Detection of Malicious Command Injection Attacks on Phase Shifter Control in Smart Grids

Shantanu Chakrabarty and Biplab Sikdar,

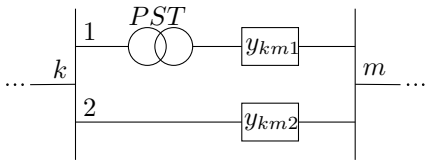
***Abstract*—Phase shifters (or phase shifting transformers) are used in power grids to regulate the flow of real power. They are used to prevent overloading of transmission lines and also to regulate cross-network power flows as per contractual obligations. In a smart/automated grid, these phase shift commands are relayed through SCADA networks. As a result, this control is vulnerable to cyber attacks, especially stealthy ones. Malicious phase shift commands can severely overload critical transmission lines, resulting in their disconnection, and also cause financial losses by disrupting cross-network trading. The protection of this control from cyber attacks, though crucial, has not received any attention in literature. This paper is the first which considers such attacks and proposes a method/algorithm to detect them, including the stealthy ones (which beat bad data detection). The proposed algorithm is based on indices that are ratios of branch or node injection currents to the terminal voltages. The effectiveness of these indices (in the context of detection) is validated mathematically. These indices are used to formulate the proposed algorithm which is found to be reliable, computationally light and easy to implement when tested on phase shifters placed in the IEEE 118-bus system. As the proposed algorithm is based on the principles of power system analysis, it is usable under any network technology.**

***Index Terms*—Cyber attacks, phase shifters, false commands**

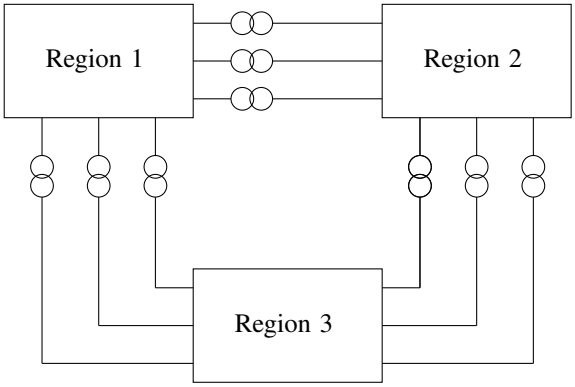
I. Introduction

Phase Shifters, more commonly Phase Shifting Transformers (PSTs), are used in power grids to regulate/control the flow of real power [1], [2], [3]. These devices achieve control of active power flows by adding a phase shift (either leading or lagging) to the phase displacement between the lines, as active power flows are strongly coupled to angles [4]. In the context of smart grids, where the controls of PSTs are automated by means of Remote Terminal Units (RTUs), PST controls are vulnerable to cyber attacks. These vulnerabilities arise due to the fact that RTUs interface PSTs to the command centre by means of a SCADA system, which are in general vulnerable [5], [6].

PSTs are essential for efficient utilization (without causing any overloads) of the transmission system [2], [7] and in maintaining contractual flows in tie-lines [3], [7]. These avenues of application of phase shifters are shown in Figures 1a and 1b. In Figure 1a, the distribution of power in lines 1 and 2 (with similar power carrying capacity) is solely governed by their admittances, y_{km1} and y_{km2}, where $y_{km2} > y_{km1}$. In situations of high demand, line 2 is likely to get overloaded while line 1 remains under-utilized. Hence, a PST is used in such cases to alleviate line 2 from overloading. Any malicious phase shift command can cause a cascaded trip of both lines 1 and 2, disconnecting a part of the system. In Figure 1b, PSTs are used to control the flow of power between the regions so that the power interchanges are as per contracts. In a news article [8], it was reported that New York Independent System Operator (NYISO) discovered that electricity traders used a circuitous (long) route to deliver electricity to states like Pennsylvania and New Jersey, as the route was cheaper. However, the flow of electricity is governed by the Kirchhoff's laws. Thus, the power flow happened through the direct route (across the New York state border) causing unexpected congestion, which eventually raised the price of electricity. To prevent such situations, PSTs are used to regulate the flow of power so that they are close to the contractual flows. However, malicious phase shift commands can be used to cause situations similar to the one in [8], leading to severe financial losses. These attacks can also cause generation-load imbalances in certain areas that rely on power from other areas. There are several other scenarios of applications of PSTs apart from the ones shown in Figures 1a and 1b. Thus, protection of this control against cyber attacks is of critical importance in the context of automated/smart grids. A news



(a) A set of parallel lines with a phase shifter



(b) Interchange Control

Figure 1: Some Examples of application of PSTs

Shantanu Chakrabarty is with Department of Computer Science, 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

article [9] speculates the vulnerability of transformers (PSTs are in general transformers) in general to cyber attacks with special mention of controls like taps.

Existing literature on cyber-attacks on smart grids (reviewed in Section II) considers various forms of attacks, with special emphasis on False Data Injection (FDI) Attacks. However, protection of control mechanisms from cyber attacks has not received adequate attention. The aspects of voltage control is considered in some works [10], [11]. However, they are purely from the perspective of either FDI attacks or in the context of distribution systems, where state estimation and bad data detection are usually not considered. To the best of our knowledge, there is no existing literature that addresses the security of phase shifter control. The current work is an attempt to fill this gap.

In this paper, a detection algorithm is proposed that can detect the presence of anomalous phase shifts (different from the selected values) resulting from cyber attacks. The algorithm is based on a detection parameter which involves four indices based on ratios of branch and injection currents to the terminal voltages. The detection is facilitated by comparison of these individual indices with their reference values calculated at the time of phase shift selection. The algorithm was found to be effective when tested on a set of PSTs placed in a IEEE 118-bus system. Apart from being reliable, this algorithm is both easy to implement and computationally inexpensive. The developed algorithm is based on the principles of power system analysis. Thus, this method is general and not dependent on the technology used in the SCADA networks. It is also worth noting that this is the first effort of its type.

The rest of the paper is organized as follows: Section II presents the literature review. The background on phase shifters, state estimation and stealthy attacks is discussed in Section III. The various possible attack scenarios that any detection technique must handle are discussed in Section IV. The classifier algorithm and its mathematical validity for detection is presented in Section V. The simulation studies are given in Section VI. Finally, conclusions are drawn in Section VII.

