A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids

Ahmed S. Musleh, *Member, IEEE*, Guo Chen, *Member, IEEE*, and Zhao Yang Dong, *Fellow, IEEE*

***Abstract*—Cyber-physical attacks are the main substantial threats facing the utilization and development of the various smart grid technologies. Among these attacks, false data injection attack represents a main category with its widely varied types and impacts that have been extensively reported recently. In addressing this threat, several detection algorithms have been developed in the last few years. These were either model-based or data-driven algorithms. This paper provides an intensive summary of these algorithms by categorizing them and elaborating on the pros and cons of each category. The paper starts by introducing the various cyber-physical attacks along with the main reported incidents in history. The significance and the impacts of the false data injection attacks are then reported. The concluding remarks present the main criteria that should be considered in developing future detection algorithms for the false data injection attacks.**

***Index Terms*—Cyber-physical attacks, data-driven detection algorithms, false data injection, machine learning, model-based detection algorithms, smart grid, state estimation, stealth attacks.**

I. Introduction

ACCORDING to the IEEE Grid Vision 2050, the main expectancy of the smart grid is to have the control and automation processes spread over the entire power grid to allow efficient and reliable bidirectional power flow [1]. This is realized through the integration of the Information and communication technologies (ICT) into the power grid which makes it a form of cyber-physical system (CPS) [2]. The dynamic integration between the real and virtual worlds opened a huge door of possible technologies, algorithms, and solutions to be developed and implemented in the smart grid such as distributed data processing and artificial intelligence [3].

With its promising technologies, smart grid shall revolutionize our society, economy, and environment. Large and small corporations expected the smart grid technologies' emerging markets and rushed to be the first to deliver. However, security aspects have taken the backseat within this rush. With the introduction of the widely varied ICT components, the vulnerability of smart grid has been compromised massively. This formed a huge concern over the reliability and the security of the ever-wanted smart grid with the massive threats ranging from economic to stability perspectives. Thus, several research efforts have been conducted toward the security augmentation of smart grid by firstly understanding the different vulnerability points and by secondly proposing suitable and reliable solutions either on the cyber or the physical layer. These efforts came in response to the ever-increasing cyber-physical attacks on smart grid as illustrated next.

A. History of Cyber-Physical Attacks in Energy Sector

Throughout the last decades, several cyber-physical attacks have been announced in the sector of energy industry. This goes as far as 1982 when the first major attack was proclaimed. These attacks had diverse levels of impact. While some have not been noticed at all, others caused explosions, million dollars losses, and life losses. The increasing number of these incidents is the real threat. Between 2011 and 2014, the Energy Department of the USA received a total of 362 power interruption reports that are related to cyber-physical attacks in one way or another; 161 were reported in 2013 compared to 31 in 2011 [4]. According to the 2017 state of industrial cybersecurity report, 54% of the companies surveyed (359 companies in 21 countries) proclaimed that they have experienced a cyber-physical security issue in the past 1 year, and 21% have experienced two issues within the same time frame [5]. Figure 1 illustrates the major incidents reported in the energy sector.

In 1982, a massive gas pipeline explosion took place in the Siberian wilderness. The details behind this explosion come from the U.S. officials' memories of the cold war era. Based on these memories, the CIA has deliberately manipulated the gas pipeline control software which led the valves' control to misbehave resulting in severe crossing of pressure limits which eventually led to a massive explosion [6].

In 2003, the well-known Slammer worm penetrated the control system of the David-Besse nuclear plant in Ohio, USA. The worm got to the plant network through the contractor's network. The effect of this penetration resulted in disabling the safety parameters and indicators system for 5 hours. Thus, the control room engineers were not able

Manuscript received May 29, 2019; revised September 8, 2019; accepted October 14, 2019. Date of publication October 30, 2019; date of current version April 21, 2020. This work was supported in part by the Australian Research Council under Grant DP180103217, Grant FT190100156, and Grant IH180100020, and in part by the UNSW Digital Grid Futures Institute, UNSW, Sydney, under a Cross Disciplinary Fund Scheme. Paper no. TSG-00757-2019. *(Corresponding author: Guo Chen.)*

The authors are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: a.musleh@student.unsw.edu.au; guo.chen@unsw.edu.au; joe.dong@unsw.edu.au).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2019.2949998

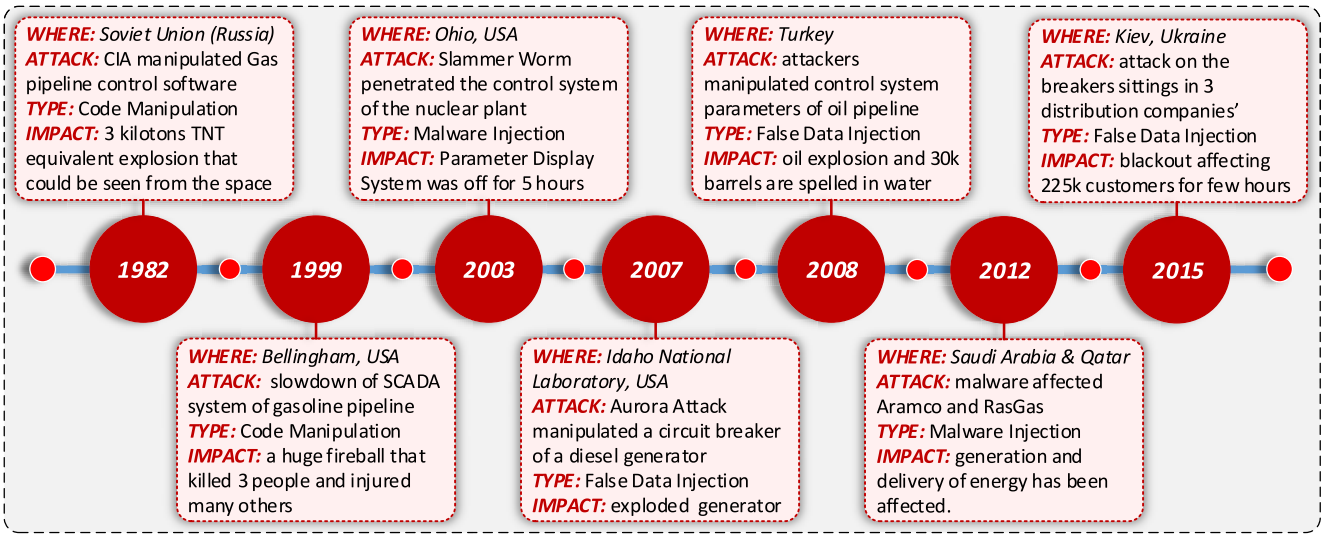

Fig. 1. Timeline of the major cyber-physical attacks in the energy industry sector.

to monitor crucial parameters such as the reactor's core temperature [7].

In 2007, the U.S. Department of Homeland Security staged a cyber-attack code-named "Aurora". During this attack, a hacker penetrated the control system of a test generator causing a rapid succession of turning on and off its circuit breaker. This created a serious desynchronization between the mechanical inertia of the generator and the electrical inertia of the grid resulting in the explosion of the $1 million generator which is widely utilized across the USA [8].

On December 23, 2015, a wide blackout took place in Kiev, Ukraine for several hours. This blackout affected three major distribution companies and more than 225,000 customers. Six months of investigations following the mysterious blackout led to the conclusion of the foreign cyber-attack involvement. During this attack, seven 110kV and 23kV substations were affected. The hackers penetrated the Supervisory Control and Data Acquisition (SCADA) system and started to open several circuit breakers in the distribution system. Consequently, the operators had no access to the SCADA system and had to restore the circuit breakers in a manual procedure [9].

Following this, another Kiev-based cyber-attack took place in 2016 where the hackers shut off 200MW of the generation capacity which is equivalent to 20% of the city's night-time electrical energy consumption [10].

These incidents and their massive impacts led the governments worldwide to recognize these emerging threats. In 2013, the White House announced the Executive Order 13636 to enhance the cybersecurity of the critical infrastructures [11]. In 2014, the National Institute of Standards and Technology (NIST) issued a three-volume report to frame the basic guidelines for the smart grid's cyber security [12]. Researchers were directed globally to further investigate the possibilities, impacts, and solutions to the cyber-physical attacks. This starts by first identifying the different attack types.

B. Taxonomy of the Cyber-Physical Attacks

Being a form of CPS means that all the types of the different cyber-physical attacks are applicable to the smart grid structure. In order to understand the different types of these attacks, it is necessary to classify them according to the way the attack is delivered [13]. Figure 2 illustrates the taxonomy of the different cyber-physical attacks according to their delivery methods that could be classified into four main groups as discussed next. It must be noted that a coordinated attack is also a possibility where multiple attacks are combined together to further enhance the attacking mechanism [14].

Cyber-based attacks are solely delivered through the cyber layer of the system. Code manipulation is considered the main attack in this category where the adversary changes the software or the firmware of the system according to his agenda. Command manipulation represents a change in the commands that are already stored in the system without creating new commands. Malware injection is a quite common type where a virus or a worm is injected in the system. False data injection attack (FDIA) manipulates the data without affecting the code of the system. Sleep deprivation refers to the rapid exhaustion of the devices by forcing them not to enter the low-power mode and to constantly perform an action or to receive, process, or transmit data. Other cyber-based attacks include supply chain attack, database manipulation, and password cracking.

Network-based attacks are constructed through the virtual network access without affecting the software or the firmware of the system nor the physical communication link. Denial of service is the main attack in this category where the network is inaccessible due to large volume of meaningless packets. Black/grey hole is the situation where the adversary drops the packets in the network either fully in the black case, or in a selective manner as in the grey case. Similarly, FDIA is possible even in the network layer as well where the adversary manipulates the data within the packets in

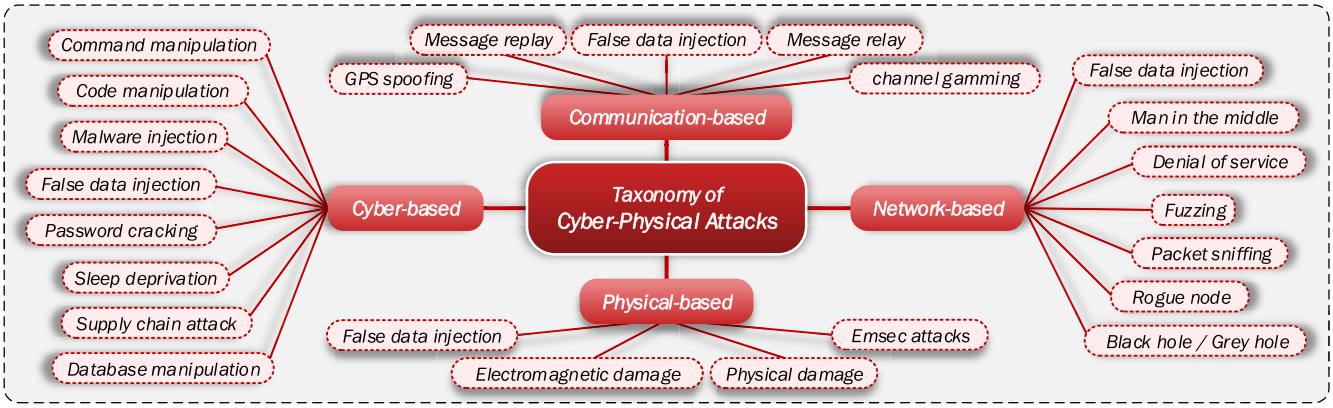

Fig. 2. The taxonomy of cyber-physical attacks according to their delivery method.

the network. Other network-based attacks include man-in-the-middle, packet sniffing, rogue node, and fuzzing. Spy-based attacks like packet sniffing are usually the preparatory step for FDIA.

Communication-based attacks rely on the actual physical communication link in delivering the attacks without any manipulation at the virtual network of the CPS. These attacks could be developed either by breaking down the communication channel (channel gamming) or by delivering falsified messages (FDIA). GPS spoofing is a form of FDIA on the GPS signal delivered to the system where the adversary imitates the GPS signal and injects falsified data in it. Message replay and relay attacks are other well-known communication-based attacks. Effects of communication-based attacks have a profound effect on the CPS since tremendous data is carried through these communication channels.

