Unified Detection of Attacks Involving Injection of False Control Commands and Measurements in Transmission Systems of Smart Grids

Shantanu Chakrabarty and Biplab Sikdar

***Abstract*—Smart grid operation and monitoring are heavily dependent on the correctness or aptness of supervisory control commands. These command channels are a part of the SCADA system, which is vulnerable to cyber-attacks. Maliciously injected commands can cause a wide range of issues including blackouts. However, the literature addressing this problem is limited. In order to fill this gap, a generalized framework is proposed to achieve simultaneous detection of attacks against various types of control devices/equipments used in transmission systems, even if they are carried out stealthily. First, generalized mathematical models of such stealthy attacks are presented. Then, based on these attack models, changes in the measurement covariance matrix that occur during an attack are exploited to formulate the proposed approach. We first mathematically characterize these changes using the eigenvectors and trace of the covariance matrix and then use them to develop a detection metric. It is observed that when the model of a false data injection (FDI) attack is considered, the developed detection metric is also capable of detecting such attacks. The algorithm that results from the detection metric is a generalized framework for detection of attacks against all types of transmission system controls and measurements. Moreover, the algorithm is non-iterative, computationally inexpensive, and independent of both the type of state estimation and communication technology used. The proposed algorithm is found to be effective, when tested on the IEEE 118-bus system.**

***Index Terms*—Cybersecurity, False Data Injection (FDI) attacks, Supervisory Control Protection.**

I. Introduction

POWER systems serve the purpose of delivering electrical energy from a place of generation to a place of consumption (distribution), through a transmission system. Traditionally, the system was monitored and controlled with significant human involvement. However, in recent times, due to advent of automation, a large part of day-to-day operation of grids is delegated to a set of computers, networked by means of communication channels. This interface between on-field devices and the central computer system is known as the Supervisory Control and Data Acquisition (SCADA) system. SCADA systems leverage on measurement data (spread across the system) to estimate the state of the system (by a process known as state estimation [1]); and based on the state information, supervisory control is executed. SCADA systems, in general, are vulnerable to cyber attacks [2], [3]. Thus, entire processes of state estimation and supervisory control are vulnerable to cyber attacks.

As far as transmission grid controls are concerned, there are two broad types of control [4]. They are active power (P) related controls where the active power flows are manipulated, and reactive power (Q) related controls, where the reactive power flows are manipulated. Q-related controls are widely used for voltage ($|V|$) control, as Q is very strongly coupled with $|V|$. Similarly, P related controls are used to control power flows either to prevent overloads or to ensure flows as per contracts. These controls are executed in the system using a wide variety of devices, that are interfaced with the SCADA system through Remote Terminal Units (RTUs). The commands to execute these controls are sent from the Control Centre (i.e., Energy Management Systems (EMS)) to these RTUs. An attack on this supervisory control mechanism is considered to have the highest impact [2], as the adversary has access to the entire range of control. Hence, a malicious operation of voltage or flow control can have catastrophic effects, both in terms of grid operation and economics [5]. In this paper, such attacks are referred to as False Command Injection (FCI) attacks [6]. The attacks on measurement data, formally known as False Data Injection (FDI) attacks [7], [8], essentially force wrong estimation of states, eventually resulting in erratic control actions.

FDI attacks are one of the most extensively studied attacks in the context of smart/automated grids [9]. In these attacks, an adversary carefully injects false data that does not alert the Bad Data Detection (BDD). Several methods have been proposed for the detection of such attacks [9], using a wide variety of approaches. However, literature on attacks involving injection of false supervisory control commands is sparse, when compared to literature on FDI attacks. As far as security of active power and voltage controls are concerned, the methods proposed in [10], [11] deal with attacks on control which result from FDI attacks. On the other hand, the methods in [6] and [12] are only applicable to detection of false transformer tap and phase shifter commands, respectively. A detailed discussion on all these references is presented in Section II. Hence, there are no works that address malicious command injection attacks across all types of transmission controls (both P and Q types), or provide an unified framework for detection of FDI and FCI attacks. This paper is an attempt to fill this gap in literature. In this paper, generalized mathematical models for stealthy attacks involving injection of malicious commands are first established. Based on these generalized attack models, the

Shantanu Chakrabarty is with Department of Electrical and Computer Engineering, National University of Singapore, Singapore, e-mail: dcsshch@nus.edu.sg (Corresponding Author)

Biplab Sikdar is with Department of Electrical and Computer Engineering, National University of Singapore, Singapore, e-mail: bsikdar@nus.edu.sg

changes that occur in the measurement covariance matrix when there is an attack are analyzed. These changes are based on the trace and eigenvectors of the covariance matrix. The changes are characterised as three propositions (that are proven). It can also be shown that when the attack models (in terms of measurements) of FDI attacks [8], [13] are considered, the three proposed propositions still hold good. These three propositions are then used to develop a detection metric. Hence, the proposed algorithm using the developed detection metric facilitates an unified scheme for detection of attacks against both commands and measurements.

The main contribution of the paper can be listed as follows:

1) The paper addresses both sub-problems of transmission grid control (active and reactive power) using a generalized approach that is independent of the control device.
2) The proposed algorithm detects the presence of both false commands and data, using an unified scheme based on changes in measurement covariance matrix (that are characterised and proven).
3) The proposed algorithm:
    a) is computationally inexpensive, as there are no iterative steps involved;
    b) does not have divergence issues as it is a single step algorithm;
    c) does not need historical data of measurements or states;
    d) is found to be effective when tested on attack scenarios on the IEEE 118-bus system.

The paper is organized as follows: A detailed discussion on literature is given in Section II. A discussion of attacks on smart grids is presented in Section III with an emphasis on stealthy attacks on transmission system controls. The complete mathematical analysis pertaining to the development of the proposed algorithm is given in Section IV, which is followed by the proposed algorithm in Section V. Simulation studies are discussed in Section VI. Finally, the conclusions are drawn in Section VII.

II. Literature Review

In this section, some important references related to research on attacks involving injection of false data and commands are outlined. State estimators are vulnerable to carefully injected measurement data that beats BDD, as discussed in [7], under a DC power flow model. In [7], conditions required to carry out such attacks are established. The same vulnerability under AC power flow model is studied in [8]. Subsequently, several approaches have been proposed to provide protection from attacks that exploit these vulnerabilities. Following the works in [7], [8], various other innovative ways of exploiting vulnerabilities of state estimators have been proposed [14], [15]. A review of FDI attacks is presented in [13], discussing physical and economic impacts of such attacks. A generalized FDI attack scheme that accounts for measurement uncertainty is discussed in [16], where a countermeasure strategy is proposed that uses a set of secured PMU measurements. An unobservable attack with an intention to overload a line is studied in [17], where the possible consequences of such attacks are analysed.

In order to address the threat of FDI attacks, numerous detection methods are proposed in literature. These methods can be broadly classified into two categories based on the power flow model used to express the relationship between measurements and state variables. The first category covers methods that consider a DC power flow model [18]–[24]. The second category includes methods that consider the non-linear AC power flow based state estimators. In practical state estimators, AC power flow model is used [16]. There have been some interesting approaches proposed to detect FDI attacks under non-linear AC state estimators. In [25], dynamics of measurement variations are tracked using Kullback–Leibler (KLD) distance. In this approach, comparison with historical data is required. Details of practical implementation of FDI attacks under AC power flow model are given in [26]. In [26], execution of FDI attacks by firmware modifications and falsification of data transmission is discussed. A novel graph theory based approach is presented in [27] based on application of outlier detection techniques. In order to make the detection approach independent of communication and networking technologies, an online detection scheme using load forecasts, generation schedules and synchrophasor data is proposed in [28]. A non-iterative technique is proposed in [29], that is based on flow measurements from SCADA and voltage measurements from PMUs. This approach is computationally inexpensive and independent of communication technologies. The use of machine learning algorithms, more specifically ELM-Based OCON Framework for FDI attack detection (under AC power flows) can be seen in [30]. This approach, along with other machine learning approaches that use DC power flow model [21], [22], is effective for detection of FDI attacks after deployment. However, these approaches require a large training set and training is usually computationally intensive. FDI attacks can also be prevented or thwarted by means of proactive perturbation of branch susceptances [31] [32] [33]. These techniques in general are known as Moving Target Defence (MTD) [31]. In [31], the completeness, deployment and operational cost of MTD are studied in detail. The conditions such that MTD is complete in defeating FDI attacks using former branch parameters are proposed. Furthermore, guidelines for effective implementation of MTD are proposed based on the mathematical analysis. The analysis of [31] is done using DC power flow model. The use of distributed flexible AC transmission system (D-FACTS) for detection of FDI attacks can be seen in [34]–[36]. Such approaches are termed as proactive false data detection (PFDD) approach. The feasibility and limitations of PFDD in detection of FDI attacks are studied in detail in [34]. In [34], the minimum effort to use D-FACTS devices to detect FDI attacks are evaluated. Furthermore, the limitations of using PFDD are discussed. A novel federated deep learning scheme, termed “DeepFed” is developed to detect threats against industrial cyber-physical systems in general is presented in [37]. The methods in [31], [34] are shown to be effective against FDI attacks. However, their applicability in the case of attacks involving command injections are not known. The application of Kalman filtering to detect FDI attacks can be seen in [38], [39]. These methods come under the purview of dynamic estimation [9]. A detailed review of dynamic state estimation is presented in [40] and a detailed review of FDI attacks under dynamic estimation is given in [9].