II. Literature Review

The existing literature on smart grid SCADA protection is primarily centred around FDI attacks. The vulnerability of existing Bad Data Detection (BDD) scheme is identified in [12], which shows that specific measurements can be tampered to influence the estimates of certain state variables while remaining undetected by the BDD. The attacks which use this vulnerability are referred to as FDI attacks. The work in [12] was essentially for state estimators which use DC power flow model. The existence of the same vulnerability in the context of state estimators with AC power flow model is established in [13]. Additionally, imperfect FDI attack strategies are given in [14].

The identification of the aforementioned vulnerability led to several efforts to mitigate such attacks. The earlier efforts were designed for state estimators which used DC power flow models [15], [16], [17]. However, in most operational systems, state estimators with AC power flow model are in use. There have been several approaches proposed to mitigate FDI attacks using Kalman filtering [18], [19], machine learning [10], [20], [21], adaptive sampling [22], graphical based methods [23] etc. Some proposed approaches are based on the predicted trends from the historical data [24], [10]. In order to make the detection approach general (irrespective of communication and networking technologies), [25] proposes an online detection scheme using load forecasts, generation schedules and synchrophasor data. A non-iterative technique is presented in [26], using bus injections and line flow measurements from SCADA system and voltage measurements from PMUs to facilitate detection by remaining independent of the networking protocol and technology. The effects of FDI attacks on real-time electricity market operation and optimal power flow (OPF) results are studied in [27] and [28], respectively.

In the case of control mechanisms, the existing literature deals with wrong control actions that result from FDI attacks [11], [10]. The attacks involving false commands to the RTUs have not received enough attention. The 2015 Ukraine attack was an example of such attacks where the breakers were operated by an attacker to cause a blackout [29], [30]. The work in [29] outlines certain aspects of the Ukraine attack, but in the purview of FDI attacks.

As far as phase shifter controls are concerned, there is no existing literature that addresses this problem.

III. Background

A. Phase Shifters in Smart Grids

1) Basic Principle: Phase shifters are used in power networks to regulate the flow of real power. These devices achieve the control of real power flow by means of a phase shift (either leading or lagging), which is added to the phase displacement between the sending and receiving ends of a line. Thus, phase shifters manipulate real power flows by manipulating the effective phase displacements between the sending and receiving ends of a line. The most common phase shifter device used in power grids is a phase shifting transformer. However, in recent times, several power electronics based devices are in use. Irrespective of the device in use, the basic principle of application in power grids remains the same.

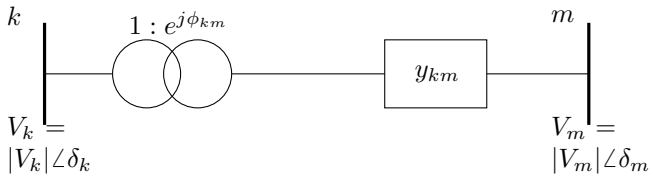


Figure 2: A phase shifter connected between nodes k and m

In Figure 2, a phase shifting transformer is considered with a transformation ratio of $1 : e^{j\phi_{km}}$, where a phase shift, ϕ_{km}, is varied such that the real power flow between nodes k and m is a certain regulated value, P_{km}^{sp} and the phase shift that achieves the regulated real power flow of P_{km}^{sp} is referred to as the selected or scheduled phase shift, denoted by ϕ_{km}^{sp}. Thus, in any phase shifter, the controlling variable is the phase

shift, ϕ_{km}, and the controlled variable is the real power flow between nodes k and m, i.e., P_{km}. So, an operator or EMS monitors these two quantities, i.e., phase shift, ϕ_{km} and real power flow, P_{km}.

B. State Estimation and Bad Data Detection

The power measurements (both line flows and injections) are non-linear functions of state variables [31]. These measurements are modelled as

$$z_k = h_k(\mathbf{x}) + e_k, \ \ \forall \ k = 1, \cdots, m \tag{1}$$

where, z_k is the k^{th} measurement, $h_k(\mathbf{x})$ is the function mapping z_k to the vector of state variables, $\mathbf{x}$, and e_k is the error in k^{th} measurement. The error, e_k, is assumed to follow a Gaussian distribution with zero mean and variance of σ_k^2.

The weighted least square estimation minimizing

$$J(\mathbf{x}) = \frac{1}{2}\sum_{k=1}^{m}\Big[\frac{z_k - h_k(\mathbf{x})}{\sigma_k}\Big]^2, \tag{2}$$

subject to several constraints (both equality and inequality) based on physical laws and operational constraints is used for the estimation of state variables, $\mathbf{x}$. Phase shift angles are included as state variables (in vector $\mathbf{x}$). The phase shift measurements, if available, become a part of the measurement vector z [32].

The first order optimality condition states that

$$\frac{\partial J(\mathbf{x})}{\partial x} = \mathbf{0}. \tag{3}$$

The application of Gauss-Newton method to find the roots of (3) results in the iterative process

$$G(\mathbf{x}^i)\Delta\mathbf{x}^i = H^T R^{-1}(z - h(\mathbf{x})), \tag{4}$$

$$\mathbf{x}^{i+1} = \mathbf{x}^i + \Delta\mathbf{x}^i, \tag{5}$$

where, H is the Jacobian matrix, $G = H^T R^{-1} H$ is the gain matrix and R is a $m \times m$ matrix with σ_k^2 on the k^{th} diagonal.

In the case of state estimation, measurements always outnumber state variables, i.e., there is enough redundancy in measurements. This redundancy in measurements enables the energy management systems (EMS) to detect faulty or infeasible measurements by means of a tool called Bad Data Detector. The most common BDD employs the normalised residual method. In this method, the normalised residual is estimated for all the measurement given by

$$\mathbf{r} = R^{(-0.5)}(\mathbf{z} - h(\mathbf{x})). \tag{6}$$

Then, $||r||_2$ is estimated. A threshold value τ is calculated based on the distribution of errors and the principle of χ^2 testing. If after state estimation, it is found that $||r||_2 > \tau$, then the EMS is notified of the presence of bad data. Thus, for any attack to be successful, it must beat the BDD.

C. Hidden or Stealthy Attacks

1) False Data Injection Attacks: When a data is falsified by an adversary, the estimate of one or more state variables gets affected. If the other measurements which are functions of the affected state variables remain unchanged, then the BDD (discussed in Section III-B) flags the falsified data as bad data [13]. In order to defeat BDD, all the measurements which are functions of the affected variables must be manipulated. Such attacks are called False Data Injection (FDI) Attacks. These attacks are well investigated in the literature.