Physical-based attacks are the physical breaches of the system. Physically damaging the system is the main type of physical-based attacks. However, without physically touching the physical parts, other physical attacks are possible such as Electromagnetic damage like an overvoltage or an electromagnetic pulse. FDIA is also a possibility at the physical layer where the input of a specific device could be manipulated to have falsified readings. Other physical-based attacks include emission security (EmSec) attacks that are dependent on the emanations of the system such as the heat, light, sound, or the electromagnetic radiation. These spy-based attacks are usually the preparatory step for a FDIA.

Looking deeply into the taxonomy of the cyber-physical attacks, we can easily note that FDIA is common between the different delivery-based categories. It could be applied at all the layers of the CPS. While all these attacks are equally dangerous, FDIA poses greater danger for its difficulty to detect as advised by NIST [12]. Unlike other attack types, the system may seem to be operating normally without noticing the existence of the FDIA.

C. Related Work and Main Contributions

Several research efforts have been made to further understand and summarize the different cyber-physical attacks including FDIA in smart grids. In [15], the authors provide a state-of-the-art survey of the most relevant cybersecurity issues in smart grids. Communication-based attacks in smart grids are surveyed in [16]. Within the same generalized perspective, authors of [17] and [18] give brief reviews of the attack threats and defense strategies in smart grids with visionary futuristic challenges to be faced in this area. A similar approach was reported in [19] with a focus on FDIA, and a brief review was given on the effect of FDIA on state estimation in [20]. To the best of the authors' knowledge, no detailed study has been conducted on the different detection algorithms of FDIA in smart grids. Therefore, with the aim of filling this vital research gap in this area, the main contributions of this paper are:

- To present a summarized and detailed review on the different detection algorithms of FDIA in smart grids.
- To compare the different detection algorithms and provide an insight on the pros and cons of each detection category.
- To provide an intuition on the remaining challenges in this area along with the comprehensive criteria for future algorithms to be developed.

This manuscript is organized within 5 sections. Section II starts by addressing the main vulnerabilities of the smart grid from FDIA. It further discusses the different possible impacts associated with these attacks at the various levels of the smart grid. Section III discusses in details the different detection algorithms developed to address the FDIA threats. Comparative analyses are illustrated in Section IV, and concluding and future research direction remarks are presented in Section V.

II. FDIA Vulnerabilities and Impacts in Smart Grids

As a form of CPS, smart grid is a complicated connection of many systems that are working together in harmonious manner. Even though these systems operate at different levels, ratings, and at distant spaces, they all have vital roles to the operation of the smart grid. Consequently, a FDIA at any of them can positively compromise the overall operation of the smart grid.

A. Vulnerabilities of Smart Grids Towards FDIA

As discussed previously, FDIA is applicable to the different systems and layers in the smart grid. These could be summarized in four categories:

- *Physical-based FDIA:* This includes the attacks on the monitoring, control, and protection devices. Full possibilities of physical layer attacks are presented in [19], where the different equipment access levels are discussed. Authors of [21] illustrate how a FDIA could be implemented in any processor-based device. They show how a FDIA is implemented via the modification of the firmware of the remote terminal units (RTU). This firmware is first extracted from the flash memory of the digitized RTU. Even though these attacks are very limited to the device that is attacked, they could still make catastrophic consequences in the smart grid.
- *Communication-based FDIA:* Authors of [22] present an in-depth analysis of the different communication systems utilized in smart grid and their associated vulnerabilities. In [23], the authors study the effects of communication-based FDIA in the networked control systems. This type of attacks is far more probable than the physical-based one. This is due to the ease of implementation. Physical and communication-based attacks require the adversary to be in a proximity to the physical device or the communication link. This limits the chances of these attacks to occur.
- *Network-based FDIA:* Unlike previous FDIA, network-based FDIA is possible from anywhere if the adversary gets access to any node in the network. Authors of [24] demonstrated how a FDIA is possible on the IEC61850 standard Ethernet-based communication protocol. They further illustrated the possible impacts in the smart distribution substation. In [25], the authors developed a testbed where the adversary can penetrate the network of the monitoring system of the smart grid. This is done through manipulating specific node in the network on a TCP/IP Modbus.
- *Cyber-based FDIA:* These attacks are the ones where the adversary penetrates either the control system or the applications associated (also known as process layer) with it such as the prediction, estimation, economic dispatch, energy trading, etc... Like network-based attacks, cyber-based attacks are highly dangerous for they have a far greater effect in the system. However, these are not that much common as compared to the network and communication-based attacks. This is due to the increased security measures on these systems such as the multiple firewalls associated. Authors of [26] illustrate several possible cyber-based FDIA and the associated impacts in the power grid.

Figure 3 illustrates the different possible vulnerabilities of smart grid towards FDIA. From these different layer-based FDIA, the only drawn conclusion is that the more technology advances, the more vulnerability points are created.

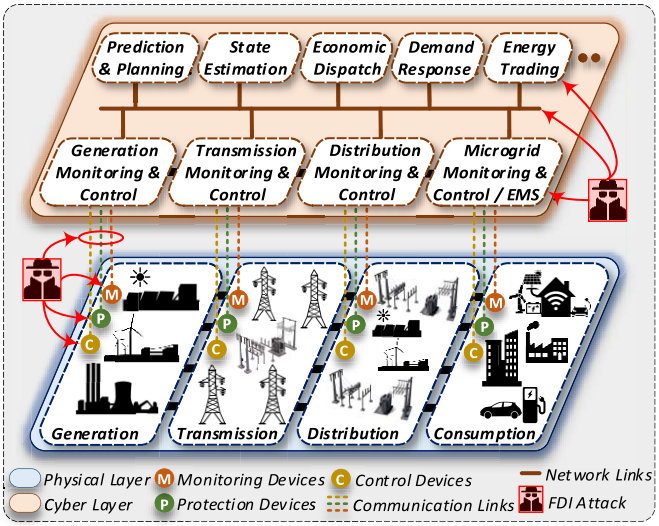

Fig. 3. Vulnerabilities of smart grid towards false data injection attacks.

B. Impacts of FDIA on Smart Grids

As illustrated in the previous section, cyber-physical attacks could lead to disastrous consequences with serious losses in budget and more importantly human lives. Authors of [27], presented the first published paper to ever investigate the varied range of possible FDIA and its impacts on smart grids. Through the last decade, FDIA's impacts have been researched significantly showing the wide range of impacts.

1) Economic Impacts: Economic impacts of FDIA are the main concerns as money worries the most. In most of the cases, the adversaries are after some economical goals, either affecting the economy of specific nation or making some personal profits out of these FDIA. Economic impacts of FDIA could be summarized in two distinctive points as discussed next.

Operational cost impacts are associated with the FDIA that leads to extreme implications on the cost of the grid operation. These include changes in the topology of the grid as well as the generation schedules. Authors of [28] illustrate the possible impacts of FDIA on the topology of the grid. They demonstrate that a well-planned FDIA attack could possibly mask a transmission line outage which would result in significant operational losses. A similar approach is illustrated in [29], where the developed topology attack could alter the operation of the power grid resulting in significant losses. Authors of [30], [31] introduced a detailed investigation of the effect of FDIA on the energy market process specifically the locational marginal prices (LMP). Since LMP depends essentially on the accurate topology and the precise real-time measurements, any wrong data in these vectors manipulate the LMP massively. In [32], the authors illustrate how a well-designed FDIA on circuit breakers' statuses could lead to significant losses reaching up to $100,000 over a single 24 hours period. Even though this FDIA poses no stability issues on the grid, its economic loss is a real threat.

Energy theft is a major goal for many adversaries committing FDIA. Through FDIA, the adversary can make actual

profits either by manipulating the data in the grid or by manipulating their own meters. Both cases result in reduced electrical bill and increased unauthorized profits [33], [34]. Authors of [35] examine the effect of FDIA on electricity market. They further develop an algorithm to find the optimal FDIA that would maximize the profit accordingly. However, they assume that the adversary has a full knowledge of the grid. To overcome this assumption, the author of [36] proposed new attack models on the LMP that could have a great effect on the energy market and does not need a full knowledge of the grid. This illustrates a particularly critical issue for the ease of conducting this FDIA.

2) Stability Impacts: Stability impacts are associated with the erroneous measures taken in response to FDIA in the smart grid. Authors of [37] illustrated how a FDIA attack could lead to an unnecessary generation rescheduling and load shedding. This is done by injecting fake measurements. Based on these fake measurements the operation and control of the power grid is taking falsified responses or no responses which leads eventually to unstable conditions. In [38], the authors illustrated how a FDIA in the GPS signal could lead to a major load shedding. This load shedding is based on the out-of-step protection scheme that utilizes GPS-based sensors. Once the GPS signal is spoofed, the protection scheme takes falsified action by initiating unnecessary load shedding. Automatic generation control (AGC) system is also considered to be an extremely attractive system for adversaries for its profound effect on the power grid. In [39], the authors developed a FDIA on the AGC system and elaborated on the dangerous impact of the frequency deviation of the generator. The effect of the FDIA in the wide area control system is studied in [40], where the falsified measurements lead the secondary voltage controller to develop inaccurate setpoints for the voltage controller in the grid. This results in demolishing the overall stability of the system. Frequency-based FDIA is studied thoroughly in [41], where the authors discuss the impacts of FDIA in frequency control of smart grid. They also illustrate how a simple FDIA could propagate and lead to a full blackout. It must be noted that stability impacts do pose economic impacts as well; they are two sides of same coin. For these many threats and impacts, numerous detections algorithms were developed in literature.

III. False Data Detection Algorithms

Several directions have been taken in the goal of detecting FDIA in smart grids. While these directions differ massively, two main themes are noted. These are model-based detection algorithms and data-driven detection algorithms.

A. Model-Based Detection Algorithms

Smart grids are modelled based on the streaming real-time measurements along with the static system data such as the system parameters and substations configuration. Intentional manipulation of these measurements or data is a form of FDIA. Based on the operating condition, the model of the smart grid could be either of quasi-static or dynamic nature [42].

Quasi-static model represents the scenario in which the system's operating points change in a smooth and slow nature with the assumption of instantaneous response of the controllers in the system. This yields negligible transient response. Under this assumption, the various systems in smart grids could be modeled using the general measurement model realized as:

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

where $\boldsymbol{z} \in \mathbb{R}^n$ represents the measurement vector of the system (e.g., voltage magnitude, voltage angle, power flow, current, etc.); $\boldsymbol{x} \in \mathbb{R}^m$ is the state vector (e.g., nodal complex voltages); $\boldsymbol{h}(.) \in \mathbb{R}^n$ are system-defined nonlinear functions that depend on the system parameters and topology and relate the measurement vector $\boldsymbol{z}$ to the state vector $\boldsymbol{x}$; and $\boldsymbol{e} \in \mathbb{R}^n$ represents the measurement error with zero mean and a variance of $\boldsymbol{\sigma}^2 \in \mathbb{R}^n$. It must be noted that the number of the states and the measurements may not be the same.

Dynamic model is adopted when the transients or the dynamical changes in the system are considered. In this modelling approach, the states of the system are dependent not only on the current measurements and data, but also on the earlier states of the system. This model can be realized as:

$$\begin{cases} z_t = \boldsymbol{h}(\boldsymbol{x}_t) + \boldsymbol{e} & \text{(2a)} \\ \boldsymbol{x}_t = \boldsymbol{f}(\boldsymbol{x}_{t-1}) + \boldsymbol{v} & \text{(2b)} \end{cases}$$

where t denotes the time instant; $\boldsymbol{f}(.) \in \mathbb{R}^m$ are system-dependent nonlinear functions that relate the state vector $\boldsymbol{x}_t$, to the previous state vector $\boldsymbol{x}_{t-1}$; and $\boldsymbol{v} \in \mathbb{R}^m$ is the error term that represents the time discretization and model approximation error with zero mean and a variance of $\mathcal{R} \in \mathbb{R}^m$.

