Mitigation of Cyber-Attacks on Wide-Area Under-Frequency Load-Shedding Schemes

Mohsen Khalaf, *Member, IEEE*, Abdelrahman Ayad, *Graduate Student Member, IEEE*, Magdy M. A. Salama, *Life Fellow, IEEE*, Deepa Kundur, *Fellow, IEEE*, and Ehab F. El-Saadany, *Fellow, IEEE*

***Abstract*—This paper investigates the problem of cyber-attacks on Wide-Area Under-Frequency Load Shedding (WAUFLS), as these schemes are critical to maintaining power systems stability. First, we perform a detailed analysis on existing WAUFLS schemes and show that an adversary can launch a False Data Injection (FDI) cyberattack by manipulating the frequency measurements or Power Flow Measurements (PFMs), which may lead to system losses, unnecessary shedding of important loads, and system-wide blackout. Second, to address this vulnerability, we propose a novel Reliable States WAUFLS (RSLS) scheme to protect against FDI cyber-attacks. The disturbance calculation and load shedding process in RSLS are based on reliable system states, obtained using a proposed data-classification method on the PFMs that secures the state estimation operation. These reliable states are then used to perform the power flow in order to calculate the power mismatch. The calculated magnitude of disturbance, as well as the obtained system states, are used to decide on the amount and locations of the load-shedding. We validate the effectiveness and accuracy of RSLS by conducting extensive simulation on the IEEE-39 bus New England system using PSCAD/EMTDC. The results confirm the proposed scheme's capabilities in evaluating system disturbance and performing load-shedding, thus protecting the system during under-frequency conditions, and demonstrate its robustness against FDI attacks.**

***Index Terms*—Wide-area protection, wide-area under-frequency load-shedding, cyber-physical security, power system state estimation, false data injection.**

I. Introduction

WIDE-AREA Monitoring, Protection and Control (WAMPAC) is the concept of centralized power system monitoring, protection and control that employs the system-wide information and communicates selected data to specific remote locations to ensure continuous reliable operation of smart grids [1], [2]. WAMPAC is facilitated by the recent advancements in the Phasor Measurement Units (PMUs), enabled by the Global Positioning System (GPS) technology, making it feasible to monitor the whole power system simultaneously. As a result of PMUs deployment, real-time voltage and current phasor measurements, as well frequency measurements, at rates up to 60 measurements/s [3], are now available providing system operators with real-time visibility of the power systems dynamics by complementing traditional SCADA measurements, generated every two or four seconds [4]. Recently, due to the availability of PMU measurements, WAMPAC is being deployed in a multitude of critical power networks functions such as Power System State Estimation (PSSE), Automatic Generation Control (AGC), real-time contingency analysis, remedial action schemes, security constrained optimal power flow, economic dispatch, unit commitment, phase angle monitoring, power oscillation monitoring, power damping monitoring, voltage stability monitoring, and dynamic line rating [5].

The integration of advanced measurement and communication technologies within the power grid increases its cyber-attack surface making the problem of cyber-physical security integral. Cyber-physical security in the context of WAMPAC largely involves cyber intrusion for the purpose of destabilizing specific power system operations. Cybersecurity of Wide-Area Protection (WAP) Schemes, including WAUFLS schemes, have been barely addressed or superficially considered for WAMPAC systems [2]. In this paper, False Data Injection (FDI) attacks are considered, as they represent one of the most insidious attacks on WAUFLS in cyber-physical security today.

The authors in [6] reviewed the operation of UFLS schemes, summarized the characteristics of these schemes and classified the UFLS schemes into traditional, semi-adaptive, and adaptive techniques. Traditionally, UFLS schemes were local and depended only on the absolute value of the frequency [7]. In essence, these techniques shed a certain amount of the load under relief when the system frequency falls below a certain threshold. If the frequency keeps on falling down after the first shed, further sheds are performed when lower thresholds are passed. The values of the thresholds and of the relative amounts of load to be shed are decided off-line, on the base of experience and simulations. This is also called a multi-stage under-frequency load shedding [6], [8]. Some of

Manuscript received 25 January 2022; revised 21 June 2022 and 30 September 2022; accepted 15 October 2022. Date of publication 31 October 2022; date of current version 21 April 2023. This work was supported in part by the Khalifa University, Abu Dhabi, UAE, under Grant CIRA-013-2020, and in part by the Mitacs Accelerate Program Fund from the University of Toronto, Toronto, ON, Canada, under Project IT15676. Paper no. TSG-00126-2022. *(Corresponding author: Mohsen Khalaf.)*

Mohsen Khalaf is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada, on leave from the Electrical Engineering Department, Assiut University, Asyut, Egypt (e-mail: m.khalaf@utoronto.ca).

Abdelrahman Ayad is with the Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0G4, Canada.

Magdy M. A. Salama is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

Deepa Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada.

Ehab F. El-Saadany is with the Advanced Power and Energy Center, EECS Department, Khalifa University, Abu Dhabi, UAE.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3218066.

Digital Object Identifier 10.1109/TSG.2022.3218066

these techniques, also referred to as semi-adaptive techniques, are developed such that it measures the Rate of Change of Frequency (ROCOF) when a certain frequency threshold is attained [9]. Adaptive UFLS schemes are by definition fully adaptable. They are supposed to be capable of modifying protective actions according to system conditions causing their activation. The adaptability feature can be achieved by several means, one of most common being estimation of power imbalance size [10], which has been used in [11], [12], [13], [14], [15], [16], [17], [18], [19]. Some adaptive UFLS schemes are based on prediction [10], [20]. Other recent approaches are data-driven-based [21] and game theory-based [22].

WAUFLS protection schemes belong to the adaptive UFLS schemes class. Recently, they have been used to provide more accurate load shedding amount and distribution because it is done globally based on the wide-system disturbance evaluation unlike the traditional schemes that makes the load shedding decision based on local information [12], [13], [23]. Although WAUFLS offer advantages stemming from the use of Power Flow Measurements (PFMs) and frequency measurements to evaluate system disturbances, this reliance also makes them vulnerable to cyber-attacks. This is because the measurements used by these schemes are transmitted under the IEC 61850 protocols [2], [24], [25], [26], which use different communication media, i.e., wireless, fiber optics, and microwaves to support increased communication between both local and remote substation devices. IEC 61850 protocols work based on the semantics of sampled value and generic object-oriented substation event messages that have been proven vulnerable against different types of cyber-attacks [24], [25], [26], [27]. An attacker can potentially direct the system to blackout if they have access to frequency measurements and/or change the shedding distribution if they have access to PFMs.

In [19], the authors used the non-recursive Newton-type algorithm to locally estimate the frequency of the system as well as the ROCOF. These values are sent to the control center and used to calculate the amount of disturbance, if any. Accordingly, a control action was then derived and distributed throughout the power system. Although this method might not be susceptible to cyber-attacks since it depends on local measurements, it still uses the swing equation which has many disadvantages. One disadvantage of current WAUFLS schemes, that depends on the estimation of power imbalance size using the swing equation, is that if generators or large synchronous motors are disconnected during the disturbance, the system inertia has to be adapted accordingly [6]. Another disadvantage is that these techniques are able to accurately determine the magnitude of disturbance only at the moment of disturbance due to the dynamic response of turbines, governors, loads and other control elements, and does not provide a real-time monitoring of system mismatch [19]. Although the topic of smart grids cyber-physical security has received a considerable attention and research focus, there has been limited efforts on the topic of cyber-physical security of WAUFLS schemes. Authors in [28], [29], [30] investigated the problem of data integrity attacks on load shedding schemes without proposing a detection/mitigation schemes.

Therefore, motivated by the above mentioned research gaps, the main contributions of this paper can be summarized as follows:

- First, we formulate the problem of FDI attacks on current WAUFLS schemes, which are based on the estimation of power imbalance following a disturbance. We show, for the first time, using mathematical formulation and simulation, that the attacker can falsify WAUFLS schemes operation at different stages by manipulating PFMs and/or frequency measurements to cause equipment damage and/or system-wide blackouts.
- Second, we propose a data classification-based method to protect the PSSE against potential FDI attacks. Once the PSSE operation is secured, the system states (voltage magnitude and phase angle at each bus) obtained from the PSSE are used to run a dynamic power flow and calculate the degree of mismatch in the power system and perform appropriate load shedding. RSLS calculates the power mismatch value reliably, regardless of the existence of FDI in power flow measurements, as the proposed approach uses reliable system states for mismatch calculation.
- In addition to mitigating FDI attacks, RSLS also tackles two major disadvantages of the current WAUFLS schemes: i) RSLS monitors the system during the disturbance event at each instant, not only at the moment of disturbance; ii) RSLS does not depend on system inertia, therefore it is valid for small and large systems in contrast to the current WAUFLS schemes that inherently depend on system inertia.

