on line power flows and bus power consumptions, and the corresponding measurements that are required to be altered. The results are also printed in a text file (*output* file). This output file is fed to the Simulink model as an input file to explore the threat space and assess the impact.

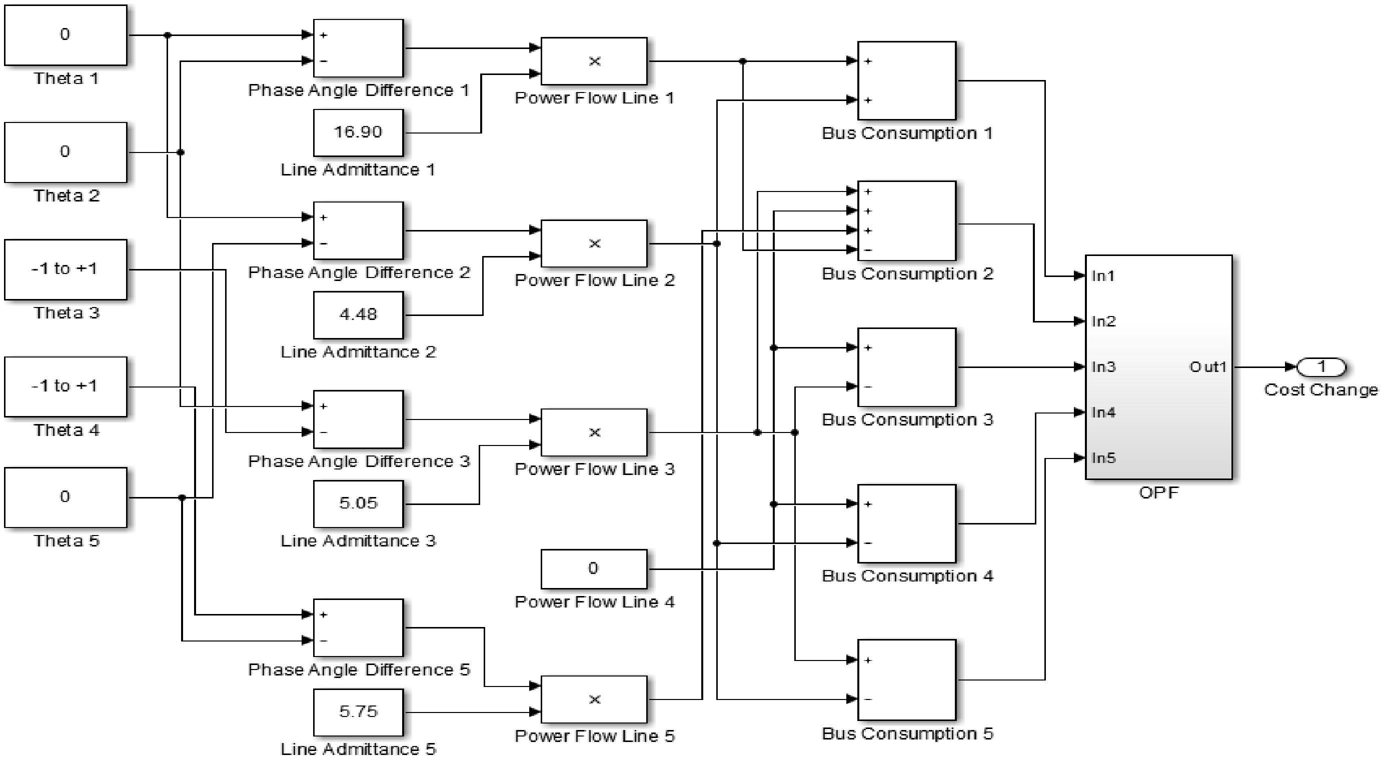


Fig. 4. The diagram of a part of the Simulink model (5 buses) corresponding to the 14-bus system case study in Section 4.

3.4.2 Implementation of Simulink Model

We develop a MATLAB program to automatically produce the Simulink model from the attack vector generated by the formal attack verification model. This program uses the same input file as the former model for necessary information about the bus system, which is required to design the Simulink model. It also takes some extra inputs, such as generation capacities, line capacities, and original loads at the buses. This program is developed in a way that it can automatically design the proper Simulink model without any manual intervention, solely based on the input files. We add constraints and restrictions based on the attack vector as mentioned in Section 3.3. Once the model is created, it is executed for a certain amount of time and the results are gathered in the MATLAB workspace. This sample time is chosen based on the number of independent sources for $\Delta\theta$s and the possible number of values for each source, such that all combinations are considered. We also leverage the MATLAB "parfor" module to run multiple instances of the Simulink model simultaneously [16].

3.4.3 Efficient Execution of the Framework

We execute the attack verification model and the Simulink model parallelly to increase the efficiency of the proposed framework. We run them parallelly using two MPI processes. While the attack verification model executing process (Process 1) identifies attack vectors, the Simulink model executing process (Process 2) explores them to verify the impact. In our proposed framework, the Simulink model mainly impacts the execution time of the framework because this model explores the complete attack space (with respect to affected states) for each attack vector identified by the attack verification model. The time for producing an attack vector by the attack verification model is much smaller than that for exploring the attack space by the Simulink model. Therefore, we devise a systematic mechanism, Algorithm 1, to run multiple instances of the Simulink model simultaneously, while a parallel process is executing the verification model. This significantly reduces the ultimate execution time. The number of simultaneous executions depends on the hardware capacity, particularly the number of processing cores of the host machine. For the execution of the Simulink model, a fixed number of cores is selected. These cores can be physical or logical (with the help of hyperthreading). Each core runs a worker process.