In the case of attacks on supervisory control, the available literature is limited when compared to FDI attacks. The works in [41]–[47] consider security of commands in general. In [42]–[45], coordinated cyber-physical attacks (CCPA) are considered. In these works, attacks involving line outages (tripping the breakers) are studied, along the lines of the 2015 Ukraine cyber-attack [48]. In [46], confidentiality attacks on cyber-physical model of wide area monitoring systems are considered, centred around the generators. The command injection attacks on generator circuit breakers (CBs) is studied in [49]. In [47], a novel method to detect false command data injection (FcDI) attacks in the hierarchical control paradigm of the smart grid is proposed. FcDI attacks are defined in [50] as insider attacks where the adversary issues fake commands to various system actuators like generators, transformers, breakers, etc. In [47], a futuristic hierarchical control paradigm is presented where decentralized local agents, containing their own state estimators and local controllers. Furthermore, DC power flow model is used in [47], and as a result, voltage control security cannot be studied.

The literature that explicitly considers security of transmission system controls, discussed in Section I, is sparse. The methods in [10], [11] deal with wrong control actions resulting from an FDI attack. The methods that address attacks on transformer tap and phase shifter commands are [6] and [12], respectively. However, these methods are device specific and are not extensible for detecting FDI attacks across the grid.

Based on the discussion of related literature above, the contents of this paper differ from the existing literature in the following ways. They are as follows:

- This paper explicitly considers the security of two sub-problems of transmission grid operation and control in detail using generalized mathematical models. This enables the inclusion of both the sub-problems of transmission grid controls, i.e., active power and voltage controls, under a unified detection approach. Furthermore, any device that deals with these sub-problems can be modelled and incorporated in the developed detection scheme.
- The approach for considering security of transmission controls is developed based on generalized mathematical models of the grid and transmission control. Thus, this method is applicable under any implementation of information and communication technology.
- Furthermore, when the mathematical model for the FDI attacks are plugged in the analysis developed in this paper, it is observed that the developed approach also is able to detect these attacks. Hence, this paper deals with a unified detection scheme for detecting FDI attacks and FCI attacks against the two sub-types of transmission control.

In summary, it is important that techniques are developed that are capable of detecting intrusions on both measurements and supervisory commands of transmission system controls. This paper is an attempt to fill this gap in the literature and the proposed algorithm detects intrusions on both measurements and transmission system control commands. At the same time, it is computationally inexpensive, non-iterative, and does not require training or historical data.

III. Attacks against Smart Grids

Attacks on data (or measurements) [7] may result in wrong control actions due to incorrect estimation. However, attacks on control commands [2], [6], [12] are considered to be most catastrophic [2], as the entire range of control actions are available. In this section, the attacks (mainly, involving false control commands) and their relevant mathematical models are discussed.

A. False Data Injection (FDI) Attacks

When a measurement is manipulated, one or more state variables are affected. Similarly, other measurements related to these affected state variables also change. If these other measurements are not manipulated according to the system laws or rules (like power balance, operational requirements, etc.), BDD is triggered. In order to achieve falsification of measurements and avoid BDD, all the measurements that depend on the changed state variables must also be falsified [7], [8]. Such attacks are known as False Data Injection (FDI) attacks. This type of attack is well-researched in literature [18]-[29]. These attacks and their difference from other types of attacks are further discussed in Section III-B.

B. False Command Injection (FCI) attacks against Transmission System Control

In general, these attacks involve an adversary taking over the supervisory control of the power grid. These attacks are usually catastrophic [2], [5], [51]. The types of controls in a transmission system are mentioned in Section I. The variables associated with transmission grid controls are defined first in Section III-B1, which is followed by an introduction to stealthy attacks involving false command injections in Section III-B2. Finally, the mathematical conditions required for stealthy command injections are derived and discussed in Section III-B3.

1) Variables in Transmission Grid Control: In a transmission grid control, mathematically, there are two types of variables, defined as follows:

Definition 1. *A controlled variable, also known as constrained variable [52], is a variable that is set to a rated or desired value during the grid operation, based on various operational and contractual requirements.*

Definition 2. *A controlling variable, also known as adjustable variable [52], is a variable that is varied by means of specifically installed equipments or control mechanisms to ensure that the requirements with regard to the controlled variable (or constrained variable) are met.*

These variables defined in Definitions 1 and 2 are principally similar (or analogous) to the ones seen in control theory, as one or more variables (controlling variables) are tuned to achieve a set or desired value of the controlled or constrained variable. However, in practical grid operation, the variables defined in Definitions 1 and 2 and the mechanism of achieving the desired value of controlled (or constrained variables) are different when compared to control theory [6], [12], [52]–[54].

In power grids, the controlling variable is one among many variables that can affect the controlled/constrained variable. The controlling variables differ from other variables in two main aspects. The first aspect is that controlled variables are highly dependent on (or sensitive to) the controlling variables and the second aspect lies in the ability of the operator/central computer to control that variable by suitable installation of equipments, like a tap changing transformer or a phase shifter.

In the context of transmission control sub-problems, discussed in Section I and [4], the controlled variable may be a state variable, like in case of voltage control using tap changers, where the tap ratio (t) is the controlling variable and the voltage magnitude ($|V|$) is the controlled variable. On the other hand, the controlled variable may be an explicit function of state variables, like in case of active power control using phase shifters, where the phase shift (ϕ) is the controlling variable and the active power flow (P_{flow}) is the contolled variable.

2) Requirements for Stealthy False Command Injection (FCI) Attacks: False Command Injection (FCI) attacks, discussed in [6], [12], [49], [50], are formally defined below in Definition 3.

Definition 3. *False Command Injection (FCI) attacks are the class of attacks where the adversary injects a set of malicious commands to compromise the control mechanisms of various installed equipments to disrupt the operation and control of a smart grid/power grid.*

An illustration of the exchange of data and commands between the Control Centre (EMS) and a substation is presented in Figure 1. The substation houses the control equipments, for example, on load tap changing transformers (OLTCs) and phase shifting transformers (PSTs). These control equipments are actuated using RTUs that relay the commands received from the EMS, shown in Figure 1 using dashed lines with direction indicative of the information flow. Similarly, the measurement data, when collected, is relayed from the substation to the control centre, shown in Figure 1 using solid lines with the direction of information flow. It is worth noting that Figure 1 is an illustration of the mechanism of exchange of data and commands and is independent of the type of information and communication technology used for automation. Whenever an adversary tampers measurement data, i.e., FDI attacks [7], [8], the adversary tampers the measurement data exchange between the substation and control centre (illustrated using solid lines in Figure 1). In FDI attacks, the necessity to beat the BDD is paramount [7], [8]. On the other hand, in case of FCI attacks, the adversary essentially injects a false or malicious command (or falsifies the command) through the channels used to relay the control command from the control centre to the equipment at the substation, shown using dashed lines in Figure 1. It is important to note that in case of FCI attacks defined in Definition 3, evasion of BDD is not a necessity, unlike FDI attacks.

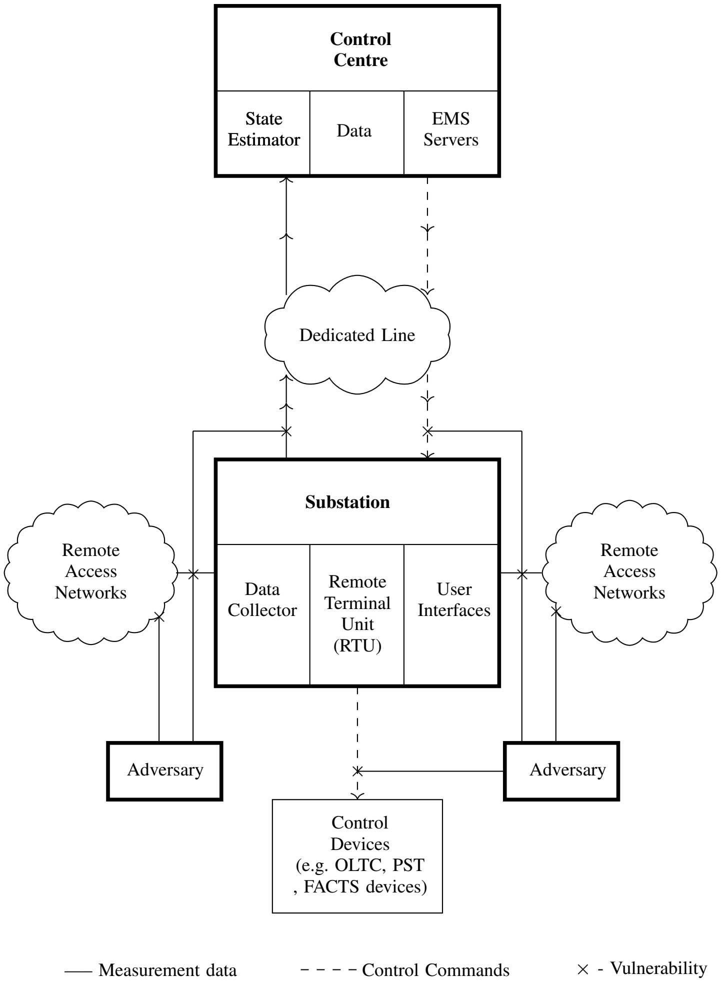

Fig. 1. An illustration of the exchange of measurement data and control commands between Control Centre and Substation.

