Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks

Shantanu Chakrabarty and Biplab Sikdar

***Abstract*—Transformer taps are used extensively to regulate bus voltages in transmission networks. Tap change commands relayed through the SCADA network are attractive targets for falsification by attackers in order to adversely affect the operation of the system. Such attacks can be hidden by selective measurement manipulations. In this paper, an algorithm is developed that detects the presence of a stealthy false tap change command. The development of the algorithm is based on the intuition that any attack involving injection of false data or commands can only influence the measurement and estimation of certain selected variables, not all of them. The algorithm is based on the ratios of injection or branch currents to the voltages of the terminal nodes of the tap changing transformers. This principle is proven analytically and validated using simulations, leading to the establishment of an index which distinguishes stealthy attacks from normal operation scenarios. This lead to the development of an algorithm which is simple to implement, computationally light and shown to be extremely reliable when tested across various cases on the IEEE 118-bus and 2383-bus Polish systems.**

***Index Terms*—Cyber-security, OLTC, transmission networks.**

NOMENCLATURE

$\mathbf{z}$	Measurement vector.
$\mathbf{x}$	State vector.
$\mathbf{e}$	Error vector.
$h(\mathbf{x})$	Function mapping $\mathbf{x}$ to $\mathbf{z}$.
ns	Number of state variables.
nm	Number of measurements.
σ_i	Standard deviation of i^{th} measurement error, e_i.
y_{km}	Admittance of transformer/transmission line.
g_{km}	conductance of transformer/transmission line.
b_{km}	Susceptance of transformer/transmission line.
Y_{km}	Equivalent admittance between nodes k and m.
t_{km}	Transformer tap ratio.
S_{km}	Apparent power flow between nodes k and m.
V_k	Voltage at node k.
$\lvert V_k\rvert$	Magnitude of voltage at node k.
δ_k	Voltage angle at node k.
I_{km}	Current flow from node k to node m.
P_{km}	Real power flow from node k to node m.
Q_{km}	Reactive power flow from node k to node m.
S_k	Apparent power injection at node k.
P_k	Real power injection at node k.
Q_k	Reactive power injection at node k.
a	Superscript to denote blatant attack.
n	Superscript to denote normal scenario.
ref	Superscript to denote reference values of quantities.
hid	Superscript to denote stealthy or hidden attack.
$\mathbf{c}$	Vector of control and controlled variables.
X_1	Set containing state variables whose true values are required to be hidden from the state estimator.
X_2	Set containing state variables whose true values are not required to be hidden from the state estimator.

I. INTRODUCTION

In a power system, the controls can be broadly classified into two categories: active power related controls (that manipulate active power flows) and reactive power related controls (that manipulate reactive power flows). One of the most popular reactive power related controls is the transformer tap control. Taps are usually employed as voltage control devices [1], [2]. Since voltage magnitudes of the buses are strongly coupled to the reactive power, taps significantly affect the reactive power flows. In a transmission system, an operator makes a choice of tap settings in a varied number of ways, depending on the requirements. They can be chosen using the solution of the adjusted load flow formulation [3] or by using the solution of an optimal power flow (OPF) [4], [5], when a certain objective is of more importance than maintenance of a scheduled voltage. The transformer tap change commands, as deemed appropriate by the Energy Management Systems (EMS), are relayed through SCADA communication channels. However, these channels are in general prone to cyber attacks, rendering this control action vulnerable [6], [7].

Any malicious exploitation of vulnerability in voltage control can have severe consequences on the operation of a power grid. Voltage control (by means of transformer taps) is one of the most important types of control that exist in a power grid [8], [3]. Voltage control is essential for secure operation of a power system [8]. According to [9], the allowable node voltage variation is very low, for instance, $400-420\,KV$ in normal operation and $380-420\,KV$ in disturbed conditions, for $400\,KV$ rated voltage. Apart from secure operation, it is an obligation of an utility to ensure power quality to their customers [8], [9]. This is especially true in case of industrial loads which are sensitive to voltages (get damaged even due to slight voltage variations from the rated value). Another aspect to consider is voltage instability (due to disturbances), which was responsible for some major blackouts in the past [9]. Thus,

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

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

it is of paramount importance to detect any malicious voltage control command (transformer tap command in this paper). The threat posed by improper use (malicious use by adversary) of transformers in general is covered in [10], where, the idea of improper voltage levels due to manipulation of taps is also discussed.

One of the most common forms of attack on power grid SCADA systems is False Data Injection (FDI) attacks [11], [12], [13]. In FDI attacks, false data that is injected is chosen such that Bad Data Detection (BDD) [14] fails to recognize it as incorrect data. FDI is well studied in the case of transmission systems [11], [12], [15], [16]. However, literature dealing with the aspects of *false control signal injection* is sparse [17]. This is true for the voltage control measures. There is some existing work concerning voltage control in distribution systems [18], [19]. However, these deal with FDI attacks that result in wrong control action. False control signal injection can be equally or more hazardous than FDI, especially if it is done stealthily with the help of FDI. An example of a false control signal injection attack is the Ukrainian blackout event of 2015 [17], there the attackers compromised the network to launch a false control signal injection attack on the circuit breakers to disconnect parts of the system.

This paper addresses the gap in existing literature by considering the problem of detecting false command injection attacks on power grids. In particular, this paper is concerned with the detection of false transformer tap change command injection attacks in transmission networks where the transformer taps are changed frequently using on-load tap changers (OLTC) to meet a set of specified voltages under an *Automatic Voltage Control scheme*. An adversary who compromises the SCADA system has access to control signals of several field devices. The adversary may thus modify other SCADA measurements in order to hide the false command injection. This paper considers such hidden attacks where concepts of FDI attacks are used to mask the presence of a malicious control signal and its consequences [12]. As discussed before, stealthy false command injection attacks on OLTCs can have severe consequences. Thus, detection schemes against such attacks are necessary. This paper is the first to consider such attacks and provide a scheme for their detection.

The main contributions of this paper are as follows:

1) An algorithm is developed that detects falsely injected tap change commands in OLTCs even though the attack is hidden by suitable manipulation of measurements. This is the first paper to consider and address such attacks.
2) The developed algorithm has the following features:
   a) It is computationally light and easy to implement.
   b) It does not need any historical data of measurements or state variations to aid detection.
   c) It works reliably well, when tested on IEEE 118-bus and 2383-bus Polish systems, even when the tap manipulation is close to the desired operational value.

The paper is organized as follows. A review of the related work is presented in Section II and an overview of the background material is presented in Section III. An overview of system model and threat model is discussed in Section IV. The attack scenarios that can arise in the context of false transformer tap change commands are discussed in Section V. The detection algorithm is presented in Section VI, followed by its validation in Section VII, and conclusions in Section VIII.

II. Literature Review

The most common attack on power systems that is considered in literature is the FDI attack. This class of attacks was introduced in [11], where a vulnerability of the existing BDD techniques was exposed in the context of state estimation with DC power flow model. The presence of the same vulnerability in BDD in the context of AC state estimation is discussed in [12]. In [12], the conditions to achieve a stealthy FDI is established in the context of AC state estimation. The work in [20] presents a vulnerability and an attack strategy where FDI attacks can be used to cause sequential outages and cascaded tripping. The implications for FDIs from the analysis of the Ukraine blackout is given in [17].

The knowledge of these vulnerabilities subsequently prompted research in several detection and mitigation techniques. The methods in [13], [21], [22] are relevant only for DC state estimation. Several detection techniques have also been proposed for the case of AC state estimation. The application of Kalman filtering to achieve FDI detection has been proposed in [15], [23]. The use of a clustering algorithm coupled with particle swarm optimization to cluster vulnerable nodes (from the point of view of voltage stability) has been proposed in [24]. This method is overall computationally expensive as it has several computationally intensive algorithms embedded in its detection process. Similar observations can be made for [15], [23]. A non iterative technique is proposed in [16], which uses power measurements (injections and flows) from SCADA system and voltage measurements from Phasor Measurement Units (PMUs) to detect FDI attacks. In [25], the probability distribution of the measurement deviation is compared with historical data to achieve detection. An emerging category of threats to smart grids called Coordinated Cyber-Physical Attacks (CCPA) have been considered in [26]. In [26], the basic principle of CCPA is investigated where methods to construct a cyber attack vector is shown such that the physical attack vector is neutralized and BDD is avoided. Counter measures are proposed to detect CCPAs based on known-secure PMU measurement verification and online tracking of power system equivalent impedance. There have been few notable works prior to [26] on CCPA. In [27], the use of Petri-nets for modelling CCPA is proposed with an example of attacks on smart meters. An overview of a smart grid security test-bed is provided in [28] to accurately represent a cyber physical environment. Several attack scenarios are then demonstrated on this test-bed to study the cyber-physical impacts. A stochastic game-theoretic approach is developed in [29] to enable the power grid to defend against CCPA. In [30], CCPA that could cause undetectable transmission line outages are studied. In order to mitigate such attacks, “an efficient greedy search-based heuristic method” is proposed as a solution.