II. Operation of Current WAUFLS Protection Schemes

The main driver for under-frequency in a power system is the imbalance between generation and load. Such conditions arise, for example, when a large generator is tripped, a sudden load is connected, or a large interconnection line is disconnected [31], [32]. Load shedding is a process used to relieve this mismatch by regaining the balance between load and generation. According to the literature, and as depicted in Fig. 1, the general procedure of WAUFLS schemes [10], [11], [15], [16], [19], [28], [33], [34], [35], [36] can be summarized as follows:

i) First, frequency measurements and PFMs are transmitted from the PMUs via the Ethernet/WAN medium to the control center. PMUs are installed in a variety of locations across the power system such as power plants, substations, office buildings, and private residences. PMU measurements are synchronized by GPS, which is used to provide the accurate time signal needed for synchrophasor calculation. Second, the cyber layer manages the communication of measurements and control decisions between the power system and the control center. This layer is also responsible for maintaining the cyber-security of the data and setting the firewall. Third, once received by the control center, measurements are processed in real-time and the control decisions are

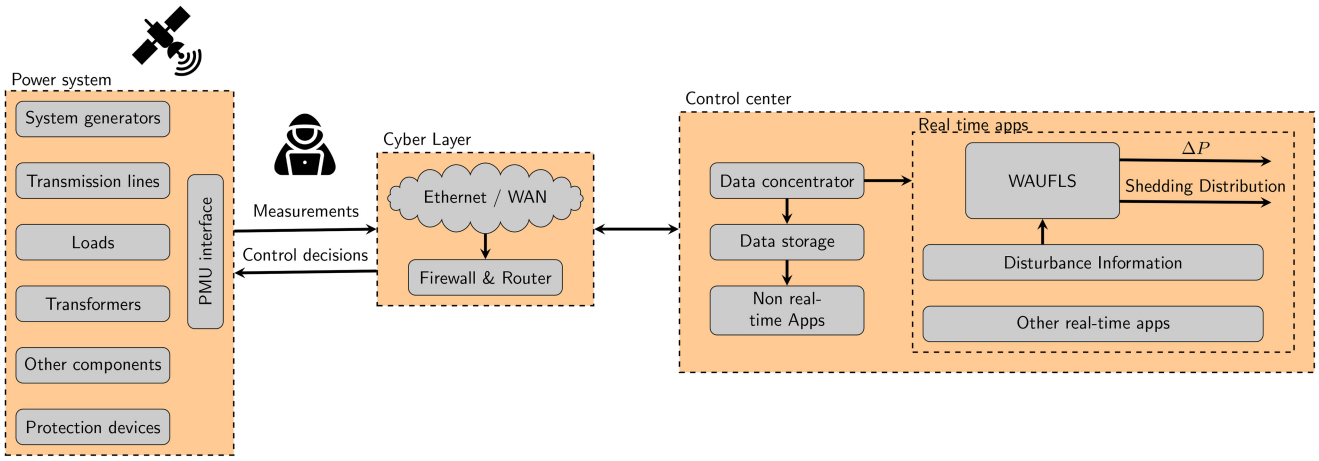


Fig. 1. Data transmission process in WAUFLS.

sent back to the power system, or stored in data storage. Measurement data from PMUs are managed in the control center by multi-layer agents. The top layer is the data concentrator, whose primary functions are to receive data from the PMUs, create GPS time-aligned records, share data with the real-time WAUFLS application agent as soon as the records are made, and forward the data records to the data storage agent and subscribed clients. The real-time WAUFLS application agent and data storage agent are in the second layer of the control center hierarchy. The third layer is the non-real-time application agent [37]. The Rate of Change of Frequency (ROCOF) is calculated either by the PMUs or locally at the control center in the grid.

ii) The frequency measurement and ROCOF values are used to evaluate system disturbance. Conventionally, the magnitude of disturbance is calculated using a reduced order System Frequency Response (SFR) model (swing equations) for all generators [11], [28]. Let Ω be the set of system buses, and Ω_G be the set of system buses with connected generators, then the swing equation for bus i can be formulated as:

$$\Delta P_i = P_{m_i} - P_{e_i} = \frac{2H_i}{f_n}\frac{df_i}{dt}, \quad \forall\, i \in \Omega_G. \tag{1}$$

where ΔP_i is the imbalance between generation and load(s) in pu, P_{m_i} is the pu input mechanical power, P_{e_i} is the pu output electrical power, H_i is the inertia constant in seconds, f_i is the frequency in Hz, and f_n is the system nominal frequency in Hz. The total resulting magnitude of disturbance can be obtained by summing the individual disturbances from each generator as follows:

$$\Delta P = \sum_{i\in\Omega_G} \Delta P_i = \frac{2\sum_{i\in\Omega_G} H_i}{f_n}\frac{df_c}{dt} \tag{2}$$

$$f_c = \frac{\sum_{i\in\Omega_G} H_i f_i}{\sum_{i\in\Omega_G} H_i} \tag{3}$$

where f_c is the frequency of the equivalent center of inertia.

iii) The control center determines the amount of load to be shed (power mismatch) based on the amount of the disturbance and system spinning reserve as follows [11]:

$$P_{shed} = 1.05 \times (\Delta P - P_{th}) \tag{4}$$

where P_{th} is the threshold value of power mismatch (available spinning reserve), and a factor of 1.05 is introduced for compensating the simplifying hypotheses adopted to develop the reduced SFR model.

iv) Finally, a shedding control action is sent by the control center, through the cyber layer, to an area or is shared between different areas based on disturbance information, which includes the nature of the disturbance, the location of the disturbance, and a load sensitivity analysis. To achieve load shedding, a combination of loads is selected such that the sum of their total active powers is as close as possible to P_{shed}. There are different criteria by which load shedding locations can be selected. However, the most common criteria used in wide-area applications is the voltage collapse-based load shedding, as the voltage collapses rapidly after a disturbance [11], [38], [39]. The shedding locations are mainly selected according to the location of disturbance [11] such that load shedding is distributed between the buses close to the disturbance based on their voltage dip during the disturbance. All area buses are ranked based on voltage dips. Accordingly, the load shedding at bus i is proportional to the bus rank, as follows

$$P_{shed,i} = \frac{\Delta V_i}{\sum_{i\in\Omega_v} \Delta V_i} \times P_{shed} \tag{5}$$

where ΔV_i is the voltage dip at bus i immediately after the disturbance, and Ω_v is the set of buses considered for the load shedding process Once the load to be shed is known for all buses, the shedding process takes place in steps.

III. Attack Model and Problem Formulation

WAUFLS schemes-in use today in digital substations-employ IEC 61850 communication protocols. However, IEC

TABLE I
ATTACK MODEL

Attacker	**Objective(s)**	- Cause system wide blackout - Cause equipment damage
	Capabilities	- Access to a subset of frequency measurements - Access to a subset of PFMs - Knowledge of system topology
	Limitation(s)	- No physical access to the system - No access to control signals
Assumption(s)		- System measurements are sent through wireless communication

61850 protocols are vulnerable to cyber-attacks. We assume digital substations employ wireless mediums, which are convenient for deployment, but amplify the attack surface because these substations are geographically dispersed and often maintain limited physical network protections [2], [24], [25], [26]. It is also assumed that the utility has placed significant resources in protecting the control center/Energy Management System (EMS), which represents a single-point-of-failure and is considered to be trusted. Given that IEC 61850 connects devices that measure both frequency and power flow measurements, one straightforward attack model involves a remote attacker gaining access to a subset of such information through IEC 61850. In addition, it is assumed that the attacker cannot access/tamper with control decisions of the control center/EMS decisions [40]. Without this constraint, it is a trivial exercise for an attacker that has successfully penetrated the protected network to trigger cascading failures across the power grid. It is therefore conceivable that an energy provider would make protecting its EMS its foremost priority. Protecting every other single communication link in the power system is extremely expensive, especially in large power systems that mainly depend on the communication network that carries hundreds of signals. Based on the aforementioned vulnerabilities, Table I summarizes the objectives, capabilities and limitations of the attacker as well as the assumptions that this work is based on.

The following sections formulate three different attack scenarios in which an opponent can target the operation of current WAUFLS schemes in the power systems. Depending on what data are available for the attacker, the attacker can launch an attack. The first scenario illustrates how can the attacker can launch an attack if they have access to one or more frequency signals enabling full control over the amount of load to be shed. The second scenario focuses on the attacker having access to PFMs; here, although the attacker cannot manipulate the amount of load to be shed, they can force the control center operator to shed load from incorrect locations. Finally, if the attacker has access to both PFMs and frequency measurements, we demonstrate how they can fake a disturbance and cause unnecessary load shedding by the control center. We demonstrate the significant impact that FDI attacks can have on WAUFLS motivating the need for mitigation.