In order to develop detection algorithms to protect transmission system control, certain practical aspects of operation must be taken into account while developing the attack model. In case of transmission system controls, the operators either at the substation, control centre, or both, usually observe or keep track (either manually or automatically) of the relevant controlled and controlling variables. For example, if a OLTC is installed for voltage control, the operators keep track of the controlled variable, i.e., voltage, $|V|$, and the controlling variable, i.e., tap ratio, t. In order to develop a detection method that is applicable for a wide range of attack scenarios, it is necessary to consider attack scenarios (or vulnerabilities), where the adversary injects malicious commands and hides the presence of these commands from both the operator at the substation and the control centre.

In other words, in order to attack control equipments (like OLTCs and PSTs) and remain stealthy, the adversary has to evade the attention of both the operator and the control centre (BDD). Such attacks are called Stealthy False Command Injection attacks, defined formally in Definition 4. On the other hand, FCI attacks where the adversary injects malicious commands and does not hide the presence of these commands are called *Blatant FCI attacks*.

Definition 4. *Stealthy False Command Injection attacks are a class of FCI attacks where the adversary injects a set of malicious commands and hides the presence of these commands from the operator at the substation and control centre by ensuring that the measured and estimated values of controlled and controlling variables, defined in Definitions 1 and 2, are close to the values selected by the control centre.*

Mathematically, to achieve such attacks, the measured and estimated values of both the controlling and controlled variables must remain close to the values selected by the control centre. In this paper, attacks pertaining to transmission control sub-problems (active power and voltage control) are considered.

3) Mathematical Conditions to Carry out Stealthy False Command Injection (FCI) Attacks: The mathematical conditions to carry out the stealthy FCI attacks in the context of transmission system control are considered. These conditions in the first case where both the controlled and controlling variables are state variables are stated and proven in [6]. In this paper, the conditions for the second case, where the controlled variable is an explicit function of controlling and other state variables is established in Proposition 1. It is worth noting that these two sets of conditions are general and cover various transmission network control equipments (like transformers, FACTS devices, etc.).

Proposition 1. *Let* $\mathbf{z} = \begin{bmatrix} z_1 & \cdots & z_{n_m} \end{bmatrix}^T$ *be the measurement vector and* $\mathbf{x} = \begin{bmatrix} x_1 & \cdots & x_{n_s} \end{bmatrix}^T$ *be the state vector. Suppose* $\mathbf{c} = \begin{bmatrix} x_i & x_{i+1} & \cdots & x_{i+k} \end{bmatrix}^T$ *and* $\mathbf{z_c} = \begin{bmatrix} z_l & z_{l+1} & \cdots & z_{l+k} \end{bmatrix}^T$ $\forall\ i \geq 1, l \geq 1, k \leq (n_s - i)$ *and* $k \leq (n_m - l)$ *be two same-length vectors (of length* $(k+1)$*) containing controlling variables and controlled variables, respectively. Let the vector,* $\mathbf{z}_c^{sel} \in \mathbb{R}^{(k+1)\times 1}$*, contain values of controlled variables (in vector* $\mathbf{z_c}$*) selected by the EMS, where, the superscript, sel, is used to denote quantities selected by the EMS. Let the controlled variable,* z_{l+k}*, be expressed as an explicit function,* $z_{l+k} = h_{l+k}(x_{i+k}, \Lambda_{i+k})$*, where* Λ_{i+k} *is the set containing other state variables except the controlling variable,* x_{i+k}*. Let a vector,* $\mathbf{d} \in \mathbb{R}^{(k+1)\times 1}$*, be defined such that its elements,* $d_{i+k} \in \Lambda_{i+k}$ $\forall\ i \geq 1, k \leq (n_s - i)$*. Let a set,* Θ_{i+k} *be defined such that* $\Theta_{i+k} = \Lambda_{i+k} - \{d_{i+k}\}$*. For an adversary to launch a malicious command to change* $\mathbf{c}$ *and remain hidden from both the operator and BDD,* $\mathbf{c}$*,* $\mathbf{d}$ *and measurements dependent on* $\mathbf{c}$ *and* $\mathbf{d}$ *must be modified to ensure that* $\mathbf{z_c} = \mathbf{z}_c^{sel} + \mathbf{e}$*,* $\forall\ \mathbf{e} \sim \mathcal{N}(0, \sigma)$ *.*

Proof. Under normal conditions, in the absence of a cyberattack, we have

$$\mathbf{z}^n = \mathbf{h}(\mathbf{x}^n) + \mathbf{e}, \tag{1}$$

where, superscript n is used to denote quantities under normal conditions. The state vector is of the form

$$\mathbf{x^n} = \begin{bmatrix} x_1^n & x_2^n & \cdots & (\mathbf{c}^n)^T & \cdots & (\mathbf{d}^n)^T & \cdots & x_{n_s}^n \end{bmatrix}^T. \tag{2}$$

When there is no cyber-attack, the controlled and controlling variables are at the values selected by the EMS. Thus, based on definitions in the statement of this proposition, we have $\mathbf{z_c^n} = \mathbf{z}_c^{\text{sel}}$.

When an adversary injects false commands to maliciously modify $\mathbf{z_c}$, we have

$$\mathbf{z}^b = \mathbf{h}(\mathbf{x}^b) + \mathbf{e}, \tag{3}$$

where, superscript b is used to denote quantities under a blatant or non-stealthy attack.

In order to keep this malicious change hidden from both the operator and EMS, the adversary has to ensure that $\mathbf{z}_c^{\text{hid}} \approx \mathbf{z}_c^n = \mathbf{z}_c^{\text{sel}}$ and $\mathbf{c}^{\text{hid}} = \mathbf{c}^n$, where the superscript, hid, denotes quantities under a stealthy attack. To achieve these requirements, the adversary has to first solve the system of equations

$$\begin{bmatrix} z_l^{\text{sel}} \\ z_{l+1}^{\text{sel}} \\ \vdots \\ z_{l+k}^{\text{sel}} \end{bmatrix} = \begin{bmatrix} h_l(x_i^n, d_i, \Theta_i^b) \\ h_{l+1}(x_{i+1}^n, d_{i+1}, \Theta_{i+1}^b) \\ \vdots \\ h_{l+k}(x_{i+k}^n, d_{i+k}, \Theta_{i+k}^b) \end{bmatrix}, \tag{4}$$

for every controlled variable, to estimate the values of d_i, d_{i+1}, $\cdots$, d_{i+k}. Let the vector containing the solution for all controlled variables, obtained by solving the system of equations (4), be denoted by $\mathbf{d}^{\text{sol}}$ $\big($where the superscript, sol, is used to denote solutions to (4)$\big)$. In order for the adversary to evade the attention of the operator at the substation, and/or control centre, the measured and estimated values of $\mathbf{c}$ and $\mathbf{d}$ must be $\mathbf{c^n}$ and $\mathbf{d}^{\text{sol}}$, respectively, to ensure that $\mathbf{z_c}^{\text{hid}} = \mathbf{z}_c^{\text{sel}} + \mathbf{e}$, $\forall\ \mathbf{e} \sim \mathcal{N}(0, \sigma)$. Hence, the state vector in a stealthy attack must be of the form,

$$\mathbf{x}^{\text{hid}} = \begin{bmatrix} x_1^b & x_2^b & \cdots & (\mathbf{c}^n)^T & \cdots & (\mathbf{d}^{sol})^T & \cdots & x_{n_s}^b \end{bmatrix}^T. \tag{5}$$

In order to beat BDD, according to [8], the following vector,

$$\mathbf{E} = \mathbf{h}(\mathbf{x}^{\text{hid}}) - \mathbf{h}(\mathbf{x}^b), \tag{6}$$

is added to (3), resulting in

$$\mathbf{z}^b + \mathbf{E} = \mathbf{h}(\mathbf{x}^{\text{hid}}) + \mathbf{e}. \tag{7}$$

Thus, based on (7), it is clear that power balance is maintained, and thus BDD gets beaten. From the form of $\mathbf{x}^{\text{hid}}$ and (6), it is clear that $\mathbf{E}$ has non-zero entries corresponding to the measurements that are functions of $\mathbf{c}$ and $\mathbf{d}$.
Hence proved. □

Based on above discussions and Proposition 1, certain remarks can be made. They are as follows:

- The conditions derived in Proposition 1 are sufficient conditions.
- Consider a pair of controlled and controlling variables, defined in statement of Proposition 1, individually, i.e., x_{i+j} and z_{l+j} $\forall\ i \geq 1,\ l \geq 1\ j = 0, 1, \cdots, k$. From the outcome of Proposition 1, it can be seen that x_{i+j}, d_{i+j} and measurements dependent on x_{i+j} and d_{i+j} must be modified to ensure that any malicious command remains hidden. Practically, this implies that if d_{i+j} is chosen as a state variable related to voltage magnitude or angle at the substation that houses the control equipment, then the adversary can carry out this attack by taking over one substation. This is because the information available

at the substation that houses the control equipments is sufficient for the adversary to launch the attack.