There are some literature on FDI attacks that instigate wrong Volt/VAR related control measures [18], [19], [31]. These methods are designed exclusively for distribution systems. In [18], a distribution system with a centralized voltage control scheme is assumed and an FDI attack is considered where sensed voltages are manipulated to maliciously induce or suppress tap changes. However, the attack does not consider the presence of any state estimators with BDD. In the presence of state estimation with BDD, such attacks are easily filtered out as bad data due to the presence of redundant measurements. In [31], the Automatic Voltage Control measures undertaken by the EMS in transmission networks are considered. However, the control measures are the active and reactive power generation, not transformer taps. In contrast, this paper deals with the security of voltage control measures undertaken by the EMS, by means of tap changing transformers under an Automatic Voltage Control scheme. This is a practical method of voltage control which has been in use for decades and is still in use [3]. Thus, its protection from cyber attacks is a necessity.

It is clear from the literature survey that most of the existing work is primarily related to FDI attacks against the state estimator. Even the work on voltage control systems are FDI attacks which falsify the measurements to instigate wrong control actions. In contrast, this paper is concerned with the detection of malicious transformer tap change command injection attacks through compromised SCADA channels, even when the attack is hidden from the operator, using suitable manipulation of measurements. One of the important features of this work is that it employs the dependencies between system measurements (power flows and injections) and the state variables in the development of the proposed detection algorithm. This line of approach shares some similarities with model-based fault detection techniques [32]-[35] used in wide variety of applications (predominantly by control community).

III. Background

A. State estimation

Power measurements (bus injections and line flows) are a non-linear function of the state variables and modelled as [14]:

$$z_i = h_i(\mathbf{x}) + e_i, \quad \forall \quad i = 1, \cdots, nm. \tag{1}$$

Here, z_i is the i^{th} measurement, $h_i(\cdot)$ is the non-linear function mapping the measurement to the states and e_i is the measurement error. This error is assumed to have zero mean and a variance of σ_i^2. $\mathbf{x}$ is the state variable, which is a vector of length ns, and nm is the total number of measurements. There is enough redundancy in place to ensure that $nm > ns$. Thus, state estimation is the process of solving an over-determined system of equations. Also, as the state variables are mapped to the measurements non-linearly, the solution process is iterative.

The weighted least square estimation can be formulated as an optimization problem as follows [14]:

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & J(\mathbf{x}) = \frac{1}{2}\sum_{i=1}^{nm}\left[\frac{z_i - h_i(\mathbf{x})}{\sigma_i}\right]^2 \\ \text{subject to} \quad & c_i(\mathbf{x}) = 0, \ i = 1, \cdots, n_c \\ & d_i(\mathbf{x}) \leq 0, \ i = 1, \cdots, n_d. \end{aligned}$$

The tap settings are included as state variables in $\mathbf{x}$. The tap measurements, when available, are a part of the measurement vector $\mathbf{z}$ [36]. The first order optimality condition of $J(\mathbf{x})$ is

$$\frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = \mathbf{0}. \tag{2}$$

The Gauss-Newton approach is usually employed to find the roots of (2). The Taylor series expansion is obtained for $\partial J(\mathbf{x})/\partial \mathbf{x}$ and higher order (second order and above) terms are neglected. This results in the iterative process given by

$$G(\mathbf{x}^u)\Delta\mathbf{x}^u = H^T R^{-1}(\mathbf{z} - h(\mathbf{x})) \tag{3}$$

$$\mathbf{x}^{u+1} = \mathbf{x}^u + \Delta\mathbf{x}^u \tag{4}$$

where, $G = H^T R^{-1} H$ is the gain matrix, R is a $nm \times nm$ matrix with the measurement variances on the diagonal, u is the iteration count and H is the Jacobian matrix, where $\left(\frac{\partial h_k}{\partial \mathbf{x}}\right)^T$ is the k^{th} row of H [14]. The state vector is updated till the convergence criterion is met.

B. Bad Data Detection

In order to detect incorrect measurements and faulty equipment, there is a mechanism (bad data detection) in place after the convergence of the state estimation [14]. The first step in the BDD process is the estimation of the normalized residual given by

$$\mathbf{r} = R^{-0.5}(\mathbf{z} - h(\mathbf{x})). \tag{5}$$

Then, $||\mathbf{r}||_2$ is estimated. A threshold value, τ is obtained using the knowledge of error distribution and χ^2 testing. If $||\mathbf{r}||_2 > \tau$, then the EMS is notified of the presence of bad data.

C. False Data Injection (FDI) and Hidden Tap Change (HTC) Attacks

1) FDI Attacks: When a measurement is manipulated, the value of one or more state variables changes. If the other measurements that are directly dependent on these state variables are not manipulated accordingly, the bad data detector (Section III-B) detects the presence of manipulated measurement as a bad data [12]. Thus, for an attacker to manipulate a measurement and remain undetected, all the measurements that are directly dependent on the changed state variables must also be manipulated. This bypasses the bad data detector since the set of manipulated measurements mimic a physically feasible scenario.

2) HTC Attacks: An attack on transformer tap control has many differences when compared to the hidden false data injection attacks discussed in Section III-C1. In HTC attacks, the control parameter, i.e., the tap setting, is subject to manipulation. In order to hide this manipulation, the adversary has to ensure that both the command (tap ratio) and the controlled parameter (regulated bus voltage magnitude) must appear close (considering measurement noise) to the selected or scheduled values, to avoid attention of the operator. This requires that their estimated and measured values be close to the selected values. To achieve this, malicious manipulation of tap settings must be accompanied by selective injection of false data [12], to avoid bad data detection. Such attacks, which beat both BDD and operators are referred to as Hidden Tap Change (HTC) or stealthy attacks in this paper. The mechanism of completely masking a malicious tap change, based on the principles in [12], is discussed in Section V.

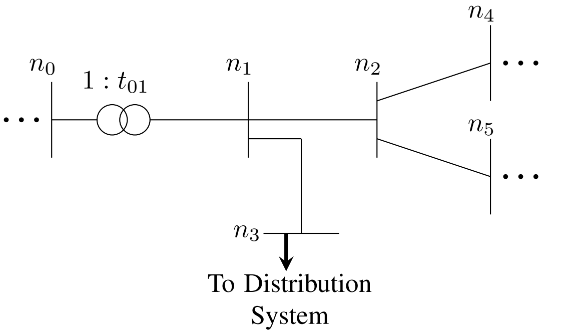


Figure 1: An illustration of a part of a transmission grid to explain FDI and HTC attacks.

As an example of these two classes of attacks, consider a part of transmission system or grid which wheels bulk power at high voltage levels, shown using one-line diagram in Figure 1. If an adversary wants to falsify the reactive power flow between nodes n_0 and n_1 (represented as $Q_{n_0n_1}$), then this falsification affects the estimation of variables on which $Q_{n_0n_1}$ depends. In Figure 1, $Q_{n_0n_1}$ is a function of voltage magnitude, $|V_{n_0}|$ (and other variables of nodes n_0 and n_1). So, in order to hide the attack, all measurements which are a function of $|V_{n_0}|$ are chosen to be manipulated so that BDD is not triggered (FDI attack) [12]. Though BDD is avoided, the estimates of state variables at nodes like n_1, n_3 and n_4 still read the true values (even after FDI attack). Thus, the attack can affect the estimate of chosen variables ($|V_{n_0}|$ in this case), not all of them. This can also be seen in case of a maliciously changed tap ratio from t_{01}^n to t_{01}^a. All the measurements which are a function of t_{01} are affected. In order to hide the change in t_{01}, only these measurements need to be manipulated. However, the effect of change due to malicious tap operation can still be observed at nodes like n_2, n_4 (where measurements are not directly dependent on t_{01}). This is because a change in reactive power flow (also active power) between nodes n_0 and n_1 has an effect on flows beyond node n_1.

IV. System Model and Threat Model

In this section, the cyber and physical model is discussed first in Section IV-A. A brief overview of the SCADA network connecting control centre and a substation (housing OLTCs) is given in Section IV-A1. Then, an overview of tap ratio selection is given in Section IV-A2. Subsequently, the threat is introduced in Section IV-B and an attack tree is drawn from the point of view of attacks on OLTCs.

A. Cyber and Physical Model

1) SCADA communication channels: In a smart grid, the control is centralized at the *control centre*. Control centre is connected to various parts of the grid by means of dedicated communication channels, as shown in Figure 2 [37]. Transformer taps are housed in one of the substations and are usually operated or controlled by the EMS through RTUs. The RTUs receive commands from the control centre through dedicated lines of communication. Similarly, measurement data from the substation is sent back to the control centre through the dedicated line of communication. The substation is also accessible to site engineers and vendors for maintenance or up-gradation. Similarly, corporate networks are also linked to the control centre, as shown in Figure 2.

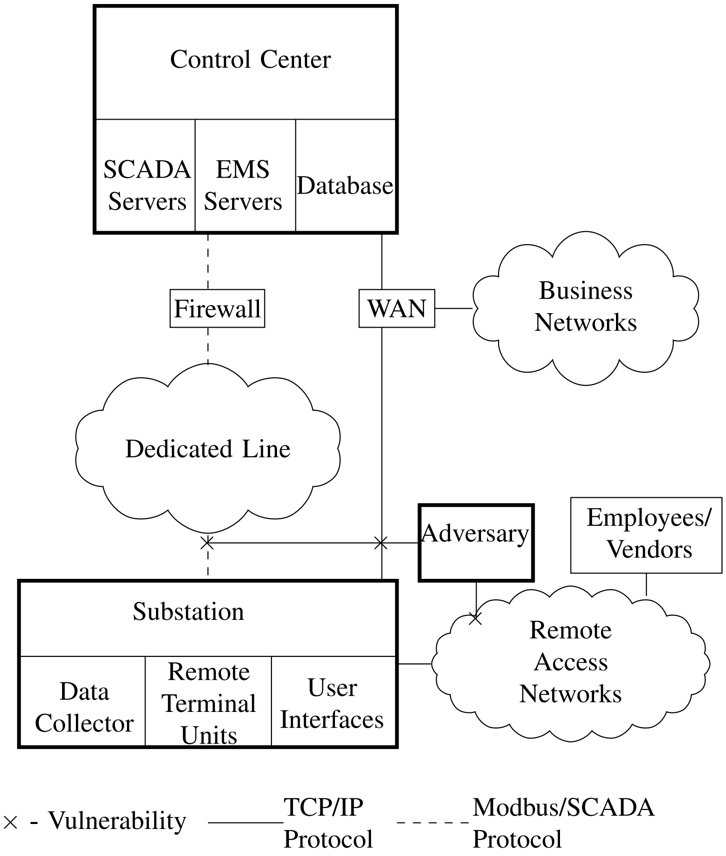


Figure 2: Network diagram showing connection between substation to control Center.

Thus, an adversary has possible access to the substation through one of the three channels, marked by "×" in Figure 2. Though, the channels connecting substations to control centres, business networks and vendors/site engineers are considered, the details related to communication protocols and data exchange mechanisms are not presented in this paper. This is because the detection method proposed is:

- based on
  - measurements used for state estimation,
  - system or grid model.
- and is independent of
  - the technology used in SCADA system,
  - the mode or delivery mechanisms of carrying out the stealthy attack.

2) Overview of tap selection: Consider the one-line system in Figure 3 where a tap setting (t_{km}) is used to enforce the voltage magnitude of the chosen bus k (i.e., the regulated bus), to meet a certain value $|V_k|^{sp}$. This voltage magnitude, $|V_k|$ is monitored and any change in $|V_k|$ indicates a change in the generation-load pattern or a topological change, prompting the pursuit of a new tap setting. Thus, there are two important quantities here: the control variable, i.e., the tap setting t_{km}, and the controlled variable, i.e., the regulated bus voltage magnitude, $|V_k|$.

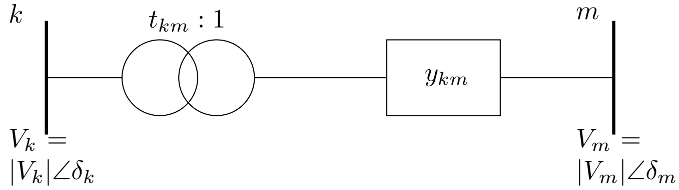


Figure 3: A transformer tap connected between nodes k and m.

B. Threat Model

It is stated in [37] that "*the highest impact an attacker can have is to gain access to the supervisory control access*". In the past, a blackout has happened because the lines were disconnected using malicious commands [17]. In the context of transformer taps too, an attacker gaining access to supervisory control of tap change can have severe consequences. These consequences have been discussed in Section I.

For an adversary to attack this mechanism of voltage control and remain undetected (by both BDD and system operator), it is necessary for the attacker to ensure that the estimated and measured values of t_{km} and $|V_k|$ appear as values selected by the EMS. To achieve this, malicious manipulation of tap settings must be accompanied by selective injection of false data [12] to beat the operator and avoid bad data detection. The attack scenarios are explained in detail in Section V. Thus, a stealthy attack essentially involves two steps, the first is taking over the RTUs to launch a false command and then manipulating the measurement data sent to EMS such that the estimates show the selected values. This can be achieved by exploiting any of the three vulnerability points shown in Figure 2.

Based on these concepts, an attack tree can be drawn as shown in Figure 4. The attack tree is from the point of view of malicious change in tap ratios (t_{km} in Figure 3) and its impact on power grid operation. In order to disrupt the operation of grid and power quality, an attacker can attack the control centre or the substation RTUs. As the control centres are recognized to be highly secured with less likelihood of getting breached [37], substation RTUs are an easier target. The adversary has a choice of launching a false command or data. As a false command injection is highly impactful [37], the choice of launching stealthy malicious tap change commands can be made by an adversary. The rest of the paper deals with the proposed detection scheme that detects the presence of such stealthily injected malicious tap change commands.

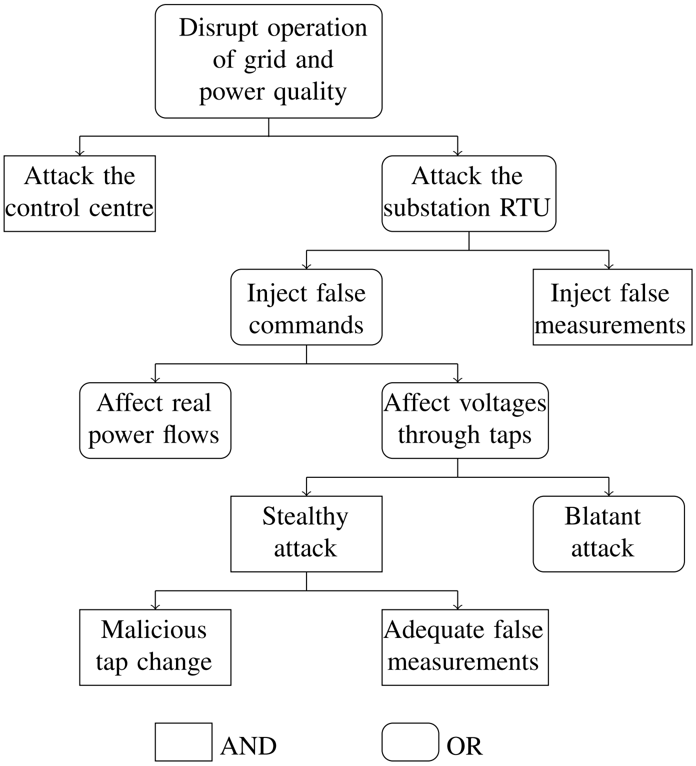

Disrupt operation of grid and power quality
Attack the control centre
Attack the substation RTU
Inject false commands
Inject false measurements
Affect real power flows
Affect voltages through taps
Stealthy attack
Blatant attack
Malicious tap change
Adequate false measurements
AND
OR

Figure 4: Attack tree highlighting the attacks on Transformer tap controls

V. Transformer Tap Setting Attack Scenarios

In this section, the mechanism of HTC attacks (introduced in Section III-C2) is discussed in detail. The aim of this paper is to develop an algorithm that can detect such stealthy attacks.

Before the discussion on various stealthy attack scenarios, it is necessary to consider the transformer tap equivalent circuit to understand the dependence of different measurements on transformer tap values. Transformer taps are modeled as a π-network [38], like a transmission line. However, in case of taps, the series and shunt admittances are a function of the tap ratios. The transformer tap in Figure 3 can be represented by a π-network as shown in Figure 5.

In the π-network, the equivalent admittances are

$$Y_{km} = t_{km} y_{km} \tag{6}$$

$$Y_{kk} = t_{km}(t_{km} - 1) y_{km} \tag{7}$$

$$Y_{mm} = y_{km}(1 - t_{km}) \tag{8}$$

where, y_{km} is the admittance of the transformer, Y_{km} is the series admittance and Y_{kk} and Y_{mm} are the shunt admittances of the equivalent π-network.