A. Targeting the Magnitude of Disturbance

Power system frequency is typically considered as a global parameter. However, results in the literature indicate that the frequency slightly differs from one neighboring area to another during system transients due to inter-area oscillations [41]. As mentioned, control centers make use of the values of a frequency and its derivative to evaluate system-wide disturbances employing swing equations to calculate the amount of load required to be shed. Equation (2) also shows that the magnitude of disturbance given by the swing equation (ΔP) depends on the ROCOF not on the frequency value itself. This allows an attacker to construct an FDI attack that does not change the magnitude of the frequency significantly, while changing its rate of change to affect the calculated magnitude of disturbance. In other words, the attacker works on manipulating the ROCOF, while largely maintaining frequency magnitude, in order to maximize the effect on the swing equation output. Hence, the attacker can control ΔP to force the control center operator to make a wrong action, either by shedding insufficient load (leading to system blackout) or shedding too much (causing damage to system equipment due to over-frequency conditions). To launch such an attack, the attacker does not need to access the system physically. Instead, they need to access one or more frequency measurement signals.

To formulate the attack mathematically, it is assumed that the attacker injects a time-varying linear signal to one or more frequency measurements. Without loss of generality, it is assumed that the FDI takes place on all frequency values. The frequency value of generator i after manipulation is

$$f_{ia} = f_i \pm m_i t \tag{6}$$

where m_i is the slope of the attack signal. Substituting the new frequency values into (3), the center of inertia frequency is

$$f_{ca} = \frac{\sum_{i\in\Omega_G} H_i f_i \pm \sum_{i\in\Omega_G} H_i m_i t}{\sum_{i\in\Omega_G} H_i} = f_c \pm \frac{\sum_{i\in\Omega_G} H_i m_i t}{\sum_{i\in\Omega_G} H_i} \tag{7}$$

and the new magnitude of disturbance can be calculated by substituting into (2), as follows:

$$\begin{aligned}\Delta P_a &= \frac{2\sum_{i\in\Omega_G} H_i}{f_n}\frac{df_{ca}}{dt} = \frac{2\sum_{i\in\Omega_G} H_i}{f_n}\frac{d}{dt}\left[f_c \pm \frac{\sum_{i\in\Omega_G} H_i m_i t}{\sum_{i\in\Omega_G} H_i}\right] \\ &= \Delta P \pm \frac{2\sum_{i\in\Omega_G} H_i m_i}{f_n} = \Delta P \pm \Delta P_{attack}\end{aligned} \tag{8}$$

Hence, the attacker needs only to calculate the slopes of the injected signal m to change the magnitude of disturbance, which then changes the total amount of load to be shed. The value of m should be crafted carefully such that it does not cause a sudden change in the frequency value. Note that the above model of the attack is generic, i.e., the attacker can still manipulate only one or two frequency values due to the limited abilities of the attacker to access geographically dispersed sensors. In this case, the value of the injected signals into other frequency measurements that are not attacked is zero. It is noteworthy that, based on (7), the change in magnitude of the frequency of the equivalent center of inertia due to an attack signal of slope m_i is very small. However, the resulting ΔP_{attack} from (8) will have a significant value even if only one or two sensors only are attacked with a signal that has a small slope m_i.

B. Targeting Load Shedding Distribution

System operators utilize bus voltage magnitudes in order to accurately perform load shedding, using (5), from buses with the highest voltage dips. Therefore, an attacker can aim to manipulate the voltage magnitudes on target buses in order to compromise the load shedding process. In this section, a stealthy FDI attack formulation that allows manipulation of specific bus voltages is presented. A FDI is considered a stealthy attack if it can bypass the Bad Data Detector (BDD), which is commonly used by system operators to flag any data anomalies. The most common BDD methods are residual-based and as such, they operate on looking at the magnitude difference between the measurements and estimated measurements from the computed state [42], [43]. This formulation serves as a basis for the attack scenario that involves compromising the shedding distribution.

1) Constrained FDI Attacks: PSSE is employed to ensure system stability and observability of state variables such as voltage magnitudes and phase angles of all buses. These states are estimated based on the available field measurements. The AC power flow model relates the power flow measurement vector $\mathbf{z}$ to the state variables vector of voltage magnitudes and phase angles $\mathbf{x}$ by

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{9}$$

where $\mathbf{h}(\mathbf{x})$ is the nonlinear mapping function between measurements and states, and $\mathbf{e}$ is the measurements error vector. In order to determine the value of measurements manipulation, the attacker then considers the power flow equations:

$$\begin{aligned} P_{ij} &= V_i'^2 \cdot g_{ij} - V_i' V_j \cdot g_{ij} \cos\left(\theta_i - \theta_j\right) \\ &\quad - V_i' V_j \cdot b_{ij} \sin\left(\theta_i - \theta_j\right) \end{aligned} \tag{10}$$

$$\begin{aligned} Q_{ij} &= -V_i'^2 \cdot \left(b_{ij} + b_{ij}^{sh}\right) + V_i' V_j \cdot b_{ij} \cos\left(\theta_i - \theta_j\right) \\ &\quad - V_i' V_j \cdot g_{ij} \sin\left(\theta_i - \theta_j\right) \end{aligned} \tag{11}$$

where V_i' is the voltage magnitude to be altered at bus i, θ_i is the voltage angle at bus i, and g_{ij}, b_{ij}, and b_{ij}^{sh} are the conductance, susceptance, and shunt susceptance of the line between bus i and j, respectively. Active and reactive power injection at bus i are represented by

$$P_i = \sum_{j \in \Omega} P_{ij}, \quad Q_i = \sum_{j \in \Omega} Q_{ij} \tag{12}$$

It follows that in order to change the voltage magnitude at bus i, power flow equations (10)-(12) are solved to determine the required changes in measurements. Let $\mathbf{c}$ represent the vector of values to be added to the state variables $\mathbf{x}$, which represent the impact on the estimated states due to the introduction of the attack vector $\mathbf{z}$. Based on this attack formulation, the condition for a stealthy FDI attack is outlined for AC systems as follows:

$$\begin{aligned} \|\mathbf{z_a} - \mathbf{h}\left(\hat{\mathbf{x}}_{\mathbf{bad}}\right)\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{h}\left(\hat{\mathbf{x}} + \mathbf{c}\right)\| \\ &= \|\mathbf{z} - \mathbf{h}\left(\hat{\mathbf{x}}\right)\| \leq \tau \end{aligned} \tag{13}$$

where $\hat{\mathbf{x}}$ is the states estimation vector, $\mathbf{a}$ is the attack vector that impacts state estimation results by shifting it by the vector $\mathbf{c}$, $\mathbf{z_a}$ is the resulting manipulated measurements vector, and τ is the BDD alarm detection threshold. Therefore, the criteria for a stealthy hidden attack vector is given by:

$$\mathbf{a} = \mathbf{h}\left(\hat{\mathbf{x}} + c\right) - \mathbf{h}\left(\hat{\mathbf{x}}\right), \tag{14}$$

which manipulates state variables by $\mathbf{c}$ without raising the BDD alarm. The algorithm is grounded in the following assumptions [43]: i) All measurements in the sub-graph surrounding a power injecting bus are to be changed; ii) power injection change summations must be kept at zero; and iii) attack vector sparsity depends on system topology. It is worth mentioning that the attack strategy must also adhere to the electrical laws of the power networks (e.g., current and power nodal balances).

2) Load Shedding Manipulation: Equipped with the ability to target specific buses and manipulate voltage magnitudes, the attacker can easily compromise the load shedding distribution process. This can be accomplished by changing the load shedding amount on a given bus and/or inducing load shedding on a bus outside of the initial load shedding setting. In other words, voltage disturbances at target locations (i.e., those which have a high voltage dip) are shown if they have a negligible voltage dip. At the same time, voltages of targeted buses (i.e., those which have a low voltage dip) are shown if they have the highest voltage dip. The attack can be formulated as follows:

i) Let Ψ represent the initial set of buses on which load shedding is to be performed, with a load shedding amount of P_{shed_ψ}, where $\psi \in \Psi$. Also, let Φ represent the set of buses the attacker is targeting to shed power from, with a load shedding amount of P'_{shed_ϕ}, where $\phi \in \Phi$. The selection of set Φ can be based on a sensitivity analysis of the system to power shedding, buses with lowest voltage dips, or buses with critical loads.

ii) The attacker then aims to change the voltage magnitudes to

$$V'_\phi = V_\phi + c_\phi, \quad \forall \phi \in \Phi \tag{15}$$

$$V'_\psi = V_\psi + c_\psi, \quad \forall \psi \in \Psi \tag{16}$$

where V'_ϕ (V'_ψ) is the new voltage magnitude for bus ϕ (ψ) after adding the attack value c_ϕ (c_ψ), as per (13) and (14). For set Φ, the attacker increases the voltage dip to incur more load shedding using (15) while decreasing the voltage dip of set Ψ to reduce the load shedding using (15).

iii) Due to the variation in voltage magnitude, the amount of shedding power for each bus P_{shed_ψ} changes. However, the total shedding amount must remain constant, as follows:

$$\sum_{\psi \in \Psi} P_{shed_\psi} = \sum_{\psi \in \Psi} P'_{shed_\psi} \tag{17}$$

Note that sets Φ and Ψ are independent and may overlap in certain buses. A special case of this attack will occur if the attacker chooses to have $\Phi = \Psi$ and only change the load distribution within the set. It is noteworthy that if the attacker does not consider (17), then

the total amount of shedding power after the attack can differ from the original power shedding amount. This difference can lead to the attack detection by the system operator.