Algorithm 1 presents how Process 2 schedules the execution of the Simulink model on the workers. Each attack vector identified by Process 1 is notified to Process 2, which the stored in a queue. Each attack vector is subsequently explored by Process 2 through one of the idle workers (Lines 7 and 8). If all of the workers are busy in exploring attack vectors, the scheduling algorithm waits for a random but small time period (Lines 5). Once an idle worker is available, an instance of the Simulink model is launched on the idle worker for the attack vector residing at the top of the queue. This process continues until all the attack vectors are generated by the verification model and explored by the Simulink model (Line 12).

3.4.4 An Example Simulink Model

Fig. 4 presents an example of a Simulink model for a 5-bus system. The diagram is a part of the Simulink model corresponding to the IEEE 14-bus system [10], considered in the case study presented in Section 4. This Simulink model corresponds to an attack vector generated by the attack verification model. For each generated attack vector,

Algorithm 1 Execute the Simulink Model (Process 2)

```
Require: $\mathbb{C}$: The set of cores/workers   ▷ Each worker executes an instance of the Simulink model.
Require: $\mathbb{A}$: The queue of attack vectors   ▷ Each attack vector identified (and notified) by Process 1 is inserted into $\mathbb{A}$.
Require: $Done$: If Process 1 is done with generating attack vectors   ▷ It is initialized to FALSE and will set to TRUE if Process 1 notifies.
while TRUE do
    while $\mathbb{Q}$ is not empty do
        $A_i$ := Dequeue($\mathbb{A}$)
        while No $C_i \in \mathbb{C}$ is idle do
            Wait for an arbitrary small period
        end while
        Select an idle worker $C_i \in \mathbb{C}$
        Execute the Simulink model on $C_i$ for $A_i$
    end while
    if $Done$ then
        if $\mathbb{Q}$ is empty then   ▷ One or more attack vectors may be identified in the mean time.
            return
        end if
    else
        Wait for an arbitrary small period
    end if
end while
```

one Simulink model is formed. As shown in Fig. 4, the phase angles of buses 1, 2, and 5 are 0, while that of buses 3 and 4 are not zero, as they are specified in the attack vector. Each non-zero phase angle is taken from a range of values generated using a custom Simulink block, which can generate real values from -1 to +1 ranges, assuming the maximum change in the measurements cannot be more than 1 unit in magnitude and the significance of digits after the decimal point is 2. Using Equation 2 in Table 2, the phase angle difference is calculated by subtracting one phase angle value from another. This subtracted result is multiplied by the admittance of the corresponding line, which ultimately represents the change in the power flow measurement.

The admittance values for lines 1, 2, 3, and 5 are 16.90, 4.48, 5.05, and 5.75, respectively. The power flow change for line 4 is 0, as specified in the attack vector. Next, bus power consumption changes are calculated according to Equation 3. Finally, the bus power consumption changes are fed into a Simulink custom block that implements the OPF process. This implementation is a customized version of the MATPOWER DC OPF function [17]. The custom block also takes bus load measurements and power generation properties as input and runs the OPF routine to calculate the change in the OPF solution, *i.e.*, the change in the optimal generation cost. For an attack vector, the Simulink model runs for all possible values of each phase angle. When the cost change is equal or greater than the criticality threshold, the corresponding attack vector (and the measurement changes) is critical. In this way, all critical threats are identified by exploring the attack space.

4 Case Studies

We create two synthetic cases based on the standard IEEE 14-bus and 30-bus test systems [10]. We perform experiments on them to analyze the impact of different attack attributes on the criticality of threats.

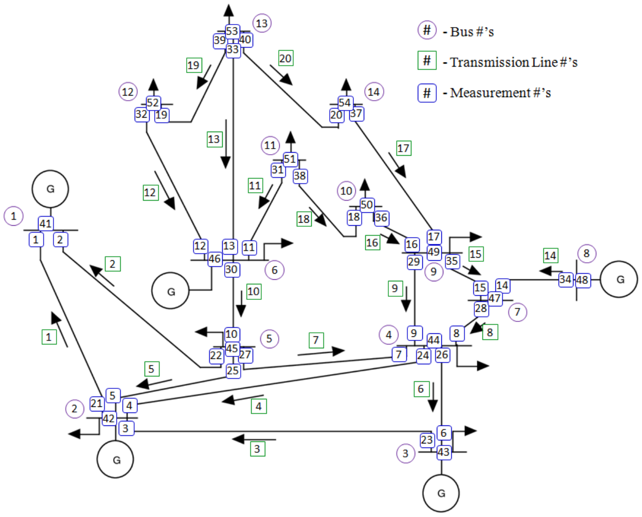


Fig. 5. The IEEE 14-bus test system: bus numbers are in circles and line numbers are in squares.