When the tap setting t_{km} is changed from its selected or scheduled value t_{km}^{sp}, for the attack to be hidden, the tap measurement device must also be tampered so that it reads the selected value t_{km}^{sp}. Otherwise, the operator is aware of the change in tap value and would instigate an investigation. However, it is worth noting that manipulation of tap setting measurements does not guarantee a stealthy attack. All other measurements which are a function of the tap setting must also

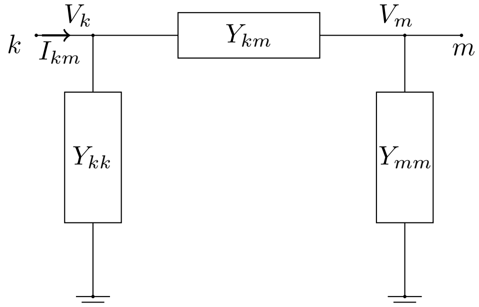


Figure 5: Equivalent π-network representation of a tap changing transformer.

be appropriately modified, otherwise the bad data detection will trigger an alarm.

The apparent power flowing from node k to m, S_{km}, in Figure 5 is given by

$$S_{km} = V_k I^*_{km}, \tag{9}$$

where V_k is the voltage of node k and I_{km} is the current flow between nodes k and m. Applying Kirchhoff's current law (KCL) at node k and using (7) and (6), we get

$$\begin{aligned} S^*_{km} &= t^2_{km} y_{km} |V_k|^2 - t_{km} y_{km} V_m V^*_k \\ &= P_{km} - jQ_{km}. \end{aligned} \tag{10}$$

Thus, from (10), it can be seen that the measurement quantities $P_{km}(= Re(S^*_{km}))$ and $Q_{km}(= -Im(S^*_{km}))$ are dependent on the tap ratio t_{km}. Similarly, the apparent power flow from node m to k is given by

$$\begin{aligned} S^*_{mk} &= y_{km} |V_m|^2 - t_{km} y_{km} V_k V^*_m \\ &= P_{mk} - jQ_{mk}. \end{aligned} \tag{11}$$

From (11), it can be seen that the active and reactive power flows from node m to k are dependent on t_{km}. Thus, for a stealthy attack, the measurements pertaining to active and reactive power flows between nodes k and m must be modified.

The apparent power injections at nodes k and m can be written as

$$S_k = S^{'}_k + S_{km} \tag{12}$$

$$S_m = S^{'}_m + S_{mk} \tag{13}$$

where $S^{'}_k$ is the sum of flows of all the lines incident at k, except S_{km}. Similarly, $S^{'}_m$ is the sum of flows of all the lines incident at m, except S_{mk}. From (12) and (13), it can be inferred that the injection measurements (both real and reactive power) at nodes k and m must also be modified, for the attack to be hidden.

Thus, the modifications needed in this case to hide a false change in tap ratio t_{km} can be summarized as:

(i) The tap measurement.
(ii) Active and reactive power injections at buses k and m.
(iii) Active and reactive power flows from k to m and also from m to k.

It should be noted that the malicious change in tap setting, though hidden, would result in a change in the regulated bus voltage magnitude $|V_k|$. This in turn will result in a new tap setting or an investigation (by the operator) if this mismatch in selected tap setting and the observed $|V_k|$ continues. For an attack to stay completely hidden (beat BDD and operator), the measurements must be tampered in such a way that the measured and estimated values of t_{km} and regulated bus voltage $|V_k|$ must be very close (approximately, considering noise in measurements) to the selected or scheduled values. It is emphasized again that only changing measurements of $|V_k|$ and t_{km} are not enough as it would not be consistent with the estimates derived from the line flow and bus injection measurements.

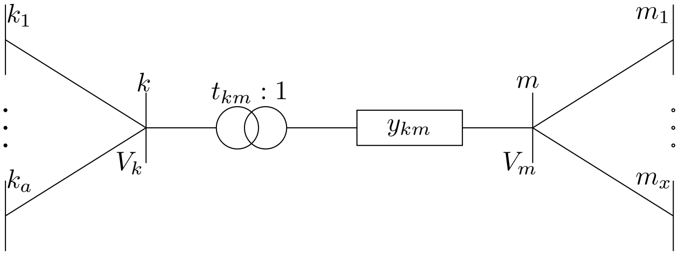


Figure 6: A tap changing transformer with other nodes in its vicinity

Apart from the measurement quantities mentioned before, there are few more quantities (which are functions of $|V_k|$) that must also be modified such that the estimated value of voltage of bus k turns out to be the selected value (or close to it, taking measurement noise into account). Consider the buses connected to node k apart from m, i.e., nodes k_1 to k_a in Figure 6. Similar to (10), the expression for the flow from k_1 to k can be written as

$$S_{k_1 k} = Y^{'}_{k_1 k_1} |V_{k_1}|^2 - Y_{k_1 k} V_k \tag{14}$$

where $Y^{'}_{k_1 k_1} = Y_{k_1 k_1} + Y_{k_1 k}$. It can be seen from (14) that the active and reactive power flows between nodes k_1 and k are a function of the voltage magnitude $|V_k|$. Thus, these measurements must be modified so that the estimated value of $|V_k|$ remains close to the regulated value. Similarly, the active and reactive power injections of bus k_1 must be modified as even they are a function of $|V_k|$ (similar to (12) and (13)). This idea can be extended to other buses connected to bus k.

The measurements that must be modified to ensure a completely stealthy attack can be summarized as follows:

(i) The tap measurement.
(ii) The voltage magnitude measurement at bus k. i.e., $|V_k|$.
(iii) The active and reactive power flows from k to m and from m to k.
(iv) The active and reactive power injections at buses k, m and $k_1, \cdots, k_a$ (all the buses connected to bus k).
(v) Additionally, the active and reactive power flows between k and buses connected to k must also be manipulated.

Usually, the number of buses connected to k is small [39], causing the admittance matrix (Y_{BUS}) to be sparse (with more than 85% of entries having a value of zero [39]). So practically, the number of measurements listed in (iv) and (v) are usually small which makes the effort required to execute such stealthy attacks very low. Thus, the detection of such attacks is extremely important.

These modifications ensure that the attack beats both BDD and the EMS. These can be established mathematically using the following proposition.

Theorem 1. *Let* $\mathbf{z} = \begin{bmatrix} z_1 & z_2 & \cdots & z_{nm} \end{bmatrix}^T$ *be the vector of measurements,* $\mathbf{x} = \begin{bmatrix} x_1 & x_2 & \cdots & x_{ns} \end{bmatrix}^T$ *be the state vector and* $\mathbf{c} = \begin{bmatrix} x_i & x_{i+1} & \cdots & x_{i+k} \end{bmatrix}^T$ $\forall\ i \geq 1, k \leq (ns - i)$ *be the vector that include the control and controlled variables. For an adversary to launch a stealthy attack (to beat BDD and the operator),* $\mathbf{c}$ *and all the measurements which are dependent on* $\mathbf{c}$ *must be modified.*

Proof. Under normal conditions when there is no attack, $\mathbf{z}$ is related to $\mathbf{x}$ as

$$\mathbf{z}^n = h(\mathbf{x}^n) + \mathbf{e} \tag{15}$$

where, $\mathbf{e} \sim \mathcal{N}(0, \sigma)$ is the error (following Normal distribution) and the superscript n is used to denote under normal conditions.

When an adversary introduces a set of false commands, we get

$$\mathbf{z}^a = h(\mathbf{x}^a) + \mathbf{e} \tag{16}$$

where, the superscript a is used to denote under a blatant or non-stealthy attack. Based on relation between measurements and state variables in power grids, it can be clearly inferred that

$$||\mathbf{z}^a - \mathbf{z}^n|| > 0. \tag{17}$$

In order to hide the presence of malicious commands from the EMS or the operator, the adversary has to hide the change in $\mathbf{c}$ from $\mathbf{c}^a$ to $\mathbf{c}^n$ (the values chosen by the operator/EMS). Then, the state vector in the case of a stealthy attack must be of the form, $\mathbf{x}^{\text{hid}} = \begin{bmatrix} x_1^a & x_2^a & \cdots & x_i^n & x_{i+1}^n & \cdots & x_{i+k}^n & \cdots & x_{ns}^a \end{bmatrix}^T$, where the superscript, hid, is used to denote under stealthy attack.