C. Faking Under-Frequency Conditions

In this scenario, the attacker's objective is to trick the system into responding as if it were experiencing under-frequency conditions that require activation of WAUFLS. The attacker can fake a disturbance condition that misguides the system operator to launching an unnecessary load shedding process by manipulating both the frequency and the PFMs. For example, if the attacker needs to fake a disturbance that includes the tripping of a specific generator, the attacker has to manipulate both the system frequency measurements and the PFMs of the meters that are close to this generator to reflect the disturbance on the state estimation results. In disturbances that affect system frequency, it is expected that the voltage magnitudes would strongly deviate from the steady-state voltage profile. The FDI attack formulation given by (14) indicates that the attacker manipulates the power flow measurement to change the voltage profile to resemble a post-disturbance one. Undoubtedly, there is always a limitation on the number of measurement nodes the attacker is able to compromise. Accordingly, the objective of the attack is to manipulate the minimum number of measurements while simultaneously attempting to generate a voltage profile that matches as much as possible an actual post-disturbance voltage profile for all the buses. There are several approaches for targeting the manipulated states, such as minimizing the number of attacked measurements, constraining the attacks to a subset of states, and minimizing the probability of detection [43]. In this scenario, the attacks are launched based on the formulation in the previous section, in addition to selecting a subset of buses based on a threshold criterion.

The first step is to analyze variations between voltage magnitudes for each bus in the system at steady-state and post-disturbance. As expected, there is an inverse relation between the number of buses and the magnitude of ΔV. We devise an FDI strategy based on the ΔV threshold, as follows:

i) Simulate a disturbance scenario and determine the deviation index D_i, between steady-state (V_{ss}) and post-disturbance voltage magnitude (V_d) for each bus $i \in \Omega$ at time step t in the simulation period T:

$$D_i = \max\left\{\text{abs}\left(V(t)_{d_i} - V(t)_{ss_i}\right)\right\}, \quad \forall t \in T, \forall i \in \Omega \tag{18}$$

Note that max operator ensures that the threshold is based on the entirety of the simulation period T, and the absolute value is considered to account for positive and negative voltage deviations. The purpose of this step is to determine the maximum deviation of all bus voltages during the disturbance.

ii) Classify each bus i according to whether it belongs to the attack set Ω_a, if it exceeds the pre-defined threshold γ, i.e., Bus $i \in \Omega_a$ if $D_i \geq \gamma$. The threshold represents the maximum allowable tolerance for voltage deviation between the disturbance and steady-state cases. A higher threshold γ implicates a smaller attack subset Ω_a, while at the same time giving a higher probability for raising suspicion with the system operator, as more buses would have a steady-state voltage profile rather than a disturbance profile. The threshold is determined by analyzing the voltage profile and normal deviations in voltages during steady-state operation.

iii) Launch a constrained FDI attack on power flow measurements that only targets buses belonging to the subset Ω_a. An indispensable condition for the success of such an attack is the ability to target specific state variables, as outlined in the attack formulation. It is intended to leave the remaining buses voltages unchanged from the state estimation process, as the variation between the state estimation voltages and the disturbances voltages would be of lesser magnitude and importance, respectively, based on the chosen case threshold. The index i determines the value of the attack element c_i to be added to the system state estimate $\hat{x}_i$, as per (14):

$$\hat{x}_{att,i} = \begin{cases} \hat{x}_i + c_i, & \text{if } i \in \Omega_a \\ \hat{x}_i, & \text{otherwise} \end{cases} \tag{19}$$

where $\hat{x}_{att,i}$ is the attacked state estimate. For this scenario, the attacker launches the attacks based on the pre-determined threshold γ. A compromise is made between the number of attacked measurements and the allowed deviation between perceived and expected voltage profiles.

IV. Mitigation Using RSLS

Relying on the value of ROCOF only to evaluate system disturbances makes the current WAUFLS schemes vulnerable to FDI attacks, as shown in the previous section. They are also inaccurate in small systems, as system inertia changes if one of the generators is tripped [6]. Furthermore, using the swing equation to determine the magnitude of disturbance is valid only at the moment of disturbance and does not provide a real-time monitoring of system mismatch [19]. In addition to mitigating the effect of FDI attacks, the proposed technique overcomes these drawbacks inherent in current schemes, as it is based on reliable system states, and is consequently able to evaluate system disturbances accurately, even if there are FDI attacks on the frequency and/or PFMs. In this section, we describe the RSLS method that is robust to FDI attacks.

The proposed scheme calculates power mismatch using dynamic power flow analysis. However, the data used to run the dynamic power flow must be obtained from a trusted source. Therefore, PSSE represents an in-between layer that processes system measurements and provides trusted system states, using the proposed measurement classification-based method explained in Section IV-A, that can be used in the power flow.

A logical overview of RSLS is depicted in the flowchart of Fig. 2. First, it receives the frequency and power flow measurements from different sensors and PMUs in the system. Then, the frequency of center of inertia (f_c) is calculated and compared to a predefined threshold (F_{min}). A value less than the

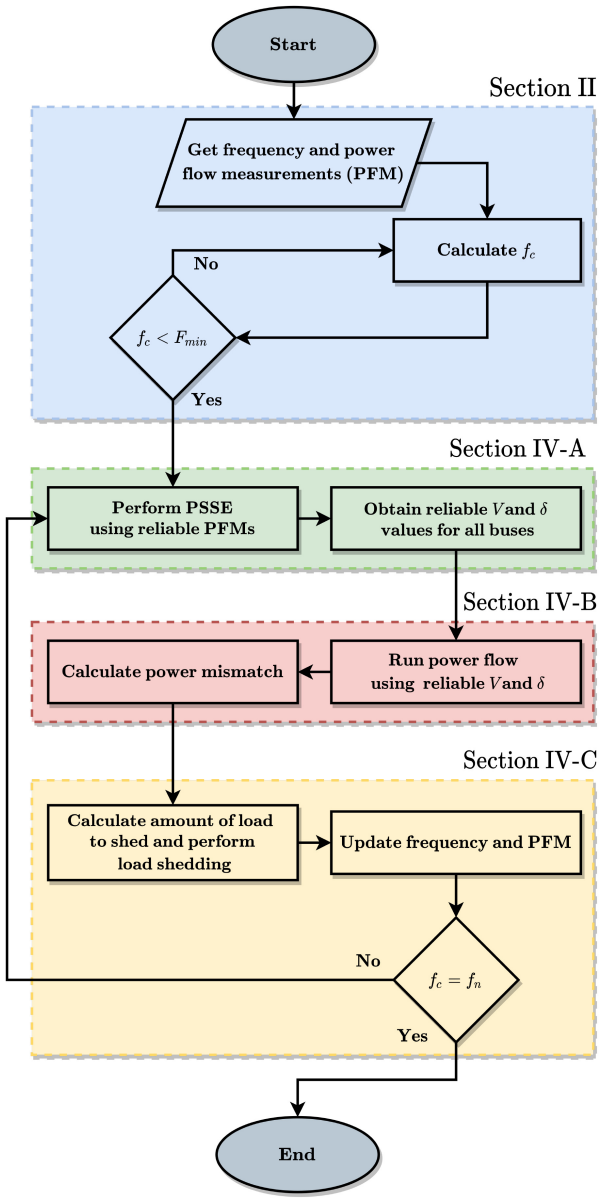


Fig. 2. RSLS flowchart.

threshold means that there is an under-frequency condition in the system due to a disturbance. At that point in time, power flow measurements are used to run the PSSE, and reliable system states (V and δ at each bus) are obtained.

The next step involves employing these reliable states to run a dynamic power flow that calculates the power mismatch due to the disturbance. Based on the calculated power mismatch,the load shedding process is performed. After shedding the necessary load, f_c is calculated based on the updated values for system frequency measurements and compared with f_n. Finally, if $f_c < f_n$, the updated power flow measurements are used to repeat the PSSE-PF process until the system frequency returns back to its nominal value. It is worth mentioning that the topology of the system should be updated as needed, prior to running both PSSE and the power flow. In the following sections, the used models of PSSE as well as dynamic power flow are described.