2) Stealthy Phase Shift Command Injection: In this paper, attacks on phase shift controls are considered. It is well-known that an attack on supervisory control can have a devastating impact [6]. In the context of PST control, some of the impacts have been discussed in Section I, using illustrations in Figures 1a and 1b. A stealthy attack on the supervisory control of PSTs is not same as FDI attacks, discussed in Section III-C1. For an attack on PST control to remain stealthy, it has to beat both BDD and the operator or EMS (that monitors phase shift and real power flow, as discussed in Section III-A1). In other words, an adversary that introduces malicious PST setting change command must ensure that the measured and estimated values of the controlled and controlling variables, i.e., ϕ_{km} and P_{km} appear to be the values selected by the EMS, i.e., ϕ_{km}^{sp} and P_{km}^{sp}. Otherwise, the operator or EMS would investigate the causes for such obvious discrepancy. Thus, in case of attacks on PST controls (or in any control commands), the adversary firstly takes over the PST controls and then manipulates the measurements to hide the effect of the malicious control signals introduced. The attack scenarios that achieve this of beating both the operator's monitoring and BDD are discussed in detail in Section IV.

IV. Attack Scenarios

The attack on phase shift control can lead to adverse effects in power grid operation, as explained in Section I. An adversary could launch an attack on the phase shift controls by gaining access to the RTUs. This unauthorised change in phase shift can cause abrupt changes in the controlled quantities like line power flows or tie line flows. However, these changes get reflected in the measurements and estimates (from the state estimator). Thus, the attack is easily detected and isolated if the operator keeps note of the desired values of phase shifts and flows. Hence, for an attack to have a significant effect, it must be stealthy or hidden [13]. It is worth considering such attacks for the completeness of the detection scheme.

Before considering the attack scenarios, it is important to consider the equivalent π-network representation [1], as shown in Figure 3, of a phase shifter (e.g., the one in Figure 2). The equivalent admittances in the π-network are as follows:

$$Y_{km} = e^{-j\phi_{km}} y_{km} \tag{7}$$

$$Y_{mk} = e^{j\phi_{km}} y_{km} \tag{8}$$

$$Y_{kk} = (1 - e^{-j\phi_{km}}) y_{km} \tag{9}$$

$$Y_{mm} = (1 - e^{j\phi_{km}}) y_{km} \tag{10}$$

where, $y_{km} (= g_{km} + jb_{km} = |y_{km}|\angle\theta_{km})$ is the admittance of the phase shifter.

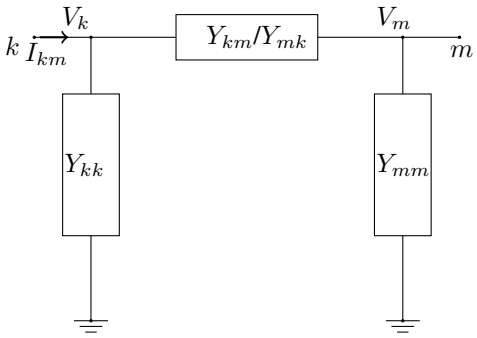


Figure 3: Equivalent π-network representation of a phase shifter

For a stealthy attack, the measured and estimated values of phase shift and its related controlled quantity, i.e., P_{km} must appear close to the values selected by the EMS. To achieve this, certain measurements must be strategically modified [13]. There are two possible cases of such attacks. They are described below.

A. When only the Manipulation of Phase Shift is Hidden

In order to hide a malicious change in phase shift, ϕ_{km}, all the measurements which are directly related to ϕ_{km} must be manipulated [13] such that the measured and estimated values of ϕ_{km} are close to the selected value, ϕ_{km}^{sp}.

The apparent power flows between nodes k and m in Figure 3 can be written as

$$\begin{aligned} S_{km}^{*} &= |V_k|^2 y_{km} - |V_k||V_m||y_{km}|e^{j(\delta_m - \delta_k - \phi_{km} + \theta_{km})} \\ &= P_{km} - jQ_{km}, \end{aligned} \tag{11}$$

$$\begin{aligned} S_{mk}^{*} &= |V_m|^2 y_{km} - |V_k||V_m||y_{km}|e^{j(\delta_k - \delta_m + \phi_{km} + \theta_{km})} \\ &= P_{mk} - jQ_{mk}. \end{aligned} \tag{12}$$

Thus, measurements of P_{km}, Q_{km}, P_{mk} and Q_{mk} must be manipulated.

Similarly, the apparent power injections at nodes k and m are

$$S_k = S_k^{'} + S_{km}, \tag{13}$$

$$S_m = S_m^{'} + S_{mk}. \tag{14}$$

where, $S_k^{'}$ is the sum of flows in all the lines incident at node k, except S_{km}. Similarly, $S_m^{'}$ is the sum of flows in all the lines incident at node m, except S_{mk}. Thus, from (13) and (14), it can be seen that the injection measurements at nodes k and m (both real and reactive) must be manipulated to hide the malicious phase shift command.

This attack makes sense when a phase shifter is one of several controls used to meet an objective of an optimal power flow (OPF) [33], [34] that are most often not directly measurable using on-field measurement devices.

B. When Manipulation of Phase Shift and Change in the Controlled Quantity are Hidden

The attack described in Section IV-A fails to remain stealthy when the controlled quantity is measurable directly. These are situations where the real power flow of a line or a group of lines is regulated to divert power flows from overloaded corridors (e.g., Figure 1a) or when a set of phase shifters are used to regulate tie-line flows as per contractual obligations (e.g, Figure 1b). In such situations, in addition to manipulation of phase shift, ϕ_{km}, the measurements pertaining to the controlled quantity, i.e., real power flow, P_{km} between nodes k and m in Figures 2 and 3 must match the scheduled value P_{km}^{sp}. However, the manipulation of measurement of P_{km} alone does not ensure a hidden attack. This is because the difference in measured value of P_{km} and the value calculated using the state estimates would be significant, triggering the BDD. This happens because of several redundant measurements.