Erroneous data that are present in the measurements collected from the smart grid could be either of natural causes (e.g., device malfunction) or of intentional causes such as FDIA. These errors or attacks could be modelled as a malicious measurement vector $z_t^{\alpha} = z_t + \boldsymbol{\alpha}_t$, where $\boldsymbol{\alpha}_t \in \mathbb{R}^n$ represents the erroneous data that manipulates the original measurements vector z_t. The traditional method considered in detecting erroneous data is based on the residual test. In this test, the residual $\boldsymbol{r}_t = \|z_t - \boldsymbol{h}(\boldsymbol{x}_t)\|$ is compared to predefined system-based threshold value τ. Thus, an erroneous datum is present if and only if $\boldsymbol{r}_t \geq \tau$. While the residual test operates adequately in the presence of malicious measurement vector z_t^{α} most of the time, it fails in detecting more complicated cases. FDIA that is detected via the traditional residual test is known to be an observable attack and is termed as *"Basic FDIA"*. On the other hand, FDIA that is not perceived via the traditional residual test is known to be unobservable attack and is termed as *"Stealth FDIA"*. A stealth FDIA is a coordinated multiple well-designed injections of a malicious measurement vector $z_t^{\alpha} = z_t + \boldsymbol{\alpha}_t$ that resembles the normal covariance of the correct measurements in the system with $\boldsymbol{\alpha}_t = \boldsymbol{h}(\boldsymbol{c}_t)$, where $\boldsymbol{c}_t \in \mathbb{R}^m$ is an arbitrary nonzero vector. This attack depends on the system-dependent nonlinear function $\boldsymbol{h}(.)$. If z_t passes the traditional residual test, then the stealth injected measurement z_t^{α} can pass the same residual test. This is proved in [43].

To be able to conduct this kind of attacks, it is assumed that the adversary has access to multiple sensors' measurements in

the system with an adequate knowledge of the system structure and parameters. An example of a stealth FDIA is a sluggish scaling manipulation of voltage magnitudes of an entire section of the smart grid. Both basic and stealth FDIA result in massive impacts in smart grids.

Based on the system model, several FDIA detection algorithms have been proposed. These algorithms could be divided into estimation-based detection and other direct calculation methods. Estimation-based FDIA detection approaches are based on two steps: 1) calculation of states estimates or prediction and 2) comparing the results with the measurements of these states. The comparison is built upon different similarity tests named as detection tests in this manuscript. On the other hand, direct calculation methods depend on the measurements and the parameters of the systems in detecting FDIA without any estimation process.

1) Estimation-Based Detection Algorithms: In power systems, state estimation utilizes different sets of measurements across the entire power grid along with the system model and parameters to find the states of the grid. Traditionally, power systems' states used to be estimated via static estimation approaches such as Weighted Least Squares (WLS) estimator. This is built upon the assumption of steady state modelling of the power system with enough redundancy. However, real-life power systems do not operate in a steady state nature because of the stochastic variations in the demand and generation [42]. To overcome this problem, dynamic state estimators such as Kalman filter were introduced into the power systems applications [44]. The different estimation-based FDIA detection approaches along with the detection tests are discussed next.

a) Static Estimation Methods: In static estimation, every estimation step is dealt with separately from the earlier step. Thus, there is no information passing to the next step. The main static state estimation-based FDIA detection approach is based on the WLS estimation method. To find the system estimated states $\widehat{\boldsymbol{x}}$ using WLS estimation, the following problem must be solved [44]:

$$\begin{aligned} \min_{\widehat{\boldsymbol{x}}} \; J(\widehat{\boldsymbol{x}}) &= \sum_{i=1}^{n} w_i (z_i - h_i(\widehat{\boldsymbol{x}}))^2 \\ &= [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}})]^T \boldsymbol{W} [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}})] \end{aligned} \tag{3}$$

where $w_i = \sigma_i^{-2}$ represents the weight for the measurement z_i, $\boldsymbol{W} \in \mathbb{R}^{n \times n}$ is a diagonal matrix composed of the weights w_i, and n is the total number of measurements. Several methods could be applied in minimizing $J(\boldsymbol{x})$; however, the standard approach adopted is the normal equations method, where the estimated states $\widehat{\boldsymbol{x}}$ are found by iteratively solving:

$$\boldsymbol{H}_k^T \boldsymbol{W} \boldsymbol{H}_k \triangle \widehat{\boldsymbol{x}}_k = \boldsymbol{H}_k^T \boldsymbol{W} [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}}_k)] \tag{4}$$

Thus,

$$\widehat{\boldsymbol{x}}_{k+1} = \widehat{\boldsymbol{x}}_k + \left[\boldsymbol{H}_k^T \boldsymbol{W} \boldsymbol{H}_k\right]^{-1} \boldsymbol{H}_k^T \boldsymbol{W} [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}}_k)] \tag{5}$$

where $\boldsymbol{H}_k = \partial \boldsymbol{h} / \partial \boldsymbol{x}$ is the Jacobian evaluated at $\boldsymbol{x} = \widehat{\boldsymbol{x}}_k$ with k denoting the iteration number. The iterations continue until $\triangle \widehat{\boldsymbol{x}}_k = \widehat{\boldsymbol{x}}_{k+1} - \widehat{\boldsymbol{x}}_k$ settles within acceptable tolerance value. In power systems, WLS estimator runs every few minutes due to the computational limitation and the iterative nature of it, yet many studies have considered the use of it in detecting FDIA for its wide utilization in industry.

Authors of [45] illustrated the effect of FDIA from economical viewpoint. Then, they utilized WLS in their detection scheme. In [46], [47], WLS was utilized to detect FDIA that would mislead the operator into topology change and wrong voltage measurements. Recursive WLS was proposed in [48] to enhance the convergence speed where the state estimation is updated with historical states as well as follows:

$$\widehat{\boldsymbol{x}}_t^{k+1} = \widehat{\boldsymbol{x}}_{t-1} + \boldsymbol{\Omega}_t^k \left[z_t - \boldsymbol{h}\left(\widehat{\boldsymbol{x}}_t^k\right) - \boldsymbol{H}_t^k \left(\widehat{\boldsymbol{x}}_{t-1} - \widehat{\boldsymbol{x}}_{t-1}^k\right)\right] \tag{6}$$

where the gain matrix $\boldsymbol{\Omega}_t^k \in \mathbb{R}^{m \times n}$ is derived as:

$$\boldsymbol{\Omega}_t^k = \boldsymbol{P}_{t-1} \boldsymbol{H}_t^{kT} \left[\boldsymbol{H}_t^k \boldsymbol{P}_{t-1} \boldsymbol{H}_t^{kT} + \boldsymbol{W}^{-1}\right]^{-1} \tag{7}$$

where $\boldsymbol{P}_{t-1} \in \mathbb{R}^{m \times m}$ is the covariance of the estimation error introduced in using the historical data characterized with the notation $t-1$. This data is based on the historical profile not the previous time step as it would be in dynamic estimation.

WLS was also utilized in [49] with the objective of detecting FDIA in voltage controllers in the transmission system. The impact of such FDIA was also illustrated. To overcome the limitations of the WLS-based detection scheme, a new approach was presented in [50] where the cyber network anomaly monitoring was integrated in the estimation process to make the detection more precise. A quantification of the cyber anomaly influence on the measurements is presented with $\boldsymbol{\Psi} \in \mathbb{R}^{n \times n}$ which is a diagonal matrix whose entries are the weight coefficients ψ^{-1} associated with the measurements. Thus, the optimization problem in (3) becomes:

$$\min_{\widehat{\boldsymbol{x}}} \; J(\widehat{\boldsymbol{x}}) = [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}})]^T \boldsymbol{\Psi} \boldsymbol{W} [\boldsymbol{z} - \boldsymbol{h}(\widehat{\boldsymbol{x}})] \tag{8}$$

where a higher value of ψ illustrates a higher possibility of FDIA on that measurement.

Unlike passive detection algorithms, proactive FDIA detection approaches change the parameters in the systems (i.e., $\mathbf{H}$) in a proactive manner to prevent the adversaries from implementing a stealth attack by knowing these parameters. The change of the system parameters is conducted by executing reactance perturbations in the system with D-FACTS devices. While this adds an extra layer of protection, the detection scheme of FDIA is still based on WLS estimation as shown in [51], [52], [53].

Median filtering (MF) was proposed in [54]. To find a state's estimation $\hat{x}_i$ at node i using MF, the direct measurement $z_{i|i}$ at node i is utilized along with the calculated measurements of z_i using the measurements from other adjacent nodes $z_{i|a1}, z_{i|a2}, \ldots, z_{i|an_a}$ with n_a illustrating the total number of adjacent nodes. The calculation of these measurements is simply based on the lines' parameters and ohm's law. Thus, the estimation is utilized as follows:

$$\hat{x}_i = median\left(z_{i|i}, z_{i|a1}, z_{i|a2}, \ldots, z_{i|an_a}\right) \tag{9}$$

The advantage of this estimation process is the low computation complexity, yet its great dependency on the system

parameters degrades its performance deeply when uncertainties are associated with these parameters. Similarly, Kriging Estimator (KE) provides a prediction of the estimated state based on the measurements from adjacent meters and is utilized in FDIA detection in [55].

In [56], [57], [58], maximum likelihood (ML) estimation is utilized in the detection process. When the measurements error is assumed to be normally distributed with zero mean, the ML estimator is realized as follows:

$$\widehat{\boldsymbol{x}} = \left[\boldsymbol{H}^T \boldsymbol{W} \boldsymbol{H}\right]^{-1} \boldsymbol{H}^T \boldsymbol{W} z \tag{10}$$

where $\boldsymbol{W} \in \mathbb{R}^{n\times n}$ is a diagonal matrix composed of the reciprocals of the measurements' variances, and $\boldsymbol{H} \in \mathbb{R}^{n\times m}$ is the linearized form of $\boldsymbol{h}(.)$ in (2a).

Minimum mean square error estimator (MMSE) was proposed in [59] where the estimation of the states is given by:

$$\begin{aligned}\widehat{\boldsymbol{x}} &= arg\ \min_{\widehat{\boldsymbol{x}}} E\left[\left\|\boldsymbol{x} - \widehat{bmx}\right\|^2\right] \\ &= \boldsymbol{P}\boldsymbol{H}^T\left(\boldsymbol{H}\boldsymbol{P}\boldsymbol{H}^T + \boldsymbol{R}\right)^{-1} z\end{aligned} \tag{11}$$

where $\boldsymbol{P} \in \mathbb{R}^{m\times m}$ is the covariance of the estimation error; $\boldsymbol{H} \in \mathbb{R}^{n\times m}$ is the linearized system-defined matrix that depends on the system parameters and topology; and $\boldsymbol{R} \in \mathbb{R}^{n\times n}$ is the measurement error covariance. This estimation technique is popular for its easiness and versatility.

b) Dynamic Estimation Methods: Dynamic state estimation methods are widely considered in power system estimation nowadays with Kalman filter (KF) being the main method in this area. In KF, two steps are performed in every estimation step. First, a prediction of the state is built based on the previous step's state. Then, a correction of the state's prediction is carried by utilizing the measurements collected at that step. Thus, the estimation is based on the current previous information as well. This enables the dynamic estimation of the states as follows [60]:

$$Prediction \begin{cases} \widehat{\boldsymbol{x}_t^-} = \boldsymbol{F}\widehat{\boldsymbol{x}}_{t-1} & (12a) \\ \boldsymbol{P}_t^- = \boldsymbol{F}\boldsymbol{P}_{t-1}\boldsymbol{F}^T + \boldsymbol{Q} & (12b) \end{cases}$$

$$Correction \begin{cases} \boldsymbol{K}_t = \boldsymbol{P}_t^-\boldsymbol{H}^T\left(\boldsymbol{H}\boldsymbol{P}_t^-\boldsymbol{H}^T + \boldsymbol{R}\right)^{-1} & (13a) \\ \widehat{\boldsymbol{x}}_t = \widehat{\boldsymbol{x}_t^-} + \boldsymbol{K}_t\left(z_t - \boldsymbol{H}\widehat{\boldsymbol{x}_t^-}\right) & (13b) \\ \boldsymbol{P}_t = (\boldsymbol{I} - \boldsymbol{K}_t\boldsymbol{H})\boldsymbol{P}_t^- & (13c) \end{cases}$$

where $\widehat{\boldsymbol{x}_t^-}, \widehat{\boldsymbol{x}}_t \in \mathbb{R}^m$ are the prior (prediction) and posterior estimated state vectors; $\boldsymbol{F} \in \mathbb{R}^{m\times m}$ is the linearized form of $\boldsymbol{f}(.)$ in (2b) which is the state transition matrix; $\boldsymbol{P}_t^-, \boldsymbol{P}_t \in \mathbb{R}^{m\times m}$ are the prior and posterior covariance of the estimation error; $\boldsymbol{Q} \in \mathbb{R}^m$ is the process noise covariance; $\boldsymbol{K}_t \in \mathbb{R}^{m\times n}$is the Kalman gain; and $\boldsymbol{H} \in \mathbb{R}^{n\times m}$ is the linearized form of $\boldsymbol{h}(.)$ in (2a) which is a system-defined matrix that depends on the system parameters and topology and relates the measurement vector $\boldsymbol{z}$ to the estimated state vector $\widehat{\boldsymbol{x}}$. $\boldsymbol{R} \in \mathbb{R}^{n\times n}$ is the measurement error covariance, and $\boldsymbol{I}$ is an identity matrix of rank $\mathbb{R}^{m\times m}$. With KF, the authors of [60] developed low-complexity estimation and detection method for online operation. Similar approaches were taken in [61], [62]. In [63], [64], KF was utilized to detect FDIA in AGC systems where the impacts of FDIA are clearly illustrated.