A. Securing PSSE Using Measurement Classification

In order to run the PSSE, the control center operator relies on PFMs that guarantee system observability. In practice, the system operator has access to redundant PFMs which generate a high number of essential sets [44]. The proposed mitigation method depends on two main steps: i) securing only the subset of critical PFMs, and ii) employing different PFMs for running the PSSE. By securing only the critical PFMs, we minimize the cost of securing the power network. Furthermore, by employing a different observable (essential) PFMs set, the attacker has negligible probability of knowing the PFMs to attack. Therefore, any attempted attack will be easily detected by the PSSE BDD.

For the PSSE operation, as outlined in Section III-B1, the PFMs including voltage magnitudes V, phase angles θ, active power injection P_i, and reactive power injection Q_i, are obtained from the sensors installed at each bus. In addition, active and reactive power flow values which are from the sensors installed at the transmission lines. Therefore, the maximum possible number of PFMs that can be obtained in a system is $N_{max} = 4N + 2b$ where N is the number of buses and b is the number of transmission lines. Since it impractical to install sensors everywhere in the power system, it is assumed that the installed sensors provide a set of data A with m measurements where $A \subset M$ and M is the set that includes all the possible measurements in that system. In this work, the available data set A is classified into essential E and non-essential W data subsets, i.e., $A = E \cup W$. Essential data subset is the minimum number of PFMs, l, that is required to achieve system observability. Essential data subsets are not unique and many essential subsets can be identified for a system based on the number of the available data in the set A. The intersection of all essential data sets gives a critical data subset C, i.e., $C = E_1 \cap E_2 \cap E_3 \cdots \cap E_n$ where n is the maximum number of essential subsets. The critical data subset is a unique subset of data that is required by the PSSE to [44]. Using the i_{th} essential subset E_i, the critical PFMs for a system can be obtained by ordering the essential measurements first, then partitioning the matrices and rewriting equation (9) as:

$$\begin{bmatrix} h_E(x) \\ h_W(x) \end{bmatrix} . [x] = \begin{bmatrix} z_E \\ z_W \end{bmatrix} \tag{20}$$

where the rows of $h_E(x)$, z_E and $h_W(x)$, z_W correspond to the essential and non essential measurements, respectively. Applying the Peters-Wilkinson decomposition [44]:

$$Z_E = L_1 . U . x \tag{21}$$

$$Z_W = L_2 . U . x \tag{22}$$

Eliminating $U.x$, the linear dependency among the essential and non-essential measurements can be given by (24). Hence, an element of z_E is critical if the corresponding column of T is null.

$$z_W = L_2 . L_1^{-1} . z_1 \tag{23}$$

$$z_W = T . z_1 \tag{24}$$

B. PSSE-PF Module

After estimating a trusted set of system states, including voltage magnitudes and phase angles at each bus, these reliable values are used to run a power flow to calculate total system mismatch. To capture the small changes in the power system during transients, a second-order power flow model [45] is used to calculate the total power mismatch. For a system with N buses, the power mismatch at bus i can be defined as the sum of the power flows in all elements (i.e., generators, loads, transmission lines, etc.) connected to this bus. The real power injection into bus i can be defined as P_i

$$P_i = \sum_{j\in\Omega} |V_i V_j Y_{ij}| cos\big(\delta_i - \delta_j - \theta_{ij}\big) \tag{25}$$

where $Y_{ij} = |Y_{ij}|\angle\theta_{ij}$ is the admittance of the transmission line connecting buses i and j. Using Taylor series expansion [45], the active power mismatch $P_{mis,i}$ at bus i can be defined as

$$\begin{aligned} P_{mis,i} = &\sum_{j\in\Omega} \frac{\partial P_i}{\partial \delta_j}\Delta\delta_j + \sum_{j\in\Omega} \frac{\partial P_i}{\partial V_j}\Delta V_j + \frac{\partial^2 P_i}{\partial V_j^2}\big(\Delta V_j\big)^2 \\ &+ \sum_{j\in\Omega\setminus\{i\}} \frac{\partial^2 P_i}{\partial \delta_i \partial V_j}\Delta\delta_i\Delta V_j + \sum_{j\in\Omega\setminus\{i\}} \frac{\partial^2 P_i}{\partial \delta_j \partial V_j}\Delta\delta_j\Delta V_j \\ &+ \sum_{j\in\Omega} \frac{\partial^2 P_i}{\partial \delta_j \partial V_i}\Delta\delta_j\Delta V_i \end{aligned} \tag{26}$$

where δ_j and V_j are the phase angle and magnitude of voltage at bus j, respectively, N is the number of system buses, and Δ represents small changes in the variables. Finally, the total system mismatch P_{mis}, which is also equal to the difference between the total generation P_G and the total load P_L, is equal to the summation of the single mismatch values at each bus, and can be evaluated

$$P_{mis} = P_L - P_G = \sum_{i\in\Omega} P_{mis,i}. \tag{27}$$

It is worth mentioning that while system losses can be neglected in large systems, in this work it is included into P_L.

C. Load Shedding Process

Since the proposed approach performs online monitoring of the amount of power mismatch, the amount of load to be shed P_{shed} is the same as the amount of power mismatch P_{mis} because the spinning reserve is already embedded in the calculations. This contrasts with other approaches that require knowledge of the system spinning reserve because they calculate the magnitude of disturbance, not the actual power mismatch in the system.

Once the amount of load shedding is determined, the locations of load shedding will be determined and (5) is used to distribute the shedding order between the selected buses. In order to avoid unnecessary load shedding, a time delay is necessary between consecutive load shedding. A long period of delay may result in disconnecting generating unit from the system, however, too short delays do not recognize transient dips [46], [47]. According to [48], the minimum time delay between consecutive stages is given by:

$$\Delta t \geq N \cdot T = \frac{N}{F_n} \tag{28}$$

where T is the time cycle, and F_n is the nominal value of system frequency, and N is the number of delay cycle, where the minimum value of N is 10 to 14 delay cycles [46].

V. Simulation Results

In this section, the reliability and the accuracy of the proposed RSLS is discussed. In addition, the robustness of the proposed mitigation scheme is tested against the shortcomings of traditional approaches, as discussed in the previous section. In so doing, we will calculate load shedding under disturbance conditions, through the usage of the PSSE-PF module. The case studies are simulated in PSCAD/EMTDC using the IEEE 39 bus New England system [49]. The following scenarios show that system frequency goes back to its nominal value after performing the load shedding using the proposed technique, which achieves system stability after a large disturbance.

A. Reliability of the Proposed Method

The proposed mitigation approach depends on running the PSSE, which is an essential operation in the power grid. The approach relies on adding a security layer to the PSSE process by using secure PFMs. However, it should be noted that this additional security layer does not incur any significant delays within the PSSE scheme as it does not change the PSSE algorithm, but only the set of measurements used.

Fig. 3 shows the probability of finding an observable set by using a specific percentage of available PFMs (with all possible combinations). For example, in the IEEE 39 bus New England system, of all PFMs set combinations involving 80% of available PFMs, 40% are essential sets that can be used for PSSE. Therefore, by using different PFMs sets of various sizes, the probability of the attacker finding the employed essential set is drastically diminishes, which increases the reliability of the PSSE. As the protection strategy depends on utilising different observable sets to obtain trusted states from the PSSE, we calculate the probability of a successful FDI attack (scheme failure probability) for a PFMs subset size as the inverse of the available number of observable sets times the probability of obtaining an observable set as shown in Fig. 3. The probability of the mitigation scheme failure against the PFMs subset size used for the PSSE is depicted in Fig. 4. The figure shows that applying a smaller subset of PFMs reduces the probability of a successful attack, as it allows a larger number of PFMs combinations to obtain the PSSE. The system operator, however, does not need to be restricted to a specific PFMs subset size.

B. Case Study: Tripping of a Large Generator

The attacker manipulates the measurement corresponding to the frequency of generator G_8 by increasing it, using an FDI signal that has slope $m_8 = 0.02$. The center of inertia frequency f_c is then calculated to be higher than the actual

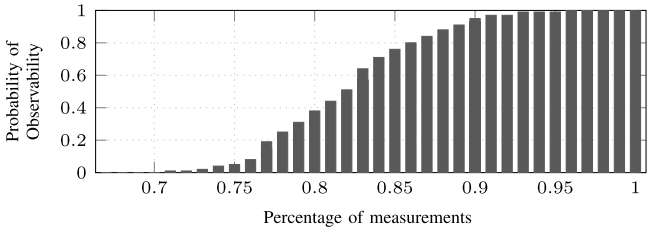


Fig. 3. PSSE Observability as function of PFMs.

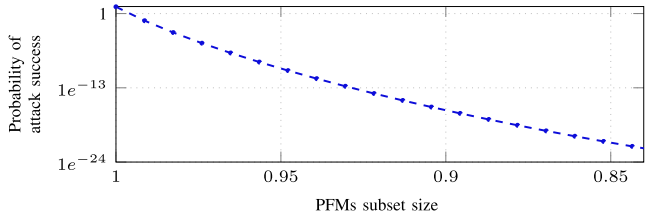
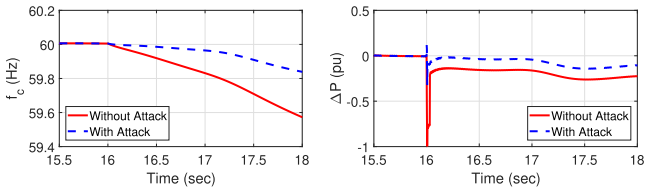
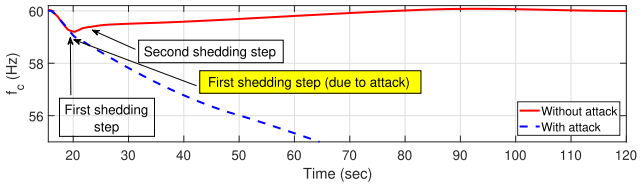


Fig. 4. Failure probability of the mitigation scheme.



(a) Real and manipulated center of inertia frequency frequency

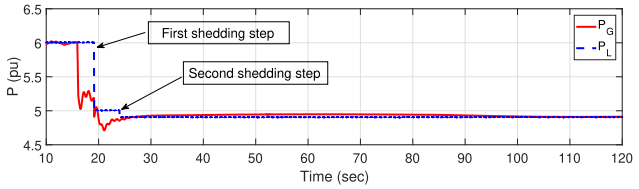


(b) Real and manipulated amount of disturbance

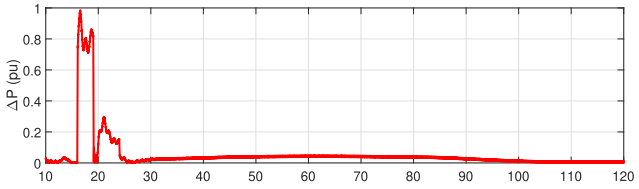
Fig. 5. Targeting lower amount of load-shedding.

center of inertia frequency of the system. This causes the calculated magnitude of disturbance ΔP to be 0.3 pu, i.e., lower than the actual disturbance in the system ($\Delta P_a < \Delta P$), as shown in Fig. 5(a). Consequently, as seen from Fig. 5(b), the control center operator will perform only one shedding step with a lower amount of load, whereas two shedding steps are needed. The highlighted shedding step is the one prompted by the attack. As can be seen, the attack causes the system frequency to keep falling, thus forcing the under-frequency control in the generators to shut down, causing a system-wide blackout.

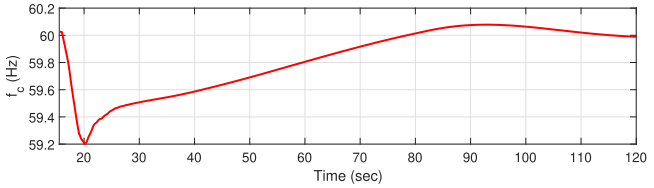
Using our mitigation technique, Fig. 6(a) shows the variations in system load versus the drop in system generation due to the disturbance. The value of the initial mismatch is 1 pu, so this is the amount of load to be shed in the first step when the frequency reached the minimum threshold (59.3 Hz). Due to the transient which occurred after shedding the load, the generation power drops slightly, so a smaller second shedding step is necessary. The calculated mismatch value, illustrated in Fig. 6(b), shows the accuracy of using the PSSE-PF module to calculate it at different stages of the disturbance. It also shows that the power mismatch is reduced to zero after the shedding



(a) Power generation vs. load power



(b) Power mismatch



(c) Frequency of center of inertia

Fig. 6. Load shedding after G_1 tripping and the effects on power mismatch and frequency values.

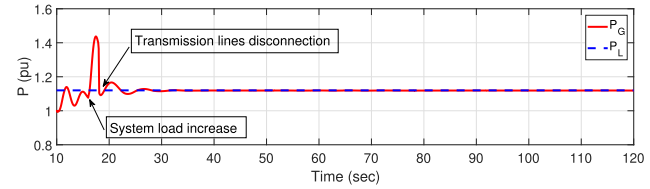
process. As a result, the frequency of center of inertia reverts to the nominal value, as depicted in Fig. 6(c), which reflects the frequency stability of the system after incorporating the proposed shedding scheme.

C. Case Study: Islanding Scenario

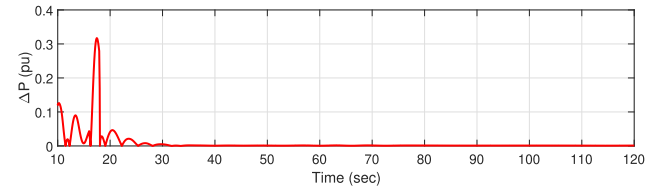
This scenario includes a sudden load increase of 0.45 pu at bus 15 at $t = 16$ sec. This results in the disconnection of the transmission lines that connect buses 1-2 and 8-9 at $t = 17$ sec because of the thermal limits. Due to this disturbance, the system becomes two islands, with one having an unbalance between load and generation due to being disconnected from the system main supply. The system can be viewed as two areas: Area 1 includes buses 1, 9 and 39, and Area 2 includes the rest of the system. An analysis of each area is carried out separately.

1) Analysis of Area 1: Area 1 includes the largest supply G_1. However, as seen in Fig. 7(a), the generation is less than the load and the rest of load power is taken from the generators of Area 2. At the moment of disturbance, G_1 was willing to participate in the load increase that occurred in Area 2, so the output power of this generator increased. After the transmission line disconnection at $t = 17$ sec, Area 1 becomes isolated and includes only G_1 and a load of 1.15 pu. The frequency of this Area remains stable after the disturbance, as shown in Fig. 7(c), because the area power mismatch is zero, Fig. 7(b). Therefore, no load shedding is needed in Area 1.

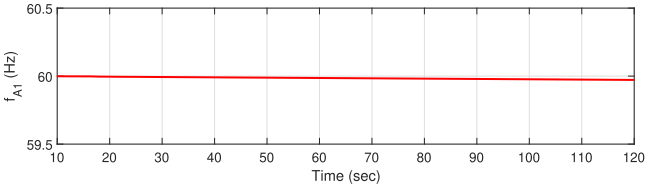
2) Analysis of Area 2: There was extra generation in Area 2 prior to the load increase that took place at $t = 16$ sec. This extra generation power is supplied to Area 1, as discussed above and as shown in Fig. 8(a). After the transmission lines are disconnected, a mismatch of 0.15 pu existed in Area 2 (see Fig. 8(b)) because the generators in this area are not able to



(a) Power generation vs. load power

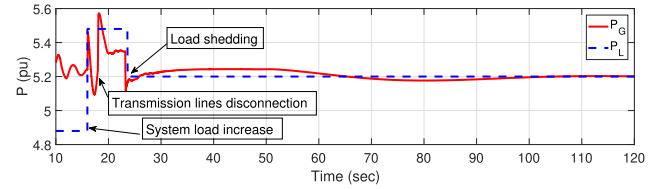


(b) Power mismatch

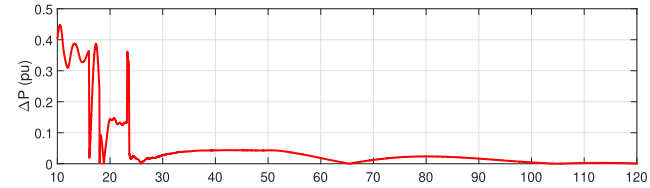


(c) Frequency of center of inertia

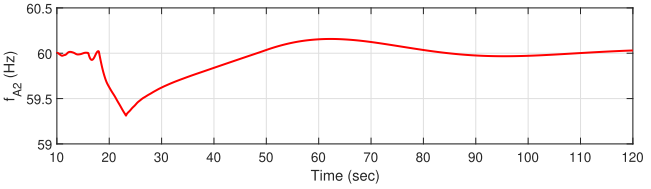
Fig. 7. Power mismatch and frequency of Area 1.



(a) Power generation vs. load power



(b) Power mismatch



(c) Frequency of center of inertia

Fig. 8. Power mismatch and frequency of Area 2.

supply the entire load demand. Hence, the system frequency starts dropping, as shown in Fig. 8(c), and reaches the load shedding threshold at $t = 24$ sec. A load shedding process then takes place and the frequency of the area returns to its nominal value. It can be seen that the frequency in the two areas returned to the nominal value after incorporating the proposed load shedding.

VI. Discussion

In this section, we discuss the main points relating to the attack model assumptions and limitations, and highlight the main advantages of the RSLS scheme.