- The attack model and its related derivations in Proposition 1 are relevant only for control sub-problems where the controlled variables are an explicit function of state variables, i.e., $z_{l+k} = h_{l+k}(x_{i+k}, \Lambda_{i+k})$, or in other words, the controlled variables are only measurements, like in case of active power control.
- As discussed before, there is another set of problems where the controlled variables can be both state variables and measurements, like in case of voltage control, where the controlled variable, i.e., voltage magnitude is a state variable and can also be measured using voltmeters. In such situations, mathematically, for a node k, the voltage magnitude measurement, $|V_k|^{meas} = |V_k| + e_k \forall\, e \sim \mathcal{N}(0, \sigma)$, where superscript, $meas$, denotes measured value. Mathematically, $|V_k|^{meas}$ can be seen as a measurement which is function of state variable, $|V_k|$. The mathematical conditions required to launch a stealthy FCI attack (defined in Definition 4) in such situations are derived in [6], as stated before in Section III-B3.
- State variables are usually voltage magnitudes and angles when the system under study does not have control equipments like tap changing transformers, phase shifting transformers, etc. However, in transmission system where there are such equipments, the equations are modelled to take these equipments into consideration [1]. In other words, state estimation is modified to incorporate them into the formulation [55], [56]. As a result the controlling variables like tap ratio and phase shift gets included in the state vector [55]. It is important to note the mathematical algorithms remain unchanged. Hence, it can be mathematically and intuitively inferred from [55] that the principles related to BDD remains unchanged [55].

IV. Principles of Detection Metrics

In this section, the principles used in the formulation of indices used for the purpose of detection of FDI and FCI attacks are discussed in detail. The discussion is done based on the attack model in Proposition 1.

A. Mathematical Model of Measurements Under Normal and Attack Scenarios

Let the measurement vector at the k^{th} snapshot be $\mathbf{z_{nk}} \in \mathbb{R}^{n_m}$. The measurements over t instants (or snapshots) can be consolidated as a matrix $\mathbf{Z_n} \in \mathbb{R}^{n_m \times t}$, where n_m is the number of measurements, such that

$$\mathbf{Z_n} = \begin{bmatrix} \mathbf{z_{n1}} & \mathbf{z_{n2}} & \cdots & \mathbf{z_{nm}} & \mathbf{z_{n(m+1)}} & \cdots & \mathbf{z_{nt}} \end{bmatrix}, \quad (8)$$

also shown in Figure 2, where, n in the subscript represents quantities under normal operating conditions (when there is no cyber-attack). In other words, the measurement vector under normal condition, i.e., $\mathbf{z_n}$ at m^{th} snapshot is represented by $\mathbf{z_{nm}}$. This convention can be similarly extended to the state vector, $\mathbf{x_n}$. The illustration in Figure 2 is based on the practical aspects of grid operation and monitoring [57]. State estimation is usually done every few minutes and measurement data is available once every few seconds. Furthermore, further advancements in information and communication technologies would provide more measurement snapshots between two state estimations. In the algorithm developed in this paper, the time-frame between two state estimations is the time-frame of the detection window.

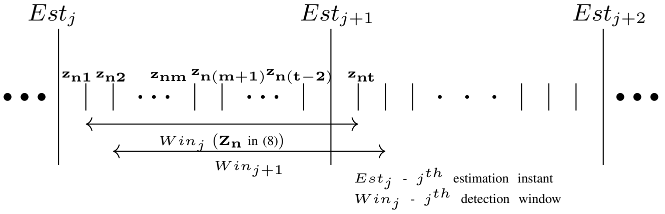
Est_j
Est_{j+1}
Est_{j+2}
$\mathbf{z_{n1}}$ $\mathbf{z_{n2}}$ $\mathbf{z_{nm}}$ $\mathbf{z_{n(m+1)}}$ $\mathbf{z_{n(t-2)}}$ $\mathbf{z_{nt}}$
Win_j ($\mathbf{Z_n}$ in (8))
Win_{j+1}
Est_j - j^{th} estimation instant
Win_j - j^{th} detection window

Fig. 2. Measurement snapshots over time

The measurements (in vector $\mathbf{z_{nm}}$) are related to the states (in vector $\mathbf{x}$), by the relation

$$\mathbf{z_{nm}} = \mathbf{h}(\mathbf{x_{nm}}) + \mathbf{e_m}. \quad (9)$$

The measurement noise, $\mathbf{e_m} \sim \mathcal{N}(0, \sigma)$ [1]. So, $E(\mathbf{e_m}) = \mathbf{0}$ and $E\big[\mathbf{e_m}(i)\mathbf{e_m}(j)\big] = 0$, where, $E(\cdot)$ is the expectation operator. Measurements related to controlled variables, defined in Proposition 1, i.e., in $\mathbf{z_c}$, are included in the measurement vector $\mathbf{z_{nm}}$. The controlling variables, in $\mathbf{c}$, are always included in the state vector $\mathbf{x_{nm}}$. In certain cases, provision for measurement of controlling variables is available. In such cases, the measured values of controlling variables also become a part of the measurements vector.

Under normal conditions, when there is no cyber-attack, the measurement model of (9) can be re-written as

$$\begin{aligned} \mathbf{z_{nm}} &= \mathbf{h}(\mathbf{x_{nm}}) + \mathbf{e_m}, \\ &= \mathbf{z}_n^{true} + \mathbf{e_m}, \ \forall \ m, \end{aligned} \quad (10)$$

based on principles of state estimation and power system analysis in general [1], [57], [58]. The state vector under normal condition is of the form $\mathbf{x^n}$ in (2).

When the stealthy attack established in Proposition 1 is carried out, we observe

$$\begin{aligned} \mathbf{z_m^b} + E &= [\mathbf{h}(\mathbf{x}_m^{hid}) - \mathbf{h}(\mathbf{x_{nm}})] + \mathbf{h}(\mathbf{x_{nm}}) + \mathbf{e_m}, \\ &= \Delta\mathbf{h_a} + \mathbf{z}_n^{true} + \mathbf{e_m} = \mathbf{z_{am}}. \end{aligned} \quad (11)$$

In (11) and the subsequent analysis, $[\mathbf{h}(\mathbf{x}_m^{hid}) - \mathbf{h}(\mathbf{x_{nm}})]$ is represented using $\Delta\mathbf{h_a}$ for convinience and for the remainder of the paper, $\Delta\mathbf{h_a}(j)$ indicates the j^{th} element of the vector $\Delta\mathbf{h_a}$. The subscript '**a**' in (11) represents quantities under a cyber-attack. The state vector under a stealthy attack, i.e., $\mathbf{x}_m^{\text{hid}}$ in (11), is of the form $\mathbf{x}^{\text{hid}}$ in (5). The measurements affected by the attack are represented by the set $Z^M = \{z(f_1), z(f_2), \cdots, z(f_b)\}$, where, $f_1, f_2, \cdots, f_b$, indicate indices of affected measurements, represented by the set M. So, $\Delta\mathbf{h_a}(j) \neq 0$ if $j \in M$. Similarly, all measurement vectors after the m^{th} snapshot can be written as

$$\mathbf{z_{ai}} = \Delta\mathbf{h_a} + \mathbf{z}_n^{true} + \mathbf{e_i}, \ \forall \ i = (m+1), \cdots, t. \quad (12)$$

B. Covariance Matrix of Measurements - Under Normal Conditions and FCI Attack

The measurements can be treated as random variables, denoted by $\mathbf{z_n}$ under normal conditions, and by $\mathbf{z_a}$ under a FCI attack established in Proposition 1. The covariance matrix for any random variable, $\mathbf{z}$, is

$$\mathbf{C} = E[(\mathbf{z} - E(\mathbf{z}))(\mathbf{z} - E(\mathbf{z}))^T], \tag{13}$$

where, the diagonal entries are

$$\mathbf{C}(ii) = E[(\mathbf{z}(i) - E(\mathbf{z}(i)))^2], \tag{14}$$

and the off-diagonal elements are

$$\mathbf{C}(ik) = E[(\mathbf{z}(i) - E(\mathbf{z}(i)))(\mathbf{z}(k) - E(\mathbf{z}(k)))]. \tag{15}$$