To overcome the complexity of the computation, distributed Kalman filter (DFK) was proposed in [65], [66], [67]. In this scheme, the computation complexity is distributed amongst the different nodes in the main system by separately handling the equations (12) and (13). The resulting estimated states of the neighborhood nodes are further fused to provide an optimal estimation of the states as follows:

$$\hat{x}_t^i = \frac{\sum_{j=1}^n \hat{x}_t^{i|j} G_{ij}}{\sum_{j=1}^n G_{ij}} \tag{14}$$

where $\hat{x}_t^i$ represents the estimated state at node i; $\hat{x}_t^{i|j}$ is the state at node i that is evaluated from the neighboring node j; G_{ij} is an adjacency indicator that is 1 when node i is adjacent to node j and 0 otherwise; and n is the total number of the nodes in the system. The reduced computation complexity advantage of the DKF approach is illustrated in [40] where a real-time testing of the detection process is implemented.

Extended Kalman filter (EKF), the nonlinear version of Kalman filter, was proposed in [68], [69]. EKF is realized by considering the nonlinear system-defined measurements and transition functions $\boldsymbol{h}(.)$ and $\boldsymbol{f}(.)$ in equations (12) and (13). The advantage of EKF is the ability to model the nonlinearities of the system model which would yield in a more precise estimate and detection of FDIA eventually.

Aside from KF, vector autoregression (VAR) is a process that captures the interdependencies between the different time series events; thus, it considers the dynamics of the system. This could be realized as follows:

$$\widehat{\boldsymbol{x}}_t = \sum_{i=1}^{p} \boldsymbol{\varphi}_i \widehat{\boldsymbol{x}}_{t-i} + \boldsymbol{v}_t \tag{15}$$

where $\widehat{\boldsymbol{x}}_t$ is the estimated (predicted) states at time t, $\boldsymbol{\varphi}_i$ is a transition matrix relating the previous states to the current one, $\boldsymbol{v}_t$ is the error from the model uncertainties, and p is the total number considered of the previous states. This method could be utilized as the prediction process to detect FDIA as illustrated in [70], [71], [72].

Unknown input observation (UIO) was utilized in FDIA detection in [73], [74]. In this regard, the system is modeled as:

$$\begin{cases} \dot{\boldsymbol{x}}_t = \boldsymbol{A}\boldsymbol{x}_t + \boldsymbol{B}\boldsymbol{u}_t + \boldsymbol{E}\boldsymbol{d}_t & (16a) \\ \boldsymbol{z}_t = \boldsymbol{C}\boldsymbol{x}_t & (16b) \end{cases}$$

where $\boldsymbol{x}_t \in \mathbb{R}^m$ represents the state vector, $\boldsymbol{z}_t \in \mathbb{R}^n$ represents the output measurement vector, $\boldsymbol{u}_t \in \mathbb{R}^r$ represents the known input vector, and $\boldsymbol{d}_t \in \mathbb{R}^q$ represents the unknown input or disturbance vector, and $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{E}, \boldsymbol{C}$ are system-defined matrices of appropriate rank. For the system in (16), the unknown input observer is designed as follows:

$$\begin{cases} \dot{\boldsymbol{y}}_t = \boldsymbol{Y}\boldsymbol{z}_t + \boldsymbol{U}\boldsymbol{u}_t + \boldsymbol{V}\boldsymbol{z}_t & (17a) \\ \widehat{\boldsymbol{x}}_t = \boldsymbol{y}_t - \boldsymbol{T}\boldsymbol{z}_t & (17b) \end{cases}$$

where $\widehat{\boldsymbol{x}}_t \in \mathbb{R}^m$ is the state estimation vector, $\boldsymbol{y}_t \in \mathbb{R}^m$ is the state of the full-order dynamic observer, and $\boldsymbol{Y}, \boldsymbol{U}, \boldsymbol{V}, \boldsymbol{T}$ are system-defined matrices of appropriate rank. Unlike estimation-based techniques, unknown input observation method utilizes the internal states of the system as well.

This improves the preciseness of the results, eases the calculations, and increases the dependency on the system model as well.

c) Main Detection Tests: Detection tests are the measures that are utilized in order to detect the FDIA following the estimation processes. These are basically a measurement of similarities between the estimated or predicted states and the actual measurements collected from the grid. Some studies utilize the straightforward residual by comparing the Euclidean distance of the residual (also known as the L_2 norm) with a predefined threshold as follows:

$$\boldsymbol{D}_{L_2}(z_t) = \begin{cases} 1, & \textit{if } \|z_t - \boldsymbol{h}(\widehat{\boldsymbol{x}}_t)\|_2 > \tau_1 \\ 0, & \textit{otherwise} \end{cases} \tag{18}$$

where $\boldsymbol{D}_{L_2}(z_t)$ represents the L_2 detector of the measurement z_t which returns a value of 1 when FDIA is present, and 0 otherwise. $\|z_t - \boldsymbol{h}(\widehat{\boldsymbol{x}}_t)\|_2$ is the Euclidean distance (L_2 norm) of the residual, and τ_1 is a system-defined threshold value. $\boldsymbol{D}_{L_2}(z_t)$ detection metric has been utilized in control centers for many years with good performance in dealing with false data. This approach is utilized in [40], [45], [48], [49], [54], [55], [67], [71], [73], [74].

To have a common scale of comparison, largest normalized residual (LNR) test was proposed in [46], [63], [68], [69], [70]. Like $\boldsymbol{D}_{L_2}(z_t)$, this detection test could be realized as follows:

$$\boldsymbol{D}_{LNR}(z_t) = \begin{cases} 1, & \textit{if } \|[z_t - \boldsymbol{h}(\widehat{\boldsymbol{x}}_t)]/\boldsymbol{\sigma}_W\|_\infty \geq \tau_2 \\ 0, & \textit{otherwise} \end{cases} \tag{19}$$

where $\boldsymbol{\sigma}_W = \textit{diag}(\boldsymbol{W})$, which is the residual error covariance matrix $\boldsymbol{W} = \boldsymbol{R} - \boldsymbol{H}[\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{H}]^{-\boldsymbol{1}}\boldsymbol{H}^{\boldsymbol{T}}$; $\boldsymbol{H}$ is the linearized system-defined matrix that depends on the system parameters and topology; and $\boldsymbol{R}$ is the measurement error covariance.

Similarly, Chi-square test (χ^2-test) was proposed by some studies [50], [61], [62], [66] and is realized as:

$$\boldsymbol{D}_{\chi^2}(z_t) = \begin{cases} 1, & \textit{if } J(\widehat{\boldsymbol{x}}_t) \geq \tau_3 \\ 0, & \textit{otherwise} \end{cases} \tag{20}$$

where $J(\widehat{\boldsymbol{x}})$ is the objective function in (3). This test is also known as the goodness of fit which specifies how much the observed data is fitting the distribution of the expected states.

A combination of two detection tests ($\boldsymbol{D}_{L_2}(z_t)$ and $\boldsymbol{D}_{LNR}(z_t)$) is considered in [71], where it is shown to provide a better performance in FDIA detection compared to the other single detection tests. Further, $\boldsymbol{D}_{L_2}(z_t)$ is seen to outperform $\boldsymbol{D}_{\chi^2}(z_t)$ in FDIA detection as illustrated in [61]. The thresholds τ_1, τ_2, τ_3 could be designed according to the detection theory as in [75]. It must be noted that setting the value of the threshold is an extremely critical process. Setting higher value for the threshold yields in low detection efficiency, while a lower threshold value results in higher false alarms.

Cumulative Sum (CUSUM) is a successive investigation method that is typically used for monitoring the variations in the collected measurements as follows:

$$\boldsymbol{D}_{CUSUM}(z_t) = \begin{cases} 1, & \textit{if} \boldsymbol{S}_t = (\boldsymbol{S}_{t-1} + [z_t - \boldsymbol{h}(\widehat{\boldsymbol{x}}_t)]) \geq \boldsymbol{\tau}_5 \\ 0, & \textit{otherwise} \end{cases} \tag{21}$$

Thus, the cumulative variations are constantly monitored. The simplicity of this technique has led many researchers to utilize it in the effort of detecting FDIA. These are reported in [47], [59], [60], [64], [65].

Kullback–Leibler distance (KLD) was utilized in [56] and is realized as follows:

$$\boldsymbol{D}_{KLD}(z_t) = \begin{cases} 1, & \textit{if } \sum_{z_t} P(\boldsymbol{x}_t) \ln \frac{P(\boldsymbol{x}_t)}{Q(\boldsymbol{x}_t)} \geq \tau_6 \\ 0, & \textit{otherwise} \end{cases} \tag{22}$$

This detection test looks at the probability distribution functions. $P(\boldsymbol{x}_t)$ resembles the probability distribution of the states' variation of the historical data, and $Q(\boldsymbol{x}_t)$ is the probability distribution of the states' variation between the previous time step and the current time step.

In a similar scheme, generalized likelihood ratio test (GLRT) has been proposed in [58]. In this test, the threshold is compared with $\boldsymbol{x}^T(\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T)\boldsymbol{x}$ and an alarm is triggered when the threshold value is exceeded. This test showed a superior performance in detecting FDIA when colored Gaussian noise is considered. While these tests vary, they all share the need for defining threshold value that is fixed for the entire testing schemes.

2) Other Model-Based Algorithms: While the main model-based FDIA detection algorithms are based on the estimation theory, other estimation-free algorithms have been also developed in this field. These algorithms are based on the model or the parameters of the system under test. Cooperative vulnerability factor (CVF) was proposed in detecting FDIA in microgrid control systems in [76]. In this algorithm, the secondary output of voltage controllers, termed as CVF, converges to zero given that the system is free of FDIA. Matrix separation (MS) was introduced in [77], [78] where the detection of the FDIA is based on the separation of nominal power grid states and anomalies matrices assuming the sparse nature of the FDIA. A voting protocol to decide on the detection of the FDIA in the system is proposed in [79] using Multi-agent systems (MAS). Joint-transformation-based KLD algorithm (JT-KLD) was utilized in [80] where a power and a log transformation are considered before detecting the FDIA using KLD as in (22). Transmission line parameters-based comparative algorithm (TLPC) was introduced to detect FDIA in [81] where the line parameters are calculated using the two ends measurements and then compared with the already known parameters values. In a similar fashion, Load forecast-based algorithm (LF) [82], [83], [84] was proposed where the detection is based on the forecasted data. Adaptive Markov Strategy (AMS) was utilized in [85] where the threshold values of the detection process is changed based on a game-theoretical analysis. An algorithm based on the comparison with local measurements (CLM) was presented in [86] where the received measurements with FDIA are compared with the local measurements. Direct detection tests were also applied in detecting FDIA such as direct measurements-based KLD (D-KLD) method [87], log-transformation-based KLD (LT-KLD) method [88], and direct measurements-based CUSUM (D-CUSUM) [89], [90]. Unlike estimation-based detection algorithms, these are direct calculative methods that utilize the system parameters directly alongside the measurements

collected. The full breakdown along with the detailed comparative information of all these methods is presented in the next section alongside the data-driven detection algorithms.