4.1 Case Study Overview

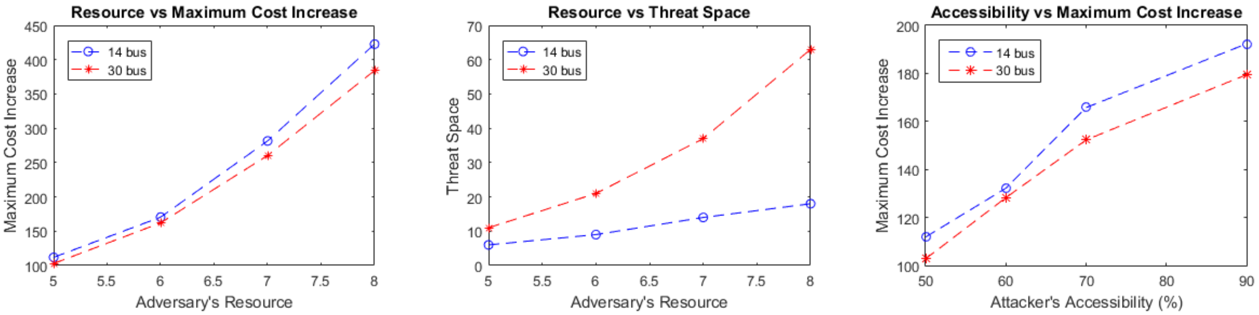
4.1.1 14-bus Case System

The topology of the 14-bus test system is shown in Fig. 5. In this bus system, there are total 14 buses and 20 lines. The input corresponding to the line information includes a set of data for each line: line number, end buses of the line, a value indicating the line admittance, the knowledge status (*i.e.*, whether the line admittance is known to the attacker), and the transmission capacity of the lines. In this case, the admittances of lines 3, 7, and 17 are unknown. Line 1 has the highest power flow capacity of 50 MW and line 9 has the least power flow capacity of 5 MW. Since each of the lines can have two measurements (one for the forward current and another one is for the backward current), it is possible to take 54 measurements at most in this IEEE 14 bus system. According to the input about the measurements in this case study, (i) all the potential measurements are taken except measurements 13, 19, 25, 31, 37, and 46 and (ii) measurements 1, 2, 11, 12, 13, 19, 21, 31, and 46 are secured (data integrity protected). The adversary often does not have access to all measurements. We consider accessibility between 50% and 90% of the measurements.

In this case study, the bus has five generators with a simple multiple segment linear cost function (in \$): $\mathcal{C}_j(P_j^G) = \alpha + \beta P_j^G$ [1]. The power generation cost coefficients corresponding to the generators at buses 1, 2, 3, 6, and 8 are (20, 30), (0, 50), (50, 40), (0, 40), and (40, 30), respectively. The loads at the buses are 0, 21.7 MW, 94.2 MW, 47.8 MW, 7.6 MW, 11.2 MW, 0, 0, 29.5 MW, 9 MW, 3.5 MW, 6.1 MW, 13.5 MW, and 14.9 MW, respectively. The OPF power generation cost in the normal state (without any attack) is \$9,342.11. The goal of the adversary is considered as increasing the cost at least 5% of the original cost.

4.1.2 30-bus Case System

In this bus system, there are total 30 buses and 41 lines. In this case study, we also consider a similar set of inputs like the 14-bus case system. The admittances of lines 5, 11, 13, 15, 21, and 23 are unknown. Line 1 has the highest power flow capacity of 76 MW and line 14 has the least power



(a) (b) (c)

Fig. 6. Threat analysis results based on the adversary's capability and constraint: (a) the maximum generation cost increase w.r.t. the resource, (b) the threat space w.r.t. the resource, and (c) the maximum generation cost increase w.r.t. the accessibility.

flow capacity of 5 MW. All the potential measurements (112 in total) are taken except measurements 4, 7, 10, 15, 19, 24, 28, 33, 35, 40, 43, 46, 51, 55, 62, 66, 69, 74, 76, 81, 87, 91, 94, 99, 104, 108, and 111. Measurements 1, 2, 4, 6, 10, 12, 13, 15, 18, 20, 27, 44, 45, 52, 54, 57, and 66 are secured. The accessibility is considered from 50% to 90% of the measurements. The power generation cost coefficients corresponding to the generators at buses 1, 2, 13, 22, 23, and 27 are (40, 0), (50, 20), (30, 20), (0, 40), (30, 40), and (40, 30), respectively. The loads at the buses are 0, 21.7 MW, 2.4 MW, 7.6 MW, 0, 0, 22.8 MW, 30 MW, 0, 5.8 MW, 0, 11.2 MW, 0, 6.2 MW, 8.2 MW, 3.5 MW, 9 MW, 3.2 MW, 9.5 MW, 2.2 MW, 17.5 MW, 0, 3.2 MW, 8.7 MW, 0, 3.5 MW, 0, 0, 2.4 MW, and 10.6 MW, respectively. The OPF power generation cost in the normal state (without any attack) is $8,402.48. The goal of the adversary is to increase the cost by at least 5% of the original cost. In the following subsection, we discuss the analysis results (as shown in Fig. 7) corresponding to these case studies. It is worth mentioning that there is no necessary connection between the analysis results corresponding to these two cases.

4.2 Impact Analysis Results

The attack vector includes a set of measurements (and the corresponding buses/substations) that needs to be altered (to some controlled sets of values) to manipulate a set of states. The attackers objective is to maximize the damage caused to the grid within the adversary properties, *i.e.*, resource, knowledge, and accessibility. Larger accessibility, higher knowledge, and/or more resources impose severer damage. Our evaluation results below justify the same.

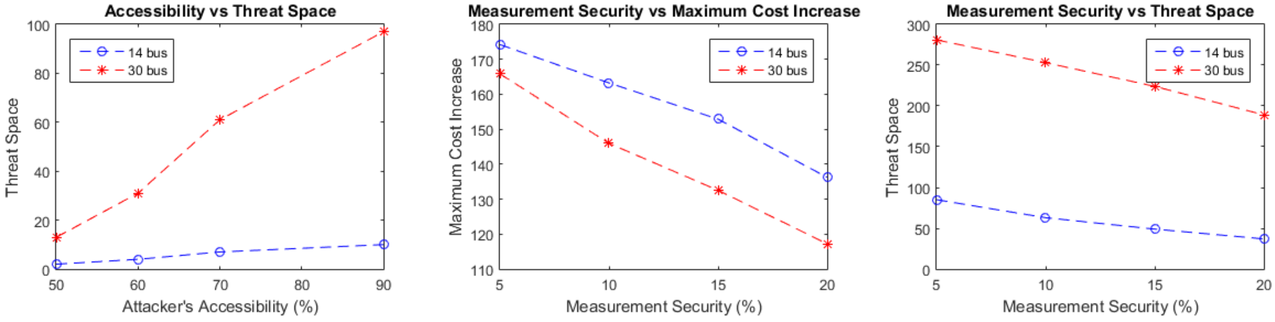
4.2.1 Adversary's Resource and the criticality of threats