Under normal conditions, the expected value of the measurement vector is

$$E(\mathbf{z_n}) = E(\mathbf{h}(\mathbf{x}) + \mathbf{e}) = \mathbf{z}_n^{true}. \tag{16}$$

Similarly, under a FCI attack, the expected value of measurement vector is

$$\begin{aligned} E(\mathbf{z_a}) &= E(\mathbf{h}(\mathbf{x}) + \mathbf{e} + \Delta\mathbf{h_a}) \\ &= \mathbf{z}_n^{true} + \frac{(t-m+1)}{t}\Delta\mathbf{h_a}. \end{aligned} \tag{17}$$

As discussed in Section IV-A, $\Delta\mathbf{h_a}$ has non-zero entries for certain measurements denoted by the set, Z^M. Hence, we observe that

$$E(\mathbf{z_a}(w)) = \begin{cases} \mathbf{z}_n^{true}(w) + \dfrac{(t-m+1)}{t}\Delta\mathbf{h_a}(w) & \forall\ w \in M \\ \mathbf{z}_n^{true}(w) & \forall\ w \notin M. \end{cases} \tag{18}$$

Under normal conditions, based on (10), (13) and (16), the covariance matrix, $\mathbf{C_n}$, can be written as

$$\mathbf{C_n} = E[\mathbf{e}\mathbf{e}^T]. \tag{19}$$

Based on (9), (14) and (15), we get

$$\mathbf{C_n} = \begin{bmatrix} \sigma_1^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_{n_m}^2 \end{bmatrix}. \tag{20}$$

Thus, based on the aspects discussed above, the covariance matrix is essentially a diagonal matrix with individual variances (of measurement errors) in the diagonal. However, when noise does not follow Gaussian model, $\mathbf{C_n}$ is not perfectly diagonal, which is discussed in detail in Section V-A.

In the case of a FCI attack, the measurement model differs depending on the indices of measurements being affected and also on the snapshot at which the control command manipulation is introduced. We have

$$\mathbf{z_{ak}}(w) - E(\mathbf{z_a}(w)) = A_1\Delta\mathbf{h_a} + \mathbf{e}_w,\ \forall\ k = 1, \cdots, (m-1), \tag{21}$$

where, $A_1 = \dfrac{(m-t-1)}{t}$, and

$$\mathbf{z_{ak}}(w) - E(\mathbf{z_a}(w)) = A_2\Delta\mathbf{h_a} + \mathbf{e}_w,\ \forall\ k = m, \cdots, t, \tag{22}$$

where, $A_2 = 1 + A_1$ and $w \in M$. However, when $w \notin M$, we have

$$\mathbf{z_{ak}}(w) - E(\mathbf{z_a}(w)) = \mathbf{e}_w,\ \forall\ k = 1, \cdots, t. \tag{23}$$

Hence, when $w \in M$, $[\mathbf{z_{ak}}(w) - E(\mathbf{z_a}(w))]$ can either take a value of $(A_2\Delta\mathbf{h_a} + \mathbf{e}_w)$ or $(A_1\Delta\mathbf{h_a} + \mathbf{e}_w)$. So, when $w \in M$, $[\mathbf{z_{ak}}(w) - E(\mathbf{z_a}(w))]$ can be represented by $(D\Delta\mathbf{h_a} + \mathbf{e}_w)$, where, D is a random variable that takes a value of either A_1 or A_2, depending on the snapshot at which the adversary performs the FCI attack. The expected value of D can be obtained as

$$\begin{aligned} E(D) &= A_1\rho_1 + A_2(1-\rho_1) \\ &= 1 - \rho_1 + A_1 = \gamma, \end{aligned} \tag{24}$$

where, $p(D = A_1) = \rho_1$ and $0 < p(D = A_1) < 1$. Similarly,

$$E(D^2) = \rho_1(1-\rho_1) + \gamma^2 = \zeta > 0. \tag{25}$$

Let $\mathbf{C_a}$ be the covariance matrix under an FCI attack. Based on (14), the diagonal elements of the covariance matrix can be written as

$$\mathbf{C_a}(i,i) = \sigma_i^2\ \forall\ i \notin M. \tag{26}$$

However, when $i \in M$, we get

$$\begin{aligned} \mathbf{C_a}(i,i) &= E\big[(\mathbf{e_m}(i) + D\Delta\mathbf{h_a}(i))^2\big] \\ &= \sigma_i^2 + \zeta\Delta\mathbf{h_a}(i)^2. \end{aligned} \tag{27}$$

Similarly, based on (15), the off-diagonal elements of the covariance matrix can be written as

$$\mathbf{C_a}(i,j) = 0, \tag{28}$$

if either i or $j \notin M$. However, if both i and $j \in M$, we get

$$\mathbf{C_a}(i,j) = \zeta\Delta\mathbf{h_a}(i)\Delta\mathbf{h_a}(j). \tag{29}$$

C. Observations Useful for Detection of FCI Attacks

The covariance matrices under both normal conditions ($\mathbf{C_n}$) and FCI attack ($\mathbf{C_a}$) were derived in Section IV-B. Important observations can be made from the deviations of $\mathbf{C_n}$ and $\mathbf{C_a}$ that enable the detection of FCI attacks. These observations are presented as three propositions in this section.

Proposition 2. *The trace of the measurement covariance matrix under a FCI attack is greater than the trace seen under normal conditions (when there is no cyber attack), i.e.,*

$$Tr(\mathbf{C_a}) > Tr(\mathbf{C_n}). \tag{30}$$

In other words, the sum of eigenvalues of the measurement covariance matrix increases under an FCI attack.

Proof. The relation in (30) can be shown easily using (20), (26) and (27). From (20), $Tr(\mathbf{C_n})$ can be written as

$$Tr(\mathbf{C_n}) = \sum_{j=1}^{n_m} \sigma_j^2. \tag{31}$$

Now, from (26) and (27), $Tr(\mathbf{C_a})$ can be written as

$$Tr(\mathbf{C_a}) = \sum_{j=1}^{n_m} \sigma_j^2 + \sum_{j \in M} \zeta\Delta\mathbf{h_a}(j)^2. \tag{32}$$

Thus, from (25), (31) and (32), it can be inferred that

$$Tr(\mathbf{C_a}) > Tr(\mathbf{C_n}).$$

□

Proposition 3. *The absolute values of off-diagonal elements of the covariance matrix given by the indices (i, j) such that $i, j \in M$, increases under a FCI attack. In other words, these off-diagonal elements become non-zero, under a FCI attack.*

Proof. This can easily be inferred from (20), (28) and (29). □

Proposition 4. *Under normal conditions, the eigenspace of the covariance matrix is spanned only by the standard basis vectors. However, under a FCI attack, the eigenspace is spanned by a combination of standard basis vectors, corresponding to true measurements and other vectors (which are not standard basis vectors), corresponding to affected measurements. In other words, $\mathbf{C_n}$ has eigenvectors which are standard basis vectors. However, $\mathbf{C_a}$ has some eigenvectors which are not standard basis vectors having non-zero entries that reflect affected measurements.*

Proof. Let $\lambda^{'}$ be an eigenvalue of a matrix, $\mathbf{A}$. In order to obtain the eigenvector corresponding to $\lambda^{'}$,

$$(\mathbf{A} - \lambda^{'}\mathbf{I})\mathbf{X} = \mathbf{0}, \tag{33}$$

must be solved, where $\mathbf{X}$ is the eigenvector corresponding to $\lambda^{'}$. $\mathbf{X}$ can be found using Gaussian elimination, i.e., by transformation of the augmented matrix, $[\mathbf{A} - \lambda^{'}\mathbf{I} \,|\, \mathbf{0}]$ to row Echelon form, followed by back substitution. However, to prove this observation, estimation of the eigenvectors is not necessary.

It can be seen from (20) that $\mathbf{C_n}$ is a diagonal matrix. Thus, it can be easily inferred that the eigenvalues of $\mathbf{C_n}$ are given as $\lambda_j = \sigma_j^2, \ \forall \ j = 1, \cdots, n_m$. Similarly, the eigenvectors can be estimated using (33) as standard basis vectors of $\mathbb{R}^m$. Hence, eigenvector corresponding to λ_j, i.e., X_j of $\mathbf{C_n}$ can be written as $X_j = e_j$ where, $e_j \in \mathbb{R}^{n_m}$ and $e_j(k) = 1$ if $k = j$, otherwise, $e_j(k) = 0 \ \forall \ k \neq j$.