B. Data-Driven Detection Algorithms

Unlike model-based detection algorithms, data-driven detection algorithms are model-free; thus, neither system's parameters nor models are involved in the detection process of FDIA. Depending on the utilization of the data in detection the FDIA in smart grids, these algorithms could be divided into three main categories: 1) machine learning algorithms, 2) data mining algorithms, and 3) other algorithms that do not involve learning or mining in them. In data-driven algorithms, the measurements $\boldsymbol{z}$ collected from the grid are usually referred to as samples $\boldsymbol{s}$.

1) Machine Learning-Based Algorithms: Machine learning (ML) is a wide field in the artificial intelligence area. With ML, we can utilize trained machines in order to do complicated tasks such as detecting FDIA in smart grids. Unlike model-based FDIA detection algorithms, ML-based algorithms are based on the data collected from the system. However, being data-driven technique means a huge dependency on historic data of the system under test to enable the learning of the machine. ML-based detection algorithms include supervised, unsupervised, and reinforcement learning methods. The classification in this manuscript is based on the learning procedure adopted by reviewed papers.

a) Supervised learning: Supervised learning is the process in which labelled data is needed for the learning process of the machine. Thus, every input is associated with specific output as $\{(\boldsymbol{s}_i, y_i)\}$, where $\boldsymbol{s}_i \in \mathbb{R}^n$ represents the i^{th} sample (measurements), and $y_i \in \{-1, 1\}$ is the label of that sample (i.e., either normal or with FDIA). Several supervised learning approaches have been considered in FDIA detection in smart grid. This starts with the simplest method known as linear regression (LR). LR models the relationship between a dependent scalar variable $f(\boldsymbol{x})$ and independent variables $\boldsymbol{x}$ as $f(\boldsymbol{x}) = \boldsymbol{w}x + \boldsymbol{b}$, where $\boldsymbol{w}$ represents the weight vector and $\boldsymbol{b}$ is a bias. LR models are often fitted using the least squares approach where the minimization problem is formed as:

$$\min_{\boldsymbol{w},\boldsymbol{b}} \sum_i \left(f(\boldsymbol{x}_i) - (\boldsymbol{w}\boldsymbol{x}_i + \boldsymbol{b})\right)^2 \tag{23}$$

LR's simplicity and ease of implementation are the main advantages of it. LR was only considered in [91] where a FDIA is detected if the measurements vector does not fit the linear model generated from the trained data.

Support vector machine (SVM) is the most utilized method in this field. It is a linear non-probabilistic binary-based classifier that depends on two parallel hyperplanes boundaries that could be represented as:

$$\begin{cases} \boldsymbol{w}^T\phi(\boldsymbol{s}_i) + b = +1, & if\ y_i = +1 \quad (24a) \\ \boldsymbol{w}^T\phi(\boldsymbol{s}_i) + b = -1, & if\ y_i = -1 \quad (24b) \end{cases}$$

where $\boldsymbol{w}$ is an orthogonal normal vector to the hyperplanes, $\phi(.)$ is a function that maps the samples $\boldsymbol{s}_i$ into a linearly separable space (e.g., kernel function), and b is an offset constant. Measurements samples that satisfy either of the questions in (24) are known as the support vectors. To ensure a good classification process, the distance between the two hyperplanes (i.e., $margin = 2/\|\boldsymbol{w}\|^2$) in (24) should be maximized my minimizing the following function:

$$\min_{\boldsymbol{w},b} \quad \frac{\|\boldsymbol{w}\|^2}{2} \tag{25}$$

$$subject\ to\ \ y_i\left(\boldsymbol{w}^T\phi(\boldsymbol{s}_i) + b\right) \geq 1\ \forall i \tag{26}$$

This quadratic programming problem could be solved via the different optimization packages available today. SVM's simplicity is the main reason for its frequent utilization in detecting FDIA as illustrated in [92], [93], [94], [95], [96], [97], [98], [99], [100]. Still, the choice of the kernel function along with the need for memory and extensive CPU time in the training process are the main drawback of this algorithm.

Inspired by biological neural networks, artificial neural networks (ANN) were created and utilized in classification, estimation, or approximating functions that depend on many inputs and are generally unknown. ANN could have more than one hidden layer (i.e., deep neural network), have feedback loop (i.e., recurrent neural network), or have simple one hidden layer with no feedback (i.e., feedforward neural network). The output of the neurons in ANN depends on two main factors. First, the weighted sum of all the inputs to the neuron plus a bias $\sum_i w_i x_i + bias$. Second, the activation function considered (e.g., logistic sigmoid function $f(x) = 1/(1 + e^{-x})$). Backpropagation is the main procedure of training the ANN, where the error in the output of the ANN is propagated backward to further improve the weights in the neurons. This includes an iterative process until the error settles within acceptable range. Feedforward neural network (FNN) has been employed in FDIA detection in [95], [96], [100], [101], [102]. To imitate the dynamical behavior of the smart grid, Recurrent neural networks (RNN) have been proposed in FDIA detection in [94], [103], [104], [105]. With the internal memory of RNN, the dynamics of the grid could be considered though the feedback loop in the layers. Deep neural network (DNN) was utilized in detecting FDIA in [97]. The higher number of hidden layers in the deep neural network is expected to yield in a more preciseness in detecting FDIA. Convolutional neural network (CNN) is a special type of the deep neural network that is widely used for pattern recognition image processing. CNN utilizes convolution instead of the general matrix multiplication at one layer at least. The ability of CNN in extracting the different feature in the samples makes it a very promising algorithm in detecting FDIA as illustrated in [99]. Autoencoder (AE) is a deep neural network that provides a nonlinear compression (encoding) and expansion (decoding) of the measurement samples. The detection scheme in this algorithm is based on the error between the decoded sample and the input to the network where an alarm is flagged when the error exceeds a certain level. This algorithm was applied in [106]. The main disadvantage in using the backpropagation method in training the neural network is the extensive time needed. To overcome this, extreme learning machine (ELM) has been proposed. Unlike backpropagation, the input weights

and hidden layers' biases are chosen randomly. This method was considered in detecting FDIA in [107], [108].

K-nearest neighbor (KNN) is well-known classification algorithm. In this algorithm, the classifier assigns the sample to the nearest possible K neighbor's class (i.e., either true measurement or FDIA). The criteria in determining the class of the sample is a straightforward measurement of the Euclidean distance between the new unlabeled sample $\boldsymbol{s}_i$ and the prelabeled samples $\boldsymbol{s}_j$ as follows:

$$d_{ij} = \left\| \boldsymbol{s}_i - \boldsymbol{s}_j \right\|_2 \tag{27}$$

Thus, the lowest distance between the new unlabeled sample and the prelabeled samples determines the classification of the new sample as either normal or FDIA. KNN was applied in detecting FDIA in [93], [99]. The main drawback of this method is the distribution and the density of the prelabeled samples. To overcome this drawback, Extended nearest Neighbor (ENN) has been considered in [93] which takes into account the global distribution of the class along the local neighbors in predicting the class for the new samples. ENN proves to have a better classification accuracy compared to KNN as illustrated in [93].

Decision tree (DT) is a predictive model which maps given samples (measurements) to specific target values. The learning process of the decision tree includes successive splitting of the input variables into subsets depending on an attribute value test. This is called recursive partitioning. This splitting stops when the error is within an acceptable range. DT was applied in FDIA detection in [97], [98]. The main advantage of the DT is the easiness in its constructing, yet an overcomplex tree could be generated that do not perform well aside from the training data. This is called overfitting. To overcome this issue, Random forests (RF) were developed. By utilizing ensemble learning, random forests are constructed using several decision trees. The classification of the random forest is based on the mode or the mean of the classification of the individual trees. This algorithm was adopted in detecting FDIA in [99], where it provides a more accurate performance than single decision trees. Similarly, gradient boosting (GB) is an ensemble of weak classifiers that are typically decision trees. Unlike random forest which combines several classifiers, gradient boosting builds up upon the week classifiers to further reduce the error. This method provides promising results in detecting FDIA as illustrated in [109], [110].

Based on Bayes' theorem, naive Bayes classifier (NPC) is a simple probabilistic classifier. It is based on the independence assumption between the considered variables. Bayes theorem defines the probability of the sample $\boldsymbol{s}$ being part of the class y_k as the follows:

$$p(y_k|\boldsymbol{s}) = \frac{p(y_k)p(\boldsymbol{s}|y_k)}{p(\boldsymbol{s})} \tag{28}$$

where $p(.)$ represents the probability value of a given sample or class. Thus, depending on this theorem, the classifier becomes:

$$y = \underset{k}{arg\ max}\ \ p(y_k) \prod_{i=1}^{n} p(\boldsymbol{s}_i|y_k) \tag{29}$$

Even though this algorithm is widely used in many classification problems, it was only considered in detecting FDIA in [97], [111].

Other supervised learning approaches for detecting FDIA in smart grids include margin classifier (MC), which is a generalized method of the SVM that shows a more accurate performance as illustrated in [100]; and structure learning (SL) [112], [113], which is a prediction method that is based on the covariance of the structure of the samples rather than their real values. The main disadvantage of supervised learning methods is the need for extensive learning as well as the labelled data.

b) Unsupervised learning: Unsupervised learning is the process of delivering unlabeled data to the machine for finding classification schemes and patterns that are hidden. Thus, the job of the machine is to divide the data points into classes according to the hidden features of the data points. Doing so, we can detect FDIA in smart grids as those should have different classes other than the normal data classes. In this regard, several unsupervised learning algorithms have been utilized in detecting FDIA in smart grid. K-means clustering (KMC) is a very popular unsupervised learning algorithm that is heavily used in classification problems. The goal of KMC is to separate $\boldsymbol{s}$ observations into k clusters. The belonging of the observations to the clusters is based on the nearest mean which is the cluster's prototype. The output of this separation is Voronoi cells. To find k sets y for an n samples $\boldsymbol{s}$, the following minimization problem should be solved:

$$\underset{y}{arg\ min} \sum_{i=1}^{k} \sum_{\boldsymbol{s} \in y_i} \left\| \boldsymbol{s} - \boldsymbol{\mu}_i \right\|^2 \tag{30}$$

where $\boldsymbol{\mu}_i$ is the mean in the set y_i. This method was applied in detecting FDIA in [111], [114], [115]. the main advantage of this method is its simplicity, while the main drawback is the high sensitivity to the noise in the samples. Fuzzy clustering (FC) or soft clustering is an extended version of KMC where a sample could belong to multiple clusters with different grades. This yields in a more detailed clustering process where the clusters could be overlapped instead of hardly defined boundaries. This method was a utilized in detecting FDIA in [114], [115] where it results in a slightly improved detection accuracy more that the KMC method.

Isolation forest (IF) is identified as an outlier detection technique. It is an ensemble of separate isolation trees. IF can contain more isolation trees when large dimensional dataset is considered. This algorithm isolates the anomalies given that they are few and different from other data. By treating FDIA as anomalies, this method was considered in detecting FDIA in [116].

Deep belief network (DBN) is a DNN-based generative model. It can be utilized in generatively pre-training a DNN by using the learned weights as the initial weights that could be tuned later using backpropagation. This helps in reducing the time required for training the network. DBN is competently trained via a layer-by-layer, unsupervised manner. This method was utilized in detecting FDIA in [117], [118]. Probabilistic

neural network (PNN) is type of FNN which is commonly utilized in pattern recognition and classification problems. The main advantage of this algorithm is that it is much faster than multilayer perceptron networks. It has been adopted in FDIA detection in [119].