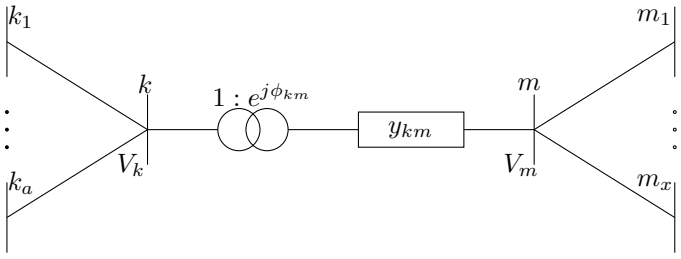


Figure 4: A Phase Shifter with other nodes in its vicinity

In order to carry out such hidden attacks, apart from ϕ_{km}, another state variable must be manipulated such that the measured and estimated values of P_{km} and ϕ_{km} remain close to the scheduled values. The real power flow from node k to m in Figures 2 and 3 can be written as

$$P_{km} = |V_k|^2 g_{km} - |V_k||V_m||y_{km}|cos(\delta_k - \delta_m + \phi_{km} - \theta_{km}). \tag{15}$$

It is well known that P_{km} is strongly coupled to δ_k, δ_m and ϕ_{km} as active power is strongly coupled to angles [4]. Thus, either δ_k or δ_m can be manipulated to achieve this goal. When δ_k is chosen, we get

$$P_{km}^{sp} = |V_k|^2 g_{km} - |V_k||V_m||y_{km}|cos(\delta_k^{mod} - \delta_m + \phi_{km}^{sp} - \theta_{km}) \tag{16}$$

where δ_k^{mod} is the required manipulated value of δ_k to ensure that the attack is hidden. δ_k^{mod} can be found by solving (16). Note that (16) has to be solved to obtain δ_k^{mod} because P_{km} is the controlled variable (as PSTs are used to control line real power flows). These values of ϕ_{km}^{sp} and δ_k^{mod} ensure that the variables being monitored (i.e., P_{km} and ϕ_{km}) show the selected values (i.e., P_{km}^{sp} and ϕ_{km}^{sp}) to the operator.

Now, similar to (15), the real power flow between node k and any other node k_l, $1 \leq l \leq a$, connected to k (except m) in Figure 4, can be written as

$$P_{kk_l} = |V_k|^2 g_{km} - |V_k||V_{k_l}||y_{km}|cos(\delta_k - \delta_{k_l} - \theta_{kk_l}) \quad \forall\ l = 1, \cdots, a. \tag{17}$$

In order to beat the BDD, all the measurements which are a function of δ_k and ϕ_{km} must also be modified (based on the

values ϕ_{km}^{sp} and δ_k^{mod}) [13]. Since the flows between k and nodes $k_1, \cdots, k_a$ are only a function of δ_k (among δ_k and ϕ_{km}), their modified version would be as follows:

$$P_{kk_l}^h = |V_k|^2 g_{km} - |V_k||V_{k_l}||y_{km}|cos(\delta_k^{mod} - \delta_{k_l} - \theta_{kk_l}) \quad \forall\ l = 1, \cdots, a \quad (18)$$

where $P_{kk_l}^h$ correspond to the modified measurements that are used/requied by the adversary to ensure a stealthy attack. Based on (16) and (18), it can be seen that the line power flows are consistent with the laws of the system (laws of energy and charge balance). The power flow meters (after the execution of the stealthy attack) would only show values P_{km}^{sp} and $P_{kk_l}^h$. Thus, there would not be any discrepancy either at the BDD or in the view of the operator. As injections are basically summation of these line flows, similar arguments hold good in their case.

Thus, an adversary proceeds as follows to achieve stealthiness in its attack. First, (16) is solved to find the required modification of δ_k (i.e., δ_k^{mod}) for a given selected pair of P_{km}^{sp} and ϕ_{km}^{sp}. Then, measurements (of other line flows) dependent on δ_k are modified (using δ_k^{mod} in (18)) to ensure that they are consistent and beat the BDD. Bus or node injection measurements (if any) are then modified (using ϕ_{km}^{sp} and δ_k^{mod}). Similarly, δ_m may also be chosen to be modified in (16) (as δ_m^{mod}) by the adversary to achieve the same objective.

Thus, in addition to measurements mentioned in Section IV-A, which are functions of phase shift, ϕ_{km}, additional measurements which are a function of δ_k must be manipulated. These measurements are the flows between node k and other nodes connected to k apart from m, i.e., nodes $k_1, \cdots, k_a$ in Figure 4. Additionally, the injection measurements at nodes $k_1, \cdots, k_a$ must be manipulated. In a practical power system, the number of nodes incident at a node are few, usually $2-4$.

The principles used to hide a false phase shift change command is the same as an usual FDI attack, as they both have to beat the same state estimator and BDD. Thus, the effort required to hide any false command injection is the same as FDI attacks.

V. Proposed Detection Algorithm

A. Development of the Classifier

The apparent power flow from node k to m in Figure 3, S_{km}, can be expressed as

$$S_{km}^* = V_k^* I_{km}. \quad (19)$$

Multiplying (19) with V_k and rearranging, we get

$$\frac{I_{km}}{V_k} = \frac{S_{km}^*}{|V_k|^2}. \quad (20)$$

Similarly, when the apparent power flow from m to k is considered, we get

$$\frac{I_{mk}}{V_m} = \frac{S_{mk}^*}{|V_m|^2}. \quad (21)$$

Let the quantities in (20) and (21) be denoted by CL_{km} and CL_{mk}, respectively.

When the injections at nodes k and m are considered for similar mathematical treatment, we get

$$CL_k = \frac{I_k}{V_k} = \frac{S_k^*}{|V_k|^2}, \quad (22)$$

$$CL_m = \frac{I_m}{V_m} = \frac{S_m^*}{|V_m|^2}. \quad (23)$$

The values of quantities in (20)-(23) obtained during the phase shift selection process are stored as reference values. Subsequently, during state estimation, these quantities are estimated and compared with stored reference values. Any significant deviations observed are indicative of a false phase shift injection. The use of these quantities for detection is validated by means of Theorem 1.