In the case of $\mathbf{C_a}$, from Proposition 3 and (28) and (29), the matrix is not diagonal. Hence, the eigenvectors of $\mathbf{C_a}$ have a different form when compared to that of $\mathbf{C_n}$. In order to show that eigenvectors corresponding to falsified measurements are not standard basis vectors, the matrix $\mathbf{C_a}$ is rearranged as

$$\mathbf{C_a^r} = \begin{bmatrix} \mathbf{C_a^{\text{true}}} & \mathbf{0}^{a \times b} \\ \mathbf{0}^{b \times a} & \mathbf{C_a^{\text{fal}}} \end{bmatrix}, \tag{34}$$

where,

$$\mathbf{C_a^{\text{fal}}} = \begin{bmatrix} (\sigma_{f_1}^2 + \zeta \Delta \mathbf{h_a}(f_1)^2) & \cdots & \zeta \Delta \mathbf{h_a}(f_1) \Delta \mathbf{h_a}(f_b) \\ \vdots & \ddots & \vdots \\ \zeta \Delta \mathbf{h_a}(f_1) \Delta \mathbf{h_a}(f_b) & \cdots & (\sigma_{f_b}^2 + \zeta \Delta \mathbf{h_a}(f_b)^2) \end{bmatrix},$$

$$\mathbf{C_a^{\text{true}}} = \begin{bmatrix} \sigma_{l_1}^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_{l_a}^2 \end{bmatrix},$$

and $\mathbf{0}^{a \times b}$ is a matrix of size $a \times b$ containing all zeros. The set $\{l_1, \cdots, l_a\}$ contains the indices of measurements which remain unaffected in a FCI attack. Thus, from (34), it can be seen that $\mathbf{C_a^r}$ is a block diagonal matrix. So, the set of eigenvalues and eigenvectors of $\mathbf{C_a^r}$ is the union of those of $\mathbf{C_a^{\text{true}}}$ and $\mathbf{C_a^{\text{fal}}}$.

Similar to $\mathbf{C_n}$, the eigenvalues of $\mathbf{C_a^{\text{true}}}$ are of the form $\lambda_j = \sigma_j^2, \ \forall \ j = l_1, \cdots, l_a$ and the eigenvectors are of the form $X_{l_j} = e_{l_j}$ where, $e_{l_j} \in \mathbb{R}^m$ and $e_{l_j}(k) = 1$ if $k = l_j$, otherwise, $e_{l_j}(k) = 0 \ \forall \ k \neq l_j$.

In order to prove this proposition, it is sufficient to show that the eigenvectors corresponding to $\mathbf{C_a^{\text{fal}}}$ are not standard basis vectors (like that of $\mathbf{C_n}$ and $\mathbf{C_a^{\text{true}}}$).

Let X_{f_j} be an eigenvector for a eigenvalue $\lambda_{f_j} \in \mathbb{R}$ (as these matrices are symmetrical). Let $X_{f_j} = e_{f_j}$, i.e., X_{f_j} is a standard basis vector. Then,

$$\mathbf{C_a^{\text{fal}}} X_{f_j} = \begin{bmatrix} \zeta \Delta \mathbf{h_a}(f_1) \Delta \mathbf{h_a}(f_j) \\ \vdots \\ (\sigma_{f_j}^2 + \zeta \Delta \mathbf{h_a}(f_j)^2) \\ \vdots \\ \zeta \Delta \mathbf{h_a}(f_b) \Delta \mathbf{h_a}(f_j) \end{bmatrix} \neq \lambda_{f_j} e_{f_j}, \tag{35}$$

which results in a contradiction. Thus, the eigenvector X_{f_j} must have non-zero entries at indices other than f_j, eventually reflecting affected measurements (due to a FCI attack). This observation holds good for other eigenvectors of $\mathbf{C_a^{\text{fal}}}$. □

Note that Propositions 2, 3 and 4 can also be formulated similarly for FDI attacks (discussed in Section III-A) and blatant command injection attacks (discussed in Section III-B), using their appropriate attack models. It is worth noting that these propositions are independent of the type of state estimation employed.

It is worth mentioning again that the conditions in Proposition 2, 3 and 4 are *sufficient conditions*. Consider a situation where an adversary injects false data without any consideration of Bad Data Detection (BDD). Such an attack where false data is injected without any consideration of BDD does not qualify as a False Data Injection (FDI) attack [7], [8]. This is because the BDD immediately detects these measurements as anomalous. If the analysis in Section IV is performed with this attack, which is not a FDI attack, it can be analytically shown that the values of quantities in Propositions 2, 3 and 4 increase. However, this attack has no meaning from a practical point of view. Hence, the point of Propositions 2, 3 and 4 is to show that when a FCI attack occurs, we observe an increase in the values of certain quantities when compared to their values seen under normal conditions.

Hypothetically, if an adversary causes all the measurements to change by a constant value, say a, then, we observe that

$$Tr(\mathbf{C_n}) = \sum_{j=1}^{n_m} \sigma_j^2$$

$$Tr(\mathbf{C_a}) = \sum_{j=1}^{n_m} \sigma_j^2 + n_m \zeta a^2.$$

Thus, it can be inferred that $Tr(\mathbf{C_a}) > Tr(\mathbf{C_n})$. The diagonal elements of $\mathbf{C_a}$ are given by

$$\mathbf{C_a}(i, j) = \zeta a^2 \ \ i \neq j.$$

Hence, it can be inferred that Proposition 2 and 3 hold good. Also, following the steps of the proof of Proposition 4 with the above attack model, it can easily be seen that with full $\mathbf{C_a}$ matrix, the statement of Proposition 4 also holds good. Thus, based on the above discussion, it can be concluded that the Propositions 2, 3 and 4 and subsequently, an algorithm based on these propositions can detect such attacks.

V. Proposed Algorithm

Based on the principles discussed and established in Section IV, a simple algorithm can be developed that enables detection of attacks on various types of commands and measurements. Before the formal formulation of the algorithm, it is important to consider some practical implications of the propositions proposed and proven in Section IV-C. First, based on the propositions, the detection indices are defined. Then, an algorithm is formulated to detect the injection of false commands and data.

A. Detection Metrics and Indices

The proposed algorithm incorporates detection metrics directly based on the propositions in Section IV-C. With $\mathbf{C}$ as the computed covariance matrix, the detection involves the following quantities (based on Propositions 2, 3 and 4):

- $Tr(\mathbf{C})$.
- $\mathbf{C}(ij)$, where, $i \neq j$.
- Eigenvectors of $\mathbf{C}$, collected in a matrix, $\mathbf{V}'$.

As defined before in Section IV-A, the variance of the i^{th} measurement error is σ_i^2. The measurement error is thus considered in the range $[-\kappa\sigma_i, \kappa\sigma_i]$ (depending on the confidence interval). In practical system operation, it is necessary to take into account the maximum value of variance possible (or the theoretical limit), to account for non-idealities in measurement noise, as practical measurement noise observed is approximately Gaussian. Based on Popoviciu's inequality [59], the maximum variance possible can be calculated to be $\sigma_i^2|_{max} = \kappa^2\sigma_i^2$. This is taken into account in the development of the algorithm.

In order to describe the algorithm formally, it is necessary to define indices that use the quantities mentioned above. The indices are defined as follows:

$$\beta_{tr} = Tr(\mathbf{C}), \tag{36}$$

$$\beta_{cov} = \sum_{i,j \in \Upsilon} \mathbf{C}(ij), \tag{37}$$

$$\beta_{eig} = \sum_{i,j \in \Psi} \mathbf{V}'(ij) - n_m. \tag{38}$$

Here, the set Υ contains the ordered pair, $\{(i,j) : |\mathbf{C}(i,j)| > \kappa^2\sigma_i^2\}$. Similarly, another set, Υ_d is defined as $\{i : |\mathbf{C}(i,i)| > \kappa^2\sigma_i^2\}$. On the other hand, Ψ contains the ordered pair $\{(i,j) : |\mathbf{V}'(i,j)| \neq 0\}$. It is worth noting that these sets (viz. Υ, Υ_d and Ψ) are direct consequences of Propositions 3 and 4. These indices and their values relative to each other depend on the sensitivities of related electrical parameters (both states and measurements) to the malicious command. These sensitivities generally vary significantly, depending on factors like local topology, present system state, rated values (of power flows) etc.

Finally, the detection metric involves adding the individual indices as

$$\beta = \beta_{tr} + \beta_{cov} + \beta_{eig}. \tag{39}$$

Based on definitions in (36), (37) and (38), when there is no cyber-attack, we can see that the possible values of β_{tr}, β_{cov} and β_{eig} are as follows:

$$\begin{aligned} \beta_{tr} &= \sum_{w=1}^{n_m} \sigma_i^2 \\ &= n_m\sigma^2 \quad , if \;\; \sigma_i = \sigma \;\; \forall \;\; i = 1, \cdots, n_m. \end{aligned}$$

Similarly, $\beta_{cov} = 0$ and $\beta_{eig} = 0$. Hence, from (39),

$$\beta^{id} = n_m\sigma^2, \tag{40}$$

where, superscript, id, is used to denote value of β ideally under normal conditions. When Popoviciu's inequality [59] is invoked, we get the maximum possible value of β as

$$\beta^{p} = n_m\kappa^2\sigma^2, \tag{41}$$

where, superscript, p, is used to denote value of β. A value of β which is appreciably larger than that given by (40) and (41) is indicative of an attack. In other words, an attack is detected if the value of β is found to be higher than a threshold value, Th, as shown in Algorithm 1. The value of Th is tuned as per the system where the detection algorithm is used, such that $Th > \beta^p$. The threshold selection is further discussed in Section VI-A.