Other unsupervised learning algorithms that are adopted in detecting FDIA include hidden Markov model (HMM) [120], [121], which is a time-series prediction model of the samples. While sharing the same working principle, each one of these algorithms has its own uniqueness even though equivalent results are noted.

c) Reinforcement Learning: In this type of learning, the machine seeks to learn the optimal action to take based on the experiences from the previous actions taken. Unlike supervised learning where samples' data are used in the training, reinforcement learning learns through trial and error. Hence, a sequence of fruitful choices will yield in the process being "reinforced" since it solves the problem in a good manner. Compared to the supervised and unsupervised learning types, this type of learning is still to further be investigated in the area of FDIA detection in smart grids. This is due to the limited literature reported in this area which is only reported in [122] where State-Action-Reward-State-Action (SARSA) is adopted. The online nature of reinforcement learning provides an advantage in dealing with very fluctuated systems such smart grids.

2) Data Mining-Based Algorithms: Data mining is the method of discovering patterns in large data sets. With data mining algorithms, we can process the variable data measurements received from a specific system in order to draw conclusions about the hidden attributes or patterns of the data. Data mining is widely intersected with statistics and machine learning methods making it a form of interdisciplinary field. In fact, many scientists consider data mining algorithms as part of unsupervised machine learning methods. However, since these algorithms are separated in literature from machine learning, they are separated in this manuscript as well. Data mining based FDIA detection algorithms are considered premature for their few utilizations in this area. Nevertheless, some approaches have been considered. For example, non-nested generalized exemplars (NNGE) were utilized in [123]. This algorithm classifies the data points into normal and abnormal based on the distance between the generalized exemplars of the classification process. The advantage of using these generalized exemplars is the reduced need for memory as only the details of these exemplars are to be stored. The classification of the new measurements samples is based on the distance between the samples and the set of the exemplars like equation (27). Hoeffding adaptive trees (HAT) was proposed in [124] for classifying FDIA along different other disturbances in the grid such as the different types of faults. It is shown that the classifier was able to adapt to the slow changes in the grid such the slow variations in the loading of the grid. This is very advantageous when dealing with highly fluctuated systems such as smart grids. Common path mining (CPM) was applied in detecting FDIA in [25], [125]. A path is a sequence of samples that are arranged in a temporal order. Thus, for each special event, there shall be a path. This includes the diverse types of faults. When a sequence of the samples does not coincide with any of the given defined paths, it is considered as FDIA. Causal events graph (CEG) was used in [126], where each event in the grid has special signature that is recognized through the events graph and a FDIA is detected if the event of the measured sample is not classified into either of the predefined events. It must be noted that these data mining algorithms are like unsupervised machine learning methods as they require historical data sets for the training purposes. The low computational complexity of the data mining algorithms, after the training step, is a huge advantage for detecting FDIA in smart grids. Therefore, many real-time online experimental tests were conducted and validated.

3) Other Data-Driven Algorithms: Other data-driven algorithms for FDIA detection are neither explicitly categorized into machine learning nor data mining methods. Signal temporal logic (STL) was proposed in FDIA detection in [127], where the DC voltages and currents are compared with the predefined upper and lower boundaries. Principal component analysis (PCA) was utilized in [128], where the covariances of the samples collected are the basis in detecting FDIA. PCA is could be employed a preprocessing dimensionality reduction prior to using other algorithms such as SVM. Distributed host-based collaborative (DHC) detection approach was developed in [129], where the identification of the compromised meter is possible in the attacked sample. Dynamic time warping clusters (DTWC) was utilized in detecting FDIA in [130]. This algorithm can accommodate time irregularities in the time series samples. Graph theory-based mathematical morphology (GTMM) detection approach was developed in [131], this method is based on the graph theory and a consensus protocol. Table I. illustrates the overall distribution of the reviewed articles along the different systems considered for tests. The table further identifies the system considered along with the consideration of stealth attacks and real-time testing in the reviewed literature.

IV. Comparative Study

While all these algorithms share the same goal of detecting FDIA in smart grids, they all differ in their pros and cons.

A. Statistics of the Published Work

Looking at the reviewed literature from a statistical viewpoint, we can draw some conclusions about the trends and patterns regarding the algorithms utilized, the systems considered, the type of attacks adopted, and the testing mechanisms. Regarding the type of algorithms developed for detecting FDIA in smart grid, data-driven algorithms represent 47.7% of the total FDIA detection algorithms reviewed, and model-based algorithms are about 52.3%. This illustrates the equality between the two main themes resulting from the freshness of the topic and the need for exploring the different possible solutions. Regarding the system consideration of FDIA, the main target for the FDIA detection studies was transmission system with 77.2% of the reported studies. Following that, several studies were conducted on the smart meters systems

TABLE I
CLASSIFICATION AND COMPARISON OF FALSE DATA INJECTION ATTACKS DETECTION ALGORITHMS

Category			Algorithm	References	Comp. Complexity: Estimation	Comp. Complexity: Detection	Detection Rate
Model-based Algorithms	Estimation-based	Static Est.	WLS	[45] [46]^{T} [47] [48] [49] [50]^{R} [51, 52, 53]^{DT}	$\mathcal{O}(n^3t)$	$\mathcal{O}(n^2)$	0.90 – 0.95
			MF	[54]	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$	0.99
			KE	[55]^{S}	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2)$	0.96
			ML	[57]^{T} [56] [58]^{T}	$\mathcal{O}(n^3 \lg n)$	$\mathcal{O}(n^2)$	0.997
			MMSE	[59]^{T}	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2t)$	Detected
		Dynamic Est.	KF	[60]^{T} [61] [62] [63]^{A} [64]^{A}	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2)$	Detected
			DKF	[40]^{R} [65] [66] [67]	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	Detected
			EKF	[68] [69]	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2)$	Detected
			VAR	[70] [71] [72]^{T}	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2)$	0.87 - 0.996
			UIO	[73]^{T} [74]	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2)$	Detected
	Others		CVF	[76]^{MTR}	NA	$\mathcal{O}(n)$	Detected
			MS	[77] [78]	NA	$\mathcal{O}(n^3t)$	0.92 – 0.95
			MAS	[79]^{O}	NA	$\mathcal{O}(n)$	Detected
			JT-KLD	[80]^{T}	NA	$\mathcal{O}(n^2)$	0.55 – 1.0
			TLPC	[81]	NA	$\mathcal{O}(n^2)$	0.85
			LF	[82]^{T} [83] [84]^{AT}	NA	$\mathcal{O}(n^2)$	0.80 – 1.0
			AMS	[85]^{DT}	NA	$\mathcal{O}(n^2t)$	Detected
			CLM	[86]^{P}	NA	$\mathcal{O}(n^2)$	Detected
			D-KLD	[87]	NA	$\mathcal{O}(n^2)$	0.50 – 1.0
			LT-KLD	[88]^{T}	NA	$\mathcal{O}(n^2)$	0.92 – 0.99
			D-CUSUM	[89] [90]	NA	$\mathcal{O}(n^2)$	0.70 – 1.0
Data-driven Algorithms	Machine Learning	Supervised L.	SVM	[92] [93] [94] [95] [96] [97] [98] [99] [100]	$\mathcal{O}(s^2n + s^3)$	$\mathcal{O}(nn_{sv})$	0.58 – 0.99
			LR	[91]^{S}	$\mathcal{O}(n^2s + n^3)$	$\mathcal{O}(n)$	Detected
			FNN	[95] [96] [100] [101] [102]^{R}	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.92 – 0.99
			CNN	[99]	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.93
			DNN	[97]	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.72 – 0.80
			RNN	[94] [103]^{S} [104]^{A} [105]	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.75 – 0.99
			GB	[109]ST [110]ST	$\mathcal{O}(snn_{tr})$	$\mathcal{O}(nn_{tr})$	0.55 – 0.97
			ELM	[107] [108]^{T}	$\mathcal{O}(snn_{no}^2t)$	$\mathcal{O}(nn_n^2)$	0.75 – 0.95
			KNN	[93] [99]	NA	$\mathcal{O}(sn)$	0.71 – 0.99
			ENN	[93]	NA	$\mathcal{O}(s^2n)$	0.92 – 0.99
			DT	[97] [98]	$\mathcal{O}(s^2n)$	$\mathcal{O}(n)$	0.37 – 0.72
			RF	[97] [99]	$\mathcal{O}(s^2nn_{tr})$	$\mathcal{O}(nn_{tr})$	0.49 – 0.71
			AE	[106]^{O}	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	Detected
			NPC	[97] [111]^{S}	$\mathcal{O}(sn)$	$\mathcal{O}(n)$	0.73 – 0.79
			MC	[100]	$\mathcal{O}(s^2n + s^3)$	$\mathcal{O}(nn_{sv})$	0.96 – 0.98
			SL	[112] [113]	$\mathcal{O}(sn^{n_{lvs}+2})$	$\mathcal{O}(n^{n_{lvs}+2})$	Detected
		Unsupervised L.	KMC	[111]^{S} [114]^{S}	$\mathcal{O}(s^{nk+1})$	$\mathcal{O}(nk)$	0.4 – 0.98
			FC	[114]^{S} [115]	$\mathcal{O}(s^{nk+1})$	$\mathcal{O}(nk)$	0.81 – 0.93
			IF	[116]	$\mathcal{O}(s^2nn_{tr})$	$\mathcal{O}(nn_{tr})$	0.93 – 0.94
			DBN	[117] [118]^{T}	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.93 – 0.98
			PNN	[119]^{S}	$\mathcal{O}(snn_n^2t)$	$\mathcal{O}(nn_n^2)$	0.96
			HMM	[120] [121]^{S}	$\mathcal{O}(s^2n)$	$\mathcal{O}(s^2n)$	0.95 – 0.99
		RL.	SARSA	[122]	$\mathcal{O}(TE)$	$\mathcal{O}(1)$	0.99
	Data Mining		NNGE	[123]^{R}	$\mathcal{O}(s^{nk+1})$	$\mathcal{O}(nk)$	0.25 – 0.93
			HAT	[124]^{R}	$\mathcal{O}(s^2n)$	$\mathcal{O}(n)$	0.92 – 0.98
			CPM	[25]^{R} [125]^{R}	$\mathcal{O}(s^{nk+1})$	$\mathcal{O}(nk)$	0.50 – 0.99
			CEG	[126]^{R}	$\mathcal{O}(snT)$	$\mathcal{O}(nT)$	Detected
	Others		STL	[127]^{MR}	NA	$\mathcal{O}(n)$	Detected
			PCA	[128]	$\mathcal{O}(sn^2t)$	$\mathcal{O}(n)$	0.95 – 0.99
			DHC	[129]	NA	$\mathcal{O}(n)$	0.80 – 0.99
			DTWC	[130]^{S}	$\mathcal{O}(s^{nk+1})$	$\mathcal{O}(nk)$	0.70 – 0.93
			GTMM	[131]^{M}	NA	$\mathcal{O}(n)$	Detected

- [x]: Transmission,
- [x]^{D}: Distribution,
- [x]^{S}: Smart Meters,
- [x]^{A}: Automatic Generation Control
- [x]^{M}: DC Microgrid,
- [x]^{P}: Protection Devices,
- [x]^{O}: others
- [x]^{R}: Real-Time Testing
- [x]^{T}: Stealth Attacks consideration,

- n: number of measurements
- s: number of training samples,
- t: number of iterations,
- n_n: max number of neurons in any layer,
- n_{no}: max number of neurons in output layer
- n_{sv}: number of support vectors,
- n_{tr}: number of trees,
- n_{lvs}: number of local vertex separators,
- k: number of k clusters/exemplars,
- T: Maximum length of a learning episode/event,
- E: Number of learning episodes

with 10.5%. Other systems such as DC microgrids, wind turbine system, and AGC systems had a percentage of 8.8%. The least share was for the distribution system with only 3.5%. This illustrates a real need to investigate FDIA and detection algorithms in this highly fluctuated system. As for the type of the FDIA tested, most of the studies considered only basic FDIA. This type of attack has 79.5% of the studies presented. Stealth attacks were considered in only 20.5% of the studies reviewed. On the other hand, most of the studies in literature did not consider real-time testing of the proposed detection algorithms. These represent 89.8% of the reviewed literature. Only 10.2% have considered real-time testing of their detection algorithms. Real-time testing is a very important criterion for FDIA detection algorithms as this is a real need for them in industry.