An adversary's resource specifies its capability of simultaneously attacking multiple measurements distributed on different buses to launch an attack. As shown in Fig. 6(a), we observe that if the adversary's resource increases, the maximum increase in the generation cost also increases. In the 14-bus case, when the resource allows the adversary to compromise 5 buses at a time, the maximum cost increase is seen as $111.86. When the attacker's resource increases to 6, 7, and 8 buses, the maximum cost increase is also increased to $170.47, $281.56, and $422.68, respectively. Similarly, in the 30-bus case, when the resource allows the adversary to compromise 5 buses at a time, the maximum cost increase is seen as $102.79. When the attacker's resource increases to 6, 7, and 8 buses, the maximum cost also increases to $162.05, $260.33, and $384.25, respectively. The figure also shows that the OPF cost increases almost linearly as the adversary's resource increases. The increase in the generation cost depends on the bus system, specifically generation costs of different generators, loads at the buses, and capacities of the transmission lines. Moreover, an stealthy attack does not increase the total load but only redistributes the loads at different buses. Therefore, creating a significant increase in the generation cost is nontrivial.

The relationship between the adversary's resource and the threat space is presented in Fig. 6(b). Threat space is defined as the number of attack vectors that can increase the cost by at least 5%. These attack vectors are critical with respect to the criticality threshold (*i.e.*, 5% increase). In the 14-bus case, when the resource allows the adversary to simultaneously compromise 5 buses, the number of attack vectors is 6. When the adversary's resource increases to 6, 7, and 8 buses, the number of attack vectors also increases to 9, 14, and 18, respectively. In the 30-bus case, when the resource allows the adversary to simultaneously compromise 5, 6, 7, and 8 buses, the number of attack vectors is 11, 21, 37, and 63, respectively. It is worth mentioning that there are many attack vectors that increase the generation cost, although only a few of them can increase the cost to equal or above the critical level.

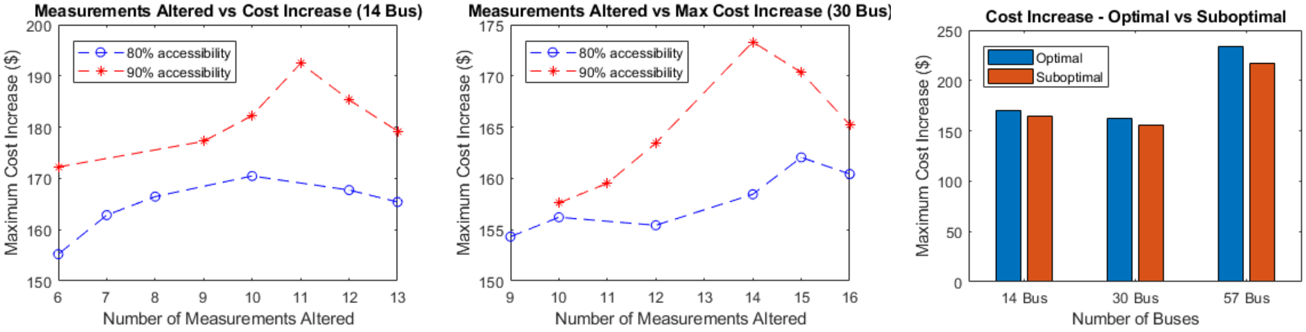
4.2.2 Adversary's Accessibility and Criticality of Threats

Fig. 6(c) shows the relationship between the adversary's access capability and the maximum increase in the generation cost. This figure presents analysis results for both the 14-bus and 30-bus cases. In the 14-bus case, we observe that when the attackers accessibility is 50% (the adversary has access to arbitrarily 50% of the total measurements), the maximum cost increase is $111.86. When the accessibility increases to 60%, 70%, and 90%, the corresponding maximum generation cost also increases to $132.17, $165.78, and $192.34, respectively. In the 30-bus case, when the attackers accessibility is 50%, 60%, 70%, and 90%, the corresponding maximum generation cost increase is $102.79, $128.24, $152.30, and $179.48, respectively. Fig. 7(a) shows the relationship between the adversary's accessibility and the threat space. In the 14-bus case, we observe that when the attacker's accessibility is 50%, we get only 2 attack vectors that increase the OPF cost by at least 5%. When the accessibility increases to 60%, 70%, and 90%, the corresponding threat space also increases to 4, 7, and 10 attack vectors, respectively. We also



(a) (b) (c)

Fig. 7. Threat analysis results based on the adversary's capability and constraint: (a) the threat space w.r.t. the accessibility, (b) the maximum generation cost increase w.r.t. measurement security, and (c) the threat space w.r.t. the measurement security.



(a) (b) (c)

Fig. 8. (a - b) The impact of the attack vector's size on the maximum increase in the generation cost: (a) 14-bus system and (b) 30-bus system, and (c) the subopttimal results versus optimal results.

observe a similar threat space increase in the 30-bus case. When the attacker's accessibility is 50%, 60%, 70%, and 90%, the corresponding number of critical attack vectors is 13, 31, 61, and 97 attack vectors, respectively.