B. Detection Algorithm

This algorithm is based on the results of Propositions 2, 3 and 4. The algorithm first computes the measurement covariance matrix, $\mathbf{C}$. Then, the indices β_{tr}, β_{cov} and β_{eig} and detection metric β are computed and the elements of sets Υ, Υ_d and Ψ are determined. A significant increase in the value of β indicates the presence of an attack and the elements of sets Υ, Υ_d and Ψ give information of the affected (FCI attacks) or compromised (FDI attacks) measurements. The steps in the algorithm are presented in Algorithm 1.

VI. Results and Discussion

The proposed algorithm is tested on the IEEE 118-bus system [60]. As stated before in Section IV-A, this algorithm facilitates the detection of both false commands (supervisory control) and data (measurement data). In order to validate the effectiveness of Algorithm 1, attack scenarios are considered where sets of falsely injected commands and data are introduced, and compared with the normal scenario (when there is no cyber-attack). There are three broad categories of attack scenarios considered. They are:

- **Case 1:** Attacks involving only false commands.
- **Case 2:** Attacks involving only false data.
- **Case 3:** Attacks involving both false data and commands.

In order to consider attacks on supervisory control, six transformers are considered, where, three of them are tap changers (OLTCs) and the other three are phase shifters

Algorithm 1: Proposed Generalized Algorithm for detection of FCI and FDI attacks

```
Data: The measurements over $t$ instants, i.e., $\mathbf{Z_n}$ and
      predefined threshold, $Th$
Result: Trig and sets $\Upsilon$, $\Upsilon_d$ and $\Psi$
Compute the covariance matrix, $\mathbf{C}$;
Estimate the eigenvectors of $\mathbf{C}$ and store in matrix $\mathbf{V}'$;
Estimate $\beta_{tr} = Tr(\mathbf{C})$;
Set $\beta_{cov} = 0$ and $\beta_{eig} = 0$;
for $i \leftarrow 1$ to $n_m$ do
    for $j \leftarrow 1$ to $n_m$ do
        if $i \sim= j;$ then
            if $|\mathbf{C}(i,j)| >= \kappa^2\sigma_i^2;$
             then
                Include $(i,j)$ in $\Upsilon$;
                $\beta_{cov} = \beta_{cov} + \mathbf{C}(i,j)$;
            else
                Set $\mathbf{C}(i,j) = 0$;
        if $i == j;$ then
            if $|\mathbf{C}(i,i)| >= \kappa^2\sigma_i^2;$
             then
                Include $i$ in $\Upsilon_d$;
for $i \leftarrow 1$ to $n_m$ do
    for $j \leftarrow 1$ to $n_m$ do
        if $\mathbf{V}'(i,j) \sim= 0;$
         then
            Include $(i,j)$ in $\Psi$;
            $\beta_{eig} = \beta_{eig} + \mathbf{V}'(i,j)$;
Adjust $\beta_{eig} = \beta_{eig} - n_m$;
Calculate $\beta = \beta_{tr} + \beta_{cov} + \beta_{eig}$;
if $\beta > Th$ then
    Trig = 1;
    Attack is detected;
    Analyse $\Upsilon$, $\Upsilon_d$ and $\Psi$ to locate affected/tampered
      measurements and commands;
else
    Trig=0;
    No Attack;
```

TABLE I

LOCATION OF THE OLTCS AND PSTS IN THE IEEE 118-BUS SYSTEM

S.no.	Type[1]	Branch[2]	fb[3]	tb[4]
1	OLTC	36	30	17
2		51	38	37
3		182	114	115
4	PSTs	101	62	67
5		127	81	80
6		148	80	96

[1] Type of transformer
[2] Line or Branch number
[3] From Bus
[4] To Bus

TABLE II

THE SPECIFIED VALUES OF CONTROLLING AND CONTROL VARIABLES.

S.no.	Type[1]	c_1^{sp2}	c_2^{sp3}
1	OLTC	1.025	0.9934
2		1.05	0.9729
3		1.025	0.95
4	PST	0.0233	-0.1619
5		0.0233	-0.2697
6		0.0466	0.3850

[1] Type of transformer
[2] $c_1^{sp} = t_{km}^{sp}$, for OLTCs and $c_1^{sp} = \phi_{km}^{sp}$, for PSTs
[3] $c_2^{sp} = |V_{km}|^{sp}$, for OLTCs and $c_2^{sp} = P_{km}^{sp}$, for PSTs

(PSTs). The OLTC tap ratios are in the range of $[0.9, 1.1]$, and they increment/decrement in steps of 0.025. Similarly, the PSTs operate in the range of $[-32°, +32°]$, in steps of $1.3333°$. The details pertaining to the location of these transformers are given in Table I. On the other hand, in case of attacks involving injection of false data, measurement data is modified such that the voltage estimates of 4 nodes are influenced. The nodes are denoted as a set $Mod = \{5, 48, 102, 117\}$. The true voltages (in pu) of these nodes are given by the set $Tr = \{0.9991, 1.026, 0.9891, 0.9738\}$. Let the state vector containing the true values of voltages in the set Tr be denoted as $\mathbf{x}^{true}$.

In case of transformers, the details pertaining to normal operation, i.e., the values of control variable ($|V_k|$ or P_{km}) and controlling variable (t_{km} or ϕ_{km}) when there is no cyber attack are given in Table II, where all quantities are in per-unit (p.u). To carry out stealthy command injection attacks, a malicious command is injected such that the taps and phase shifts are changed by one setting (i.e., one discrete step, also $|\Delta c| = 0.025$, for OLTCs and $|\Delta c| = 1.333°$, for PSTs), using the principles in [6] and Proposition 1.

In case of FDI attacks, measurement data is falsified to change the voltage estimate of the nodes in Mod from their true value, contained in the set Tr, such that, $\mathbf{x}^{est} = \mathbf{x}^{true} + a \times \Gamma$. Here, $\mathbf{x}^{est}$ is state vector that contains the wrong estimate of voltages in Mod. Γ is a vector containing zeros except for indices of voltages of nodes in set Mod, where the entries of Γ are 1. The FDI attack is carried out using the principles in [8], such that an attack vector given by $h(\mathbf{x}^{est}) - h(\mathbf{x}^{true})$, is added to the measurement vector. The value of a is varied to create different attack scenarios to demonstrate the effectiveness of Algorithm 1 against FDI attacks.

In practical power systems, the measurements are noisy and imperfect. So, a measurement noise (Gaussian) of 1% (σ) for power measurements and 0.3% for voltage measurements [61], [62] is considered. In order to test the effectiveness of the algorithm in the presence of noise, each scenario is run for 100 times.

The attack scenarios as well as normal scenarios are simulated and Algorithm 1 is implemented to test its effectiveness in separating attacks from normal scenarios. The values of β (from (39)) are recorded and tabulated in Table III. In case of normal scenarios, the maximum values of β are recorded, whereas in case of attacks, minimum values of β are recorded, unless otherwise stated. This is to test the performance of the algorithm in the presence of noisy measurements.

TABLE III
THE VALUES OF β RECORDED UNDER NORMAL AND ATTACK SCENARIOS

Case	Attack	β
Normal	$a = 0$ & $\lvert\Delta c\rvert = 0$	0.0579
FCI	$\lvert\Delta c\rvert$-one step	1.4588×10^3
FDI	$a = 1 \times 10^{-4}$*	0.0527
	$a = 0.0012$	16.01
	$a = 0.0023$	197.98
	$a = 0.0034$	464.3750
	$a = 0.0045$	697.6473
	$a = 0.0056$	855.21
	$a = 0.0067$	978.46
	$a = 0.0078$	1.1×10^3
	$a = 0.0089$	1.18×10^3
	$a = 0.01$	1.27×10^3
Both FDI and FCI	$\lvert\Delta c\rvert$-one step & $a = 0.0001$	1.457×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0012$	1.4964×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0023$	1.625×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0034$	1.6956×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0045$	1.814×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0056$	1.868×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0067$	2.00×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0078$	2.11×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.0089$	2.193×10^3
	$\lvert\Delta c\rvert$-one step & $a = 0.01$	2.395×10^3

* The only case where detection is not possible

In Table III, it can be seen that the value of detection metric, β, increases when there is an attack, when compared to the value seen in normal conditions. Based on the values recorded in Table III, the following observations can be made:

- For all attack cases, except when $a = 0.0001$, the minimum values of β in case of attacks are higher than the maximum values of β under normal scenarios.
- The above mentioned observation is more pronounced in cases when falsification of estimates is in the range of values (above $a = 0.0045$) that can practically cause an appreciable impact in the grid.
- It is not possible to detect an attack when $a = 1 \times 10^{-4}$ as the value of β observed is close to that seen in normal operation. However, is not a problem as a state estimate deviation of 1×10^{-4} in all likelihood requires measurement changes that are in the order of noise. Practically, an adversary is likely to introduce attacks that cause significant deviations (from true values). Based on Table III, it is seen that the value of β increases in such cases.
- This algorithm is effective in detecting false command injection attacks in transformers even when the change in tap position is by one step.
- Once an attack is flagged, a close look at the sets Υ, Υ_d and Ψ gives the measurements or controlled variables under attack, which is a direct consequence of Propositions 3 and 4.