B. Comparative Study on the Detection Algorithms

Table I. summarizes the experimental performance analysis of all the algorithms presented in the reviewed literature in the detection of the FDIA in smart grids. To have a common comparative study among all the reviewed algorithms, two main metrics are considered. First, the computational complexity of the proposed algorithm where the worst-case scenario is considered. The $\mathcal{O}$ notation is utilized in describing the computational complexity of the algorithms [132]. For example, $\mathcal{O}(1)$ suggests that the algorithm is solved in constant time, while $\mathcal{O}(n)$ suggests that the algorithm is solved in linear time such that more time is required for higher values of n which is the number of the measurements. Furthermore, the presence of other parameters like s (number of the training samples) does not increase the computational complexity only, but the storage requirement of the process as well. The second evaluation metric is the detection rate of the FDIA. It must be noted that the testing procedure of the proposed FDIA detection algorithms differ massively. While some papers simulate hundreds of random FDIA and calculate the detection rate of the results, others test their proposed detection algorithm on few cases of FDIA only. Therefore, the range of the detection

rate of the proposed algorithm is provided for some algorithms, and the detection performance is described for the algorithms without a reported detection rate. Furthermore, it must be noted that these detection rates are based on the proposed FDIA that vary massively from simple and basic FDIA to the stealth FDIA. Thus, these detection rates are just to provide an overview of the detection performance of the proposed algorithm along the proposed system under test and FDIA type. However, to have a fair comparison between the different algorithms, the considered system under test as well as the types of the FDIA should be the same.

1) Model-Based Detection Algorithms: WLS-based detection of FDIA is seen to be the most computationally complex algorithm in the model-based detection algorithms. The estimation process of the WLS estimator can be of complexity class of $\mathcal{O}(n^3t)$ for nonlinear systems where several iterations are needed for the estimation. In contrast, MF has the least estimation complexity of $\mathcal{O}(n)$ as only the median is found in the series of the measurement received. The main advantage of non-estimation model-based detection algorithms is the reduced computational complexity where only the detection process is needed without any estimation. While all the algorithms reviewed in the literature achieve a very good detection rate, some algorithms show a wide distribution of the detection rate. This is evident with JT-KLD and D-KLD with detection rates of 0.55-1.0 and 0.50-1.0, respectively. These variations in the detection rate are due to the different FDIA considered along with the different values for the parameters considered in the detection process such as the threshold value. For example, reducing the threshold value would result in increasing the detection rate; however, it would also increase the rate of the false alarms where the measurement is falsely detected as FDIA. This is a main challenge in detecting FDIA.

2) Data-Driven Detection Algorithms: SVM was the most considered algorithm in detecting FDIA in smart grids. Several FDIA as well as different measurement pre-processing techniques was considered with the SVM-based detection algorithm such as PCA and AE. This yielded in wide distribution of the detection rate as 0.58-0.99. The need for the training samples in the data-driven detection algorithms increases the computational complexity far more than the model-based detection algorithms. This is seen in the training process where the computational complexity depends mostly on the measurements' number n alongside the samples' number s. For example, the training of the SVM is considered to have a computational complexity of $\mathcal{O}(s^2n + s^3)$. Other algorithms' computational complexity depends on other parameters as well. For instance, the training of FNN has a complexity of $\mathcal{O}(snn_n^2t)$, where n_n is the maximum number of neurons in the any layer and t is the iterations numbers. In a similar pattern, the detection rate of the algorithms considered differ in a wide range in response to the different systems, FDIA types, values of the parameters, and numbers of the samples. For example, the more training samples we have, the better detection rate we would have. However, this would increase the computational complexity along the needed memory to store the all of these samples.

TABLE II
A SUMMARY OF THE ADVANTAGES AND DISADVANTAGES OF FDIA DETECTION ALGORITHMS' TYPES

Algorithm	*Pros*	*Cons*
Model-based Detection Algorithms	▪ No training required ▪ No need for historical data set ▪ Reduced memory need	▪ Need for system model ▪ Need for system parameters ▪ Threshold selection ▪ Extensive computation ▪ Serious detection delay ▪ Unscalable ▪ Possible Divergence
Data-driven Detection Algorithms	▪ Independent of system and parameters ▪ Fast detection process ▪ Real-Time compatible ▪ Scalable	▪ Need for extensive training ▪ Need for training data set (labelled or unlabelled) ▪ Need for extra memory space ▪ Overfitting the training samples

3) System-Wise Comparison: Based on the literature review results obtained in Table I, the best method to be applied to a given system could be decided based on the computational complexity, the detection rate reported along with the consideration of the stealth FDIA in the conducted experiments. For example, LT-KLD [88], LF [82], and DBN [117] provide good detection rate with a slight computational complexity in detecting stealth FDIA in transmission systems. Similarly, GB [109], [110] demonstrates advanced performance in the detection of stealth attacks in smart meters systems. In AGC systems, LF [84] illustrates a better performance compared to the other algorithms. In microgrid control, CVF [76] was only considered in detecting stealth FDIA. AMS [85] illustrates a reduced complexity algorithm in detecting FDIA in distribution systems compared to WLS algorithm. CLM [86] was the only algorithm in detecting FDIA in protection systems. Again, it must be stressed that to have a fair comparison between the different algorithms, the considered system under test as well as the types of the FDIA should be the same to have a common ground.

C. Pros and Cons of Each Detection Category Methods

To distinguish between the different FDIA detection algorithms in smart grid, it is a must to summarize the main advantages and disadvantages of them. The pros and cons of each algorithm category are summarized in Table II. The main advantage of model-based detection algorithms is the independence from the historical data set which is a must for the data-driven detection algorithms. Thus, neither training nor extra memory space is required for saving the massive amount of the training samples which is the case for most of the data-driven algorithms. On the contrary, the need for the system parameters and model is the main drawback of the model-based algorithms. Slight uncertainties in these parameters may yield false detection performance. Furthermore, the extensive computational complexity needed for each measurement sample received is a huge pardon. This gets worse when an iterative process is involved with possible divergence issues. This affects the scalability of these algorithms. Finally, the choice of a fixed threshold setting in the process might lead to falsified detection performances specially when the system experiences any dynamics or loading variations. This issue has

been addressed in [73], [74], [85], where an adaptive threshold is considered.

The independence of the system parameters and the model is the main advantage for the data-driven detection algorithms. This reduces the erroneous performance in the detection due to the parameters and modelling uncertainties. Further, the reduced computational complexity after the training stage makes these algorithms much more compatible for real-time detection of FDIA unlike most of the model-based algorithms where the estimation must be carried before the detection process. On the other hand, the need for the many training samples along with the extensive training process is the main downside for these algorithms. This requires more storage requirements compared to the model-based algorithms. Also, overfitting is a very serious issue in this area. This means that these algorithms perform great for the selected training samples but not for the entire population of the possible measurements in the system. Thus, choosing the samples for the training is also a big hassle with these algorithms.

D. Main Remaining Challenges

Throughout this review process, the following remaining challenges are identified as the main pillars that shall be address in future research projects:

- The effect of uncertainties in the systems parameters, modelling, and measurements.
- The dynamic nature of the smart grids with the different states and operation conditions. The fluctuation nature of the distribution systems should have more focus especially with the recent expanded distributed generation and microgrid trends.
- The ever-increasing volume of the smart grids and data which increases the computational complexity.

V. CONCLUSION

The reviewed history, variety, and impacts of the FDIA illustrate a real need to develop advanced detection algorithms to address these growing threats. Different directions have been taken to detect FDIA in smart grids. Some of them are model-dependent and others are data-driven. Each of these categories has its own pros and cons. The goal is to develop an algorithm with minimum possible drawbacks. To sum up, through this survey and considering NIST's guidelines for the smart grid cybersecurity [12], the following main criteria are paramount in developing future FDIA detection algorithms:

- Support for legacy grid standards, protocols, and systems with their limited communication and computing resources.
- High detection speed to ensure the least damage resulted from the FDIA.
- High sensitivity to detect the smallest possible FDIA.
- Scalability to guarantee the covering of the massive number of nodes in smart grid.
- Adaptivity to the changes in the system topology and parameters as well as the new emerging types of FDIA.
- Generality to be independent of the model and parameters of the system.
- Selectivity to identify the exact measurements that are affected with the FDIA.
- Robustness to ensure the least possible false alarms.
- Self-configuring to reduce the need of expert knowledge.
- Deterministic computing to allow real-time detection.
- Layered detection schemes as there is no such thing as 100% secure algorithm.

REFERENCES

[1] G. Simard, *IEEE Grid Vision 2050*, IEEE PES, Piscataway, NJ, USA, 2013.

[2] M. Faheem *et al.*, "Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges," *Comput. Sci. Rev.*, vol. 30, pp. 1–30, Nov. 2018.

[3] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. IEEE* , vol. 104, no. 5, pp. 1058–1070, May 2016.

[4] S. Toppa. (Mar. 2015). *The National Power Grid Is Under Almost Continuous Attack, Report Says*. Accessed: Mar. 29, 2019. [Online]. Available: https://bit.ly/1FH246I

[5] *The State of Industrial Cybersecurity 2017*, Bus. Advantage, Orpington, U.K., 2017.

[6] T. Reed, *At the Abyss: An Insider's History of the Cold War*. Novato, CA, USA: Presidio Press, 2005.

[7] T. L. Hardy, *Software and System Safety: Accidents, Incidents, and Lessons Learned*. Bloomington, IN, USA: AuthorHouse, 2012.

[8] M. Swearingen, S. Brunasso, J. Weiss, and D. Huber, (Jan. 9, 2013), *What You Need to Know (and Don't) About the AURORA Vulnerability, PowerMag*. Accessed: Apr. 15, 2019. [Online]. Available: https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1

[9] *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Elect. Inf. Sharing Anal. Center, Washington, DC, USA, 2016.

[10] J. Condliffe, *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*, MIT Technol. Rev., Cambridge, MA, USA, 2016.

[11] Executive Office of the President. (Feb. 19, 2013). *Improving Critical Infrastructure Cybersecurity*. Accessed: Apr. 22, 2019. [Online]. Available: https://bit.ly/2DRnTo5

[12] *Guidelines for Smart Grid Cybersecurity*, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2014.

[13] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Butterworth-Heinemann, Oxford, U.K., 2015.

[14] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[15] C.-C. Suna, A. Hahna, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[16] Y. Lopes *et al.*, "Vulnerabilities and threats in smart grid communication networks," in *Security Solutions and Applied Cryptography in Smart Grid Communications*. Hershey, PA, USA: IGI Glob., 2017, pp. 1–28.

[17] Z. ElMrabet, N. Kaabouch, H. ElGhazi and H. ElGhazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[18] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[19] C. Konstantinou and M. Maniatakos, "Hardware-layer intelligence collection for smart grid embedded systems," *J. Hardw. Syst. Security*, vol. 3, no. 2, pp. 132–146, 2019.

[20] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection 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.

[21] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proc. 2nd ACM Workshop Cyber Phys. Syst. Security Privacy*, 2016, pp. 81–92.

[22] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.* , vol. 51, no. 1, pp. 42–49, Jan. 2013.

[23] R. Kubo, "Detection and mitigation of false data injection attacks for secure interactive networked control systems," in *Proc. IEEE Int. Conf. Intell. Safety Robot. (ISR)*, Shenyang, China, 2018, pp. 7–12.

[24] R. Macwan *et al.*, "Collaborative defense against data injection attack in IEC61850 based smart substations," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, 2016, pp. 1–5.

[25] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.

[26] 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.

[27] 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.

[28] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[29] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[30] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.