A. Attack Model Assumptions

In this work we have considered several limitations based on realistic assumptions from the literature and power engineering practices:

i) The attacker must follow the FDI attack formulations to create the attack vector **a** in order to remain stealthy and undetected by BDD alarms. These conditions are outlined by equations (9)-(14).

ii) As the attacker attempts to create voltage disturbance during the load shedding manipulation process, i.e., equations (15)-(16); the disturbance vectors (c_ϕ, c_ψ) are also constrained by the FDI attack vector c from (14).

iii) In order to avoid raising system operator suspicions, the total load shedding amount on all system buses must remain unchanged, as described by the attack constraint (17).

iv) Important limitations and assumptions on the attacker capabilities must be considered when analyzing the case studies. These assumptions are shown in Table I.

B. RSLS Scheme Advantages

The proposed RSLS has several advantages over the traditional schemes that use the swing equation. These advantages include:

i) The calculated value for the power mismatch is trusted, regardless of the existence of FDI in power flow measurements, as the proposed approach uses reliable system states to calculate it. However, the calculated value using the swing equation might be misleading if there is an FDI on frequency measurements. Therefore, UFLS schemes based on the swing equation are accurate only at the moment of disturbance. In contrast, the RSLS is able to accurately monitor the system at all times (before, during, and after a disturbance), as well as during FDI attacks. Consequently, RSLS is more robust against FDI attacks.

ii) RSLS uses a PSSE-PF module, which provides real-time monitoring for the value of power mismatch due to the fact that PSSE is used in almost all recent control centers to provide real-time monitoring of the system based on the PMUs measurements that are being sent in high resolution. Nevertheless, because of the dynamic response of governors, turbines, loads and other control elements, the validity of the swing equation output is limited and considered only at the moment of disturbance [19].

iii) The dependency on PSSE allows the proposed RSLS to have the advantages of WAMPAC schemes which utilizes system-wide data to control and provide protection to the whole system, and hence, avoid system cascading following a large disturbance.

iv) The frequency magnitude is employed in the proposed scheme to detect disturbances. Therefore, it works with

any frequency signal from the system because the frequency magnitude at different points in the system is the same, with only the ROCOF changing from point to point. On the other hand, the swing equation uses both ROCOF and the frequency of center of inertia (f_c) to calculate the mismatch. The accuracy of f_c calculation depends on the number of the available frequency measurements, with higher measurements being more accurate. Therefore, RSLS can be considered more reliable.

v) RSLS is valid for large and small systems, whereas the approaches that use the swing equation are valid only for large systems. Following a large disturbance that includes tripping of the generators or large synchronous motors, the swing equation does not give accurate results because it depends on the inertia of the system. This can be approximated, in large systems by assuming that a large percentage of the total inertia is still available. However, for small systems, an underestimation of the actual disturbance might result [6]. Therefore, the proposed scheme is more accurate for a wider range of system sizes.

vi) RSLS calculates the power mismatch, which is the amount of load to be shed directly because it monitors the system online and runs power flow at every time step. On the other hand, the swing equation calculates the magnitude of disturbance, which still requires the control center operator to find and obtain information about the available spinning reserve to decide on the amount of load shedding.

vii) In contrast with previous schemes, a significant number of frequency sensors in the grid can be removed because RSLS utilizes the Power Flow sensors that are already installed. Additionally, secured channels (such as point-to-point fiber optics links) are only to be installed to communicate the critical measurements, which might increase the cost, but enhance the security of the whole system.

VII. Conclusion

The analysis presented in this paper demonstrates how current WAUFLS protection schemes are vulnerable to FDI cyebr-attacks at various stages of the protection scheme, potentially leading to equipment damage or system-wide blackout. In this work, three FDI cyber-attack scenarios are formulated and investigated. A novel RSLS based on reliable measurements approach was proposed. A PSSE-PF model was used to calculate the total system mismatch. This model is composed of two main chained components: first, the PSSE uses PFMs and calculates reliable system states, and second, the dynamic power flow utilizes the obtained reliable system states to determine the power mismatch and, accordingly, the amount of load to shed. Consequently, the load-shedding is distributed between the buses based on the proximity to the disturbance according to their voltage dip during the disturbance. Furthermore, a data classification method is proposed to secure the operation of PSSE. Simulations compare the impacts of FDI attacks on current WAUFLS performance when employing the proposed mitigation approach on the IEEE 39-bus New England system using PSCAD/EMTDC. The results demonstrate the capability and reliability of the RSLS to protect the system during under-frequency conditions, even during an FDI cyber-attack on system measurements.

References

[1] V. Terzija et al., "Wide-area monitoring, protection, and control of future electric power networks," *Proc. IEEE*, vol. 99, no. 1, pp. 80–93, Jan. 2011.

[2] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *J. Adv. Res.*, vol. 5, no. 4, pp. 481–489, 2014.

[3] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, Jun. 2010.

[4] H. Gharavi and B. Hu, "Synchrophasor sensor networks for grid communication and protection," *Proc. IEEE*, vol. 105, no. 7, pp. 1408–1428, Jul. 2017.

[5] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[6] B. Delfino, S. Massucco, A. Morini, P. Scalera, and F. Silvestro, "Implementation and comparison of different under frequency load-shedding schemes," in *Proc. Power Eng. Soc. Summer Meeting*, vol. 1, 2001, pp. 307–312.

[7] A. Ketabi and M. H. Fini, "An underfrequency load shedding scheme for hybrid and multiarea power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 82–91, Jan. 2015.

[8] W. Liu, W. Gu, W. Sheng, X. Meng, Z. Wu, and W. Chen, "Decentralized multi-agent system-based cooperative frequency control for autonomous microgrids with communication constraints," *IEEE Trans. Sustain. Energy*, vol. 5, no. 2, pp. 446–456, Apr. 2014.

[9] S. Banijamali and T. Amraee, "Semi-adaptive setting of under frequency load shedding relays considering credible generation outage scenarios," *IEEE Trans. Power Del.*, vol. 34, no. 3, pp. 1098–1108, Jun. 2019.

[10] U. Rudez and R. Mihalic, "WAMS-based underfrequency load shedding with short-term frequency prediction," *IEEE Trans. Power Del.*, vol. 31, no. 4, pp. 1912–1920, Aug. 2016.

[11] K. Seethalekshmi, S. N. Singh, and S. C. Srivastava, "A synchrophasor assisted frequency and voltage stability based load shedding scheme for self-healing of power system," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 221–230, Jun. 2011.

[12] H. Seyedi and M. Sanaye-Pasand, "New centralised adaptive load-shedding algorithms to mitigate power system blackouts," *IET Gener. Transm. Distrib.*, vol. 3, no. 1, pp. 99–114, 2009.

[13] M. S. Pasand and H. Seyedi, "New centralized adaptive under frequency load shedding algorithms," in *Proc. Large Eng. Syst. Conf. Power Eng.*, 2007, pp. 44–48.

[14] J. Wang, H. Zhang, and Y. Zhou, "Intelligent under frequency and under voltage load shedding method based on the active participation of smart appliances," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 353–361, Jan. 2017.

[15] C. Li et al., "Continuous under-frequency load shedding scheme for power system adaptive frequency control," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 950–961, Mar. 2020.

[16] A. Rafinia, N. Rezaei, and J. Moshtagh, "Optimal design of an adaptive under-frequency load shedding scheme in smart grids considering operational uncertainties," *Int. J. Elect. Power Energy Syst.*, vol. 121, Oct. 2020, Art. no. 106137.

[17] F. Elyasichamazkoti and S. Teimourzadeh, "Secure under frequency load shedding scheme with consideration of rate of change of frequency," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, 2021, pp. 552–557.

[18] A. Rafinia, J. Moshtagh, and N. Rezaei, "Towards an enhanced power system sustainability: An MILP under-frequency load shedding scheme considering demand response resources," *Sustain. Cities Soc.*, vol. 59, Aug. 2020, Art. no. 102168.

[19] V. V. Terzija, "Adaptive underfrequency load shedding based on the magnitude of the disturbance estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1260–1266, Aug. 2006.