In order to beat the BDD, it is established [12] that the following quantity,

$$\mathbf{A} = h(\mathbf{x}^{\text{hid}}) - h(\mathbf{x}^a), \tag{18}$$

must be added to (16), to get

$$\mathbf{z}^a + \mathbf{A} = h(\mathbf{x}^{\text{hid}}) + \mathbf{e} \tag{19}$$

Thus, it is clear that BDD gets beaten as the power balance relation between $\mathbf{z}$ and $\mathbf{x}$ is maintained, as seen in (19). Even here, based on the form of state vector (introduced by the adversary to mask the change in $\mathbf{c}$), i.e., $\mathbf{x}^{\text{hid}}$, it can be seen that

$$||\mathbf{z}^a + \mathbf{A} - \mathbf{z}^n|| > 0. \tag{20}$$

From the expression of $\mathbf{A}$ in (18) and the forms of state vectors, $\mathbf{x}^{\text{hid}}$ and $\mathbf{x}^a$, it is clear that it has non-zero entries corresponding to measurements which are a function of vector $\mathbf{c}$. Thus, $\mathbf{c}$ and all measurements which are a function of variables in vector $\mathbf{c}$ must be modified to achieve stealthy malicious command injection attack. Thus, the information regarding other state variables and its related measurements are not a necessity.

Hence Proved.

□

The condition stated in Theorem 1 is a *sufficient condition*. This is because mathematically or theoretically, there is a possibility of an adversary with infinite capacity. This aspect and its practical infeasibility are discussed in detail in Section VI-B.

In the context of transformer taps, $\mathbf{c} = \begin{bmatrix} t_{km} & |V_k| \end{bmatrix}^T$. Thus, measurements which are dependent on t_{km} and $|V_k|$ must be modified to achieve a stealthy attack. The description preceding Theorem 1 (involving equations (9) to (14)) explain the outcome of Theorem 1 using closed form expressions describing the relation between measurements and state variables.

VI. Proposed Scheme for Detecting HTC attacks

A. The Quantity Used as the Classifier

The apparent power flowing from node k to node m can be expressed as

$$S_{km} = V_k I_{km}^*. \tag{21}$$

Rearranging (21), we get

$$I_{km} = \frac{S_{km}^*}{V_k^*} \implies \frac{I_{km}}{V_k} = \frac{S_{km}^*}{|V_k|^2}. \tag{22}$$

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

$$\frac{I_{mk}}{V_m} = \frac{S_{mk}^*}{|V_m|^2}. \tag{23}$$

Let us denote the quantities in (22) and (23) as YY_{km} and YY_{mk}, respectively. This quantity YY_{km} is essentially the admittance seen by the current flowing from node k towards node m. YY_{mk} can be interpreted similarly.

This method of analysis can also be extended to the bus injections. Performing similar mathematical operations on the bus injections of buses k and m, we get

$$YY_k = \frac{I_k}{V_k} = \frac{S_k^*}{|V_k|^2}, \tag{24}$$

$$YY_m = \frac{I_m}{V_m} = \frac{S_m^*}{|V_m|^2}. \tag{25}$$

The values of YY_{km}, YY_{mk}, YY_k and YY_m are determined when the tap is selected. These values can be used as a reference to compare with the values obtained during the state estimation to look for any significant deviations. Any significant deviation would be indicative of the presence of an attack. In order to validate the use of these indices towards the development of a detection algorithm, the following theorem is proposed and proven.

Theorem 2. *Let the estimated value of* YY_{km} *corresponding to the tap selection of a tap ratio* t_{km}^{sp}*, in order to maintain a regulated voltage of* V_k^{sp} *at bus k, be denoted by* YY_{km}^{ref}*. Also, during any hidden tap change attack, let the estimated value of* YY_{km} *be* YY_{km}^{hid}*. Then, for any power system operation* *with perfect measurements (noiseless), the following relation must hold true:*

$$\left| |YY_{km}^{hid}| - |YY_{km}^{ref}| \right| > 0.$$

Proof. Let the regulated voltage of bus k be V_k^{sp} and the selected tap value be t_{km}^{sp}. As the measurements relevant to the index YY_{km} are the flows from k to m, the expression for the apparent power flow between k and m can be written as in (10), as

$$\begin{aligned} S_{km}^*(T) &= t_{km}^2 y_{km} |V_k|^2 - t_{km} y_{km} V_m V_k^* \\ &= P_{km} - jQ_{km} \qquad (26) \\ &= h_R(T) - jh_I(T). \end{aligned}$$

In (26), $T = \{t_{km}, |V_k|, \delta_k, |V_m|, \delta_m\}$ is the set of state variables that affect the quantities P_{km} and Q_{km}. The set of state variables T can be split into two sets, one with the variables, whose changes are hidden, i.e., $X_1 = \{t_{km}, |V_k|\}$ and the other set with variables whose changes are not hidden (i.e., their true values brought about by the attack are not hidden), i.e., $X_2 = \{|V_m|, \delta_k, \delta_m\}$. Thus, $T = \{X_1, X_2\}$. Let $HH(X_1, X_2) = [h_R(T) \ \ h_I(T)]^T$.

In a normal scenario, when there is no cyber attack, the variables are represented by a superscript n (i.e, $T^n = \{t_{km}^n, |V_k|^n, \delta_k^n, |V_m|^n, \delta_m^n\}$). Then, from (26), we can write

$$\begin{aligned} S_{km}^*(T^n) &= (t_{km}^n)^2 y_{km} (|V_k|^n)^2 \\ &\quad - t_{km}^n |y_{km}| |V_m^n| |V_k^n| e^{j(\delta_m^n - \delta_k^n + \theta_{km})} \qquad (27) \end{aligned}$$

$$\frac{S_{km}^*(T^n)}{(|V_k|^n)^2} = (t_{km}^n)^2 y_{km} - t_{km}^n |y_{km}| \left(\frac{|V_m|^n}{|V_k|^n} \right) e^{j(\delta_m^n - \delta_k^n + \theta_{km})}. \qquad (28)$$

Based on the definition in (23) and as there is no noise in the measurements, we can express (28) as

$$YY_{km}^{\text{ref}} = (t_{km}^n)^2 y_{km} - t_{km}^n |y_{km}| \left(\frac{|V_m|^n}{|V_k|^n} \right) e^{j(\delta_m^n - \delta_k^n + \theta_{km})} \qquad (29)$$

where, $y_{km} = g_{km} + jb_{km} = |y_{km}| \angle \theta_{km}$ is the admittance of transformer. The absolute value of YY_{km}^{ref} can thus be written as

$$|YY_{km}^{\text{ref}}| = \sqrt{A(T^n) + B(T^n)} \qquad (30)$$

where

$$A(T^n) = (t_{km}^n)^4 |y_{km}|^2 \qquad (31)$$

$$B(T^n) = (t_{km}^n)^2 |y_{km}|^2 \left(\frac{|V_m|^n}{|V_k|^n} \right)^2 - 2|y_{km}| (t_{km}^n)^3 \left(\frac{|V_m|^n}{|V_k|^n} \right)$$
$$(g_{km} cos(\delta_m^n - \delta_k^n + \theta_{km}) + b_{km} sin(\delta_m^n - \delta_k^n + \theta_{km})). \qquad (32)$$

When there is a false tap selection command injection by an adversary, the tap ratio and all the other state variables of the set T change. Let the state variables under this scenario be represented by adding a superscript a to them. Thus, $T^a = \{t_{km}^a, |V_k|^a, \delta_k^a, |V_m|^a, \delta_m^a\}$. Then, the measurement vector is

$$HH(T^a) = \begin{bmatrix} h_R(T^a) \\ h_I(T^a) \end{bmatrix}. \qquad (33)$$

For the adversary to make this attack a hidden one, the values of elements of subset X_1 of set T must remain the same as the normal values (when there is no attack) as discussed in Section V, i.e., $X_1^{\text{hid}} = X_1^n$ (superscript, hid, is used to denote the state variables in case of hidden attack). The subset X_2 is not changed, i.e, $X_2^{\text{hid}} = X_2^a$. Thus, if T^{hid} is used to denote the set of state variables when there is a hidden attack, we get $T^{\text{hid}} = \{X_1^n, X_2^a\} = \{t_{km}^n, |V_k|^n, \delta_k^a, |V_m|^a, \delta_m^a\}$.