Theorem 1. *Let CL_{km}^{ref} be the estimated value of CL_{km} during the selection of phase shift, ϕ_{km}^{sp}, to maintain the real power flow from node k to m at P_{km}^{sp}. During a hidden false phase shift command injection, let the estimated value of CL_{km} be CL_{km}^h. Then, for a power system operation with perfectly noiseless measurements, the following relation holds:*

$$\left| |CL_{km}^h| - |CL_{km}^{ref}| \right| > 0.$$

Proof. The measurements relevant to CL_{km} are the active and reactive power flows from nodes k to m, based on (11) and (20). Let these measurements be represented as a measurement vector

$$M(T) = \begin{bmatrix} M_1(T) \\ M_2(T) \end{bmatrix} = \begin{bmatrix} P_{km}(T) \\ Q_{km}(T) \end{bmatrix}, \quad (24)$$

where, $T = \{\phi_{km}, \delta_k, |V_k|, |V_m|, \delta_m\}$, i.e., T is the set of state variables that affect the measurements pertaining to P_{km} and Q_{km}. This set T has two subsets $X_1 = \{\phi_{km}, \delta_k\}$ and $X_2 = \{|V_k|, |V_m|, \delta_m\}$. The elements of set X_1 are modified by the adversary to hide the attack, as discussed in Section IV-B. On the other hand, the elements of set X_2 are not influenced by the adversary.

During normal operation, when there is no attack, the set of state variables, T, can be represented by adding a superscript n to it, i.e., $T^n = \{X_1^n, X_2^n\} = \{\phi_{km}^n, \delta_k^n, |V_k|^n, |V_m|^n, \delta_m^n\}$. Based on (11), we can write

$$\frac{S_{km}^*(T^n)}{(|V_k|^n)^2} = y_{km} - \left(\frac{|V_m|^n}{|V_k|^n}\right)|y_{km}|e^{j(\delta_m^n - \delta_k^n - \phi_{km}^n + \theta_{km})}. \quad (25)$$

Based on the definition in (20) and the fact that there is no noise in measurements, we can express (25) as

$$CL_{km}^{ref} = y_{km} - \left(\frac{|V_m|^n}{|V_k|^n}\right)|y_{km}|e^{j(\delta_m^n - \delta_k^n - \phi_{km}^n + \theta_{km})}. \quad (26)$$

The absolute value of CL_{km}^{ref} can be expressed as

$$|CL_{km}^{ref}| = \sqrt{CL_a(T^n) + CL_b(T^n)} \quad (27)$$

where,

$$CL_a(T^n) = |y_{km}|^2 \quad (28)$$

$$CL_b(T^n) = |y_{km}|^2 \left(\frac{|V_m|^n}{|V_k|^n}\right)^2 - 2|y_{km}| \left(\frac{|V_m|^n}{|V_k|^n}\right) (g_{km} cos(\delta_m^n - \delta_k^n - \phi_{km}^n + \theta_{km}) + b_{km} sin(\delta_m^n - \delta_k^n - \phi_{km}^n + \theta_{km})). \quad (29)$$

When a false phase shift injection attack is carried out by the adversary, all the state variables including the phase shift, ϕ_{km}, change. Let this set of state variables be denoted by $T^a = \{X_1^a, X_2^a\} = \{\phi_{km}^a, \delta_k^a, |V_k|^a, |V_m|^a, \delta_m^a\}$. This results in the measurement vector

$$M(T^a) = \begin{bmatrix} M_1(T^a) \\ M_2(T^a) \end{bmatrix} = \begin{bmatrix} P_{km}(T^a) \\ Q_{km}(T^a) \end{bmatrix}. \quad (30)$$

For this attack to remain a hidden one, the measured and estimated values of phase shift, ϕ_{km}, and real power flow, P_{km}, must remain close to the selected values. If a subscript, h, is used to denote the state vector corresponding to a hidden attack, then $\phi_{km}^h = \phi_{km}^n$. The state variable δ_k is modified for the relation in (16) to hold good, i.e., $\delta_k^h = \delta_k^{mod}$. The elements of subset X_2 remain unchanged, i.e., modifying their values makes the attack impractical as a large set of meters have to be tampered. Thus, $X_2^h = X_2^a$. Thus, we get $T^h = \{X_1^h, X_2^h\} = \{\phi_{km}^n, \delta_k^{mod}, X_2^a\}$.

For a hidden attack, the quantity $(M(T^h) - M(T^a))$ must be added to (30), resulting in the measurement vector $M(T^h)$. Following the steps in (25) and (26), the absolute value of CL_{km}^h can be expressed as

$$CL_{km}^h = \sqrt{CL_a(T^h) + CL_b(T^h)} \quad (31)$$

where, $CL_a(T^h) = CL_a(T^n)$ and

$$CL_b(T^h) = |y_{km}|^2 \left(\frac{|V_m|^a}{|V_k|^a}\right)^2 - 2|y_{km}| \left(\frac{|V_m|^a}{|V_k|^a}\right) (g_{km} cos(\delta_m^a - \delta_k^{mod} - \phi_{km}^n + \theta_{km}) + b_{km} sin(\delta_m^a - \delta_k^{mod} - \phi_{km}^n + \theta_{km})). \quad (32)$$

Comparing $CL_b(T^n)$ and $CL_b(T^h)$ in (29) and (32), the following observations can be made

- $\frac{|V_m|^a}{|V_k|^a} \neq \frac{|V_m|^n}{|V_k|^n}$.
- $(\delta_m^n - \delta_k^n) \neq (\delta_m^a - \delta_k^{mod})$.

Thus, it can be stated that

$$\begin{aligned} & CL_b(T^h) \neq CL_b(T^n) \\ \implies \quad & |CL_{km}^h| \neq |CL_{km}^n| \\ \implies \quad & \left| |CL_{km}^h| - |CL_{km}^{ref}| \right| > 0. \end{aligned}$$

Hence proved. □

Similarly, the proposition in Theorem 1 can be proven for CL_{mk}, CL_k and CL_m.

B. Discussions on Some Practical Aspects

In a practical power system operation, the measurements are noisy. Let CL_{km}^n be the estimated value of CL_{km} under normal conditions (no attack), with noisy measurements. In the absence of noise, it is clear that $CL_{km}^n = CL_{km}^{ref}$. In the presence of noise, $CL_{km}^n \approx CL_{km}^{ref}$, i.e., they are not exactly equal. Based on the proof of Theorem 1, it is clear to see that $\left| |CL_{km}^h| - |CL_{km}^{ref}| \right| > \left| |CL_{km}^n| - |CL_{km}^{ref}| \right|$, as variations in state estimation due to measurement noise is negligible when compared to changes forced due to a cyber attack on phase shift control.