[31] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[32] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based Cyber topology attack with application to the australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 7, pp. 3820–3829, Jul. 2018.

[33] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[34] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.

[35] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.

[36] 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.

[37] 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, 2016.

[38] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber Phys. Syst. Theory Appl.*, vol. 2, no. 4, pp. 180–187, 2017.

[39] R. Tan *et al.*, "Optimal false data injection attack against automatic generation control in power grids," in *Proc. ACM/IEEE 7th Int. Conf. Cyber Phys. Syst. (ICCPS)*, 2016, pp. 1–10.

[40] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, Mar. 2019.

[41] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018.

[42] J. Zhao *et al.*, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.

[43] 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. 21–32, 2011.

[44] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[45] J. Duan, W. Zeng, and M.-Y. Chow, "Resilient distributed DC optimal power flow against data integrity attack," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3543–3552, Jul. 2018.

[46] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, and C.-K. Wen, "Local cyber-physical attack with leveraging detection in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2017, pp. 461–466.

[47] Q. Jiang, H. Chen, L. Xie, and K. Wang, "Real-time detection of false data injection attack using residual prewhitening in smart grid network," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2017, pp. 83–88.

[48] J. G. Sreenath, A. Meghwani, S. Chakrabarti, K. Rajawat, and S. C. Srivastava, "A recursive state estimation approach to mitigate false data injection attacks in power systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2017, pp. 1–5.

[49] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13787–13798, 2017.

[50] T. Liu *et al.*, "Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection," *Future Gener. Comput. Syst.*, vol. 49, pp. 94–103, Aug. 2015.

[51] 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.*, to be published.

[52] 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.

[53] B. Li, R. Lu, G. Xiao, Z. Su, and A. Ghorbani, "PAMA: A proactive approach to mitigate false data injection attacks in smart grids," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2018, pp. 1–6.

[54] I. Lukicheva, D. Pozo, and A. Kulikov, "Cyberattack detection in intelligent grids using non-linear filtering," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Europe (ISGT-Europe)*, 2018, pp. 1–6.

[55] M. G. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, "Adaptive statistical detection of false data injection attacks in smart grids," in *Proc. IEEE Glob. Conf. Signal Inf. Process. (GlobalSIP)*, 2016, pp. 826–830.

[56] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4930–4941, Sep. 2018.

[57] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[58] B. Tang, J. Yan, S. Kay, and H. He, "Detection of false data injection attacks in smart grid under colored Gaussian noise," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2016, pp. 172–179.

[59] I. Akingeneye and J. Wu, "Low latency detection of sparse false data injections in smart grids," *IEEE Access*, vol. 6, pp. 58564–58573, 2018.

[60] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[61] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[62] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[63] M. Khalaf, A. Youssef, and E. El-Saadany, "Detection of false data injection in automatic generation control systems using Kalman filter," in *Proc. IEEE Elect. Power Energy Conf. (EPEC)*, 2017, pp. 1–6.

[64] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4985–4995, Sep. 2019.

[65] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[66] Y. Jiang and Q. Hui, "Kalman filter with diffusion strategies for detecting power grid false data injection attacks," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, 2017, pp. 254–259.

[67] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 697–707, Mar. 2017.

[68] H. Karimipour and V. Dinavahi, "Robust massively parallel dynamic state estimation of power systems against cyber-attack," *IEEE Access*, vol. 6, pp. 2984–2995, 2018.

[69] H. Karimipour and V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids," in *Proc. IEEE Int. Conf. Smart Energy Grid Eng. (SEGE)*, 2017, pp. 388–393.

[70] W. Shi, Y. Wang, Q. Jin, and J. Ma, "PDL: An efficient prediction-based false data injection attack detection and location in smart grid," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, 2018, pp. 676–681.

[71] J. Zhao, G. Zhang, M. L. Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.

[72] A. Anwar, A. N. Mahmood, and Z. Tari, "Ensuring data integrity of OPF module and energy database by detecting changes in power flow patterns in smart grids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3299–3311, Dec. 2017.

[73] Y. Li, J. Li, X. Luo, X. Wang, and X. Guan, "Cyber attack detection and isolation for smart grids via unknown input observer," in *Proc. 37th Chin. Control Conf. (CCC)*, 2018, pp. 6207–6212.

[74] X. Wang, X. Luo, M. Zhang, and X. Guan, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *Int. J. Elect. Power Energy Syst.*, vol. 110, pp. 208–222, Sep. 2019.

[75] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York, NY, USA: Springer-Verlag, 1994.

[76] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, "A stealth cyber attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[77] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go- decomposition (GoDec) approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2892–2904, May 2019.

[78] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[79] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4741–4750, Sep. 2019.

[80] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89–97, Jan. 2018.

[81] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep. 2018.

[82] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[83] R. J. R. Kumar and B. Sikdar, "Efficient detection of false data injection attacks on AC state estimation in smart grids," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2017, pp. 411–415.

[84] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[85] J. Hao *et al.*, "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2398–2408, Jul. 2018.

[86] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 305–318, Jan. 2019.

[87] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[88] K. Khanna, S. K. Singh, B. K. Panigrahi, R. Bose, and A. Joshi, "On detecting false data injection with limited network information using transformation based statistical techniques," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Chicago, IL, USA, 2017, pp. 1–5.

[89] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[90] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[91] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *Int. J. Elect. Power Energy Syst.*, vol. 91, pp. 230–240, Oct. 2017.

[92] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[93] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, 2016, pp. 1395–1402.

[94] S. Binna, S. R. Kuppannagari, D. Engel, and V. K. Prasanna, "Subset level detection of false data injection attacks in smart grids," in *Proc. IEEE Conf. Technol. Sustain. (SusTech)*, Long Beach, CA, USA, 2018, pp. 1–7.

[95] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, "Real-time cyber-physical false data attack detection in smart grids using neural networks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, 2017, pp. 1–6.

[96] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber Phys. Syst. Theory Appl.*, vol. 2, no. 4, pp. 161–171, 2017.

[97] K. Vimalkumar and N. Radhika, "A big data framework for intrusion detection in smart grids using Apache spark," in *Proc. Int. Conf. Adv. Comput. Commun. Informat. (ICACCI)*, 2017, pp. 198–204.

[98] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[99] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inf. Security Appl.*, vol. 46, pp. 42–52, Jun. 2019.

[100] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017.

[101] K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Gener. Transm. Distrib.*, vol. 12, no. 5, pp. 1052–1066, Mar. 2018.

[102] M. E. Hariri, T. A. Youssef, H. F. Habib, and O. Mohammed, "Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, 2017, pp. 1–5.

[103] G. Fenza, M. Gallo, and V. Loia, "Drift-aware methodology for anomaly detection in smart grid," *IEEE Access*, vol. 7, pp. 9645–9657, 2019.

[104] A. Ayad, M. Khalaf, and E. El-Saadany, "Detection of false data injection attacks in automatic generation control systems considering system nonlinearities," in *Proc. IEEE Elect. Power Energy Conf. (EPEC)*, 2018, pp. 1–6.

[105] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, 2018, pp. 1–5.

[106] H. Zhao, H. Liu, W. Hu, and X. Yan, "Anomaly detection and fault analysis of wind turbine components based on deep learning network," *Renew. Energy*, vol. 127, pp. 825–834, Nov. 2018.

[107] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019.

[108] L. Yang, Y. Li, and Z. Li, "Improved-ELM method for detecting false data attack in smart grid," *Int. J. Elect. Power Energy Syst.*, vol. 91, pp. 183–191, Oct. 2017.

[109] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.

[110] R. Razavi, A. Gharipour, M. Fleury, and I. J. Akpan, "A practical feature-engineering framework for electricity theft detection in smart grids," *Appl. Energy*, vol. 238, pp. 481–494, Mar. 2019.

[111] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[112] H. Sedghi and E. Jonckheere, "Statistical structure learning to ensure data integrity in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1924–1933, Jul. 2015.

[113] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2013, pp. 1–5.

[114] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2019.

[115] J. L. Viegas and S. M. Vieira, "Clustering-based novelty detection to uncover electricity theft," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, 2017, pp. 1–6.
[116] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2765–2777, Oct. 2019.
[117] L. Wei, D. Gao, and C. Luo, "False data injection attacks detection with deep belief networks in smart grid," in *Proc. Chin. Autom. Congr. (CAC)*, 2018, pp. 2621–2625.
[118] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[119] A. A. Ghasemi and M. Gitizadeh, "Detection of illegal consumers using pattern classification approach combined with Levenberg–Marquardt method in smart grid," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 363–375, Jul. 2018.
[120] S. Ntalampiras, "Fault diagnosis for smart grids in pragmatic conditions," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1964–1971, May 2018.
[121] B. Li, R. Lu, and G. Xiao, "HMM-based fast detection of false data injections in advanced metering infrastructure," in *Proc. IEEE Glob. Commun. Conf.*, 2017, pp. 1–6.
[122] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.
[123] U. Adhikari, T. H. Morris, and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3928–3941, Sep. 2018.
[124] U. Adhikari, T. H. Morris, and S. Pan, "Applying Hoeffding adaptive trees for real-time cyber-power event and intrusion classification," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4049–4060, Sep. 2018.
[125] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 650–662, Jun. 2015.
[126] U. Adhikari, T. H. Morris, and S. Pan, "A causal event graph for cyber-power system events using synchrophasor," in *Proc. IEEE PES Gen. Meeting Conf. Expo.*, 2014, pp. 1–5.
[127] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.
[128] Y. Ding and J. Liu, "Real-time false data injection attack detection in energy Internet using online robust principal component analysis," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, 2017, pp. 1–6.
[129] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.
[130] E. Villar-Rodriguez, J. D. Ser, I. Oregi, M. N. Bilbao, and S. Gil-Lopez, "Detection of non-technical losses in smart meter data based on load curve profiling and time series analysis," *Energy*, vol. 137, pp. 118–128, Oct. 2017.
[131] A. A. Saad, S. Faddel, and O. Mohammed, "A secured distributed control system for future interconnected smart grids," *Appl. Energy*, vol. 243, pp. 57–70, Jun. 2019.
[132] I. Chivers and J. Sleightholme, "An introduction to algorithms and the big O notation," in *Introduction to Programming With Fortran*. Cham, Switzerland: Springer, 2015.

Ahmed S. Musleh (S'11–M'17) received the B.Sc. degree (Highest Hons.) in electrical engineering from Abu Dhabi University, Abu Dhabi, UAE, in 2014, and the M.Sc. degree in electrical engineering from Petroleum Institute (currently, Khalifa University), Abu Dhabi, in 2016. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. His research interests include smart grid technologies, wide area monitoring and control, cyber-physical security, and machine learning applications. He was a recipient of the Abu Dhabi University Overall Award of Excellence in 2014 and the Petroleum Institute Graduate Fellowship in 2015.

Guo Chen (M'10) received the Ph.D. degree in electrical engineering from the University of Queensland, Brisbane, Australia, in 2010. He held academic positions with the Australian National University, the University of Sydney, and the University of Newcastle. He is currently a lecturer with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. His research interests include sustainable energy system modeling, artificial intelligence and neural networks, optimization and control, cyber security and their applications in smart grid, and smart home. He was a recipient of the Australian Research Council Discovery Early Career Researcher Award Fellowship and UNSW Scientia Fellowship. He is a Editor of the IEEE TRANSACTIONS ON SMART GRID.

Zhao Yang Dong (M'99–SM'06–F'16) received the Ph.D. degree in electrical engineering from the University of Sydney, Australia, in 1999. He is currently a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, Australia. From 2013 to 2017, he served as the Head of the School of Electrical and Information Engineering, University of Sydney. He is a immediate Ausgrid Chair Professor and the Director of the Centre for Intelligent Electricity Networks, University of Newcastle, Australia. His research interest includes smart grid, power system planning, power system security, load modeling, renewable energy systems, electricity market, and computational intelligence and its application in power engineering. He has served as a Editor for the IEEE TRANSACTIONS ON SMART GRID, the IEEE POWER AND ENERGY SOCIETY LETTERS, the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, and *IET Renewable Power Generation*.