The condition for hidden attacks [12] states that the following quantity must be added to the measurement vector $H(T^a)$,

$$AA = HH(T^{\text{hid}}) - HH(T^a). \qquad (34)$$

AA contains the necessary changes in measurements of P_{km} and Q_{km} required to hide the attack from BDD and the operator. Adding (33) and (34) results in the measurement vector $HH(T^{\text{hid}})$. Thus, using derivations similar to (27)-(30), we can express YY_{km}^{hid} as

$$|YY_{km}^{\text{hid}}| = \sqrt{A(T^{\text{hid}}) + B(T^{\text{hid}})} \qquad (35)$$

where

$$A(T^{\text{hid}}) = (t_{km}^n)^4 |y_{km}|^2 \qquad (36)$$

$$B(T^{\text{hid}}) = (t_{km}^n)^2 |y_{km}|^2 \left(\frac{|V_m|^a}{|V_k|^n} \right)^2 - 2|y_{km}| (t_{km}^n)^3$$
$$\left(\frac{|V_m|^a}{|V_k|^n} \right) (g_{km} cos(\delta_m^a - \delta_k^a + \theta_{km}) + b_{km} sin(\delta_m^a - \delta_k^a + \theta_{km})). \qquad (37)$$

It is worth noting that tap changes predominantly affect reactive power (Q) flows. Though reactive power (Q) is strongly coupled to voltage magnitudes ($|V_k|$ and $|V_m|$), it is not completely independent of voltage angles or phase displacement ($(\delta_k - \delta_m)$), which can also be seen in Equations (26) and (27) (as $Q_{km} = -Im(S_{km}^*)$). Also, the overall flow profile (around nodes k and m) changes due to any change in S_{km} (as can be inferred from KCL and KVL), eventually affecting the voltage angles. Thus, a malicious tap change command changes the phase displacement from $(\delta_k^n - \delta_m^n)$ to $(\delta_k^a - \delta_m^a)$.

So, when $B(T^n)$ and $B(T^{\text{hid}})$ are compared, the following observations are made:

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

Thus, it can be clearly inferred that

$$\begin{aligned} & B(T^{\text{hid}}) \neq B(T^n) \\ \implies \quad & |YY_{km}^{\text{hid}}| \neq |YY_{km}^{\text{ref}}| \\ \implies \quad & \left| |YY_{km}^{\text{hid}}| - |YY_{km}^{\text{ref}}| \right| > 0. \end{aligned}$$

Hence proved. □

The main mathematical proposition in Theorem 1, which forms the basis to develop a detection algorithm, can also be similarly proven for other indices, viz. YY_{mk}, YY_k and YY_m.

In Theorem 2, the basis for the detection algorithm is established mathematically using closed form expressions. In power system analysis, closed form expressions are used to establish power balance or charge balance (based on Kirchoff's voltage and current laws [40], as seen in equations (27) and (28)). However, in state estimation analysis, in order to consider the effect of noise, the most optimal estimates are sought, that fit the measurements by solving an optimization problem iteratively (weighted least square estimation) [14], [40], as described in Section III-A. So, in presence of noise in measurements, the proposition in Theorem 2 can be shown using an analysis similar to the proof of Theorem 1. This is presented as Corollary 2.1.

Corollary 2.1. *In presence of noise in measurements, the proposition in Theorem 2 holds.*

Proof. The proof is very similar to that of Theorem 1. However, it involves measurements relevant to the index YY_{km}, i.e., P_{km} and Q_{km}. Here, the same notations of Theorems 1 and 2 are followed, unless otherwise stated.

In presence of noise, the measurements (as seen and estimated by the EMS during tap selection), can be represented as follows:

$$\begin{bmatrix} P_{km}^{\text{ref}} \\ Q_{km}^{\text{ref}} \end{bmatrix} = \begin{bmatrix} h_R(T^n) \\ h_I(T^n) \end{bmatrix} + \begin{bmatrix} e_p \\ e_q \end{bmatrix} \tag{38}$$

Here, $|V_k|$ and t_{km} are at their specified values, the superscript, ref, is used to denote the reference values and $\begin{bmatrix} e_p & e_q \end{bmatrix}^T \sim \mathcal{N}(0, \sigma)$ is the noise vector, following Normal distribution.

In case of an attack, (38) changes to

$$\begin{bmatrix} P_{km}^{a} \\ Q_{km}^{a} \end{bmatrix} = \begin{bmatrix} h_R(T^a) \\ h_I(T^a) \end{bmatrix} + \begin{bmatrix} e_p \\ e_q \end{bmatrix} \tag{39}$$

Based on the principles of hidden attack (as discussed before in proofs of Theorems 1 and 2), the following quantity is added to (39):

$$AA = \begin{bmatrix} h_R(T^{\text{hid}}) \\ h_I(T^{\text{hid}}) \end{bmatrix} - \begin{bmatrix} h_R(T^a) \\ h_I(T^a) \end{bmatrix} \tag{40}$$

The addition of AA results in

$$\begin{bmatrix} P_{km}^{a} \\ Q_{km}^{a} \end{bmatrix} + AA = \begin{bmatrix} h_R(T^{\text{hid}}) \\ h_I(T^{\text{hid}}) \end{bmatrix} + \begin{bmatrix} e_p \\ e_q \end{bmatrix} \tag{41}$$

As discussed before in the proof of Theorem 1 (equations (17) and (20)), the system state and measurements are now changed due to the modifications by the adversary. This results in

$$\begin{aligned} &\left|\left| \begin{bmatrix} P_{km}^{a} \\ Q_{km}^{a} \end{bmatrix} + AA - \begin{bmatrix} P_{km}^{\text{ref}} \\ Q_{km}^{\text{ref}} \end{bmatrix} \right|\right| > 0 \\ \implies &\left|\left| \begin{bmatrix} P_{km}^{\text{hid}} \\ Q_{km}^{\text{hid}} \end{bmatrix} - \begin{bmatrix} P_{km}^{\text{ref}} \\ Q_{km}^{\text{ref}} \end{bmatrix} \right|\right| > 0 \end{aligned} \tag{42}$$

where, $\begin{bmatrix} P_{km}^{\text{hid}} \\ Q_{km}^{\text{hid}} \end{bmatrix} = \left(\begin{bmatrix} P_{km}^{a} \\ Q_{km}^{a} \end{bmatrix} + AA \right)$, contain the measurements seen by the state estimator due to stealthy attack.

Thus, based on the expressions of YY_{km} and S_{km}^* ((22) and (26)) and proved relation of (42), it can be easily inferred that $\left| |YY_{km}^{\text{hid}}| - |YY_{km}^{\text{ref}}| \right| > 0$ holds good for a stealthy attack, even in presence of noise. □

The relation in Theorem 2 can also be validated by analysing the current flowing between nodes k and m in Figure 5, which can be expressed as

$$I_{km} = Y_{kk}V_k + Y_{km}(V_k - V_m). \tag{43}$$

Using (6) and (7), (43) can be expressed as

$$I_{km} = t_{km}^2 y_{km} V_k + y_{km} V_m. \tag{44}$$

Dividing both sides by V_k, we get

$$YY_{km} = \frac{I_{km}}{V_k} = t_{km}^2 y_{km} + y_{km}\Big(\frac{V_m}{V_k}\Big). \tag{45}$$

It can be seen that YY_{km} is a function of voltages V_k ($= |V_k| \angle \delta_k$) and V_m (=$|V_m| \angle \delta_m$). As discussed in Section V, for a stealthy attack, it is only necessary that the estimated tap value, t_{km}, and the voltage magnitude of the regulated bus, $|V_k|$, remain around the specified or selected value (taking measurement noise into account). However, the estimated values of $|V_m|$, δ_k and δ_m remain unaffected by the attack (i.e., their measurements and estimates show true values). The same explanation can be extended to YY_{mk}, YY_k and YY_m. The attack scenarios considered in this paper evade the existing defence mechanisms (i.e., BDD and operator monitoring). However, as shown in Theorem 2, it is possible to detect the presence of such attacks using the indices defined in Section VI-A. The result of Corollary 2.1 further establishes this deduction, in presence of noisy measurements.

B. Practical Considerations

In case the attacker has unlimited capacity, then it is possible for him/her to show a different snapshot (based on past recorded data) of the system, effectively hiding any intrusion. Due to large geographical spread of power grids, this is most likely achievable by means of attacks on the control centre. As stated before, control centres are highly secured and attacks are extremely unlikely [37], [11] (though possible). So, attacks through substations are more likely. Based on Figure 6, using the same notations in Section VI-A and Theorem 1, it can be seen that to beat the algorithm, $\mathbf{cb} = \begin{bmatrix} |V_{k_1}| \cdots |V_{k_a}| \ \delta_{k_1} \cdots \delta_{k_a} \ |V_{m_1}| \cdots |V_{m_x}| \ \delta_{m_1} \cdots \delta_{m_x} \ |V_k| \ |V_m| \ \delta_k \ \delta_m \ t_{km} \end{bmatrix}^T$ and all measurements which are a function of $\mathbf{cb}$ must be modified for a single OLTC, as opposed to $\mathbf{c} = \begin{bmatrix} t_{km} & |V_k| \end{bmatrix}^T$ and measurements dependent on $\mathbf{c}$, for a stealthy attack.