The main idea of Theorem 1 can also be visualised using analysis of the equivalent circuit of a phase shifter in Figure 3. The current flowing from node k to m, I_{km}, can be expressed as

$$I_{km} = Y_{kk} V_k + Y_{km}(V_k - V_m). \quad (33)$$

Using (7) to (10) and the definition in (20), (33) can be expressed as

$$CL_{km} = \frac{I_{km}}{V_k} = y_{km} - y_{km}\left(\frac{V_m}{V_k}\right) e^{-j\phi_{km}}. \quad (34)$$

From (34), it can be seen that CL_{km} is a function of phase shift, ϕ_{km}, and voltages, V_k ($= |V_k| \angle \delta_k$) and V_m ($= |V_m| \angle \delta_m$). In order to carry out a hidden attack, the adversary has to ensure that the estimate of ϕ_{km} remains close to the specified/selected value of ϕ_{km}^{sp}. Also, the measurement and estimate of δ_k is modified to ensure that the measurement and calculated values of P_{km} reads P_{km}^{sp}. The measurements and estimates of the remaining state variables would show the values resulting from the attack. It is worth noting that it is impractical for an adversary to influence all the state variables as the number of measurements to tamper becomes very large. Also, the use of indices CL_k and CL_m which are based on bus injections, involve voltages of all the nodes connected to k and m. This ensures that an attack, though hidden, gets noticed by the detection scheme. As far as non-stealthy attacks are concerned, they can be easily detected.

Another important consideration is to determine whether it is possible to bypass the detection classifiers, CL_{km}, CL_{mk}, CL_k and CL_m. It was shown in Section IV that for an attack to be stealthy, measurements which are a function of ϕ_{km} and δ_k must be modified. In order to beat the developed detection classifiers, an adversary has to modify all measurements which are functions of state variables (both $|V|$s and δs) of nodes $k, k_1, \cdots, k_a$, $m, m_1, \cdots, m_x$ and phase shift, ϕ_{km}, for each phase shifter. Thus, a large number of correlated measurements have to be modified. This would require an adversary to have real time information of the entire system (or at-least, a large part of the system) or a control of the entire control centre. Both these scenarios are highly unlikely in practice [6], [12].

C. Formulation of the Classifier used in Detection Algorithm

The proposed algorithm is based on the comparison of absolute values of CL_{km}, CL_{mk}, CL_k and CL_m with their respective reference values, calculated during the phase shifter setting selection. Let the reference values of CL_{km}, CL_{mk}, CL_k and CL_m be CL_{km}^{ref}, CL_{mk}^{ref}, CL_k^{ref} and CL_m^{ref}, respectively.

Let the difference in the absolute values of CL_{km} and CL_{km}^{ref} be represented as

$$CL_1 = \left| |CL_{km}| - |CL_{km}^{ref}| \right|. \quad (35)$$

Similarly, corresponding to other three indices, we get

$$CL_2 = \Big||CL_{mk}| - |CL_{mk}^{ref}|\Big|, \tag{36}$$

$$CL_3 = \Big||CL_{k}| - |CL_{k}^{ref}|\Big|, \tag{37}$$

$$CL_4 = \Big||CL_{m}| - |CL_{m}^{ref}|\Big|. \tag{38}$$

The classifier used for detection is obtained by addition of (35) to (38), resulting in

$$\begin{aligned} CL = &\Big||CL_{km}| - |CL_{km}^{ref}|\Big| + \Big||CL_{mk}| - |CL_{mk}^{ref}|\Big| \\ &+ \Big||CL_{k}| - |CL_{k}^{ref}|\Big| + \Big||CL_{m}| - |CL_{m}^{ref}|\Big|. \end{aligned} \tag{39}$$

The classifier defined in (39) is computationally less intensive and it is very easy to implement by addition of a few lines of code. The detection algorithm using this index is presented in Section V-D.

Algorithm 1: Proposed False Phase Shift Command Injection Attack Detector

Data: Reference values CL_{km}^{ref}, CL_{mk}^{ref}, CL_{k}^{ref} and CL_{m}^{ref} and the predetermined Threshold Th
Output: Trigger

```
Calculate CL using (39);
if CL > Th then
    Trigger = 1;
    Unauthorized phase shift command is detected;
else
    Trigger = 0;
    go back to step 1;
```

D. Algorithm

The steps involved in the proposed algorithm are shown in Algorithm 1. This algorithm is essentially based on comparison of the classifier, CL, defined in (39) with a predetermined threshold, Th. Any value of CL greater than Th is indicative of an attack on the phase shift control. The selection of this threshold is discussed in Section VI-A.

VI. Simulation Results and Discussions

In order to study the effectiveness of the developed algorithm, it is tested on the IEEE 118-bus system [35]. In the test system (i.e., IEEE 118-bus system), seven phase shifters (i.e., phase shifting transformers) are placed. The details pertaining to the location of these phase shifters are given in Table I. The phase shifters are placed such that there is a scope to divert or control the flow of power (both generation and load) over the usual operation range of PSTs. In other words, their locations are chosen such that the operators may control or divert flows to choose the share of power flows through various corridors (to meet certain demand or to wheel a certain generated power). It is well-known that PSTs operate within a designed range, in discrete steps. In the case of PSTs considered (in Table I), each PST operates in the range, $[-32°, +32°]$, in steps of $1.3333°$.

PS number	Line[1]	fb[2]	tb[3]
1	16	11	13
2	52	37	39
3	71	49	51
4	101	62	67
5	127	81	80
6	148	80	96
7	185	75	118

[1] Line or Branch number
[2] From Bus
[3] To Bus

Table I: Location of the Phase Shifters in the IEEE 118-bus system

PS number	P_{km}^{sp} [1]	ϕ_{km}^{sp} [2]
1	0.4042	0.0233
2	0.4802	-0.0233
3	0.8042	0.0466
4	-0.1538	0.0233
5	-0.2249	0.0233
6	0.3867	0.0466
7	0.2521	-0.0466

[1] Scheduled Real Power Flow
[2] Selected Phase Shift [1]

Table II: The specified power flows and the phase shifts to achieve these flows

As mentioned in Section II, PST settings are chosen to meet a set of desired flows across lines. To demonstrate the effectiveness of the proposed algorithm in attack scenarios, it is essential to first establish the normal operating conditions. The desired power flows and the phase shifts selected [1] to meet these flows are given in Table II. These are the values selected by the operator or the EMS to achieve the above mentioned objectives. Thus, for a stealthy attack, the adversary must tamper with the measurements such that the measured and estimated values of ϕ_{km} and P_{km} read close to the ones given in Table II, using the principles discussed in Section IV.