[20] F. Hashiesh, H. E. Mostafa, A.-R. Khatib, I. Helal, and M. M. Mansour, "An intelligent wide area synchrophasor based system for predicting and mitigating transient instabilities," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 645–652, Jun. 2012.
[21] H. Golpira, H. Bevrani, A. R. Messina, and B. Francois, "A data-driven under frequency load shedding scheme in power systems," *IEEE Trans. Power Syst.*, early access, May 3, 2022, doi: 10.1109/TPWRS.2022.3172279.
[22] M. Gautam, N. Bhusal, and M. Benidris, "A cooperative game theory-based approach to under-frequency load shedding control," in *Proc. IEEE Power Energy Soc. General Meeting (PESGM)*, 2021, pp. 1–5.
[23] M. Karimi, P. Wall, H. Mokhlis, and V. Terzija, "A new centralized adaptive underfrequency load shedding controller for microgrids based on a distribution state estimator," *IEEE Trans. Power Del.*, vol. 32, no. 1, pp. 370–380, Feb. 2017.
[24] M. G. da Silveira and P. H. Franco, "IEC 61850 network cybersecurity: Mitigating GOOSE message vulnerabilities," presented at the 6th Annu. PAC World Amer. Conf., 2019.
[25] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.
[26] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary, "A test bed dedicated to the study of vulnerabilities in IEC 61850 power utility automation networks," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2016, pp. 1–4.
[27] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
[28] M. Khalaf, A. Hooshyar, and E. El-Saadany, "On false data injection in wide area protection schemes," in *Proc. IEEE Power Energy Soc. General Meeting (PESGM)*, 2018, pp. 1–5.
[29] J. Duan and M.-Y. Chow, "Data integrity attack on consensus-based load shedding algorithm for power systems," in *Proc. IECON 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, 2017, pp. 7641–7646.
[30] A. Ayad, M. Khalaf, and E. F. El-Saadany, "Cyber-physical security of state estimation against attacks on wide-area load shedding protection schemes," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, 2019, pp. 1–5.
[31] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*, vol. 7. New York, NY USA: McGraw-Hill, 1994.
[32] H. Karimi, M. Karimi-Ghartemani, and M. R. Iravani, "Estimation of frequency and its rate of change for applications in power systems," *IEEE Trans. Power Del.*, vol. 19, no. 2, pp. 472–480, Apr. 2004.
[33] R. Małkowski and J. Nieznański, "Underfrequency load shedding: An innovative algorithm based on fuzzy logic," *Energies*, vol. 13, no. 6, p. 1456, 2020.
[34] S. Azizi, M. Sun, G. Liu, and V. Terzija, "Local frequency-based estimation of the rate of change of frequency of the center of inertia," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4948–4951, Nov. 2020.
[35] R. Horri and H. M. Roudsari, "Adaptive under-frequency load-shedding considering load dynamics and post corrective actions to prevent voltage instability," *Electr. Power Syst. Res.*, vol. 185, Aug. 2020, Art. no. 106366.
[36] J. Jallad, S. Mekhilef, H. Mokhlis, and J. A. Laghari, "Improved UFLS with consideration of power deficit during shedding process and flexible load selection," *IET Renew. Power Gener.*, vol. 12, no. 5, pp. 565–575, 2018.
[37] Y. Zhang et al., "Wide-area frequency monitoring network (FNET) architecture and applications," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 159–167, Sep. 2010.
[38] T. Shekari, F. Aminifar, and M. Sanaye-Pasand, "An analytical adaptive load shedding scheme against severe combinational disturbances," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4135–4143, Sep. 2016.
[39] M. Abedini, M. Sanaye-Pasand, and S. Azizi, "Adaptive load shedding scheme to preserve the power system stability following large disturbances," *IET Gener. Transm. Distrib.*, vol. 8, no. 12, pp. 2124–2133, 2014.
[40] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 223–232, Jan. 2015.
[41] A. M. Khalil and R. Iravani, "A dynamic coherency identification method based on frequency deviation signals," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 1779–1787, May 2016.
[42] A. Ayad, H. Farag, A. Youssef, and E. El-Saadany, "Cyber–physical attacks on power distribution systems," *IET Cyber Phys. Syst. Theory Appl.*, vol. 5, no. 2, pp. 218–225, 2020.
[43] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[44] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.
[45] M. S. Sachdev and T. K. P. Medicherla, "A second order load flow technique," *IEEE Trans. Power App. Syst.*, vol. PAS-96, no. 1, pp. 189–197, Jan. 1977.
[46] *IEEE Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration*, IEEE Standard C37.117-2007, Aug. 2007.
[47] P. Lü, J. Zhao, J. Yao, and S. Yang, "A decentralized approach for frequency control and economic dispatch in smart grids," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 3, pp. 447–458, Sep. 2017.
[48] B. Hoseinzadeh, F. M. F. Da Silva, and C. L. Bak, "Adaptive tuning of frequency thresholds using voltage drop data in decentralized load shedding," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2055–2062, Jul. 2015.
[49] A. Pai, *Energy Function Analysis for Power System Stability*. New York, NY, USA: Springer, 1989.

Mohsen Khalaf (Member, IEEE) was born in Asyut, Egypt, in 1990. He received the B.Sc. and M.Sc. degrees in electrical engineering from Assiut University, Asyut, in 2012 and 2015, respectively, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2020. He is currently a Postdoctoral Fellow with the University of Toronto, Toronto, ON, Canada, working in collaboration with Hydro Quebec, Montreal, QC, Canada, to identify power systems vulnerabilities against cyberattackers. He is also an Assistant Professor with Assiut University. His research interests include smart grids monitoring, protection and control, distributed generation, and cyber-physical security of power systems. He is a Registered Engineer at the Egyptian Syndicate of Engineering in Egypt and Engineer-in-Training in the Province of Ontario, Canada.

Abdelrahman Ayad (Graduate Student Member, IEEE) received the B.Sc. degree in electrical power engineering from Alexandria University, Alexandria, Egypt, in 2016, and the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with McGill University, Montreal, QC, Canada. He is also a Research Assistant with the Renewable Energy Integration Group, CanmetEnergy, Natural Resources Canada, Varennes, QC, Canada. His main research interests include low-carbon energy systems long-term planning, large scale renewable energy resources integration, and the applications of machine learning in modern energy systems. In 2021, he was the recipient of the Natural Sciences and Engineering Research Council Alexander Graham Bell Canada Graduate Scholarship-Doctoral and the Fonds de recherche du Québec-Nature et technologies Doctoral Scholarship.

Magdy M. A. Salama (Life Fellow, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Cairo University, Cairo, Egypt, in 1971 and 1973, respectively, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 1977, where he is currently a Professor with the Department of Electrical and Computer Engineering. His research interests include the planning, operation and control of distribution systems, smart microgrids, power-quality monitoring and mitigation, asset management, and electromagnetics. He has consulted widely with governmental agencies and the electrical industry. He is a Registered Professional Engineer in the Province of Ontario, Canada.

Deepa Kundur (Fellow, IEEE) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto in 1993, 1995, and 1999, respectively.

She is a Professor and the Chair of The Edward S. Rogers Sr. Department of Electrical and Computer Engineering with the University of Toronto. She is an author of over 200 journal and conference papers and is a recognized authority on cybersecurity issues. Her research interests lie at the interface of cybersecurity, signal processing and complex dynamical networks.

Prof. Kundur has been the recipient of Teaching Awards at both the University of Toronto and Texas A&M University. She has served as the Honorary Chair of the 2021 IEEE Electric Power and Energy Conference and as the General Chair of 2021 International Conference on Smart Grids for Smart Cities. She has served in numerous conference executive organization roles, including as the Publicity Chair for ICASSP 2021, the Track Chair for the 2020 IEEE International Conference on Autonomous Systems, the General Chair of the 2018 GlobalSIP Symposium on Information Processing, Learning and Optimization for Smart Energy Infrastructures, and the TPC Co-Chair for IEEE SmartGridComm 2018. Her research has received the best paper recognitions at numerous venues, including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She is a Fellow of the Canadian Academy of Engineering and a Senior Fellow of Massey College.

Ehab F. El-Saadany (Fellow, IEEE) was born in Cairo, Egypt, in 1964. He received the B.Sc. and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, in 1986 and 1990, respectively, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 1998.

He was a Professor with the ECE Department, University of Waterloo till 2019, where he was the Director of the Power M.Eng. Program from 2010 and 2015. He is currently a Professor with the Department of Electrical Engineering and Computer Science and the Director of the Advanced Power and Energy Research Center, Khalifa University, UAE. He has graduated 30 Ph.D. and 22 M.Sc. students and published 450+ international journal and conference papers in addition to 3 U.S. patents. He is an Internationally recognized expert in the area of sustainable energy integration and smart distribution systems. He is an internationally recognized expert in Distribution Systems with Scopus H-Index 66 and over 17 300 citations. His research interests include smart grid operation and control, microgrids, self-healing, cyber-physical security of smart grids, protection, power quality, embedded generation and transportation electrification.

Dr. El-Saadany is a two-time recipient of Canada Research Chair Award in Energy Systems from 2009 to 2014 and Smart Distribution Systems from 2014 to 2018. He is the recipient of the Mission Innovation Champion Award in 2020 and the Prestigious Khalifa Award in 2021. He is an Editor of the IEEE TRANSACTIONS ON SMART GRID, the IEEE TRANSACTIONS ON POWER SYSTEMS, and the IEEE POWER SYSTEMS LETTERS. He is a Registered Professional Engineer in the Province of Ontario. He is an IEEE Fellow for his contributions in distributed generation planning, operation and control.