Practically, to achieve a stealthy attack against transformer tap control, information regarding the substation containing tap changing transformer (meter measurements and command signals) and lines connected to regulated bus (which is usually known at a substation) is sufficient (Theorem 1). Due to redundancy, other related measurements can also be estimated. On the other hand, to beat the proposed technique, a very large number of correlated measurements have to be modified. In addition to that, entire information pertaining to the system (including real time load variations) are required to beat the method (as demonstrated using simulations of Case 4 in Section VII). This is highly unlikely in practice [11].

Remark. *Based on Theorems 1, 2 and Corollary 2.1, in practical power system operation,* $\left| |YY_{km}^{hid}| - |YY_{km}^{ref}| \right| > \left| |YY_{km}^{n}| - |YY_{km}^{ref}| \right|$.

This can be easily explained as the difference in $|YY_{km}^{n}|$ and $|YY_{km}^{\text{ref}}|$ is only due to difference in noise seen in measurements. On the other hand, the difference in $|YY_{km}^{\text{hid}}|$ and

Algorithm 1: Proposed False Transformer Tap Command Injection Attack Detector

```
Data: The reference values $YY_{km}^{\text{ref}}$, $YY_{mk}^{\text{ref}}$, $YY_{k}^{\text{ref}}$ and
      $YY_{m}^{\text{ref}}$ and the predefined Threshold $Th$
Output: Trig
1 Calculate $YYD$ using (46);
2 if $YYD > Th$ then
3     Trig = 1;
4     The presence of a false tap command is detected;
5 else
6     Trig = 0;
7     go back to step 1;
```

$|YY_{km}^{\text{ref}}|$ is due to change in the system brought about by the adversary (as seen in Theorems 1 and 2 and Corollary 2.1).

C. Classifier Formulation and Detection Algorithm

In order to develop the attack detection algorithm, an index is formulated. If this index exceeds a certain threshold value, then it is declared that the tap control is under attack. This index is based on the comparison of the absolute values of the quantities (YY_{km}, YY_{mk}, YY_k and YY_m) with the reference values (estimated during the tap selection process). Let the reference values of YY_{km}, YY_{mk}, YY_k and YY_m be YY_{km}^{ref}, YY_{mk}^{ref}, YY_{k}^{ref} and YY_{m}^{ref}, respectively.

Using the absolute values of the deviations of the indices from their reference values and adding them results in the following index denoted by YYD:

$$\begin{aligned} YYD = &\Big||YY_{km}| - |YY_{km}^{\text{ref}}|\Big| + \Big||YY_{mk}| - |YY_{mk}^{\text{ref}}|\Big| \\ &+ \Big||YY_{k}| - |YY_{k}^{\text{ref}}|\Big| + \Big||YY_{m}| - |YY_{m}^{\text{ref}}|\Big|. \quad (46) \end{aligned}$$

This classifier and the resulting detection algorithm are simple to implement with few additional lines of code in the bad data detection stage at the EMS, for each of the taps. The steps are given in Algorithm 1. In this algorithm, a predefined threshold, Th, is used to classify attacks from normal operating conditions. The selection of Th is discussed in Section VII-A. It is worth noting that the algorithm in its final form in Algorithm 1 is neither iterative nor does it involve solving a large system of equations. Thus, the computational burden of the proposed detection scheme is low.

VII. Simulation Results

The algorithm developed to detect the presence of an attack on tap settings is tested on the IEEE 118-bus [41] and 2383-bus Polish system [42]. In both systems, six tap changing transformers are placed for simulations pertaining to the proposed detection scheme. The details of their location and the regulated buses (whose voltages are being controlled) are given in Table I.

It is well-known that tap-changing transformers have tap setting control in discrete steps. They also have tap-limits, typically from 0.9 to 1.1. Thus, each of the six tap-changing transformers are considered to have tap settings between 0.9 and 1.1 with every tap setting incrementing/decrementing the winding by 2.5%, i.e., tap ratios increment/decrement in steps of 0.025. To simulate the operation of the power grid, the tap values are selected to meet a set of regulated voltages. This can be done using various tap selection algorithms based on power flow analysis [3] or optimal power flow based methods [4], [5] representing the specifications of voltages of regulated buses as equality constraints while meeting certain objective functions. In this work, as no objective function is of interest, the method based on power flow analysis is used to estimate tap values. The specified voltages (in pu) of the regulated buses and the tap settings required to meet these specified voltages are given in Table II.

Table I: Location and regulated buses of the transformer taps

System	Tap number[1]	FB[2]	TB[3]	RB[4]
118-bus	1	11	13	11
	2	30	17	30
	3	38	37	38
	4	64	61	64
	5	96	97	96
	6	114	115	114
2383-bus	1	354	2	354
	2	322	7	322
	3	617	35	617
	4	77	48	717
	5	1650	116	1650
	6	143	145	143

[1] Tap serial number (also referred to as tap no.)
[2] From Bus
[3] To Bus
[4] Regulated Bus

Table II: The specified voltages of the regulated buses and the tap settings required to achieve it

System	Tap number	RB[1]	V^{sp}[2]	t_{km}^{sp}[3]
118-bus	1	11	0.9836	1.025
	2	30	0.9934	1.025
	3	38	0.9729	1.05
	4	64	0.9875	1.025
	5	96	0.9882	1.025
	6	114	0.95	1.025
2383-bus	1	354	0.9753	1.025
	2	322	0.9926	1.00
	3	617	1.0052	1.025
	4	717	0.9754	1.05
	5	1650	0.9898	1.00
	6	143	0.9860	1.025

[1] Regulated Bus
[2] Specified Voltage
[3] Selected tap values

To test the developed algorithm, stealthy attacks were simulated such that the measurements and estimated values of the tap settings and regulated bus voltages read values in close vicinity (due to measurement noise) to the ones given in Table II. The attacks were crafted using the principles established in Section V. Thus, measurements related to the tap values and regulated bus voltages were manipulated. There are four cases considered here, including the case when there is no attack.

The cases are listed as follows:

- **Case 1:** Normal Scenario when there is no attack
- **Case 2:** When the adversary changes the tap settings by two or more than two steps.
- **Case 3:** When the tap settings are changed by just one step.
- **Case 4:** When the tap settings are manipulated by just one step and the system load point changes stochastically (using standard normal distribution).

In cases 2, 3 and 4, the relevant measurements are manipulated so that the estimated and measured values of the taps and regulated bus voltages remain close (taking errors in estimation due to measurement noise into account) to the ones in Table II. The measurement error or noise is considered to be 1% for power measurements and 0.3% for voltage measurements [43], [44]. Thus, to study the accuracy of the developed method in presence of noise, Cases 1, 2 and 3 are run for 200 times and Case 4 is run for 500 times.

It can be easily inferred from Theorem 2 and Corollary 2.1 that the algorithm works effectively even if the load is different from the one seen during tap selection. The aggregate load change or state change in a practical power grid is very slow [45], [46]. Thus, different loading points are generated using a standard normal distribution (using MATLAB function $rand(n,1)$ [47]), within 10% from the base values (system load in normal scenario and Cases 1 and 2). There are 10 load points considered with 50 simulation runs under each loading point. This results in 500 runs on both the systems. This study is just an additional result to further establish the effectiveness of the algorithm, as it is not practically feasible for an adversary to keep up (or have a definite knowledge) with the changes in system load over a period of time.

In normal scenarios, when there is no attack (Case 1), the maximum values of YYD are recorded. In cases 2, 3 and 4, the minimum values are recorded. They are presented in Table III. The values of YYD recorded are pu values. From the values in Table III, it can easily be seen that the minimum values of YYD observed in all the attacks are significantly higher than the maximum values of YYD observed when there is no attack. The sensitivities of $\left||YY_{km}| - |YY_{km}^{\text{ref}}|\right|$ and $\left||YY_{mk}| - |YY_{mk}^{\text{ref}}|\right|$ to an attack can be inferred from equations (32), (37) and (42) in Theorem 2 and Corollary 2.1. However, their relative sensitivities are comparable, as the measurements involved differ due to line losses (both active and reactive power). On the other hand, the sensitivities of $\left||YY_{k}| - |YY_{k}^{\text{ref}}|\right|$ and $\left||YY_{m}| - |YY_{m}^{\text{ref}}|\right|$ vary depending on the number of lines connected to the nodes k and m (as injections are sum of flows, as seen in (12) and (13)). Thus, the trends observed in YYD due to attacks basically reflect Theorem 2 and Corollary 2.1. It is worth noting that YYD values observed in certain taps (tap no. 6 in 118-bus and tap numbers 4 and 6 in 2383-bus system) are significantly more sensitive to an attack. This is because, based on the definitions of $|YY_{km}|$, $|YY_{mk}|$, $|YY_k|$ and $|YY_m|$, it is clear that the sensitivity is mainly governed by the sensitivities of apparent power flows and injections, i.e., S_{km}, S_{mk}, S_k and S_m. The sensitivities of these quantities (all quantities in general) to a change in system state vary significantly (both within the same system and across systems). This is a normal and well-known phenomenon observed in power (or smart) grids. Even analysis involving sensitivities study sensitivities individually (at every node or line or device) [48], as they are known to vary significantly.