It is important to note that the developed method is a unified detection scheme that is capable of detecting FDI and FCI attacks. The effectiveness of the developed method is shown to be effective, both mathematically using Propositions 2, 3 and 4 and through simulations in Table III. This detection method is the first to detect attacks against two types of transmission system controls under an unified framework.

TABLE IV
COMPARISON OF THE PERFORMANCE OF THE PROPOSED METHOD WITH KL DIVERGENCE BASED APPROACH [25] AND GRAPH THEORY BASED APPROACH [27] UNDER FDI ATTACKS

	Proposed[1]	KLD[2]	GT[3]
Successful detection %	90.91	90.45	90.18
False Positives	0	5	0
False Negatives	0	0	8

[1] Proposed Method used only to detect FDI attacks
[2] KL divergence based approach [25]
[3] Graph Theory based approach [27]

TABLE V
ACCURACY OF THE PROPOSED METHOD ACROSS ALL THE CASES

Percentage of cases of successful detection	95.45%
Number of false positives	0
Number of false negatives	100

The proposed detection method is compared to previous FDI attack detection techniques by running the proposed method exclusively against FDI attacks. The proposed method is compared with two existing FDI attack detection algorithms. The first algorithm is based on Kullback–Leibler divergence, in [25]. Here, the distribution of measurement variations during real-time system operation is compared with the distribution of the historical normal operation. The second algorithm is a graph-theory based approach where outliers in measurement variation, i.e., outside $\mu \pm \kappa\sigma$, where, $\kappa > 3$ ($\kappa = 4$, based on discussion in Section V-A). Following the identification of outliers, graph theory based analysis is performed to detect FDI attacks [27]. The performance of the three methods against FDI attacks is presented in Table IV. We note that the proposed method is comparable (marginally superior) to the two existing methods. However, it is worth reiterating that the proposed method is capable of detecting attacks against the active power and voltage control commands in transmission systems. Also, this is the first unified approach to protect transmission system controls against cyber-attacks. Hence, the entire functionality of the proposed method cannot be compared with any existing technique.

A. Threshold Selection

The accuracy of the proposed algorithm for the cases considered is tabulated in Table V. In total, the algorithm was tested across 2200 cases. The algorithm successfully classified attacks in 2100 of 2200 cases. The algorithm fails to recognize an attack for only one scenario ($a = 10^{-4}$), where the attack does not introduce any appreciable impact on the operation of the power system. Hence, for all practical purposes, this algorithm detects false injection of data and commands effectively. Based on the values of β in Table III, it is seen that a threshold, $Th = 10$, seems adequate to facilitate detection. It is interesting to note that this algorithm detects false data injection attack when the change in estimates is as low as 10^{-3} pu. Similarly, this algorithm also detects a false transformer tap and phase shifter commands, even when the change is by one discrete step.

VII. Conclusion

In this paper, a generalized scheme is developed that is capable of detecting both false data and false command injection attacks, even when these attacks are carried out stealthily. Mathematical models of stealthy attacks involving transmission system control command injections are established. Based on these established models, the change in measurement covariance matrix is studied mathematically and three propositions that enable detection of such attacks are proposed and proven. These propositions are used to develop an unified detection algorithm. The detection algorithm is computationally inexpensive and non-iterative. When this algorithm is tested on the IEEE 118-bus system, it is able to detect both false data and commands reliably. It is worth noting that this is the first work that proposes an unified method to detect attacks on both measurement data and supervisory control.

References

[1] A. Abur and A. G. Exposito, *Power System State Estimation Theory and Implementation*, ser. Power Engineering. MARCEL DEKKER, INC., 2004.

[2] C. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

[3] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman, "Challenges in power system information security," *IEEE Security Privacy*, vol. 10, no. 4, pp. 62–70, July-Aug 2012.

[4] M. R. Giuseppe Fusco, *Adaptive Voltage Control in Power Systems*, 2007.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, July 2017.

[6] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov 2020.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[8] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[9] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[10] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, July 2016.

[11] 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 Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, March 2019.

[12] S. Chakrabarty and B. Sikdar, "Detection of malicious command injection attacks on phase shifter control in power systems," *IEEE Transactions on Power Systems*, vol. 36, no. 1, pp. 271–280, Jan 2021.

[13] 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 Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[14] Z. Yu and W. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[15] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system non-linear state estimation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 6–8, Jan 2016.

[16] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sept 2017.

[17] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4775–4786, Sept 2018.

[18] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

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

[20] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, July 2012.

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

[22] 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. 26 022–26 033, Nov 2017.

[23] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, Feb 2017.

[24] 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. 13 787–13 798, July 2017.

[25] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sept 2015.

[26] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, ser. CPS-SPC '16:. ACM, Oct 2016, pp. 81–92.

[27] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system ac state estimation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2465–2475, Apr 2021.

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

[29] R. J. R. Kumar and B. Sikdar, "Efficient detection of false data injection attacks on ac state estimation in smart grids," in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct 2017, pp. 411–415.

[30] 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. 31 762–31 773, Mar 2019.

[31] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2020.

[32] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, ser. MTD '14. New York, NY, USA: Association for Computing Machinery, Nov 2014, p. 59–68. [Online]. Available: https://doi.org/10.1145/2663474.2663482

[33] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 2019.

[34] 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 Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, Feb 2020.

[35] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Mar 2019.

[36] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *2012 45th Hawaii International Conference on System Sciences*, Jan-Feb 2012, pp. 2104–2113.

[37] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "Deepfed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, Aug 2021.

[38] 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 Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.

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

[40] J. Zhao, A. Gómez-Expósito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, A. K. Singh, J. Qi, Z. Huang, and A. P. S. Meliopoulos, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3188–3198, July 2019.

[41] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, Nov 2016.

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

[43] Z. Zhang, S. Huang, Y. Chen, B. Li, and S. Mei, "Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game," *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[44] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1552–1564, Mar 2021.

[45] Z. Zhang, S. Huang, F. Liu, and S. Mei, "Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages," *IEEE Access*, vol. 8, pp. 134 257–134 267, July 2020.

[46] S. M. Dibaji, M. Pirani, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "Secure control of wide-area power systems: Confidentiality and integrity threats," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 7269–7274.

[47] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, Nov 2016.

[48] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, July 2017.

[49] N. Saxena, L. Xiong, V. Chukwuka, and S. Grijalva, "Impact evaluation of malicious control commands in cyber-physical smart grids," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 208–220, Apr-Jun 2021.

[50] L. Beibei, *Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems*, 2019.

[51] NCCIC/ICS-CERT. (2016) Cyber-attack against ukrainian critical infrastructure. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[52] G. Maria, A. Yuen, and J. Findlay, "Control variable adjustment in load flows," *IEEE Transactions on Power Systems*, vol. 3, no. 3, pp. 858–864, 1988.

[53] N. M. Peterson and W. S. Meyer, "Automatic adjustment of transformer and phase-shifter taps in the newton power flow," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-90, no. 1, pp. 103–108, Jan 1971.

[54] B. Stott and O. Alsac, "Fast decoupled load flow," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-93, no. 3, pp. 859–869, May 1974.

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

[56] P. A. Teixeira, S. R. Brammer, W. L. Rutz, W. C. Merritt, and J. L. Salmonsen, "State estimation of voltage and phase-shift transformer tap settings," *IEEE Transactions on Power Systems*, vol. 7, no. 3, pp. 1386–1393, Aug 1992.

[57] R. B. Bobba, J. Dagle, E. Heine, H. Khurana, W. H. Sanders, P. Sauer, and T. Yardley, "Enhancing grid measurements: Wide area measurement systems, naspinet, and security," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 67–73, Jan-Feb 2012.

[58] G. Kusic, *Computer-Aided Power Systems Analysis*, ser. Power Engineering. CRC Press, 2009.

[59] T. Popoviciu, "Sur l'approximation des fonctions convexes d'ordre supérieur," *Mathematica (Cluj)*, vol. 10, pp. 49–54, 1935.

[60] U. of Washington. (1999) Power system test case archive. [Online]. Available: http://www.ee.washington.edu/research/pstca/

[61] Y. Wang, W. Xu, and J. Shen, "Online tracking of transmission-line parameters using scada data," *IEEE Transactions on Power Delivery*, vol. 31, no. 2, pp. 674–682, April 2016.

[62] "IEEE standard for scada and automation systems," *IEEE STD C37.1-2007 (Revision of IEEE STD C37.1-1994)*, pp. 1–143, May 2008.