4.2.3 Measurement Security and Criticality of Threats

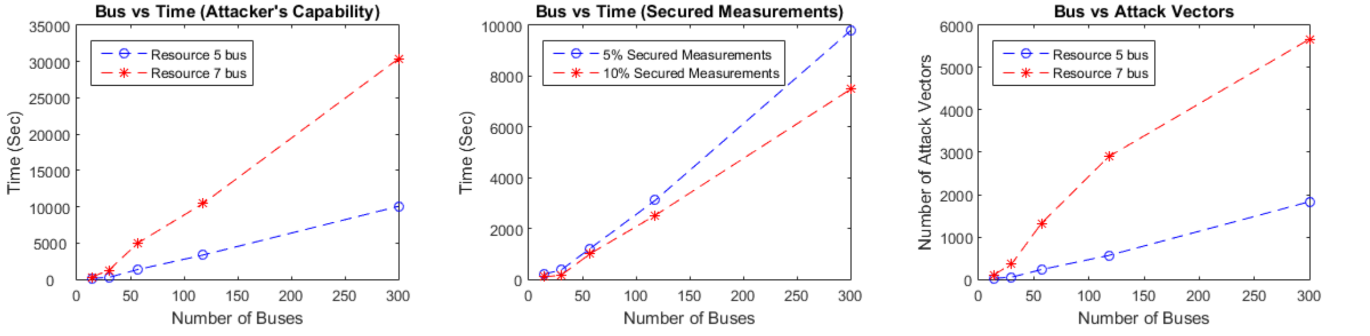
We analyzed the relationship between the number of secured measurements and the maximum increase in the generation cost. Fig. 7(b) presents the corresponding analysis results for both of the 14-bus and 30-bus systems. In the 14-bus case, when the number of secured measurements is 5% (*i.e.*, arbitrarily 5% of the total measurements), the maximum cost increase is found as $174.23. When the measurement security increases to 10%, 15%, and 20%, the corresponding maximum generation cost decreases to $163.25, $152.88, and $136.23, respectively. In the 30-bus system, when the number of secured measurements is 5%, 10%, 15%, and 20%, the corresponding maximum generation cost is $165.85, $145.96, $132.53, and $117.23, respectively.

Fig. 7(c) shows the threat space varying the measurement security. We observe that when 5% of the total number of measurements is secured in the 14-bus system, there are 85 attack vectors that can increase the OPF cost by at least 5%. When the percentage of secured measurement is 10%, 15%, and 20%, the corresponding threat space also decreases to 63, 49, and 37 attack vectors, respectively. In the 30-bus case, we observe 281, 253, 224, and 189 critical attack vectors when the percentage of secured measurement is 5%, 10%, 15%, and 20%, respectively. When a measurement is secured, *i.e.*, data integrity protected, an adversary cannot alter the measurement (without being detected). As a result, this measurement cannot be used for launching a stealthy attack. Therefore, a larger number of secured measurements creates a further restricted attack capability. The potential stealthy attack space thus decreases, which in turn decreases the number of critical attack vectors. The maximum increase in the generation cost often decreases, as shown in Fig. 7(b), from a decreased number of critical attacks.

4.3 Attack Vector Properties and Suboptimality

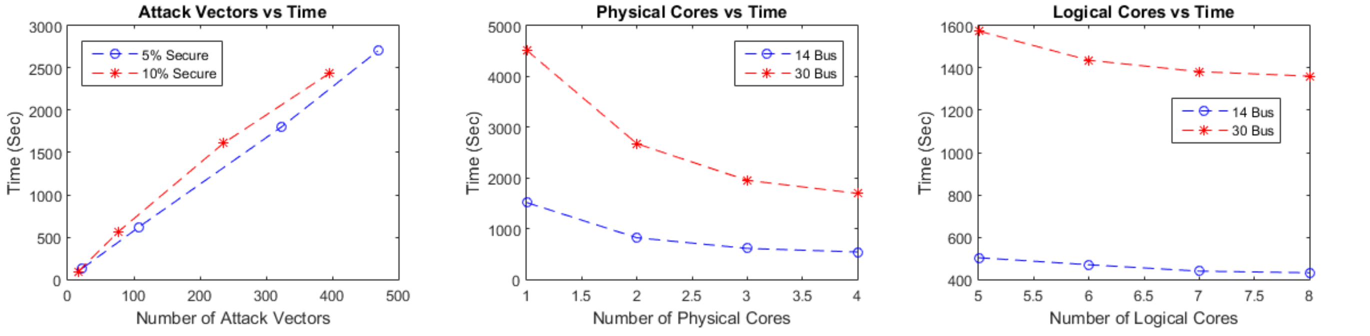
We evaluate if the property of an attack vector has an impact on the optimality of the solution. The crucial property of an attack vector is its size, which is the number of measurements to be altered (or buses/substations to be attacked) simultaneously to launch a stealthy attack. We evaluate that if the larger sized attack vectors have chances to create higher damage. According to the simulation results (Fig. 8(a) and Fig. 8(b)) we find that the impact is often positive to some extent. That is, for a larger number of altered measurements, the maximum increase in the generation cost is often higher. However, the pattern is not always increasing. Usually, after some points the increase in the generation cost starts to fall. Hence, the largest attack vector size cannot but provide a suboptimal increase. Fig. 8(c) presents the suboptimal values and the corresponding optimal values in 14-bus, 30-bus, and 57-bus systems, where the top 10% large sized attack vectors are explored to find the suboptimal increases. In these simulated experiments, it is assumed that 70% of the measurements are secured and the attacker's resource limits the simultaneous access to 6, 12, and 18 buses for 14-bus, 30-bus, and 57-bus systems.

We also observe a similar behavior when we evaluate if the number of states to be manipulated by an attack vector influences the optimal behavior.



(a) (b) (c)

Fig. 9. (a-b) The execution time w.r.t. the problem size considering (a) two different resource limits and (b) two different sizes of secured measurements, and (c) the number of attack vectors w.r.t. the problem size considering attacker's resource.



(a) (b) (c)

Fig. 10. The execution time w.r.t. (a) the number of attack vectors, (b) the physical cores of the computing system, and (c) the logical cores of the computing system.

5 Scalability Evaluation

In this section, we present the evaluation results corresponding to the scalability of the proposed framework.