Table III: The specified voltages of the regulated buses and the tap settings required to achieve it

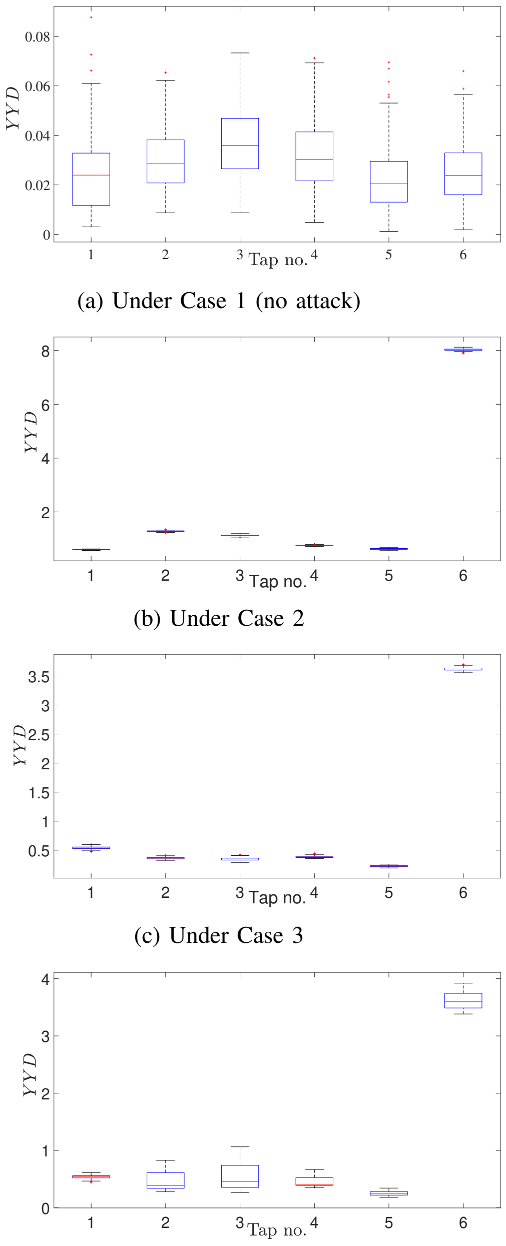
System	Tap no.	Case 1	Attacks (YYD^{min}[2])		
		(YYD^{max} [1])	Case 2	Case 3	Case 4
118-bus	1	0.0877	0.5670	0.4791	0.4420
	2	0.0653	1.2303	0.3246	0.2723
	3	0.07329	1.0475	0.2844	0.2625
	4	0.07122	0.7123	0.3544	0.3472
	5	0.0695	0.5600	0.1940	0.1882
	6	0.0659	7.8972	3.5543	3.3833
2383-bus	1	0.0761	2.7846	1.3961	1.3954
	2	0.0513	2.2801	1.0979	1.1105
	3	0.0523	1.9341	0.9139	0.9211
	4	0.0628	100.9603	53.54	29.46
	5	0.0547	2.4284	1.2024	1.2165
	6	0.0608	97.8884	49.814	3.1319

[1] Maximum value of YYD recorded
[2] Minimum value of YYD recorded

Another important aspect to note is that the reference values of the indices in the calculation of index YYD can be prone to errors. However, if the reference values are significantly erratic, then the selected tap ratio would not be able to maintain the specified voltage. When there is no false tap selection command, the estimated and measured voltages of the regulated buses would indicate that. Thus, there is no possibility of a false alarm. This would only prompt the EMS to select a new ratio if the deviation in voltages are significant enough (in the order of the voltage change that can be caused by at least one step increment/decrement of tap). In case of an attack, the adversary can only use the values selected by the EMS (irrespective of its aptness) as the basis to hide the attack. This attack would then be easily detected by the algorithm due to a significant increase in the value of YYD.

A. Threshold Selection

Based on the observed values of the index YYD in all the cases, the threshold, Th, is chosen to be 0.15. This value can classify the false command injections even when the malicious tap selection change command changes the tap ratio by one step. Thus, the value of Th used in Algorithm 1 is 0.15. However, any value between 0.12-0.17 can facilitate a reliable detection. A set of box-plots for the values of YYD are presented for all the cases (when tested on IEEE 118-bus system) in Figure 7. From the box plots, it is clear that a threshold of $Th = 0.15$ is capable of classifying attacks from normal operation. From the values in Table III, it can be seen that this threshold is effective even in the 2383-bus system. The accuracy of the developed algorithm is tabulated in Table IV and it is found that the algorithm detects the attack in all



(a) Under Case 1 (no attack)

(b) Under Case 2

(c) Under Case 3

(d) Under Case 4

Figure 7: Box plots representing the variation of YYD for cases studied in 118-bus system

Table IV: Accuracy of the developed method across all cases

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

the cases. This finding can also be validated using Table III and box-plots in Figure 7.

VIII. Conclusion

In this paper, the issue of false injection of transformer tap change commands in transmission networks is discussed. The various attack scenarios that can arise, including the most stealthy ones, are studied. Based on observations drawn from the attack scenarios, an algorithm is developed which compares several indices with the values that are obtained during the tap selection process in the EMS. The deviations are consolidated into one single index that enables the detection of HTC attacks. The developed algorithm is very simple to implement and computationally light. Its performance was found to be good in every test case it was subjected to, on the IEEE 118-bus and 2383-bus Polish systems. It is worth noting that this is a first effort of its kind as it deals with false command injection as well as the process of hiding the false command by means of suitable false data injection. As a future endeavour, various FACTS based controls can be explored in the context of this work.

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] 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.

[2] B. Stott, "Review of load-flow calculation methods," *Proceedings of the IEEE*, vol. 62, no. 7, pp. 916–929, July 1974.

[3] 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.

[4] "Complementarity model for load tap changing transformers in stability based opf problem," *Electric Power Systems Research*, vol. 76, no. 6, pp. 592 – 599, 2006.

[5] W. Rosehart, C. Roman, and A. Schellenberg, "Optimal power flow with complementarity constraints," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 813–822, May 2005.

[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] 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.

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

[9] A. Kanicki, *Voltage Control in Distribution Systems*, ser. Handbook of Power Quality. John Wiley & Sons, Ltd, 2008.

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

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, Jun. 2011. [Online]. Available: https://doi.org/10.1145/1952982.1952995

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *2014 American Control Conference*, June 2014, pp. 4372–4378.

[20] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, March 2019.

[21] 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.

[22] 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.

[23] 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.

[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, 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, Sep. 2015.

[26] 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.

[27] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec 2011.

[28] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, June 2013.

[29] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 684–694, March 2018.

[30] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan 2018.

[31] 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.

[32] R. Isermann, "Model-based fault-detection and diagnosis – status and applications," *Annual Reviews in Control*, vol. 29, no. 1, pp. 71 – 85, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1367578805000052

[33] S. Li and J. Wen, "A model-based fault detection and diagnostic methodology based on pca method and wavelet transform," *Energy and Buildings*, vol. 68, pp. 63 – 71, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378778813005410

[34] R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Distributed fault detection and isolation of large-scale discrete-time nonlinear systems: An adaptive approximation approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 275–290, Feb 2012.

[35] K. Turksoy, A. Roy, and A. Cinar, "Real-time model-based fault detection of continuous glucose sensor measurements," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 7, pp. 1437–1445, July 2017.

[36] 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.

[37] 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.

[38] H. H. Z. L. V. Barboza and R. Salgado, "Load tap change transformers: A modeling reminder," *IEEE Power Engineering Review*, vol. 21, no. 2, pp. 51–52, Feb 2001.

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

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

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

[42] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[43] 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.

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

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

[46] L. Liu, M. Esmalifalak, and Z. Han, "Detection of false data injection in power grid exploiting low rank and sparsity," in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 4461–4465.

[47] Mathworks, *MATLAB®- The language of Technical Computing*, ser. Language Reference Manual, Version 5. Mathworks, 1997.

[48] F. Capitanescu and T. Van Cutsem, "Unified sensitivity analysis of unstable or low voltages caused by load increases or contingencies," *IEEE Transactions on Power Systems*, vol. 20, no. 1, pp. 321–329, 2005.

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.