Model-Measurement Data Integrity Attacks

Gang Cheng, *Graduate Student Member, IEEE*, Yuzhang Lin, *Member, IEEE*, Jun Yan, *Member, IEEE*, Junbo Zhao, *Senior Member, IEEE*, and Linquan Bai, *Senior Member, IEEE*

***Abstract*—The vulnerabilities of information and communication technology (ICT) infrastructures leave room for cyber attacks threatening the reliable operations of power systems. Based on the real-world evidence of the Ukraine power grid attack and the popular technical discussion that cyber attacks could be launched at the control-center level, this paper reveals a new attack strategy: model-measurement data integrity (MMI) attack. Instead of compromising measurements only, we investigate the possibility where network parameters are coordinately manipulated when constructing false data injection attack (FDIA) vectors. Furthermore, we model cyber adversaries' possible behavior of co-planning the manipulated measurement channels and parameter attack vectors prior to the launch of FDIAs. The revealed MMI attack strategy allows a drastic reduction of measurement channels to compromise in run-time for keeping the stealth property. Simulations in the IEEE 14-bus test system and the IEEE 118-bus test system demonstrate the feasibility of the revealed MMI attack strategy.**

***Index Terms*—Cyber security, false data injection attack, network parameter, optimization, power system modeling, state estimation.**

I. Introduction

STATE estimation (SE) plays an essential role in power system monitoring and control by providing real-time situational awareness to support various advanced applications. The measurement data utilized in SE are typically gathered from the supervisory control and data acquisition (SCADA) system or phasor measurement units (PMUs), whose supporting information and communications technology (ICT) infrastructures are vulnerable to a variety of cyber attacks [1], [2]. Adversaries may temper the readings of meters [3], manipulate the substation networks [4], or even hack into the control center [5], [6] to falsify the information technology (IT) software or databases [7] and mislead the SE function. Possible consequences introduced by cyber attacks may include the falsification of locational marginal prices (LMPs) [8], [9], malfunctions of safety and stability control systems [10], [11], or even blackouts of power systems [12], [13].

As a major type of cyber attacks against power system SE, data integrity attacks, also known as false data injection attacks (FDIAs), were first proposed by Liu et al. [14]. Successful FDIAs have two critical characteristics: *stealth* and *sparsity*. *Stealth* implies that the injected false data can mislead SE without being detected by the conventional residual-based bad data detection (BDD) methods [15]. *Sparsity* implies that false data should be injected into the fewest measurement channels to reduce the required attack resources and the risk of detection [16].

Numerous studies have been carried out regarding the construction of stealthy and sparse FDIAs. For example, [16] proposes two security indices by exploiting the l_0- and l_1-norm to investigate the *sparsity* of FDIAs. The smallest set of attacked meters [17] and an attack subgraph [18] are determined for stealthy FDIAs with the least effort by exploring the graph theory. In [19], two typical attack scenarios, i.e., random and targeted attacks, are studied. Cyber attacks against PMUs and an optimal restoration strategy are investigated in [20]. Unlike the attack strategies in [16], [17], [18], [19], [20], where accurate and complete network information is assumed to be known for attackers, FDIAs with incomplete network information have also been widely studied. In [21], the feasibility of constructing perfect and imperfect FDIAs with incomplete network information is verified. Local attack strategies are proposed in [22], [23]. The uncertainties and upper bounds of successful FDIAs with incomplete network information are analyzed in [24].

As reviewed above, FDIA strategies involving the manipulations of measurement data have been widely investigated. These data are collected at substations and transmitted across wide-area networks (WANs) with a large surface for attacks. Recently, the manipulation and exploitation of databases at the control-center level have received increasing attention. Compared to the substation-level measurement data, databases at the control center are well-protected and more challenging to access. Nevertheless, adversaries still have the chance to intrude into the industrial control system (ICS) network to wrest the control authority, temper the human-machine interface (HMI), and forge the databases [25]. Moreover, malicious employees can implement *insider attacks* with less effort because they have intimate knowledge of the entire power system and the authority to access the databases [26], [27]. The possibility of control-center-level attacks has been verified by the real-world event of the Ukrainian power grid attack

Manuscript received 23 June 2022; revised 5 October 2022 and 24 January 2023; accepted 1 March 2023. Date of publication 7 March 2023; date of current version 23 October 2023. This work was supported by the National Science Foundation (NSF) Award under Grant 1947617. Paper no. TSG-00899-2022. *(Corresponding author: Yuzhang Lin.)*

Gang Cheng and Yuzhang Lin are with the Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA 01854 USA (e-mail: gang_cheng@student.uml.edu; yuzhang_lin@uml.edu).

Jun Yan is with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada (e-mail: jun.yan@concordia.ca).

Junbo Zhao is with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: junbo@uconn.edu).

Linquan Bai is with the Department of Systems Engineering and Engineering Management, University of North Carolina at Charlotte, Charlotte, NC 28223 USA (e-mail: linquanbai@uncc.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2023.3253781.

Digital Object Identifier 10.1109/TSG.2023.3253781

in December 2015 [5], [6], where adversaries hacked into the information and operational networks and manipulated data in the control center. Apart from this event, many other cyber-attack incidents have also been reported and summarized in [28], [29], demonstrating cyber adversaries' possible capability to intrude into well-protected control center networks and falsify data. In view of such realistic threats, a significant volume of literature has investigated attack models at the control-center level. A transmission line rating attack to manipulate nodal prices in real-time markets is studied in [30]. A cyber attack against load forecasting [31] is investigated to misguide operators to make unsuitable decisions for electricity delivery. A cyber-vulnerability analysis model is developed in [32], where the attack paths include unit bids, generation capacities, and line ratings. Cyber attacks against critical network parameters are investigated in [33] to gain unlawful benefits from electricity markets.

Meanwhile, network parameters play a critical role in SE and other energy management system (EMS) applications. Although they are stored at control center networks, their vulnerability to outsider and insider FDIAs cannot be overlooked for the following reasons. 1) While stealthy *measurement* FDIAs require simultaneous tempering of multiple meters of communication links deployed in different locations, *parameter* FDIAs can be launched as long as cyber adversaries acquire the credentials to model databases. 2) Network *parameters* only need to be modified once to exert permanent impacts, which could be done whenever the cyber adversaries are most ready. On the contrary, to launch a *measurement* FDIA, measurement data streams have to be manipulated continuously in run-time. 3) While *measurement* FDIAs can only affect online EMS applications, *parameter* FDIAs can affect both online and offline applications, yielding a wider range of impact. Therefore, *parameter* FDIAs could be rather advantageous for cyber adversaries under certain circumstances.

Although preliminary studies on *parameter* FDIAs have been reported recently [33], [34], [35], [36], several major issues remain to be addressed. 1) Existing works only focus on specific types of parameters (e.g., critical parameters in [33] and transformer tap ratios and phase-shift angles in [34]), and there lacks a general framework for modeling *parameter* FDIAs. 2) The different characteristics of *parameter* FDIAs (one-time and offline implementation) and *measurement* FDIAs (continuous and real-time implementation) have not been considered or coordinated. 3) The sparsity of attack vectors has not been fully optimized since the l_1-norm optimization problem has not been fully adjusted to ensure sparsity and the change of measurement channels due to operating point variation during FDIA has not been considered.

This paper develops a general framework to cover network parameter FDIAs, measurement FDIAs, and their coordination in the context of AC SE, namely model-measurement data integrity (MMI) FDIA. Compared with the existing literature, the unique contributions of the proposed framework are as follows.

1) A generic attack model that covers all types of network parameters and measurements is proposed. It is observed that by strategic injection of false parameters into the model database, attackers can drastically reduce the number of measurement channels to be compromised.

2) Based on the fact that network parameters only need to be manipulated *once* and measurement streams need to be *continuously* manipulated in *run-time*, a two-stage coordinated attack framework is proposed. The *pre-attack* stage determines false parameter vectors and the set of measurement channels to be manipulated offline, and the *run-time-attack* stage determines the false measurement vectors for each measurement snapshot online. This framework better mimics attackers' behaviors of planning and preparing for attacks in advance.

3) An adaptive group basis pursuit (AGBP) optimization algorithm is developed to enhance the *sparsity* of compromised measurement channels. The weight adaptation scheme for the regularization terms leads to the *oracle property* with sparser solutions than existing l_1-regularization-based FDIA algorithms.

The rest of this paper is organized as follows. Section II reviews the basics of SE, BDD, and FDIAs in AC SE. Section III provides an overview of the proposed MMI FDIA framework. Section IV details the *pre-attack* and *run-time-attack* procedures. Section V presents the weight adaptation scheme to enhance the attack *sparsity*. Section VI presents the solution algorithm of the developed optimization formulation. Section VII demonstrates the effectiveness of the developed framework via simulations. Section VIII concludes the paper.

II. Preliminaries

A. Power System State Estimation

In the AC-based SE, the relationship between measurements and state variables can be expressed as follows [37]:

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e}, \tag{1}$$

where $\boldsymbol{z} \in \mathbb{R}^{m\times 1}$ is the measurement vector; m is the number of measurement channels; $\boldsymbol{x} \in \mathbb{R}^{n\times 1}$ is the state variable vector; n is the number of state variables; $\boldsymbol{h}(\cdot)$ is the function relating $\boldsymbol{x}$ to $\boldsymbol{z}$; and $\boldsymbol{e} \in \mathbb{R}^{m\times 1}$ is the measurement error vector. It is assumed that measurement errors follow Gaussian distributions with zero mean and covariance matrix $\boldsymbol{R} \in \mathbb{R}^{m\times m}$, i.e., $\boldsymbol{e} \sim \boldsymbol{N}(\boldsymbol{0}, \boldsymbol{R})$.

The most common weighted least squares (WLS) SE is constructed as:

$$\min_{\hat{\boldsymbol{x}}} \boldsymbol{J}(\boldsymbol{x}) = [z - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [z - \boldsymbol{h}(\boldsymbol{x})], \tag{2}$$

where $\hat{\boldsymbol{x}} \in \mathbb{R}^{n\times 1}$ is the vector of state estimates and $\boldsymbol{J}(\cdot)$ is the objection function based on the WLS criterion. The Gauss-Newton algorithm [37] is used to solve the WLS problem (2).

B. Bad Data Detection Methods

The Chi-square test and the largest normalized residual (LNR) test are the most widely used BDD methods in WLS SE. The Chi-square test detects bad data by comparing the objective function value, i.e., $\boldsymbol{J}(\hat{\boldsymbol{x}})$, with a threshold $\chi^2_{(m-n),\zeta}$ with a confidence level ζ and $(m\text{-}n)$ degrees of freedom. If $\boldsymbol{J}(\hat{\boldsymbol{x}}) \geq \chi^2_{(m-n),\zeta}$, bad data will be suspected.

The LNR test is a more accurate method for BDD. It is devised by using the normalized residuals,

$$r_i^N = \frac{|r_i|}{\sqrt{\Omega_{ii}}} = \frac{\left|z_i - h_i(\hat{\boldsymbol{x}})\right|}{\sqrt{\Omega_{ii}}}, \tag{3}$$

$$\boldsymbol{\Omega} = \left[\boldsymbol{I}_m - \boldsymbol{H}\left(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\right]\boldsymbol{R}, \tag{4}$$

where i is the index of a measurement; $\boldsymbol{I}_m \in \mathbb{R}^{m\times m}$ is an identity matrix. If the LNR is larger than a set threshold, the corresponding measurement will be suspected as bad data.

The Chi-square test and the LNR test are residual-based methods. Generally, bad data can be detected only when it induces large measurement residuals in SE. To bypass the residual-based detection methods, the malicious false data must be deliberately designed to achieve the *stealth* property.

C. False Data Injection Attacks in AC SE

An AC-based measurement FDIA can be designed to stealthily mislead SE by the following criterion [15],

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}), \tag{5}$$

where $\boldsymbol{a}$ represents the measurement attack vector; $\hat{\boldsymbol{x}}$ is the state estimates in the absence of FDIAs; $\boldsymbol{c}$ is a bias vector superposed onto state estimates. The manipulated measurements will be $z_{\boldsymbol{a}} = z + \boldsymbol{a}$, resulting in measurement residuals as follows:

$$\begin{aligned} \boldsymbol{r}_a &= z_a - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) = z + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= z + \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= z - \boldsymbol{h}(\hat{\boldsymbol{x}}) = \boldsymbol{r}, \end{aligned} \tag{6}$$

where $\boldsymbol{r}_a$ represents the measurement residual vector in the presence of FDIAs. Therefore, the false measurements, i.e., z_a, will not be detected by conventional residual-based BDD methods. In addition to the *stealth* property, attackers also wish to launch an FDIA by manipulating the minimal number of measurements as either part of the meters are well protected or the attack budget is limited [38], [39]. This is translated into an l_0 optimization problem [16]:

$$\begin{aligned} \min_{\boldsymbol{a}} \quad & \|\boldsymbol{a}\|_0 \\ s.t. \quad & \boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \\ & a_o = 1, \ \forall o \in \Upsilon, \end{aligned} \tag{7}$$

where a_o represents that the attack target is to manipulate the oth measurement channel by one per unit; Υ denotes the set of measurement channels as attack targets.

However, there are two issues with using the l_0-norm. 1) Problem (7) is non-convex and generally difficult to solve; 2) The entries in solution vector $\boldsymbol{a}$ based on the l_0 optimization may be extremely large, resulting in a divergence issue [16]. Therefore, l_1 optimization is used to construct the AC-based FDIAs:

$$\begin{aligned} \min_{\boldsymbol{a}} \quad & \|\boldsymbol{a}\|_1 \\ s.t. \quad & \boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \\ & a_o = 1, \ \forall o \in \Upsilon. \end{aligned} \tag{8}$$

The l_1-norm can achieve a compromise between the *sparsity* and the magnitudes of the attack vector $\boldsymbol{a}$. Moreover, the solution to problem (8) can be transformed into the solution to a successive set of linear programming (LP) problems, which can be efficiently solved by existing methods [40].

Limitations: The above FDIA strategy only involves the manipulation of measurement data and does not consider the vulnerability of network parameters. In addition, the measurement attack vectors are optimized snapshot by snapshot independently. As the system operating point varies, the measurement channels to be manipulated in different snapshots may be different, resulting in a large number of channels to be manipulated over the entire course of FDIAs. Furthermore, attackers do not know which measurement channels should be manipulated until they obtain the measurement data and solve (8) during the attack; thus, they cannot prepare for intrusion into measurement channels in advance. Finally, the *sparsity* may not be optimally achieved as various quantities may be in different scales yet are given uniform weights in the objective function.

III. Framework of Proposed Attack Strategy

In this section, the framework of the proposed MMI attack strategy will be presented. It consists of two parts: the *pre-attack* stage and the *run-time-attack* stage. The *pre-attack* stage is an offline attack planning stage that can occur over a long period, i.e., weeks to months. It represents the attackers' activities to prepare for the implementation of the attacks. In this stage, attackers aim to determine the set of measurement channels to compromise and the set of parameters to falsify by exploiting historical state estimates. Based on this, they can begin breaching the target measurement channels and manipulating the target network parameters when opportunities arise. On the other hand, the *run-time-attack* stage refers to a relatively much shorter online attack stage that lasts minutes to hours. It represents the attackers' activities to manipulate real-time measurement streams to achieve their goals, e.g., gaining financial profits or inflicting damages to the power system. The *run-time-attack* stage is performed based on the outcomes of the *pre-attack* stage, i.e., the compromised measurement channels and falsified parameter data. It obtains the *current* state estimate and determines the falsified measurement values to be injected at every instant in the *attack interval*. The proposed two-stage MMI FDIA framework is shown in Fig. 1.

It should be noted that the MMI attack model assumes that the adversaries have some means to access the control center network, but this does not imply that they have unlimited capabilities or resources. As a result, a minimization of attack effort is still critically needed by the adversaries for the following reasons: 1) Limited opportunities to launch FDIAs for insider attackers. Although malicious employees have intimate knowledge of the entire power system and the authority to access the databases, the opportunities of launching insider attacks are still restricted. For example, opportunities will arise only when malicious employees are on duty in the control center. The time window for implementing the attack is limited, and the time required to implement the attack is related to

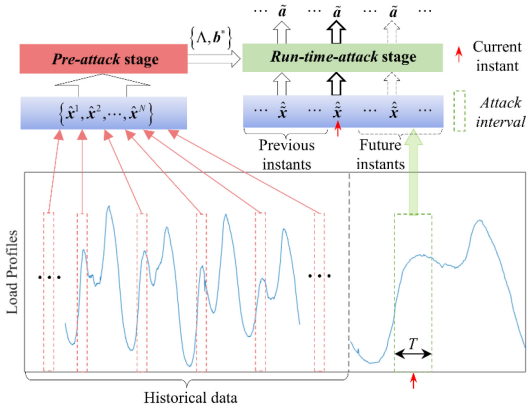

Fig. 1. Data sampling scheme and framework of the proposed paradigm.

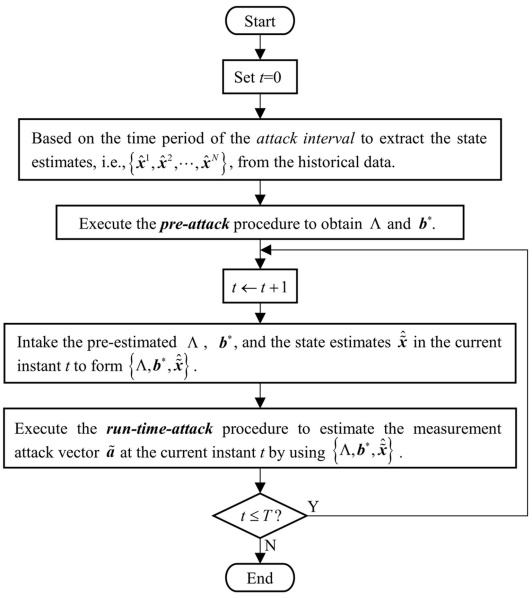

Fig. 2. A high-level framework of the proposed MMI attack strategy.

the number of network parameters to manipulate. 2) Risk of detection. In control centers, simultaneous changes of a large number of network parameters appear suspicious and could quickly draw the attention of operators. Hence, to reduce the risk to be detected, attackers desire to minimize the number of parameters to manipulate in the database. 3) Limited access to meters. Measurement falsification is non-trivial as well. Measurement data must be manipulated in a live streaming fashion. Therefore, even attackers that have access to the control center network do not have unlimited capability to falsify arbitararily many measurements as they desire. Hence, they are likely to implement a model that minimizes the number of measurement channels.

According to Eq. (8), the measurement attack vector $\boldsymbol{a}$ is related to $\hat{\boldsymbol{x}}$, $\boldsymbol{h}(\cdot)$, and a_o. In transmission systems, the daily load profiles have strong regularities [41], and the parameters and topologies do not change frequently [42]. For instance, a few days' load profiles of ISO New England [43] are presented in Fig. 1. Consequently, if attackers plan to launch FDIAs in a given interval, they can collect enormous historical data with similar patterns to help plan the attack, i.e., determining the measurement channels to compromise and the parameter data to falsify. This motivates the *pre-attack* stage of the proposed framework. When the actual attack is carried out, attackers only need to manipulate the pre-determined set of measurement channels, as described by the *run-time-attack* stage.

Define the span of the *run-time-attack* stage as the *attack interval*. Let $\{\hat{\boldsymbol{x}}^1, \hat{\boldsymbol{x}}^2, \ldots, \hat{\boldsymbol{x}}^N\}$ represent the set of state estimates from historical data, where N is the number of snapshots. In order to represent the trend of power flows in the *attack interval*, in the *pre-attack* procedure, enormous snapshots of data are collected from similar historical days. The pattern of power flows is impacted by a variety of factors. To ensure that the pre-selected measurement channels and network parameters are most effective for the *run-time-attack* stage, the time interval of historical data used in the *pre-attack* stage should be similar to the targeted *run-time-attack* interval in the following aspects: time of day, day of week, season of year, weather condition, holidays, etc., to ensure that the power flow patterns of historical data are as similar to those in the targeted *run-time-attack* interval to the greatest extent. The data sampling scheme is shown in Fig. 1. Let Λ and $\boldsymbol{b}^*$ represent the set of measurement channels for intrusion and the parameter attack vector, respectively, both determined in the *pre-attack* stage. Let $\hat{\tilde{\boldsymbol{x}}}$ and $\tilde{\boldsymbol{a}}$ represent state estimate vector and the measurement attack vector in the *run-time-attack* stage, respectively. A high-level framework of the proposed MMI attack strategy is presented in Fig. 2, where T represents the length of the *attack interval*.

IV. Attack Problem Formulation

In Section III, the high-level framework of the proposed MMI FDIA strategy has been discussed. In this section, the mathematical problem formulations of both the *pre-attack* and the *run-time-attack* strategies will be presented in detail.

The following measurement equations with network parameters explicitly shown will be used:

$$\boldsymbol{z} = \boldsymbol{h}_p(\boldsymbol{x}, \boldsymbol{p}) + \boldsymbol{e}, \tag{9}$$

where $\boldsymbol{p} \in \mathbb{R}^{s\times 1}$ is the network parameter vector; s is the number of network parameters; $\boldsymbol{h}_p(\cdot)$ is the nonlinear function relating $\boldsymbol{x}$ and $\boldsymbol{p}$ to $\boldsymbol{z}$. The stealthy MMI FDIA condition with both the measurement attack vector $\boldsymbol{a} \in \mathbb{R}^{m\times 1}$ and the parameter attack vector $\boldsymbol{b} \in \mathbb{R}^{s\times 1}$ is given by:

$$\boldsymbol{a} = \boldsymbol{h}_p(\hat{\boldsymbol{x}} + \boldsymbol{c}, \boldsymbol{p} + \boldsymbol{b}) - \boldsymbol{h}_p(\hat{\boldsymbol{x}}, \boldsymbol{p}). \tag{10}$$

A. Determination of Compromised Measurement Channels and Parameter Attack Vector in the Pre-Attack Stage

In the *pre-attack* stage, the cyber adversaries aim to identify the set of measurement channels to compromise and determine the network parameters to falsify based on historical measurement data. Four points below are to be noted.

1) The primary objectives are to keep the attack stealthy and to minimize the number of measurement channels to compromise. The coordinated manipulation of network parameters will help reduce the number of measurement channels to compromise.

2) The number of falsified parameters is also to be minimized, but it is of secondary importance. The reason is that once the cyber adversaries access the network parameter database, increasing the number of falsified parameters does not cost as much as increasing the number of compromised measurement channels.

3) If the attack targets (i.e., variables that attackers aim to manipulate) are not wide-spread, only local measurements and network parameters need to be obtained and manipulated by attackers, and there is no need to obtain complete information of the grid [21].

4) The result should satisfy the *stealthy* property under various operating points, so multiple measurement snapshots that cover the range of possible operating points when the run-time attack is launched should be incorporated into the problem.

Based on the above rationales, the *pre-attack* stage is formulated into an AGBP problem as given below,

$$\begin{aligned}\left[\hat{\boldsymbol{a}},\hat{\boldsymbol{b}},\hat{\boldsymbol{c}}\right] = \underset{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}}{\operatorname{argmin}} \ & \sum_{i=1}^{m+s+1} w_i\|\boldsymbol{M}_i\|_2 \\ s.t. \ & \boldsymbol{a} = \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}+\boldsymbol{c},\boldsymbol{p}+\boldsymbol{b}\right)-\boldsymbol{h}_p\left(\hat{\boldsymbol{x}},\boldsymbol{p}\right) \\ & a_o = \widehat{a}, \ \forall o \in \Upsilon \\ & \underline{\boldsymbol{p}} \le \boldsymbol{b} \le \bar{\boldsymbol{p}}, \end{aligned} \tag{11}$$

where $\boldsymbol{M}_i$ is the ith group in vector $\boldsymbol{M}$; w_i is the weight of the ith group; $\widehat{a}$ is the target value of variables to be manipulated; $\underline{\boldsymbol{p}}$ and $\bar{\boldsymbol{p}}$ represent the plausible lower and upper bounds of the parameter attack vector $\boldsymbol{b}$, respectively. The symbol "hat" is used to denote an estimated value. Noticeably, the inequality constraints enable a customized parameter attack vector with respect to quantities and types. If some parameters cannot be modified, one should simply set $\underline{p} = \bar{p} = 0$ for these parameters.

The developed AGBP problem sparsifies the variables in the objective function in a *group* manner. It puts the measurement attack values in different snapshots but of the same channel into the same group, each network parameter attack value into an individual group, and all state biases into one group. As such, the vector $\boldsymbol{M}$ can be expressed as,

$$\boldsymbol{M}_i = \begin{cases} \left[a_i^1,\ldots,a_i^j,\ldots,a_i^N\right]^T, & i \in \{1,2,\ldots,m\} \\ b_{i-m}, & i \in \{m+1,\ldots,m+s\} \\ \left[\left(\boldsymbol{c}^1\right)^T,\ldots,\left(\boldsymbol{c}^j\right)^T,\ldots,\left(\boldsymbol{c}^N\right)^T\right]^T, & i = m+s+1, \end{cases} \tag{12}$$

where a_i^j represents the measurement attack value of the ith channels in the jth snapshot; N is the number of measurement snapshots; $\boldsymbol{c}^j \in \mathbb{R}^{n\times 1}$ is the state bias vector for the jth snapshot. The formulation will lead to 1) minimization of the number of measurement channels (instead of the number of measurement data points) to compromise; 2) minimization of the number of network parameters to falsify; and 3) no sparsification of the state bias vector, as it does not cost attack resources. It should be noted that measurement data points and measurement channels are essentially different. A measurement data point refers to the measured value of a physical variable in an individual snapshot. A measurement channel refers to the sensing and communication resources dedicated to collecting measurement data points associated with a physical variable. The developed AGBP problem aims to achieve the optimal sparsity of attacked measurement channels instead of measurement data points, and it tends to enforce the attacked measurement data points to stay in the same set of measurement channels (attacked channels).

The setting of weight w_i in the objective function is a key task for enhancing *sparsity* in AGBP. This problem will be discussed in Section V.

In measurement FDIA model (8), the conditions for having feasible solutions satisfying the stealth constraint (5) have been analyzed and demonstrated [1], [14], [16], [24], [38]. In our developed MMI FDIA model, a higher degree of freedom is provided to the adversary, as they can manipulate not only measurements or also model parameters. In this case, it is even easier to find a feasible solution to (11) satisfy the stealth constraint (10), and all the conditions for existence of solutions derived for pure measurement FDIAs (e.g., [1], [14], [16], [24], and [38]) are *sufficient* conditions for the existence of solutions for the proposed MMI FDIA. A simple example is that any measurement attack vector $\boldsymbol{a}$ generated from a pure measurement FDIA (e.g., [1], [14], [16], [24], and [38]) is a solution to the proposed MMI FDIA by setting the parameter attack vector $\boldsymbol{b}$ to zero.

As the MMI FDIAs are developed based on the nonlinear AC power flow models, the AGBP problem (11) cannot be readily solved. Expanding the nonlinear function $\boldsymbol{h}_p(\hat{\boldsymbol{x}}+\boldsymbol{c},\boldsymbol{p}+\boldsymbol{b})$ into its Taylor series around $\boldsymbol{b}^k$ and $\boldsymbol{c}^k$ and neglecting the higher order terms, the nonlinear AGBP problem can be transformed into a successive set of linearized problems and solved iteratively. In this paper, the initial guesses of $\boldsymbol{b}$ and $\boldsymbol{c}$ are set to zero. At the kth iteration, the linearization yields,

$$\boldsymbol{a}^k = \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}+\boldsymbol{c}^k,\boldsymbol{p}+\boldsymbol{b}^k\right)+\boldsymbol{H}_p^k\Delta\boldsymbol{b}^k+\boldsymbol{H}_x^k\Delta\boldsymbol{c}^k-\boldsymbol{h}_p\left(\hat{\boldsymbol{x}},\boldsymbol{p}\right), \tag{13}$$

where k is an index of iteration; $\Delta\boldsymbol{b}^k$ and $\Delta\boldsymbol{c}^k$ represent the update values; $\boldsymbol{H}_p^k = \partial\boldsymbol{h}_p/\partial\boldsymbol{p}|_{\boldsymbol{b}=\boldsymbol{b}^k,\boldsymbol{c}=\boldsymbol{c}^k}$; and $\boldsymbol{H}_x^k = \partial\boldsymbol{h}_p/\partial\boldsymbol{x}|_{\boldsymbol{b}=\boldsymbol{b}^k,\boldsymbol{c}=\boldsymbol{c}^k}$.

The kth iteration of the AGBP problem (11) can be written in compact form as follows:

$$\begin{aligned}\left[\hat{\boldsymbol{a}},\Delta\hat{\boldsymbol{b}},\Delta\hat{\boldsymbol{c}}\right] = \underset{\boldsymbol{a},\Delta\boldsymbol{b},\Delta\boldsymbol{c}}{\arg\min} \ & \sum_{i=1}^{m+s+1} w_i\left\|\Delta\boldsymbol{M}_i^k\right\|_2 \\ s.t. \ & \boldsymbol{L}^k\Delta\boldsymbol{M}^k = \boldsymbol{Q}^k \\ & \underline{\boldsymbol{p}} \le \boldsymbol{b}^k+\Delta\boldsymbol{b}^k \le \bar{\boldsymbol{p}}, \end{aligned} \tag{14}$$

where

$$\Delta\boldsymbol{M}_i^k = \begin{cases} \left[a_i^{1,k},\ldots,a_i^{j,k},\ldots,a_i^{N,k}\right]^T, & i \in \{1,2,\ldots,m\} \\ \Delta b_{i-m}^k, & i \in \{m+1,\ldots,m+s\} \\ \left[\left(\Delta\boldsymbol{c}^{1,k}\right)^T,\ldots,\left(\Delta\boldsymbol{c}^{j,k}\right)^T,\ldots,\left(\Delta\boldsymbol{c}^{N,k}\right)^T\right]^T, & i = m+n+1, \end{cases} \tag{15}$$

$$\boldsymbol{L}^k = \begin{bmatrix} \mathfrak{I}^1 & -\boldsymbol{H}_p^{1,k} & -\boldsymbol{H}_x^{1,k} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathfrak{I}^2 & -\boldsymbol{H}_p^{2,k} & \mathbf{0} & -\boldsymbol{H}_x^{2,k} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathfrak{I}^N & -\boldsymbol{H}_p^{N,k} & \mathbf{0} & \mathbf{0} & \cdots & -\boldsymbol{H}_x^{N,k} \\ \widehat{\mathfrak{I}} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}, \tag{16}$$

$$\boldsymbol{Q}^k = \begin{bmatrix} \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^1 + \boldsymbol{c}^{1,k}, \boldsymbol{p} + \boldsymbol{b}^k\right) - \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^1, \boldsymbol{p}\right) \\ \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^2 + \boldsymbol{c}^{2,k}, \boldsymbol{p} + \boldsymbol{b}^k\right) - \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^2, \boldsymbol{p}\right) \\ \vdots \\ \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^N + \boldsymbol{c}^{N,k}, \boldsymbol{p} + \boldsymbol{b}^k\right) - \boldsymbol{h}_p\left(\hat{\boldsymbol{x}}^N, \boldsymbol{p}\right) \\ \widehat{\boldsymbol{a}} \end{bmatrix}, \tag{17}$$

where the binary matrix $\mathfrak{I}^j \in \mathbb{R}^{m\times(m\cdot N)}$ extracts the measurement attack vector $\boldsymbol{a}^j$ from $\boldsymbol{M}$, where only the $(i, j{+}(i{-}1){\times}N)$th entries ($i = 1,\ldots,m$, and $j = 1,\ldots,N$) are 1; the binary matrix $\widehat{\mathfrak{I}} \in \mathbb{R}^{N\times(m\cdot N)}$ is the attack target, i.e., $a_o = \widehat{a}$, where only the $(j, j{+}(o{-}1){\times}N)$th entries are 1; $\hat{\boldsymbol{a}} = [\,\widehat{a}, \widehat{a}, \ldots, \widehat{a}\,]^T \in \mathbb{R}^{N\times 1}$ is the attack target vector; $\hat{\boldsymbol{x}}^j$ is the state estimate vector for the jth snapshot.

By successively solving Problem (14), the overall solution can be updated via the following equations,

$$\hat{\boldsymbol{b}}^{k+1} = \hat{\boldsymbol{b}}^k + \Delta\hat{\boldsymbol{b}}^k, \tag{18}$$

$$\hat{\boldsymbol{c}}^{k+1} = \hat{\boldsymbol{c}}^k + \Delta\hat{\boldsymbol{c}}^k, \tag{19}$$

where $\hat{\boldsymbol{b}}^k$ and $\hat{\boldsymbol{c}}^k$ represent the solution vector at the kth iteration for the parameter attack vector and the state bias vector, respectively; $\hat{\boldsymbol{c}}^k = [(\hat{\boldsymbol{c}}^{1,k})^T, (\hat{\boldsymbol{c}}^{2,k})^T, \ldots, (\hat{\boldsymbol{c}}^{N,k})^T]^T \in \mathbb{R}^{(N\cdot n)\times 1}$. Note that the final solution of the measurement attack vector $\boldsymbol{a}$ is directly obtained at the final iteration. The updated estimates, i.e., $\hat{\boldsymbol{b}}^{k+1}$ and $\hat{\boldsymbol{c}}^{k+1}$, will be used as initial guesses to expand the Taylor series at a new data point. The updated estimates will typically be better approximations to the nonlinear function's solutions than the previous estimates, and the method can be iterated to achieve more accurate solutions. Theoretically, if $\Delta\hat{\boldsymbol{b}}^k$ and $\Delta\hat{\boldsymbol{c}}^k$ converge to zero, the higher-order terms of the Taylor series will be zero. Thus, equation (13) for the stealth condition will be exactly met,

$$\begin{aligned} \boldsymbol{a}^k &= \boldsymbol{h}_p\left(\hat{\boldsymbol{x}} + \boldsymbol{c}^k, \boldsymbol{p} + \boldsymbol{b}^k\right) + \boldsymbol{H}_p^k\Delta\boldsymbol{b}^k + O\left(\left\|\Delta\boldsymbol{b}^k\right\|^2\right) \\ &\quad + \boldsymbol{H}_x^k\Delta\boldsymbol{c}^k + O\left(\left\|\Delta\boldsymbol{c}^k\right\|^2\right) - \boldsymbol{h}_p(\hat{\boldsymbol{x}}, \boldsymbol{p}). \\ &\Downarrow\ \ \Delta\boldsymbol{b}^k \to \mathbf{0},\ \ \Delta\boldsymbol{c}^k \to \mathbf{0} \\ \boldsymbol{a}^k &= \boldsymbol{h}_p\left(\hat{\boldsymbol{x}} + \boldsymbol{c}^k, \boldsymbol{p} + \boldsymbol{b}^k\right) - \boldsymbol{h}_p(\hat{\boldsymbol{x}}, \boldsymbol{p}). \end{aligned} \tag{20}$$

In algorithmic implementation, the outer loop terminates when $\Delta\hat{\boldsymbol{b}}^k$ and $\Delta\hat{\boldsymbol{c}}^k$ satisfy the termination tolerance, i.e., $\|\Delta\hat{\boldsymbol{b}}^k\|_\infty \le \epsilon^b$ and $\|\Delta\hat{\boldsymbol{c}}^k\|_\infty \le \epsilon^c$. By controlling the tolerance ϵ^b and ϵ^c, the original nonlinear constraint (10) for ensuring stealthy attack can be satisfied at any desirable accuracy level.

Based on the vector solution $\boldsymbol{M}^*$, the set of manipulated measurement channels can be expressed as,

$$\Lambda = \left\{\mathrm{i} \mid \left\|\boldsymbol{M}_i^*\right\|_0 \neq 0\right\}, i \in \{1, 2, \ldots, m\}, \tag{21}$$

where $\boldsymbol{M}_i^*$ is the solution of the ith group; Λ is the set of measurement channels to manipulate, which will be used to prepare for the intrusion and to guide the *run-time-attack* stage.

B. Determination of Measurement Attack Vectors in the Run-Time-Attack Stage

In Section IV-B, the set of measurement channels to manipulate and the parameter attack vector are determined in an offline fashion. In this subsection, this information will be used to construct measurement attack vectors based on the system operating conditions in the *attack interval*.

With the set of the measurement channels to compromise obtained from the *pre-attack* stage, the least squares (LS) criterion is utilized to construct measurement attack vectors that satisfy the *stealth* condition to the greatest extent:

$$\begin{aligned} \left[\hat{\widetilde{\boldsymbol{a}}}, \hat{\widetilde{\boldsymbol{c}}}\right] = \underset{\widetilde{\boldsymbol{a}}, \widetilde{\boldsymbol{c}}}{\operatorname{argmin}}\ & \left\|\widetilde{\boldsymbol{a}} - \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}} + \widetilde{\boldsymbol{c}}, \boldsymbol{p} + \boldsymbol{b}^*\right) + \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}}, \boldsymbol{p}\right)\right\|_2^2 \\ s.t.\ \ & \widetilde{a}_o = \widehat{a}, \forall o \in \Upsilon \\ & \widetilde{a}_i = 0, \forall i \notin \Lambda, \end{aligned} \tag{22}$$

where $\hat{\widetilde{\boldsymbol{x}}} \in \mathbb{R}^{n\times 1}$ is the state estimate vector in the *attack interval*; $\widetilde{\boldsymbol{c}}$ is the bias vector injected into $\hat{\widetilde{\boldsymbol{x}}}$; $\boldsymbol{b}^*$ is the pre-estimated parameter attack vector from the *pre-attack* stage; $\widetilde{a}_o$ is the attack target in the *attack interval*; $\widetilde{a}_i = 0, \forall i \notin \Lambda$ represents that the measurement channels that do not belong to set Λ should not be manipulated in the *run-time-attack* stage.

Similar to Eq. (13), the approximation of the objective function in Eq. (22) at the kth iteration can be presented as,

$$\widetilde{\boldsymbol{a}}^k \approx \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}} + \widetilde{\boldsymbol{c}}^k, \boldsymbol{p} + \boldsymbol{b}^*\right) + \widetilde{\boldsymbol{H}}_x^k\Delta\widetilde{\boldsymbol{c}}^k - \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}}, \boldsymbol{p}\right), \tag{23}$$

where k is an index of iteration, and variables with a tilde sign represent those in the *run-time-attack* stage.

The kth iteration can be written in a compact form as follows:

$$\begin{aligned} \left[\hat{\widetilde{\boldsymbol{a}}}, \Delta\hat{\widetilde{\boldsymbol{c}}}\right] = \underset{\widetilde{\boldsymbol{a}}, \Delta\widetilde{\boldsymbol{c}}}{\arg\min}\ & \left\|\widetilde{\boldsymbol{L}}^k\Delta\widetilde{\boldsymbol{M}}^k - \widetilde{\boldsymbol{Q}}^k\right\|_2^2 \\ s.t.\ \ & \widetilde{a}_o = \widehat{a}, \forall o \in \Upsilon \\ & \widetilde{a}_i = 0, \forall i \notin \Lambda, \end{aligned} \tag{24}$$

where

$$\widetilde{\boldsymbol{L}}^k = \left[\boldsymbol{I}_m\ -\widetilde{\boldsymbol{H}}_x^k\right], \tag{25}$$

$$\Delta\widetilde{\boldsymbol{M}}^k = \left[\left(\widetilde{\boldsymbol{a}}^k\right)^T\ \left(\Delta\widetilde{\boldsymbol{c}}^k\right)^T\right]^T, \tag{26}$$

$$\widetilde{\boldsymbol{Q}}^k = \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}} + \widetilde{\boldsymbol{c}}^k, \boldsymbol{p} + \boldsymbol{b}^*\right) - \boldsymbol{h}_p\left(\hat{\widetilde{\boldsymbol{x}}}, \boldsymbol{p}\right), \tag{27}$$

and $\boldsymbol{I}_m \in \mathbb{R}^{m\times m}$ is an identity matrix.

By successively solving Problem (24), the overall solution can be updated via the following equation,

$$\hat{\widetilde{\boldsymbol{c}}}^{k+1} = \hat{\widetilde{\boldsymbol{c}}}^k + \Delta\hat{\widetilde{\boldsymbol{c}}}^k. \tag{28}$$

Similar to the *pre-attack* stage, the final measurement attack vector $\widetilde{\boldsymbol{a}}$ is directly obtained at the last iteration. The iteration will terminate when $\|\Delta\hat{\widetilde{\boldsymbol{c}}}^k\|_\infty \le \epsilon^c$.

V. Enhancing Sparsity via Weight Adaptation

The original AGBP problem (11) and its linearized version (14) aim to minimize the number of compromised measurement channels to the FDIA that could be launched with the least effort. However, the *sparsity* cannot be maximized if the weights in the objective function are set to unity or randomly given. This section will address the weight adaptation problem for AGBP. It has been shown that with unity weights, quantities with larger scales will be penalized more heavily, resulting in sub-optimal *sparsity* [44]. This is of greater concern in our proposed MMI FDIA formulation, where various measurements and network parameters commonly have various scales.

To truly minimize the set of compromised measurement channels, we develop a weight adaptation scheme motivated by the adaptive group LASSO formulation [45], [46] and the grid search algorithm [47], [48]. The adaptive group LASSO estimator enjoys the *oracle* property and can achieve the *sparsity* property for different groups and perform consistent variable selection [49]. In this paper, ridge regression is used to obtain the initial estimates for weight settings due to its stability [49]. The ridge regression variant of Problem (11) with the removal of inequality constraints can be equivalently expressed as a successive set of linearized problems,

$$\left[\hat{\boldsymbol{a}}, \Delta\hat{\boldsymbol{b}}, \Delta\hat{\boldsymbol{c}}\right] = \underset{\boldsymbol{a},\Delta\boldsymbol{b},\Delta\boldsymbol{c}}{\arg\min} \left\|\boldsymbol{L}^k\Delta\boldsymbol{M}^k - \boldsymbol{N}^k\right\|_2^2 + \lambda\left\|\Delta\boldsymbol{M}^k\right\|_2^2, \tag{29}$$

where λ is the regularization coefficient.

The weights in (11) can then be defined using the ridge-regression-based solution,

$$w_i = \begin{cases} \left\|\hat{\boldsymbol{a}}_i^{ridge}\right\|_2^{-\gamma}, & i \in \{1, 2, \ldots, m\}, \\ \left|\hat{b}_{i-m}^{ridge}\right|^{-\gamma}, & i \in \{m+1, \ldots, m+s\}, \\ 0, & i = m+s+1, \end{cases} \tag{30}$$

where $\hat{\boldsymbol{a}}_i^{ridge} \in \mathbb{R}^{N\times 1}$ and $\hat{b}_{i-m}^{ridge}$ are the estimates of the measurement attack vectors and the parameter attack value in the ith group, respectively; γ is a tuning parameter commonly ranging from 0.5 to 2. Note that the weight of the last group, the state bias vector $\boldsymbol{c}$, is set to zero since they should not be penalized.

It can be found that the values of weights are subjected to two tuning parameters, i.e., λ and γ. Therefore, an optimal pair of (λ, γ) needs to be searched to achieve the sparsest set of compromised measurement channels. The steps of the proposed weight adaptation scheme are summarized as follows.

Step 1: Set $q = 1$, $\vartheta^0 = 0$, and initialize the search interval for λ and γ, i.e., $\lambda \in [\lambda_{\min}, \lambda_{\max}]$ and $\gamma \in [\gamma_{\min}, \gamma_{\max}]$.

Step 2: Choose η_1 and η_2 candidates for λ and γ in the corresponding intervals, respectively.

Step 3: Compute $\hat{\boldsymbol{a}}_i^{ridge}$ and $\hat{b}_{i-m}^{ridge}$ by solving the ridge regression problem in (29) with respect to all λ; then, compute w_i via Eq. (30) with respect to all γ.

Step 4: Execute the *pre-attack* procedure to test the performances of all sets of weights obtained in *Step 3*; then, find the optimal λ_t and γ_t that result in $\vartheta^q = \min|\Lambda|$.

Step 5: If $\vartheta^q = \vartheta^{q-1}$, go to *Step 6*; otherwise, find the adjacent λ_{t-1}, λ_{t+1}, γ_{t-1}, and γ_{t+1} based on the optimal λ_t and γ_t, then shrink the search intervals for λ and γ by setting $\lambda_{\min} \leftarrow \lambda_{t-1}$, $\lambda_{\max} \leftarrow \lambda_{t+1}$, $\gamma_{\min} \leftarrow \gamma_{t-1}$, $\gamma_{\max} \leftarrow \gamma_{t+1}$, $q \leftarrow q + 1$, and go to *Step 2*.

Step 6: Output the optimal weights corresponding to λ_t and γ_t.

Note that the solutions $\hat{\boldsymbol{a}}$, $\hat{\boldsymbol{b}}$, and $\hat{\boldsymbol{c}}$ for the AGBP problems (11) under different weights obtained from different tuning parameters (λ, γ) are *independently* obtained, and the weight leading to the sparsest solution $\hat{\boldsymbol{a}}$ is finally selected as the optimal one. As the AGBP problems under different weights are processed separately and in parallel, no numerical convergence issue is present in this selection process.

VI. ADMM-Based Solution Algorithms

In this section, the alternating direction method of multipliers (ADMM) is customized and exploited to solve the proposed AGBP problem (14) for the *pre-attack* stage and the proposed LS problem (24) for the *run-time-attack* stage.

A. ADMM Algorithm

ADMM is an algorithm blending the decomposability of dual ascent with the superior convergence properties of the method of multipliers [50]. It solves problems in the form of:

$$\begin{aligned} &\min_{\boldsymbol{u},\boldsymbol{v}} \ f(\boldsymbol{u}) + g(\boldsymbol{v}) \\ &s.t. \ \ \boldsymbol{A}\boldsymbol{u} + \boldsymbol{B}\boldsymbol{v} = \boldsymbol{d}, \end{aligned} \tag{31}$$

via the following iterations:

$$\boldsymbol{u}^{l+1} := \underset{\boldsymbol{u}}{\arg\min}\left(f(\boldsymbol{u}) + (\rho/2)\left\|\boldsymbol{A}\boldsymbol{u} + \boldsymbol{B}\boldsymbol{v}^l - \boldsymbol{d} + \boldsymbol{y}^l\right\|_2^2\right), \tag{32}$$

$$\boldsymbol{v}^{l+1} := \underset{\boldsymbol{v}}{\arg\min}\left(g(\boldsymbol{v}) + (\rho/2)\left\|\boldsymbol{A}\boldsymbol{u}^{l+1} + \boldsymbol{B}\boldsymbol{v} - \boldsymbol{d} + \boldsymbol{y}^l\right\|_2^2\right), \tag{33}$$

$$\boldsymbol{y}^{l+1} := \boldsymbol{y}^l + \boldsymbol{A}\boldsymbol{u}^{l+1} + \boldsymbol{B}\boldsymbol{v}^{l+1} - \boldsymbol{d}, \tag{34}$$

where l is the index for iterations in ADMM algorithm, ρ is the augmented Lagrangian parameter. In this paper, ρ is set to 1.

B. Solution Algorithm for the AGBP Problem in the Pre-Attack Stage

The developed AGBP problem at the kth iteration can be written in the form of Eq. (31),

$$\begin{aligned} \left[\hat{\boldsymbol{a}}, \Delta\hat{\boldsymbol{b}}, \Delta\hat{\boldsymbol{c}}\right] = \underset{\boldsymbol{a},\Delta\boldsymbol{b},\Delta\boldsymbol{c}}{\arg\min} \ & f\left(\Delta\boldsymbol{M}^k\right) + \sum_{i=1}^{m+s+1} w_i\left\|\boldsymbol{v}_i^k\right\|_2 \\ s.t. \ \ & \Delta\boldsymbol{M}^k - \boldsymbol{v}^k = \boldsymbol{0} \\ & \underline{\boldsymbol{p}} \le \Delta\boldsymbol{b}^k + \boldsymbol{b}^k \le \bar{\boldsymbol{p}}, \end{aligned} \tag{35}$$

where $f(\cdot)$ is the indicator function of $\boldsymbol{L}^k\Delta\boldsymbol{M}^k = \boldsymbol{Q}^k$. The iterative procedures of solving the AGBP problem using the

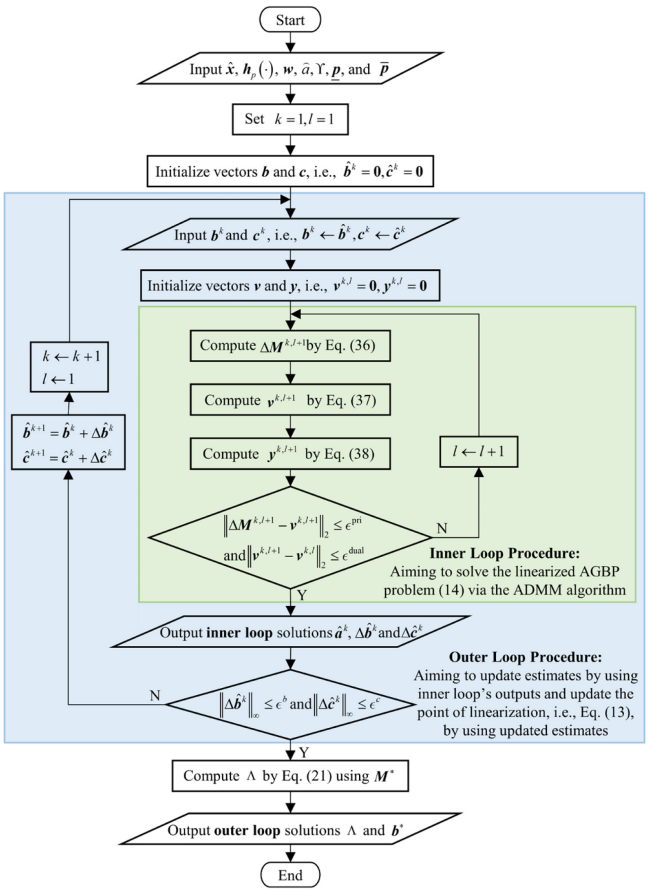

Fig. 3. Flowchart of the solution algorithm for the AGBP problem.

ADMM algorithm are as follows:

$$\Delta \boldsymbol{M}^{k,l+1} := \left(\boldsymbol{I}-\left(\boldsymbol{L}^k\right)^T\left(\boldsymbol{L}^k\left(\boldsymbol{L}^k\right)^T\right)^{-1}\boldsymbol{L}^k\right)\left(\boldsymbol{v}^{k,l}-\boldsymbol{y}^{k,l}\right) + \left(\boldsymbol{L}^k\right)^T\left(\boldsymbol{L}^k\left(\boldsymbol{L}^k\right)^T\right)^{-1}\boldsymbol{Q}^k, \tag{36}$$

$$\boldsymbol{v}_i^{k,l+1} := \boldsymbol{S}_{w_i}\left(\Delta \boldsymbol{M}_i^{k,l+1}+\boldsymbol{y}_i^{k,l}\right), \tag{37}$$

$$\boldsymbol{y}^{k,l+1} := \boldsymbol{y}^{k,l}+\Delta \boldsymbol{M}^{k,l+1}-\boldsymbol{v}^{k,l}. \tag{38}$$

Eq. (37) is the soft thresholding operator, which is defined as

$$\boldsymbol{S}_{w_i}\left(\boldsymbol{\psi}_i^k\right)=\begin{cases}\left(1-w_i/\left\|\boldsymbol{\psi}_i^k\right\|_2\right)\cdot\boldsymbol{\psi}_i^k, & \left\|\boldsymbol{\psi}_i^k\right\|_2 > w_i,\\ \boldsymbol{0}, & \left\|\boldsymbol{\psi}_i^k\right\|_2 \le w_i,\end{cases} \tag{39}$$

where $\boldsymbol{\psi}_i^k=\Delta \boldsymbol{M}_i^{k,l+1}+\boldsymbol{y}_i^{k,l}$. It should be noted that the lower and upper bounds of the parameter attack vector $\boldsymbol{b}$ are enforced as shown in Problem (11), so as to avoid detection by simple rules of thumb. Consequently, for the parameter attack vector, the soft thresholding operator is modified as follows,

$$\boldsymbol{S}_{w_i}\left(\psi_i^k\right)=\begin{cases}\overline{\psi}_i^k, & \psi_i^k \ge \overline{\psi}_i^k,\\ \psi_i^k-w_i, & w_i < \psi_i^k < \overline{\psi}_i^k,\\ 0, & \left|\psi_i^k\right| \le w_i,\\ \psi_i^k+w_i, & \underline{\psi}_i^k < \psi_i^k < -w_i,\\ \underline{\psi}_i^k, & \psi_i^k \le \underline{\psi}_i^k,\end{cases} \quad i=m+1,\ldots,m+s, \tag{40}$$

where $\underline{\psi}_i^k$ and $\overline{\psi}_i^k$ are the lower and upper bounds of vector ψ_i^k, respectively. In this paper, the parameter attack vector is constrained between $\underline{\boldsymbol{p}}$ and $\bar{\boldsymbol{p}}$. Hence, $\underline{\psi}_i^k$ and $\overline{\psi}_i^k$ are set as,

$$\underline{\psi}_i^k=\underline{p}_{i-m}-\hat{b}_{i-m}^k,\ \ i=m+1,\ldots,m+s, \tag{41}$$

$$\overline{\psi}_i^k=\bar{p}_{i-m}-\hat{b}_{i-m}^k,\ \ i=m+1,\ldots,m+s, \tag{42}$$

where $\hat{b}_{i-m}^k$ is the estimate of the parameter attack at the kth iteration; $\underline{p}_{i-m}$ and $\bar{p}_{i-m}$ represent the corresponding entries of $\underline{\boldsymbol{p}}$ and $\bar{\boldsymbol{p}}$, respectively.

The termination criterion can be set as that $\|\Delta \boldsymbol{M}^{k,l+1}-\boldsymbol{v}^{k,l+1}\|_2 \le \epsilon^{\text{pri}}$ and $\|\boldsymbol{v}^{k,l+1}-\boldsymbol{v}^{k,l}\|_2 \le \epsilon^{\text{dual}}$. The flowchart of the solution algorithm is shown in Fig. 3, which consists of the inner loop and outer loop procedures. The inner loop procedure aims to solve the linearized AGBP problem via the ADMM algorithm to obtain the updates, i.e., $\hat{\boldsymbol{a}}^k$, $\Delta\hat{\boldsymbol{b}}^k$ and $\Delta\hat{\boldsymbol{c}}^k$, and the outer loop procedure aims to update the estimates for variables $\boldsymbol{b}$ and $\boldsymbol{c}$ and generates a new linearized problem around the new values of $\boldsymbol{b}$ and $\boldsymbol{c}$ for the inner loop to solve.

C. Solution Algorithm for the LS Problem in the Run-Time-Attack Stage

We treat the LS problem as a LASSO problem without the penalty term, and thus, it can be readily solved by the ADMM algorithm.

The LS Problem (24) at the kth iteration can be written in the form of Eq. (31),

$$\left[\hat{\widetilde{\boldsymbol{a}}},\Delta\hat{\widetilde{\boldsymbol{c}}}\right]=\underset{\widetilde{\boldsymbol{a}},\Delta\widetilde{\boldsymbol{c}}}{\arg\min}\ \left\|\widetilde{\boldsymbol{L}}^k\Delta\widetilde{\boldsymbol{M}}^k-\widetilde{\boldsymbol{Q}}^k\right\|_2^2+0\cdot\left\|\widetilde{\boldsymbol{v}}^k\right\|_1$$
$$s.t.\ \ \Delta\widetilde{\boldsymbol{M}}^k-\widetilde{\boldsymbol{v}}^k=\boldsymbol{0}$$
$$\widetilde{a}_o=\widehat{a},\forall o\in\Upsilon$$
$$\widetilde{a}_i=0,\forall i\notin\Lambda. \tag{43}$$

The iterative procedures for solving the LS problem using the ADMM algorithm are as follows:

$$\Delta\widetilde{\boldsymbol{M}}^{k,l+1}=\left(\left(\widetilde{\boldsymbol{L}}^k\right)^T\widetilde{\boldsymbol{L}}^k+\boldsymbol{I}\right)^{-1}\left(\left(\widetilde{\boldsymbol{L}}^k\right)^T\widetilde{\boldsymbol{Q}}^k+\widetilde{\boldsymbol{v}}^{k,l}-\widetilde{\boldsymbol{y}}^{k,l}\right), \tag{44}$$

$$\widetilde{v}_i^{k,l+1}=\begin{cases}0, & i\notin\Lambda,\\ \widehat{a}, & i\in\Upsilon,\\ \Delta\widetilde{M}_i^{k,l+1}+\widetilde{y}_i^{k,l}, & otherwise,\end{cases} \tag{45}$$

$$\widetilde{\boldsymbol{y}}^{k,l+1}=\widetilde{\boldsymbol{y}}^{k,l}+\Delta\widetilde{\boldsymbol{M}}^{k,l+1}-\widetilde{\boldsymbol{v}}^{k,l+1}, \tag{46}$$

where l is the index of the iteration in the ADMM algorithm.

The termination criterion can be set as that $\|\Delta\widetilde{\boldsymbol{M}}^{k,l+1}-\widetilde{\boldsymbol{v}}^{k,l+1}\|_2 \le \epsilon^{\text{pri}}$ and $\|\widetilde{\boldsymbol{v}}^{k,l+1}-\widetilde{\boldsymbol{v}}^{k,l}\|_2 \le \epsilon^{\text{dual}}$. The flowchart of the solution algorithm is shown in Fig. 4, which consists of the inner loop and outer loop procedures. The inner loop procedure aims to solve the linearized LS problem to obtain the updates, i.e., $\hat{\widetilde{\boldsymbol{a}}}^k$ and $\Delta\hat{\widetilde{\boldsymbol{c}}}^k$, and the outer loop procedure aims to update the estimates for variable $\widetilde{\boldsymbol{c}}$ and generates a new linearized problem around the new values of $\widetilde{\boldsymbol{c}}$ for the inner loop to solve.

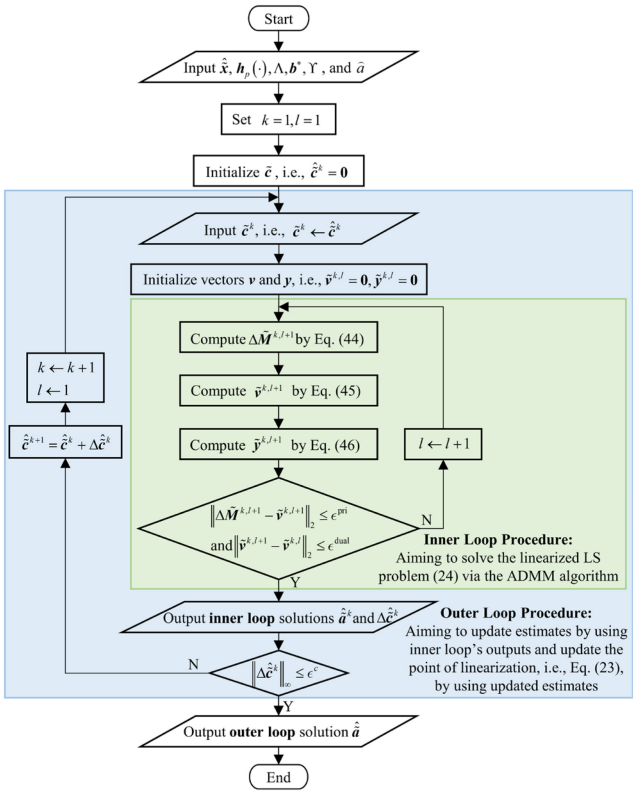

Fig. 4. Flowchart of the solution algorithm for the LS problem.

To ensure the *stealth* of FDIAs in the *run-time-attack* stage (i.e., on-line stage), the attack strategies obtained from the *pre-attack* stage (i.e., off-line stage) should be re-evaluated at times. The re-evaluation of the attack strategies obtained from the *pre-attack* stage is determined on whether the power flow pattern in the *run-time-attack* stage deviates significantly from that in the *pre-attack* stage. One feasible means to evaluate the degree of deviation is to observe the value of the objective function in Eq. (22). Specifically, the value of the objective function can be calculated prior to the actual implementation of FDIAs and compared with a specific threshold. If the value of the objective function is larger than the threshold, it implies that the *stealth* of FDIAs in the *run-time-attack* stage will be weakened due to the deviation of the power flow pattern from the *pre-attack* stage. Then, the *run-time-attack* stage should not be implemented, and the *pre-attack* stage should be re-evaluated. Otherwise, the pre-selected set of measurement channels for intrusion and pre-estimated false parameter values can still be utilized to launch the *run-time attack*.

D. Convergence of the Solution Algorithm

The convergence properties of the solution algorithms are discussed as follows.

1) Convergence of the Inner Loop Procedure: The inner loop aims to solve a linearized AGBP problem (14) via the ADMM algorithm. In [50], [51], [52], it has been proven that if the objective functions, i.e., f and g in the ADMM algorithm, are closed, proper, and convex, and the Lagrangian L_0 has a saddle point, then the primal residual can converge to zero and the objective function can converge to the optimal solution. Besides, it has been proven that the ADMM algorithm is still convergent when solving nonconvex problems as long as specific constraints are satisfied [53], [54], such as the objective functions f and g are Lipchitz differentiable, the penalty parameter is chosen large enough, etc. In the *inner loop procedure* of our proposed AGBP problem, the objective functions f and g are all convex, wherein f is a linear indicator function and g is a l_2-norm-based function. Moreover, constraints are all linear. Hence, the convergence of the *inner loop procedure* using the ADMM algorithm can be achieved.

2) Convergence of the Outer Loop Procedure: The outer loop aims to solve the nonlinear AGBP problem (14) via successive linearization. Note that this is a widely used method for solving nonlinear programming problems [55], [56], [57]. While the convergence from any initial guess to the solution point cannot be rigorously proven, this method has achieved wide success in the optimization of power systems and many other areas. Just to name a few among many, power system state estimation with nonlinear measurement models using the WLS estimator [37], [58] and the least absolute value (LAV) estimator [37], [59], model reduction of induction machines using the nonlinear LASSO [60], autonomous tracking and state estimation using the generalized group LASSO [61], etc. As has been shown extensively in existing literature, this method has satisfactory performance for a wide variety of nonlinear programming problems in practice. Furthermore, as shown in Section IV-A, it is guaranteed that when the termination criteria of the outer loop $\|\Delta\hat{\boldsymbol{b}}^k\|_\infty \le \epsilon^b$ and $\|\Delta\hat{\boldsymbol{c}}^k\|_\infty \le \epsilon^c$ are met, the solution to the original nonlinear AGBP problem is obtained.

In the outer loop procedure, as the algorithm converges more easily when the initial guess is closer to the solution point, taking the state estimate of the same measurement scan instead of the flat start (i.e., setting voltage magnitudes to nominal and angles to zero) as the initial guess makes the algorithm converge much faster. The state estimate could be the one from system operator's historical database or one obtained by feeding the measurement scan to a state estimation algorithm developed by the cyber adversaries.

VII. Case Studies

In this section, the developed two-stage MMI FDIA strategy is tested on IEEE 14-bus and 118-bus systems [62]. In the IEEE 14-bus system, there are 47 SCADA measurements including 5 voltage magnitude measurements, 8 pairs of active and reactive power injection measurements, and 13 pairs of active and reactive power flow measurements. In the IEEE 118-bus system, there are 410 SCADA measurements including 54 voltage magnitude measurements, 52 pairs of active and reactive power injection measurements, and 126 pairs of active and reactive power flow measurements. The measurement errors follow a Gaussian distribution with zero mean and standard deviation of 0.01 p.u.

To verify the effectiveness of the proposed MMI FDIA strategy, 10 simulation cases are designed: Cases 1-5 for the IEEE 14-bus system and Cases 6-10 for the IEEE 118-bus system. Moreover, three scenarios are designed for each case. *Scenario 1*: Network parameters are *not* manipulated, and only

TABLE I
ATTACK TARGETS OF THE 10 SIMULATED FDIA CASES

IEEE 14-bus System	Case 1	Case 2	Case 3	Case 4	Case 5
	V_3	P_3	Q_2	$P_{2\text{-}4}$	$Q_{1\text{-}5}$
IEEE 118-bus system	Case 6	Case 7	Case 8	Case 9	Case 10
	V_{34}	P_{32}	Q_{15}	$P_{8\text{-}30}$	$Q_{33\text{-}37}$

measurements are manipulated as in conventional measurement FDIAs [17], [18], [19], [20]; *Scenario 2*: Measurements and network parameters are coordinately manipulated, but there is no weight adaptation to enhance the *sparsity* of measurement channels, i.e., unity weights are set in (11); *Scenario 3*: Measurements and network parameters are coordinately manipulated, and the proposed weight adaptation scheme is applied. The attack targets, i.e., a_o, of the 10 cases are shown in Table I. The magnitude of a_o is 0.1 p.u., i.e., $\widehat{a} = 0.1$, for all cases. In real-world power systems, the value of the attack target can be customized by attackers to achieve their particular goals, such as gaining illegal profit from electricity markets. In this section, the simulations aim to verify the effectiveness of the proposed MMI attack strategy in general. Hence, a uniform value, i.e., $\widehat{a} = 0.1$, is selected for all cases. The upper and lower bounds for the parameter attack vector are set to $2\boldsymbol{p}$ and $-0.8\boldsymbol{p}$, respectively, i.e., $0.2\boldsymbol{p} \leq \boldsymbol{p} + \boldsymbol{b} \leq 3\boldsymbol{p}$. The bounds make sure that the falsified values of the model parameters look plausible and cannot be easily detected by simple rules of thumb, for example, line reactance should not be negative, or should not be orders-of-magnitude different from a normal value, etc. The tolerances for the ADMM algorithm are set to that $\epsilon^{\text{pri}} = 10^{-6}$ p.u. and $\epsilon^{\text{dual}} = 10^{-6}$ p.u., and the tolerances for the estimation of measurement and parameter attack vectors are set to that $\epsilon^{b} = 10^{-6}$ p.u. and $\epsilon^{c} = 10^{-6}$ p.u. Compared with the normal ranges of the decision variables, which are commonly larger than 10^{-2} p.u., these tolerances are small enough to declare convergence of the algorithm without affecting the accuracy of the solution. In addition, the absolute values of entries in the measurement or parameter attack vector below 10^{-3} or 10^{-4} p.u. have negligible impacts on the *stealth* of FDIAs as measurement errors will overshadow the 10^{-3} or 10^{-4} p.u. FDIA estimation error range, and thus they will be dropped. The Chi-square test is used to detect the false data, and the *false alarm rate setting* is set to 1% for all cases.

A. Validation of the Coordinated Manipulation of Measurements and Network Parameters in a Single Snapshot

This subsection aims to validate the concept of coordinated manipulation of measurement and network parameter data, and illustrate its benefit (and thus motivation) for cyber adversaries. It does not involve the two-stage sophisticated strategy described in Section III, but simply assumes that measurements and network parameters are coordinately manipulated in a single snapshot. This is done by executing the AGBP problem (11) with $N = 1$, in which case each group reduces to a single quantity.

The numbers of compromised measurement channels under the 3 scenarios in all the 10 cases are shown in Fig. 5. It can be found that the number of compromised measurement channels

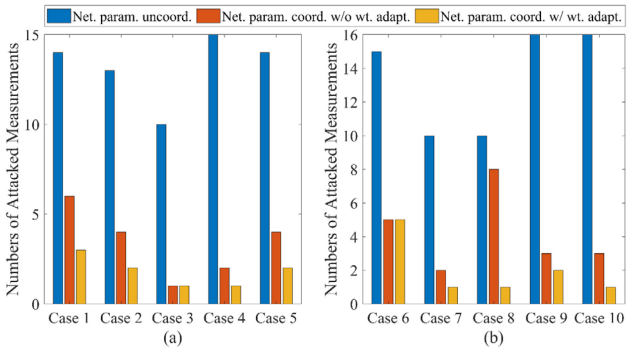

Fig. 5. Numbers of compromised measurement channels in the 10 cases under the 3 scenarios. a) the IEEE 14-bus system; b) the IEEE 118-bus system.

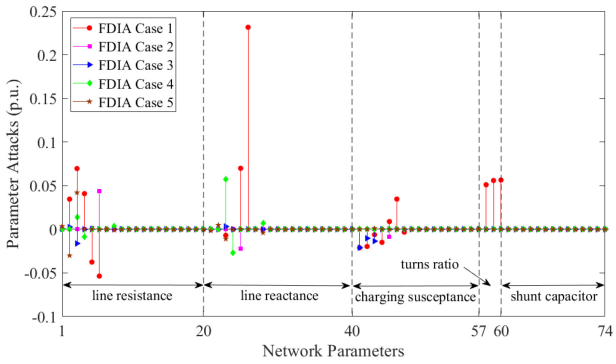

Fig. 6. Parameter attack vectors in Cases 1-5 (the IEEE 14-bus system) with the weight adaptation, i.e., *Scenario 3*.

is significantly reduced when the parameters are coordinately manipulated. This shows that by strategically manipulating a few network parameters in the model database (exemplified by the parameter attack vectors in Cases 1-5 of the IEEE 14-bus system under *Scenario 3* are shown in Fig. 6), the cyber adversaries can breach into much fewer measurement channels for keeping the FDIA stealthy. This could be a desirable strategy for cyber adversaries, as under certain circumstances, manipulating the *streaming* data in multiple measurement channels in *run-time* could be a more challenging task than falsifying network parameters *only once*. This advantage will be further illustrated and discussed in Section VII-B. Furthermore, it is observed that compared with the unity weight setting, i.e., *Scenario 2*, the number of compromised channels is further reduced when the weight adaptation scheme described in Section V is employed, i.e., *Scenario 3*. This verifies the importance of adaptive weight setting for achieving the *sparsity* of measurement channels.

In order to verify the *stealth* of the proposed attack strategy, the measurement residuals in Cases 1-5 of the IEEE 14-bus system under *Scenario 3* along with measurement residuals in the absence of FDIAs are shown in Fig. 7. It can be seen from this figure that the measurement residuals of different measurement channels in the 5 cases closely match the measurement residuals in the absence of FDIAs. This implies that the proposed MMI FDIAs will not change the measurement residuals, and thus cannot be differentiated from the normal operating condition. For further verification, the conventional residual-based BDD method, i.e., the Chi-square test,

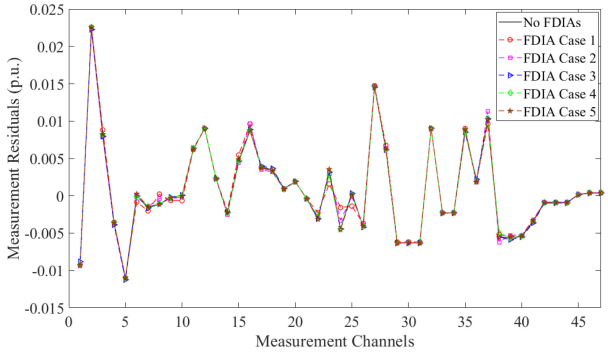

Fig. 7. Measurement residuals in Cases 1-5 (the IEEE 14-bus system) with the weight adaptation, i.e., *Scenario 3*, along with those in the absence of FDIAs.

TABLE II
PRs IN CASES 1-5 (THE IEEE 14-BUS SYSTEM) WITH THE WEIGHT ADAPTATION, i.e., SCENARIO 3, ALONG WITH PR IN THE ABSENCE OF FDIAS

No FDIA	FDIA				
	Case 1	Case 2	Case 3	Case 4	Case 5
1.05%	1.05%	1.05%	1.05%	1.00%	1.05%

TABLE III
PRs IN CASES 6-10 (THE IEEE 118-BUS SYSTEM) WITH THE WEIGHT ADAPTATION, i.e., SCENARIO 3, ALONG WITH PR IN THE ABSENCE OF FDIAS

No FDIA	FDIA				
	Case 6	Case 7	Case 8	Case 9	Case 10
0.95%	0.85%	1.00%	0.90%	0.95%	1.00%

is repeated 2000 times with the average result reported. The positive rate (PR) represents the percentage of samples for which the Chi-square test claims detection of an anomaly. Note that the PR value is not zero even in the absence of FDIAs, since the *false alarm rate setting* of the test is 1%. The PRs in different cases with the weight adaptation of IEEE 14-bus and 118-bus systems are shown in Table II and Table III, respectively, along with those in the absence of FDIAs. In Table II, the PR is 1.05% when there is no FDIA, closely matching the *false alarm rate setting* of 1%. Noticeably, the PRs of the 5 cases in the presence of FDIAs are also close to the *false alarm rate setting*, implying that the BDD cannot differentiate between the cases with or without FDIAs under background measurement noise that normally exists. Similar results are seen in Table III. All the results in the two tables again demonstrate the *stealth* of the proposed MMI FDIA strategy.

B. Validation of the Proposed Two-Stage MMI FDIA Strategy

The simulation cases in Section VII-A demonstrates the concept of MMI FDIA on a single measurement snapshot. This subsection aims to comprehensively verify the two-stage MMI FDIA framework, where the sets of compromised measurement channels and the network parameter attack vector are determined offline based on historical measurement snapshots (i.e., the *pre-attack* stage), and the measurement attack vectors are determined online for each incoming measurement snapshot in run-time (i.e., the *run-time-attack* stage). In the

TABLE IV
NUMBERS OF COMPROMISED MEASUREMENT CHANNELS IN THE ATTACK INTERVAL UNDER 3 SCENARIOS (THE IEEE 14-BUS SYSTEM)

	Case 1	Case 2	Case 3	Case 4	Case 5
Scenario 1	15	13	14	19	15
Scenario 2	10	11	4	10	9
Scenario 3	7	5	3	7	7

TABLE V
NUMBERS OF COMPROMISED MEASUREMENT CHANNELS IN THE ATTACK INTERVAL UNDER 3 SCENARIOS (THE IEEE 118-BUS SYSTEM)

	Case 6	Case 7	Case 8	Case 9	Case 10
Scenario 1	16	10	11	17	15
Scenario 2	9	8	9	6	5
Scenario 3	8	4	5	4	2

pre-attack stage, 10 snapshots from the historical data are used to solve the AGBP problem, i.e., $N = 10$, retrieved from the ISO New England public dataset [43]. The *attack interval* is chosen as 4:00-8:00 on Dec. 2, 2021, i.e., $T = 4h$. In the *attack interval*, 10 measurement snapshots retrieved at randomly selected instants are used for online measurement attack vector construction.

As the outcomes of the *pre-attack* stage, the numbers of compromised measurement channels in the attack interval of IEEE 14-bus and 118-bus systems under all the 3 scenarios are shown in Tables IV and V, respectively. The results indicate that: 1) the number of attacked measurement channels can be reduced by coordinately manipulating measurements and parameters; 2) the *sparsity* of measurement attack vectors can be further enhanced via the proposed weight adaptation scheme. The actual manipulated measurement data points at different instants in the *run-time-attack* stage of the IEEE 14-bus system are illustrated in Fig. 8. Compared with the sole measurement attacks, MMI attacks require the manipulation of much fewer measurement channels in real-time. For example, in Case 2, the number of compromised measurement channels is reduced from 13 to 5. The results indicate that compared with conventional measurement FDIAs, the *sparsity* of compromised measurement channels can be greatly enhanced even if multiple snapshots are incorporated in the AGBP problem (as opposed to the single-snapshot case in Section VII-A). Obviously, both the coordinated manipulation of network parameters and the adaptation of weights are contributing to this enhancement.

Besides the above two reasons, however, there is a third noteworthy reason for the minimization of the number of compromised measurement channels: the set of compromised channels is planned across various operating points in the *pre-attack* stage. With the *group sparsity* formulation, the AGBP problem at the *pre-attack* stage encourages sharing of the same compromised channels in the multiple snapshots covering various system operating points, and once these channels are selected, the cyber adversaries can keep the attack stealthy with the same set of channels regardless of the operating point changes. The conventional attack strategies, however, do not offer such offline planning features and solve the measurement attack vectors of different snapshots in the *real-time* attack independently. As a result, although the attacked

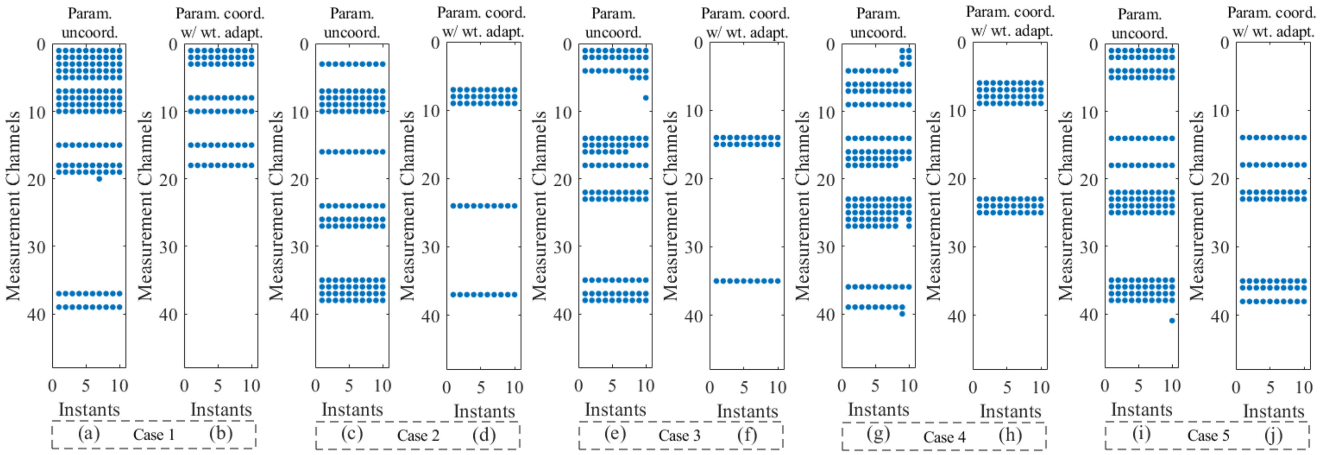

Fig. 8. Compromised measurement data points at different instants in the run-time-attack stage of the IEEE 14-bus system. a), c), e), g), and i) Cases 1, 2, 3, 4, and 5, respectively, where parameters are uncoordinated, i.e., *Scenario 1*; b), d), f), h), and j) Cases 1, 2, 3, 4, and 5, respectively, where measurements and parameters are coordinately manipulated with the weight adaptation scheme, i.e., *Scenario 3*.

measurement data points are minimal for each snapshot, the channels may change across different snapshots due to the fluctuation of system operating points. This implies that cyber adversaries may need to manipulate data points in different channels at different instants during an attack, leading to a large number of measurement channels being compromised. For example, in Fig. 8-g, the 8^{th} instant (snapshot) and the 9^{th} instant (snapshot) require manipulation of many different channels, and cyber adversaries have to access all of them. In fact, as they cannot exactly predict which channels will be needed, they have to intrude into an even larger set of channels that are potentially needed. Our proposed MMI FDIA strategy, by contrast, has a consistent set of measurement channels to manipulate across all the instants (snapshots). Furthermore, these channels are selected prior to the *run-time-attack* stage, which minimizes the risk of requiring unpredicted channels. This attack strategy can greatly reduce the efforts to launch an FDIA in power systems.

As in the two-stage MMI FDIA strategy, the manipulated measurement channels are pre-determined and not allowed to change in the *run-time-attack* stage, the constructed measurement attack vectors in the *attack interval* may not be a perfect match with the *stealth* condition. To evaluate the *stealth* performance of the proposed strategy, the same Chi-square test is applied. The PRs at different instants in the IEEE 14-bus system and the IEEE 118-bus system under *Scenario 3* are shown in Tables VI and VII, respectively, along with those in the absence of FDIAs. The PRs with and without MMI FDIA are at a similar level, indicating that the statistically effective detection of the FDIAs based on the Chi-square test is impossible. The results demonstrate that the developed attack strategy keeps the desirable *stealth* feature when multiple measurement snapshots with various operating points are involved.

TABLE VI
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 14-BUS SYSTEM)

In-stants	No FDIA	FDIAs				
		Case 1	Case 2	Case 3	Case 4	Case 5
1	0.75%	0.65%	0.70%	0.65%	0.80%	0.85%
2	1.25%	1.20%	1.20%	1.20%	1.20%	1.10%
3	1.05%	1.10%	1.10%	1.10%	1.05%	1.10%
4	1.00%	1.00%	1.00%	1.00%	1.00%	1.10%
5	0.75%	0.80%	0.65%	0.70%	0.80%	0.65%
6	0.95%	0.95%	1.00%	0.95%	1.00%	1.10%
7	0.95%	0.95%	1.00%	0.95%	0.95%	1.05%
8	0.75%	0.80%	0.75%	0.80%	0.90%	0.90%
9	1.20%	1.20%	1.25%	1.30%	1.25%	1.25%
10	1.25%	1.30%	1.20%	1.20%	1.30%	1.20%
Ave.	0.99%	1.00%	0.99%	0.99%	1.03%	1.03%

TABLE VII
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 118-BUS SYSTEM)

In-stants	No FDIA	FDIAs				
		Case 6	Case 7	Case 8	Case 9	Case 10
1	1.00%	1.05%	1.05%	1.10%	1.00%	1.00%
2	0.95%	0.85%	0.95%	0.90%	0.95%	0.95%
3	0.90%	0.80%	0.85%	0.85%	0.95%	0.85%
4	1.10%	1.05%	1.15%	1.15%	1.15%	1.10%
5	0.95%	1.05%	0.95%	0.85%	0.95%	0.95%
6	1.00%	1.00%	1.00%	1.05%	1.05%	1.00%
7	1.45%	1.30%	1.30%	1.40%	1.35%	1.45%
8	1.15%	1.00%	1.10%	1.15%	1.15%	1.10%
9	0.65%	0.70%	0.65%	0.65%	0.70%	0.65%
10	0.70%	0.80%	0.75%	0.70%	0.70%	0.75%
Ave.	0.99%	0.96%	0.98%	0.98%	1.00%	0.98%

C. Validation of the Proposed Two-Stage MMI FDIA Strategy Under Network Parameter Uncertainties and Moving Target Defense

In Section VII-B, the *stealth* and *sparsity* of the proposed two-stage MMI attack strategy have been demonstrated under constant network parameters. In real-world power systems, a few network parameters may slightly change with the variations of external environments or operating states. For example, line resistance will be affected by the ambient temperature, and turns ratios of transformers and susceptance of shunt capacitor/reactor banks will be adjusted for voltage regulation. Moreover, network parameters may also change with the implementation of the moving target defense (MTD) strategy using distributed flexible AC transmission system (D-FACTS) devices, which can thwart FDIAs by proactively

TABLE VIII
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 14-BUS SYSTEM WITH NETWORK PARAMETER UNCERTAINTIES)

In-stants	No FDIA	FDIAs				
		Case 1	Case 2	Case 3	Case 4	Case 5
1	1.35%	1.30%	1.00%	1.35%	1.10%	1.30%
2	1.60%	1.75%	1.50%	1.70%	1.10%	1.70%
3	1.40%	1.60%	1.35%	1.50%	1.10%	1.80%
4	1.45%	1.55%	1.50%	1.50%	1.55%	1.60%
5	1.70%	1.80%	1.45%	1.80%	1.35%	1.85%
6	2.45%	2.40%	2.10%	2.25%	1.45%	2.35%
7	2.10%	1.95%	1.85%	1.85%	1.60%	2.40%
8	1.95%	1.85%	1.85%	1.95%	1.40%	2.15%
9	2.25%	2.35%	2.05%	2.10%	1.65%	2.55%
10	1.90%	2.00%	1.80%	1.85%	1.50%	2.05%
Ave.	1.82%	1.86%	1.65%	1.79%	1.38%	1.98%

TABLE IX
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 118-BUS SYSTEM WITH NETWORK PARAMETER UNCERTAINTIES)

In-stants	No FDIA	FDIAs				
		Case 6	Case 7	Case 8	Case 9	Case 10
1	2.70%	2.45%	2.75%	2.75%	2.45%	2.70%
2	3.45%	3.70%	3.45%	3.55%	3.30%	3.45%
3	2.25%	2.20%	2.25%	2.25%	2.25%	2.20%
4	2.50%	3.20%	2.50%	2.50%	2.50%	2.50%
5	2.55%	2.95%	2.55%	2.60%	2.50%	2.50%
6	2.90%	2.65%	2.85%	2.95%	2.70%	2.90%
7	3.30%	3.50%	3.35%	3.25%	3.30%	3.25%
8	3.50%	3.50%	3.50%	3.55%	3.45%	3.45%
9	2.85%	3.05%	2.95%	2.85%	2.80%	2.85%
10	3.15%	3.40%	3.35%	3.20%	3.15%	3.20%
Ave.	2.92%	3.06%	2.95%	2.95%	2.84%	2.90%

perturbing the line reactance [23], [63], [64], [65], [66], [67], [68], [69]. In this subsection, the effectiveness of the proposed MMI attack strategy will be demonstrated under network parameter uncertainties and MTD, respectively.

1) MMI Attack Strategy Under Network Parameter Uncertainties: To mimic the uncertainties of network parameters in realistic power systems, simulations in this subsection assume that part of the network parameters, including line resistance, turns ratios of transformers, along with susceptance of shunt capacitor/reactor banks, change between the *pre-attack stage* and the *run-time-attack* stage.

In the *pre-attack* stage, network parameters of the IEEE 14-bus system and the IEEE 118-bus system are extracted from standard databases [62]. In the *run-time-attack* stage, it is assumed that line resistance follows a uniform distribution on the interval $[0.95\boldsymbol{r}_{std}, 1.05\boldsymbol{r}_{std}]$, where $\boldsymbol{r}_{std}$ represents the vector of standard line resistance; turns ratios of transformers are increased by 0.02 p.u.; and susceptance is increased by 50% for all shunt capacitor/reactor banks. It should be noted that only the turns ratios of transformers and susceptance of shunt capacitor/reactor banks are reported to the control center in the *run-time-attack* stage; the variations of line resistances are unknown to both grid operators and cyber adversaries.

The PRs at different instants in the *attack interval* of the two test systems under *Scenario 3* along with those in the absence of FDIAs are presented in Tables VIII and IX, respectively.

TABLE X
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 14-BUS SYSTEM UNDER MOVING TARGET DEFENSE)

In-stants	No FDIA	FDIAs				
		Case 1	Case 2	Case 3	Case 4	Case 5
1	0.70%	0.85%	0.80%	0.85%	56.05%	100%
2	0.65%	0.70%	0.60%	0.75%	63.90%	100%
3	0.95%	0.90%	0.85%	0.85%	64.10%	100%
4	1.25%	1.35%	1.35%	1.40%	66.45%	100%
5	0.80%	0.80%	0.85%	0.80%	66.60%	100%
6	1.20%	1.15%	1.05%	1.00%	65.80%	100%
7	1.20%	1.25%	1.20%	1.25%	72.60%	100%
8	1.05%	1.05%	1.15%	1.05%	70.55%	100%
9	1.40%	1.40%	1.35%	1.40%	75.70%	100%
10	1.05%	0.95%	1.05%	1.00%	81.15%	100%
Ave.	1.03%	1.04%	1.03%	1.04%	68.29%	100%

Two interesting results can be found in these two tables: i) PRs are increased in the absence of FDIAs in Tables VIII and IX compared to that in Tables VI and VII. The reason is that line resistance is *not* reported to the control center in the *run-time-attack* stage. With a mismatch between the network model and the measurements, larger PRs are present even in the absence of FDIAs in the *run-time-attack* stage. ii) In all cases, the PRs in the presence of FDIAs and the PRs in the absence of FDIAs are still at a very similar level, demonstrating the *stealth* of FDIAs (i.e., the infeasibility to distinguish between FDIAs and regular noises) under network parameter uncertainties.

2) MMI Attack Strategy Under Moving Target Defense: It is shown recently that by perturbing line reactances via D-FACTS, the stealth of FDIA could be broken to facilitate attack detection [63], [64], [65], [66], [67], [68], [69]. In most power systems today, D-FACTS devices are still scarce. The simulations in this section assume that 40% transmission lines are equipped with D-FACTS devices, representing a possible future scenario with the significant proliferation of D-FACTS technologies. In the *pre-attack* stage, network parameters of IEEE 14-bus and 118-bus systems are extracted from standard databases [62]. In the *run-time-attack* stage, it is assumed that D-FACTS devices can perturb the line reactance within a rational interval, i.e., $[0.5\boldsymbol{X}_{std}, 1.5\boldsymbol{X}_{std}]$, where $\boldsymbol{X}_{std}$ represents the value of standard line reactance. It should be noted that MTD is implemented by randomly choosing the branches equipped with D-FACTS devices and the values of perturbations for all cases.

The PRs at different instants in the *attack interval* of the two test systems under *Scenario 3* along with those in the absence of FDIAs are presented in Tables X and XI, respectively. Two interesting results can be found in these two tables. i) PRs of Cases 4, 5, and 6 are larger than the case without FDIA, implying a full or partial success of the MTD in thwarting MMI FDIAs. Meanwhile, the PRs of Cases 1, 2, 3, 7, 8, 9, and 10 remain similar to the case without FDIA, indicating that the MTD is not effective in these cases. For example, in Case 1, the manipulated measurement channels include V_1, V_2, V_3, P_3, P_5, Q_2, and Q_5, and the falsified parameters include resistance/reactance/changing susceptance at branches 1-2, 1-5, 2-3, 2-4, 5-6, 4-9, and 4-7. In MTD, the perturbed reactance/changing susceptance are located at branches 9-10,

TABLE XI
PRs IN THE ATTACK INTERVAL UNDER SCENARIO 3 ALONG WITH THOSE IN THE ABSENCE OF FDIAs (THE IEEE 118-BUS SYSTEM UNDER MOVING TARGET DEFENSE)

In-stants	No FDIA	FDIAs				
		Case 6	Case 7	Case 8	Case 9	Case 10
1	1.05%	26.05%	1.10%	1.75%	1.05%	1.30%
2	1.15%	16.30%	1.30%	1.45%	1.15%	1.60%
3	0.80%	18.70%	1.05%	1.30%	0.85%	1.50%
4	1.05%	16.50%	1.20%	1.50%	1.05%	1.30%
5	0.80%	43.90%	0.95%	1.10%	0.90%	1.35%
6	1.15%	28.75%	1.20%	1.55%	1.15%	1.35%
7	1.25%	22.30%	1.40%	1.60%	1.25%	1.50%
8	1.15%	34.20%	1.30%	1.65%	1.25%	1.60%
9	0.65%	23.65%	0.65%	1.10%	0.65%	0.95%
10	0.70%	31.95%	0.80%	1.10%	0.65%	1.15%
Ave.	0.98%	26.23%	1.10%	1.41%	1.00%	1.36%

9-14, 10-11, 6-11, 6-12, 6-13, 12-13, and 13-14. In Case 5, the manipulated measurement channels include Q_1, Q_5, P_{1-2}, P_{1-5}, Q_{1-2}, Q_{1-5}, and Q_{2-4}, and the falsified parameters include resistance/reactance/changing susceptance at branches 1-2, 1-5, 2-5, 2-4, 2-3, 3-4, 4-5, 5-6, 4-9, and 4-7. In MTD, the perturbed reactance/changing susceptance are located at branches 1-2, 1-5, 2-5, 2-4, 2-3, 3-4, 4-5, and 7-8. Based on the network topology of the IEEE 14-bus system, it can be found that the manipulated measurement channels and parameters do not cover or adjoin any branch that is equipped with D-FACTS devices in Case 1, but they cover or adjoin most of the branches that are equipped with D-FACTS devices in Case 5. The simulation results suggest that the MMI attack vector can still bypass BDD if the manipulated measurement channels and parameters do not include or adjoin branches that are deployed with D-FACTS devices in MTD. This echoes the existing research on MTD against measurement attacks only [63], [64], [65]: *MTD can thwart all possible measurement FDIAs if and only if the deployment of D-FACTS devices covers branches at least containing a spanning tree of the grid graph*. In our designed cases, only 40% branches, i.e., 8 branches for the IEEE 14-bus system and 72 branches for the IEEE 118-bus system, are assumed to be equipped with D-FACTS devices. Hence, attackers may still have opportunities to launch stealthy FDIAs to modify the state variables on these buses whose incident branches are not deployed with D-FACTS devices. ii) PRs of Cases 4, 5, and 6 are different, implying that the performance of MTD varies even among the cases where it shows effectiveness. The performance of MTD may be affected by the distribution of measurement errors, the values of attack targets, and the degree of line perturbations, etc. Overall, the simulation results provide intuitive insight into the effect of MTD on the detection of MMI attacks, yet systematic studies are required to further understand and extend the design of MTD for defense against the joint model-measurement attacks, which is well beyond the scope of this paper.

VIII. CONCLUSION AND FUTURE WORK

This paper proposes a general two-stage MMI FDIA framework to reveal the cyber threats against both measurement data and network parameter data as well as their possible interaction. Compared with the bulk of the existing measurement FDIA strategies, it is shown that the coordination with network parameter FDIA significantly reduces the required number of measurement channels to manipulate in run-time. The MMI FDIA is formulated as an AGBP problem to achieve the *sparsity* and *stealth* properties. It is shown that the weight adaptation is critical for sparsifying the measurement channels to compromise. The proposed attack takes a two-stage process to mimic the attack planning activities of cyber adversaries. It is shown that such planning activities can help select measurement channels to keep the attack *stealthy* during the whole attack interval with operating point variations. Simulation results in the IEEE 14-bus test system and the IEEE 118-bus test system demonstrate the *stealth* and *sparsity* of the developed MMI FDIA framework.

Future studies may involve the impact analysis of MMI FDIAs on power system operations and effective countermeasures. It is known that the operation of electricity markets is heavily dependent on network parameters. Errors in network parameters can impact the transmission line congestion patterns, LMPs, and financial transmission right (FTR) revenues, thus misleading the operation of electricity markets [36]. Compared to conventional errors or measurement FDIAs, MMI FDIAs incorporate the manipulations of measurements and network parameters simultaneously, which is more complex and may lead to unpredictable results. Hence, the impact analysis of MMI FDIAs on the electricity market is worth further investigation. Moreover, security assessment, including contingency analysis and transient stability simulation algorithms, is an essential function in modern EMS. An accurate security assessment can provide operators with reliable dispatch plans for system operation. Similarly, the security assessment algorithms are also heavily dependent on network parameters. If network parameters are manipulated or biased, operators may miss critical security violation scenarios and make a wrong decision, resulting in severe consequences, such as cascading failures, once a fault occurs. Hence, it is desirable to study the impact of MMI FDIAs on security assessment in the future.

In addition, effective countermeasures against MMI attacks are worth further investigation in the future. One possible defense strategy is to develop a secure dedicated backup mechanism to detect model parameter falsifications. Specifically, the backup database should not be automatically synchronized with the regular database, which is subject to malicious false data injection. On the contrary, it is located in a well-protected "trust zone", and the data communication between the trust zone and the external network (including the regular database) is one-way: only the trust zone can access the external network, not the other way around. At the same time, the trust zone is also installed with an FDIA detection algorithm that stores the information about which parameters are likely to be manipulated by cyber adversaries, which is obtained from an impact analysis of model parameters on power flow patterns. With this, the FDIA detection algorithm located in the trust zone can identify suspicious parameter change behaviors and raise alarms to security personnel for investigating the related activities.

Another possible defense approach is the MTD by proactively perturbing branch reactance with D-FACTS [63], [64], [65], [66], [67], [68], [69]. This idea is shown to be capable of breaking the stealth property of measurement FDIAs, thus making them detectable. However, D-FACTS devices will remain limited in number in most power systems in the near future. While there have been extensive studies on the MTD for measurement FDIAs [63], [64], [65], [66], [67], [68], [69], it is critical to investigate the necessary/sufficient conditions for D-FACTS configurations against MMI FDIAs as well as optimal placement and operation strategies. In addition, it is imperative to study how the distribution of measurement errors, the values of attack targets, and the degree of line reactance perturbations impact the performance of MTD, as shown to be critical by the simulation results in this paper.

Besides the aforementioned potential strategies, other countermeasures could also be developed against the proposed MMI attack model. Overall, the ultimate motivation of the paper is to draw the attention of the technical community on the security vulnerabilities regarding model-measurement datasets in power system operation and encourage research and implementation of effective defense measures.

REFERENCES

[1] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control*, Atlanta, GA, USA, 2010, pp. 5991–5998.

[2] Y. Mo et al., "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[3] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[4] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[5] *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, E-ISAC, Washington, DC, USA, 2016.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[7] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[8] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 128–138, Jan. 2019.

[9] J. Chen et al., "Impact analysis of false data injection attacks on power system static security assessment," *J. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, Jul. 2016.

[10] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber–physical power system," *IET Cyber Phys. Syst. Theory Appl.*, vol. 4, no. 2, pp. 101–107, Jun. 2019.

[11] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber–physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[12] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[13] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 1–33, 2011.

[15] G. Cheng, Y. Lin, J. Zhao, and J. Yan, "A highly discriminative detector against false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2318–2330, May 2022.

[16] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.

[17] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[18] 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.

[19] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.

[20] S. N. Edib, Y. Lin, V. M. Vokkarane, F. Qiu, R. Yao, and D. Zhao, "Optimal PMU restoration for power system observability recovery after massive attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1565–1576, Mar. 2021.

[21] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[22] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[23] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.

[24] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[25] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan./Feb. 2012.

[26] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior rule-based insider threat detection for smart grid," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 190–205, Apr. 2016.

[27] Z. Liu and L. Wang, "Defense strategy against load redistribution attacks on power systems considering insider threats," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1529–1540, Mar. 2021.

[28] K. E. Hemsley and R. E. Fisher, "History of industrial control system cyber incidents," Idaho Nat. Lab, Idaho Falls, ID, USA, Rep. INL/CON-18-44411-Rev002, 2018.

[29] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber–physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[30] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.

[31] M. Cui, J. Wang, and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyberattacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724–5734, Sep. 2019.

[32] Q. Zhang and F. Li, "Cyber-vulnerability analysis for real-time power market operation," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3527–3537, Jul. 2021.

[33] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438–3446, Jul. 2020.

[34] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.

[35] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2487–2497, Sep. 2015.

[36] Y. Lin, A. Abur, and H. Xu, "Identifying security vulnerabilities in electricity market operations induced by weakly detectable network parameter errors," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 627–636, Jan. 2021.

[37] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*, New York, NY, USA: Marcel Dekker, 2004.

[38] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection attack on state estimation in power systems—Attacks impacts and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[39] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts," *Renew. Sust. Energy Rev.*, vol. 163, Jul. 2022, Art. no. 112423.
[40] A. M. Tillmann, "Equivalence of linear programming and basis pursuit," *Proc. Appl. Math. Mech.*, vol. 15, no. 1, pp. 735–738, Oct. 2015.
[41] N. I. A. Tawalbeh, "Daily load profile and monthly power peaks evaluation of the urban substation of the capital of Jordan Amman," *Electr. Power Energy Syst.*, vol. 37, pp. 95–102, May 2012.
[42] P. Zarco and A. G. Exposito, "Power system parameter estimation: A survey," *IEEE Trans. Power Syst.*, vol. 15, no. 1, pp. 216–222, Feb. 2000.
[43] "System load graphs: ISO New England-real-time maps and charts." Accessed: Dec. 2020, [Online]. Available: https://www.iso-ne.com/isoexpress/web/charts
[44] E. J. Candes, M. B. Wakin, and S. Boyd, "Enhancing sparsity by reweighted $\ell 1$ minimization," *J. Fourier Anal. Appl.*, vol. 14, pp. 877–905, Dec. 2008.
[45] H. Wang and C. Leng, "A note on adaptive group lasso," *Comput. Stat. Data Anal.*, vol. 52, pp. 5277–5286, Aug. 2008.
[46] C. Zhang and Y. Xiang, "On the oracle property of adaptive group lasso in high-dimensional linear models," *Stat. Papers*, vol. 57, no. 1, pp. 249–265, Mar. 2016.
[47] B. Jimnez, J. L. Lzaro, and J. R. Dorronsoro, "Finding optimal model parameters by discrete grid search," *Adv. Soft Comput.*, vol. 44, pp. 120–127, 2007.
[48] P. Liashchynskyi and P. Liashchynskyi, "Grid search, random search, genetic algorithm: A big comparison for NAS," 2019, *arXiv:1912.06059*.
[49] H. Zou, "The adaptive lasso and its oracle properties," *J. Amer. Stat. Assoc.*, vol. 101, no. 476, pp. 1418–1429, 2006.
[50] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, Jan. 2011.
[51] J. Eckstein and D. P. Bertsekas, "On the Douglas—Rachford splitting method and the proximal point algorithm for maximal monotone operators," *Math. Program.*, vol. 55, pp. 293–318, Apr. 1992.
[52] R. Nishihara, L. Lessard, B. Recht, A. Packard, and M. Jordan, "A general analysis of the convergence of ADMM," in *Proc. 32nd Int. Conf. Mach. Learn.*, 2015, pp. 343–352.
[53] Y. Wang, W. Yin, and J. Zeng, "Global convergence of ADMM in nonconvex nonsmooth optimization," *J. Sci. Comput.*, vol. 78, pp. 29–63, Jan. 2019.
[54] Q. Liu, X. Shen, and Y. Gu, "Linearized ADMM for nonconvex nonsmooth optimization with convergence analysis," *IEEE Access*, vol. 7, pp. 76131–76144, 2019.
[55] F. Palacios-Gomez, L. Lasdon, and M. Engquist, "Nonlinear optimization by successive linear programming," *Manage. Sci.*, vol. 28, no. 10, pp. 1106–1120, 1982.
[56] J. Nocedal and S. J. Wright, *Numerical Optimization*. New York, NY, USA: Springer, 2006.
[57] M. A. Noor and M. Waseem, "Some iterative methods for solving a system of nonlinear equations," *Comput. Math. Appl.*, vol. 57, no. 1, pp. 101–106, 2009.
[58] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including PMU and SCADA measurements," *Electr. Power Syst. Res.*, vol. 81, no. 7, pp. 1514–1524, 2011.
[59] Z. Fang et al., "A comprehensive framework for robust AC/DC grid state estimation against measurement and control input errors," *IEEE Trans. Power Syst.*, vol. 37, no. 2, pp. 1067–1077, Mar. 2022.
[60] M. Rasouli, D. T. Westwick, and W. D. Rosehart, "Reducing induction motor identified parameters using a nonlinear LASSO method," *Electr. Power Syst. Res.*, vol. 88, pp. 1–8, Jul. 2012.
[61] R. Gao, S. Särkkä, R. Claveria-Vega, and S. Godsill, "Autonomous tracking and state estimation with generalized group lasso," *IEEE Trans. Cybern.*, vol. 52, no. 11, pp. 12056–12070, Nov. 2022.
[62] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[63] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020.
[64] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. Inf. Forensic Security*, vol. 15, pp. 2320–2335, 2020.
[65] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and M.-Y. Chow, "Security enhancement of power system state estimation with an effective and low-cost moving target defense," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Nov. 29, 2022, doi: 10.1109/TSMC.2022.3222793.
[66] S. Lakshminarayana and D. K. Y. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, Mar. 2021.
[67] B. Liu and H. Wu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4345–4357, Sep. 2020.
[68] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 763–776, Aug. 2018.
[69] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 245–256, Mar. 2022.

Gang Cheng (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering and automation from Henan Polytechnic University, Jiaozuo, China, in 2016, and the M.S. degree in control theory and control engineering from Guangxi University, Nanning, China, in 2019. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA, USA. His current research interests include situational awareness, cyber security, and data analysis of power systems.

Yuzhang Lin (Member, IEEE) received the bachelor's and master's degrees from Tsinghua University, Beijing, China, and the Ph.D. degree from Northeastern University, Boston, MA, USA. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA, USA. His research interests include modeling, situational awareness, data analytics, and cyber-physical resilience of smart grids. He is a recipient of the NSF CAREER Award. He serves as the Co-Chair of the IEEE PES Task Force on Standard Test Cases of Power System State Estimation, and the Secretary of IEEE PES Distribution System Operation and Planning Subcommittee.

Jun Yan (Member, IEEE) received the B.Eng. degree in information and communication engineering from Zhejiang University, China, in 2011, and the M.S. and Ph.D. (with Excellence in Doctoral Research) degrees in electrical engineering from the University of Rhode Island, USA, in 2013 and 2017, respectively. He is currently an Assistant Professor with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada. His research focuses on computational intelligence and cyber–physical security, with applications in smart grids, smart cities, and other smart critical infrastructures. His research has been funded by NSERC, FRQNT, FRQSC, CFI, and Mitacs. He was also the recipient of several best paper awards at IEEE ICC, IEEE WCCI, and among others.

Junbo Zhao (Senior Member, IEEE) received the Ph.D. degree from the Bradley Department of Electrical and Computer Engineering, Virginia Tech in 2018.

He is an Assistant Professor with the Department of Electrical and Computer Engineering, University of Connecticut. He was an Assistant Professor and a Research Assistant Professor with Mississippi State University and Virginia Tech from 2019 to 2021 and from 2018 to 2019, respectively. He was a Research Assistant Professor with Virginia Tech from May 2018 to August 2019. He did the summer internship at Pacific Northwest National Laboratory from May to August 2017. He has published three book chapters and more than 140 peer-reviewed journal and conference papers, where more than 70 appear in IEEE Transactions. His research interests are cyber-physical power system modeling, estimation, security, dynamics and stability, uncertainty quantification, renewable energy integration and control, robust statistical signal processing, and machine learning. He is the receipt of the best paper awards of 2020 and 2021 IEEE PES General Meeting (three papers) and 2019 IEEE PES ISGT Asia. He received the 2020 Top 3 Associate Editor Award from IEEE TRANSACTIONS ON SMART GRID, the 2020 IEEE PES Outstanding Engineer Award, and the 2021 IEEE PES Outstanding Volunteer Award. He has been listed as the 2020 and 2021 World's Top 2% Scientists released by Stanford University in both Single-Year and Career tracks. He serves as the Editor for IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE TRANSACTIONS ON SMART GRID, and IEEE POWER AND ENGINEERING LETTERS, an Associate Editor of *International Journal of Electrical Power & Energy Systems*, and the Subject Editor of *IET Generation, Transmission & Distribution*. He is currently the Chair of the IEEE Task Force on Power System Dynamic State and Parameter Estimation, the IEEE Task Force on Cyber-Physical Interdependency for Power System Operation and Control, the Co-Chair of the IEEE Working Group on Power System Static and Dynamic State Estimation, the Secretary of the IEEE PES Bulk Power System Operation Subcommittee, and the Officer of the IEEE PES Renewable Systems Integration Coordinating Committee.

Linquan Bai (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Tianjin University, Tianjin, China, in 2010 and 2013, respectively, and the Ph.D. degree in electrical engineering from the University of Tennessee, Knoxville, TN, USA, in 2017.

He is an Assistant Professor with the University of North Carolina at Charlotte, Charlotte, NC, USA. His research interests include grid integration of distributed energy resource, power system operation and optimization, and electricity markets. He is an Associate Editor of IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, IEEE POWER ENGINEERING LETTERS, and *Journal of Modern Power System and Clean Energy*.