There are four broad scenarios that have been considered to test the performance of the proposed detection algorithm. They are as listed follows:

- **Case 1:** Normal operating condition when there is no attack.
- **Case 2:** When the PST tap is manipulated by two or more steps, i.e., the phase shift is manipulated by more than $2.6666°$.
- **Case 3:** When the phase shift is manipulated by one step, i.e., by $1.3333°$.
- **Case 4:** When the phase shift is manipulated by one step, i.e., by $1.3333°$ and:
  - **Case 4a:** The load is increased by 10%.
  - **Case 4b:** The load is decreased by 10%.

The scenario considered in Case 1 is used to establish the normal operation, in order to facilitate comparison with the attack scenarios. In the scenario of Case 2, a stealthy attack is considered where the adversary manipulates the phase shift by $2.6666°$ or more, which is a practically probable scenario. This is because an adversary is more likely to launch an attack that significantly deviates from the normal operation. The scenario in Case 3 considers cases where the phase shift is manipulated

PST number	Mean	Minimum	Maximum	Standard Deviation
1	0.0220	0.0017	0.0795	0.0153
2	0.0254	0.0043	0.0673	0.0126
3	0.0254	0.0017	0.0766	0.0160
4	0.0192	0.0029	0.0506	0.0103
5	0.0216	0.0037	0.0537	0.0104
6	0.0131	0.0011	0.0442	0.0066
7	0.0245	0.0039	0.0626	0.0129

Table III: Mean, minimum, maximum and standard deviation of CL in Case 1

PST number	Mean	Minimum	Maximum	Standard Deviation
1	1.5775	1.5563	1.6252	0.0121
2	4.5683	4.5390	4.6085	0.0134
3	1.7852	1.7459	1.8292	0.0136
4	1.2840	1.2566	1.3276	0.0140
5	2.8413	2.8112	2.8859	0.0145
6	0.8398	0.8219	0.8663	0.0081
7	1.6753	1.6515	1.7383	0.0142

Table IV: Mean, minimum, maximum and standard deviation of CL in Case 2

PST number	Mean	Minimum	Maximum	Standard Deviation
1	0.2000	0.1821	0.2411	0.0120
2	2.3741	2.3458	2.4095	0.0120
3	0.2471	0.2153	0.2927	0.0139
4	0.5290	0.5011	0.5615	0.0118
5	1.0700	1.0237	1.1125	0.0165
6	0.4803	0.4591	0.5062	0.0081
7	0.2143	0.1842	0.2633	0.0164

Table V: Mean, minimum, maximum and standard deviation of CL in Case 3

PST number	Mean	Minimum	Maximum	Standard Deviation
1	0.2280	0.1915	0.2821	0.0188
2	2.3384	2.3170	2.3723	0.0116
3	0.8731	0.8471	0.9353	0.0155
4	0.5241	0.4931	0.5509	0.0115
5	2.7888	2.7532	2.8257	0.0139
6	1.3015	1.2759	1.3243	0.0086
7	0.1920	0.1598	0.2456	0.0189

Table VI: Mean, minimum, maximum and standard deviation of CL in Case 4a

by just one step, i.e., by $1.3333°$. This is not a likely attack scenario (as an adversary is more likely to be interested in forcing significant consequences). However, Case 3 is included to test the effectiveness of the proposed algorithm under small (and thus harder to detect) malicious changes in PST settings. To study the performance of the detection algorithm under a load change, Case 4 is considered. There are two sub-cases for Case 4. In Case 4a, the malicious phase shift is by one step and the load increases by 10%. Similarly, in Case 4b, the load decreases by 10%. Thus, Cases 3 and 4 are basically studied to test the performance of the proposed algorithm in presence of small (as small as one step) malicious changes of PST settings (from the selected values), though Case 2 and attacks more severe than Case 2 are likely scenarios of attack. It is important to note that irrespective of the application of PSTs, the attack scenarios would manifest similar to Cases 2, 3 and 4 (w.r.t. a malicious change in PST setting).

In a practical grid operating environment, the measurements are noisy. The measurement noise is taken as 1% for power measurements and 0.3% for voltage measurements [36], [37]. Hence, in order to evaluate the effectiveness of the proposed algorithm in the presence of noise, the cases 1, 2, 3, 4a and 4b are run for 200 times. The important statistical parameters, viz., mean, minimum, maximum and standard deviation are noted over these 200 runs. So, the total number of cases considered are as follows:

- *Normal Scenario:* This scenario is considered only in Case 1. So, there are 7 PSTs and 200 runs of the algorithm. Thus, the total number of cases is 1400.
- *Attack Scenarios:* These scenarios are considered in Cases 2, 3, 4a and 4b. So, the total number of cases is $4 \times 7 \times 200 = 5600$.

Under normal conditions (Case 1), the statistical parameters of CL are tabulated in Table III. Ideally, these values should be zero. However, due to the presence of noise, the values obtained from the simulations are non-zero. Similarly, for Case 2, the statistical parameters of CL are tabulated in Table IV. It can be easily seen that the values of CL increase significantly. We note that even the *minimum values of CL in Case 2* are significantly higher than the *maximum values of CL seen in Case 1*. Thus, presence of the attack can be easily detected by Algorithm 1. The statistical parameters of CL for Case 3 are tabulated in Table V. Similar to Case 2, even in Case 3, the minimum values of CL are higher than the maximum values of CL seen in Case 1. Thus, detection is possible even when the malicious change in PST setting is only one step.