5.1 Methodology

We evaluate the scalability of our proposed framework by analyzing the time requirements for executing the framework in different problem sizes and the adversary properties. Problem size depends primarily on the number of buses. We evaluated the scalability of our model based on different sizes of IEEE test systems, *i.e.*, 14-bus, 30-bus, 57-bus, 118-bus, and 300-bus [10]. The adversary properties represent the attack capabilities (*i.e.*, resource, accessibility, etc.), as discussed in Section 2.2. Measurements are arbitrarily selected to specify properties like access capability and measurement security. The generation and load structures are also arbitrarily chosen. We run our experiments on an Intel Core i7 Processor with 16 GB memory.

5.2 Evaluation Results and Discussion

5.2.1 Impact of Problem Size on Execution Time

Fig. 9(a) and Fig. 9(b) show the execution time of our proposed framework with respect to different problem sizes. The impact analysis is executed on different IEEE test systems, up to the number of 300 buses. We perform our experiments through different random scenarios, especially in terms of the attacker's resource limitation and the number of secured measurements. We observe that with respect to the bus size the increase in the execution time is linear. In our framework, we have two major models: the SMT-based attack vector verification/generation model and the Simulink model for attack space exploration and impact assessment. As the number of buses increases, the size of these two models increases, and thus the execution time increases. As the figure shows, the proposed framework performs significantly better compared to [7], even the latter work only when looking for a single critical threat. The reason behind this twofold. First, as we discussed in Section 3.4.3, we conduct a parallel execution of these two models, as well as multiple instances of the Simulink model. The impact of parallelism will be further analyzed later in this section. Second, more importantly, the Simulink model identifies only the valid and distinct attacks/load changes, instead of infinitesimally many indistinguishable cases, to verify the desired impact (refer to Section 3.3.1). In fact, the execution time depends on the number of attack vectors to be explored by Simulink model. Fig. 9(c) presents the number of possible attack vectors with respect to the problem size. The number of attack vector increases with the increase in the bus size. For the same bus size, when the adversary has more resources, a larger number of attack vectors is produced by the attack vector verification model. Fig. 10(a) shows the impact of the number of attack vectors on the execution of the proposed impact analysis framework for the 118-bus system. Since the Simulink model explores each attack vector, when the number of attack vector increases, the execution time of the framework increases.

We observe in Fig. 9(a) and Fig. 9(b) that for a specific bus size, the execution time differs in different scenarios. In the case of the scenario with a larger resource capability (7 bus), the execution time is larger than that of the smaller capability (5 bus) and the execution time increases rapidly in the former case. This is because the number of attack vectors increases when the capability increases. Similarly, when 5% of the measurements is secured, our framework takes a longer time to execute compared to that of the 10% case. The fewer measurements secured, the more number of attack vectors there are to explore for impact assessment.

5.2.2 Impact of Parallelism on Execution Time

Fig. 10(b) and Fig. 10(c) show the impact of the number of cores available in the computing machine on the proposed framework's execution time. The results show that the execution time decreases with increasing numbers of cores. As shown in Fig. 10(b), the execution time decreases rapidly as the number of physical cores increases. At a specific number of cores, the impact of a larger number of cores on the execution time is more visible when the problem size increases. With the increase in the number of physical cores, our framework can run multiple simultaneous executions of the Simulink model and the number of simultaneous executions is directly proportional to the number of cores.

Logical cores are virtually implemented (using hyperthreading) and one physical core can have two logical cores [18]. Although increasing the number of logical cores to execute the Simulink model improves the time efficiency of the framework, this improvement is not as significant as the improvement achieved by increasing that of the physical cores. Fig. 10(c) demonstrates this behavior.

6 Discussion

Here we discuss few points that need further elaboration.

6.1 Frameowrk Execution Time

It can be argued that the atacker's resource limit may be much larger than 7 buses, which will increase the execution time impractically high. Here, the resuource limit specifies the number of buses that can simultaneously be compromised on a single attack attempt. An attacker can attack a bus only if it is accessible and its measurements are not secured. The grid buses are typically established in physically secured locations. Usually, it is non-trivial to gain remote access to these buses. Therefore, it is practical to assume that an attacker has access to a small number of buses, while the capability of simultaneously accessing these buses is limited. That is why, we consider arbitrary small numbers of buses as the simultaneous attack resource.

On the other hand, the execution time of our framework can easily be improved by increasing the computing power of the executing machine. As our evaluation results demonstrate, the execution time of the Simulink module depends on the number of cores of the host machine. We have used a general-purpose computer with 4 cores where each core has a processing speed of 1.8 GHz. If we can increase the number of cores and/or the computing capability (processing power, cache memory, etc.) of each core, the execution time can be reduced drastically.

6.2 Measurement Security

While one can argue for securing all the measurements in a power grid, there are costs associated with securing the measurements. Although power grids are increasing using modern technologies, many legacy devices still exist due to various technical complexities and economic constraints. Moreover, the SCADA devices are built by different vendors where vendor-specific technologies are being used. A SCADA network often consists of devices from multiple vendors. Therefore, to make a measurement secured, the grid component must have the capability to implement necessary security mechanisms, while the implementation needs to be compatible with all associated equipment. To make the measurement transmission secured, which is the data integrity protection in this case, data encryption or hash-based data validation must be ensured.

6.3 Attacker's Limited Knowledge and Accessbility

To launch stealthy false data injection attack on the system, an adversary requires knowledge of the system topology, electrical properties of the transmission lines (i.e., the impedance), and measurement configurations. In order to remain stealthy, the attacker must ensure $\mathbf{a} = \mathbf{H}\mathbf{c}$. To build the Jacobian matrix $\mathbf{H}$, one needs the complete information (the bus connectivity and the line admittances) of the grid [6], which is not trivial. As discussed in [13], this knowledge can be gained through offline and/or online data collections. Offline data collection can take weeks, months, or even years to get access to the grid topology maps, which can be done through intruders or former utility company employees. Moreover, collected data may not be enough to implement an attack. Some offline data can also be outdated due to new construction or expansion of the transmission lines. The locations of circuit breaker switches, transformer tap changers, etc. also significantly affect the connectivity and admittance matrices. An adversary can deploy some sensors to do online data collection. However, due to restricted physical access to the grid (substations) and limited resources, online data collection may not be feasible. Therefore, in most practical cases, an adversary cannot but launch stealthy attacks with incomplete information and limited access to the substations.

An adversary's accessibility is his ability to access state estimation measurements in the substation level. On one hand, the grid buses are typically established in physically secured locations. On another hand, it is non-trivial to gain remote access to these buses, specifically due to proprietary network or industrial communication protocol. Some measurements may also have data integrity protection. Based on this, in this work, we assume that an adversary cannot access all the measurements of the system.

6.4 Proposed Defense Mechanisms against Stealthy Attacks and Our Framework

In the literature, we can identify many FDI attack defense mechanisms. Bobba et al [19] proposed solutions for protecting the state estimation against stealthy attacks by securing a set of strategically selected basic measurements that can observe the grid or verifying the state variables independently using PMU. PMU can directly measure the bus voltage phasor (including magnitudes and phase angles) with GPS timestamp and often PMU measurements are assumed here as secured, although these measurements are vulnerable, *e.g.*, due to GPS signal spoofing [20], [21],

[22], [23]. Similar PMU deployment-based solutions are proposed in [24], [25], [26]. In our previous work [12], we also proposed a mechanism to select a set of measurements (or buses) to be secured to protect state estimation against stealthy attacks when an adversary has resource, access, and knowledge limitations.

All these defense approaches rely on securing measurements either by deploying necessary PMUs or by implementing cryptographic (data integrity protection) algorithms. Our proposed formal framework considers measurement security. Hence, if the set of secured measurements are sufficient to protect state estimation, the framework will return unsat, *i.e.*, no attack vector. If PMUs are deployed in the grid and it is assumed that the states of the PMU deployed buses cannot be attacked (as a PMU can directly measure the phase magnitude/angle of the bus), we just need to add a constraint as $\neg c_j$ as true.

Another group of works, such as [27], [28], proposed mechanisms based on the generalized likelihood ratio test to detect UFDI attacks. A similar approach is proposed in [29] with the help of the adaptive cumulative sum control chart test. Our framework can consider these defense mechanisms by limiting the mesurement (state) changes to the acceptable threshold values, although such limiting constraints will certainly reduce the number of potential attack vectors, and so the critical ones.

7 Related Work

Although cyber vulnerabilities of power grids have been discussed in literature over the last decade [30], [31], most prior and ongoing work on cyber security analysis of power systems largely revolves around the concept of stealthy attacks, named Undetected False Data Injection (UFDI) attacks. The concept of such stealthy attacks is first presented in [6], and extended later in [32]. The authors discussed the attacks through different scenarios, such as limited access to measurement sensors/meters and limited resources to compromise them, 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. 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 [33]. Kin Sou et al. claimed that an l_1 relaxation-based technique provides an exact optimal solution of the data attack construction problem [34].

UFDI attacks with incomplete or partial information (*i.e.*, partial knowledge of the bus system with respect to electrical properties of the transmission lines) are discussed in [11], [13]. It is also shown in [35] that an adversary can launch UFDI attacks despite having no knowledge about the topology. The idea of the authors is to estimate the linear structure of the topology from the measurements and then launch UFDI attacks based on the estimated topology. A modeling of the game between an attacker and a defender with respect to the impact of UFDI attacks on energy markets is presented in [36]. Algebraic conditions of undetected topology attacks in power grids are identified in [37], although these conditions do not coordinate the typical UFDI attacks.

The notion of unidentified attacks is presented in [38], where the grid operator can detect the existence of bad data, but cannot identify the bad measurements specifically. Another kind of cyber attacks, namely load redistribution attacks, is introduced in [39]. Later in [40], these attacks are discussed for scenarios where the attacker has incomplete information. We presented a formal model to comprehensively verify stealthy attacks on state estimation considering various attack attributes simultaneously [12]. We provided a framework to formally assess the impact of stealthy attacks on the economic operation of the system considering the interdependency between state estimation and OPF [7]. Later, we performed a similar impact analysis with respect to topology poisoning-based stealthy attacks [41].

There are few works that attempted to use Simulink based design in formal modeling. In [42], the authors propose a verifier for a contract based system, which is modeled using Simulink. This SMT-based verifier validates the correctness of the Simulink model using system annotations. In [43], the authors proposed a technique to verify the control system properties, modeled using Simulink. They used a platform named Why3, which is used for deductive program verification. Although these two works apply the idea of utilizing formal methods for the Simulink model verification, we integrate these two methodologies from an analytical point of view in which the output from a formal model is efficiently explored using a Simulink model.

8 Conclusion

In this paper, we have proposed a framework to find critical threats by analyzing the impact of stealthy attacks on the generation cost with respect to the OPF routine and a flexible attack model. This framework provides an efficient analysis of economic impact by integrating formal method-based modeling with Simulink-based system design. This hybrid framework also applies parallelism to enhance its time-efficiency. We have implemented this framework and evaluated its scalability. We have observed that for a problem with 300 buses, this framework needs a few hours to perform a comprehensive impact analysis on a computing system with four physical cores. The proposed framework is useful in performing impact analysis of cyber attacks and thus understanding the dependability of the system. In the future, we would like to apply this hybrid framework to analyze impacts of stealthy attacks on other EMS modules.

Acknowledgement

This work is supported by the National Science Foundation, USA, under Project CNS-1657302.

References

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

[2] A. Ipakchi and F. Albuyeh. Grid of the future. In *IEEE Power and Energy Magazine*, pages 52–62, March 2009.

[3] 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 SmartGridComm*, pages 244 – 249, October 2010.

[4] A. Monticelli. *Network Topology Processing*. Power Electronics and Power Systems. Springer US, 1999.

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

[6] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. In *ACM CCS*, pages 21–32, November 2009.

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

[8] L. de Moura and N. Bjørner. Satisfiability modulo theories: An appetizer. In *Brazilian Symposium on Formal Methods*, 2009.

[9] MathWorks. Simulation and model-based design. http://www.mathworks.com/products/simulink/.

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

[11] 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, December 2010.

[12] M. A. Rahman, E. Al-Shaer, and R. Kavasseri. Security threat analytics and countermeasure synthesis for state estimation in smart power grids. In *IEEE/IFIP DSN*, June 2014.

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

[14] MathWorks. Model and simulate electrical power systems. http://www.mathworks.com/products/simpower/.

[15] Z3 theorem prover. Microsoft Research. https://github.com/Z3Prover/z3/wiki.

[16] Mathworks parfor: Parallel for loop. https://www.mathworks.com/help/distcomp/parfor.html?requestedDomain=www.mathworks.com.

[17] Matpower: A matlab power system simulation package. http://www.pserc.cornell.edu/matpower/.

[18] Intel hyper-threading technology. https://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html.

[19] 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*, April 2010.

[20] Q. Yang, D. An, and W. Yu. On time desynchronization attack against ieee 1588 protocol in power grid systems. In *IEEE Energytech*, 2013.

[21] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li. Time synchronization attack in smart grid: Impact and analysis. *IEEE Transactions on Smart Grid*, 2013.

[22] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domnguez-Garca. Spoofing gps receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, 2013.

[23] S. Barreto, A. Suresh, and J.-Y. Le Boudec. Cyber-attack on packet-based time synchronization protocols: The undetectable delay box. In *IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, 2016.

[24] 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, June 2011.

[25] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks: characterizations and countermeasures. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 232–237, October 2011.

[26] A. Giani abd E. Bitar, M. Garcia, P. Khargonekar M. McQueen, and K. Poolla. Smart grid data integrity attacks. *IEEE Transactions on Smart Grid*, 2013.

[27] O. Kosut, L. Jia, R. J. Thomas, and L. Tong. Limiting false data attacks on power system state estimation. In *IEEE Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March.

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

[29] Y. Huang, H. Li, K. Campbell, and Z. Han. Defending false data injection attack on smart grid network using adaptive cusum test. In *Annual Conf. on Information Sciences and Systems*, March 2011.

[30] J. Salmeron, K. Wood, and R. Baldick. Analysis of electric grid security under terrorist threat. *Power Systems, IEEE Transactions on*, 19(2):905–912, May 2004.

[31] C.W. Ten, C.C. Liu, and G. Manimaran. Vulnerability assessment of cybersecurity for scada systems. *Power Systems, IEEE Transactions on*, 23(4):1836–1846, November 2008.

[32] Y Liu, P. Ning, and M. 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, June 2011.

[33] 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.

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

[35] M. Esmalifalak, Huy Nguyen, Rong Zheng, and Zhu Han. Stealth false data injection using independent component analysis in smart grid. In *IEEE SmartGridComm*, pages 244–248, October 2011.

[36] M. Esmalifalak, G. Shi, Z. Han, and L. Song. Bad data injection attack and defense in electricity market using game theory study. *IEEE Transactions on Smart Grid*, 4(1):160–169, March 2013.

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

[38] Z. Qin, Q. Li, and M.-C. Chuah. Unidentifiable attacks in electric power systems. In *Cyber-Physical Systems (ICCPS), IEEE/ACM Third International Conference on*, pages 193–202, April 2012.

[39] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, 2(2):382–390, June 2011.

[40] X. Liu and Z. Li. Local load redistribution attacks in power systems with incomplete network information, April 2014.

[41] M. A. Rahman, E. Al-Shaer, and R. Kavasseri. Impact analysis of topology poisoning attacks on economic operation of the smart power grid. In *International Conference on Distributed Computing Systems (ICDCS)*, July 2014.

[42] P. Roy and N. Shankar. Simcheck: A contract type system for simulink. *Innovations in Systems and Software Engineering*, 7(2):73–83, June 2011.

[43] D. Araiza-Illan, K. Eder, and A. Richards. Formal verification of control systems' properties with theorem proving. In *International Conference on Control*, pages 244–249, July 2014.

Mohammad Ashiqur Rahman is an Assistant Professor in the Department of Computer Science at Tennessee Tech University, USA. He received the BS and MS degrees in computer science and engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, in 2004 and 2007, respectively, and obtained the PhD degree in computing and information systems from the University of North Carolina at Charlotte in 2015.

Rahman's research interest includes computer and information security analysis, risk assessment and security hardening, secure and dependable resource management, and distributed and parallel computing. His research area covers a wide area of security and dependability problems in both cyber and cyber-physical systems. He has already published over 40 peer-reviewed journals and conference papers. He has also served on the technical programs and organization committees for various IEEE and ACM conferences.

Amarjit Datta is pursuing his MS degree in Computer Science at Tennessee Tech University, USA. He received his BS in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka in 2009. Then, he worked as a software engineer in different multi-national companies till joining at Tennessee Tech in August 2015. Datta's primary research area includes information and network security and resource management for cyber-physical systems, particularly smart grids, renewable energy, and Internet of Things. He focuses on modeling of the problems formally and solving them efficiently for automated synthesis of management strategies.