Case 4 is studied to test the performance of the algorithm under a load change. The statistical parameters of CL are tabulated in Tables VI and VII for Cases 4a and 4b, respectively. From the comparison of values of CL observed in Tables VI, VII and III, it is clear that the differences in the CL values facilitate detection (based on Algorithm 1). A control decision in an operational power system is made based on the present state (and generation-load pattern) of the system. When the load (or system state) changes normally (when there is no attack), in order to meet the control requirements, i.e., the desired flows across lines where PSTs are placed, the phase shift is updated by the EMS through RTUs (as the past control decision cannot achieve the desired flow). When an adversary manipulates the phase shift, he/she can only fool the EMS into seeing its last selected value. This is because it is not possible for the adversary to keep up with the load changes, i.e., the adversary will not know the changed value of the load since it is random and the exact value of load change is unpredictable. Thus, under load changes, an adversary can only resort to using the last selected values of the PST settings (which are not valid any more). The detection metric facilitates detection even under these conditions (as can be inferred from proposition and proof of Theorem 1). Thus, even in the situations of load change, the detection algorithm works effectively, which is an advantage.

The observations made so far can be summarized as follows:

- The minimum values of CL observed under all attacks (from Tables IV to VII) are greater than the maximum value of CL observed under normal conditions, when there is no attack (from Table III).

PST number	Mean	Minimum	Maximum	Standard Deviation
1	0.2035	0.1747	0.2673	0.0186
2	2.4215	2.3938	2.4690	0.0126
3	0.1618	0.1445	0.2028	0.0090
4	0.5089	0.4817	0.5494	0.0138
5	2.6072	2.5691	2.6483	0.0158
6	1.6433	1.6252	1.6655	0.0080
7	0.3945	0.3622	0.4421	0.0141

Table VII: Mean, minimum, maximum and standard deviation of CL in Case 4b

- The increase in the values of CL is very large when the manipulation of phase shift is as low as $2.6666°$. The aim of any adversary would be to cause a significant manipulation of phase shift, which is thus easily detected by the proposed algorithm.
- For all practical purposes, a change in the load does not affect the performance of the algorithm. This was verified using Cases 4a and 4b.

A. Threshold Selection

The results for the accuracy of the algorithm in terms of correctly classifying attacks and normal scenarios, when evaluated over 5600 attack scenarios and 1400 normal (i.e., non-attack) scenarios, are tabulated in Table VIII. The algorithm

Percentage of cases of successful detection	99.75%
Number of false positives	0 out of 1400
Number of false negatives	17 out of 5600

Table VIII: Accuracy of the Proposed Method across all the cases

detected 5583 out of 5600 attack scenarios successfully using a threshold value, Th, of 0.15. Similarly, the 1400 normal scenarios were classified as normal operation, resulting in no false positives. Based on the CL values recorded in Tables III-VII, a threshold of $Th = 0.15$ can be seen to be adequate. The use of this threshold enables detection in 99.75% of the cases considered (as shown in Table VIII). The very small number of cases where the algorithm mis-classified an attack scenario were when the malicious change was of a single step and the load point was 10% away from the base value. In a practical scenario, a one step change of $1.3333°$ degrees in phase shift would hardly cause any damage. These cases of one step change were included to demonstrate that this algorithm is not only extremely effective when the attacker intends significant damage (which is most likely in an attack), but also works quite well when the change is very small. In practical scenarios, the changes in phase shift enforced by the adversary would be greater than $1.3333°$ to force any significant consequences and the proposed mechanism successfully detected all attack test cases where the PST tap is manipulated by two or more steps. Thus, a threshold, Th, of 0.15 is adequate for all practical purposes.

VII. Conclusions

In this paper, the problem of protection of phase shifters from cyber attacks is discussed. Various attack scenarios, especially the stealthy ones are considered. Indices based on the ratios of injection or branch currents to terminal voltages are formulated. These indices are mathematically validated in the purview of detection. An algorithm is thus formulated using these indices. The proposed algorithm is tested on the IEEE 118-bus system and is found to be reliable, computationally inexpensive and easy to implement. It is worth noting that this is the first work that considers such attacks. As this algorithm is developed based on principles of power system analysis involving the controlled and the controlling variables, this algorithm can be extended to protection of any modern power electronics based phase shifter.

Acknowledgment

This work was supported in part by the National Research Foundation, Prime Ministers Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and in part by the Singapore Telecommunications Ltd.

References

[1] 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.

[2] J. Verboomen, D. Van Hertem, P. H. Schavemaker, W. L. Kling, and R. Belmans, "Analytical approach to grid operation with phase shifting transformers," *IEEE Transactions on Power Systems*, vol. 23, no. 1, pp. 41–46, Feb 2008.

[3] R. Baldick and E. Kahn, "Contract paths, phase-shifters, and efficient electricity trade," *IEEE Transactions on Power Systems*, vol. 12, no. 2, pp. 749–755, May 1997.

[4] 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.

[5] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, July 2010.

[6] 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.

[7] "Phase shifters." [Online]. Available: https://new.siemens.com/global/en/products/energy/high-voltage/transformers/phase-shifting-transformers.html

[8] L. Rulison, "Power play costs $100m," *The Times Union*, p. E1, September 2008.

[9] B. Sobczak and P. Behr, "China and america's 400-ton electric albatross," *E & E News*, 2019.

[10] 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.

[11] 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.

[12] 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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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 Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

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

[23] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[24] 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, Sep. 2015.

[25] 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.

[26] 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.

[27] S. Tan, W. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan 2018.

[28] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, "Toward data integrity attacks against optimal power flow in smart grid," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1726–1738, Oct 2017.

[29] 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.

[30] 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

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

[32] 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.

[33] T. Ding, R. Bo, Z. Bie, and X. Wang, "Optimal selection of phase shifting transformer adjustment in optimal power flow," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2464–2465, May 2017.

[34] A. Nikoobakht, J. Aghaei, H. Farahmand, V. Lakshmanan, and M. Korpås, "Flexibility of controllable power transformers for managing wind uncertainty using robust adjustable linearised optimal power flow," *IET Renewable Power Generation*, vol. 13, no. 2, pp. 262–272, 2019.

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

[36] 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.

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

Shantanu Chakrabarty received B.E degree in Electrical Engineering from University College of Engineering (Autonomous), Osmania University, in 2010, and, M.E in Electrical Engineering and Ph.D degrees from Indian Institute of Science, Bangalore, in 2012 and 2018, respectively.

He is currently working as a Research Fellow in National University of Singapore, Singapore. His areas of interest include power system analysis, smart grid cyber-security and critical infrastructure cyber-security.

Biplab Sikdar (S'98-M'02-SM'09) received the B.Tech degree in Electronics and Communication Engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech degree in Electrical Engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D degree in Electrical Engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include wireless network, and security of IoT and cyber-physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing.