Detection of Malicious Command Injection Attacks Against Static Var Compensators in Smart Grids

Shantanu Chakrabarty and Biplab Sikdar.

***Abstract*—In a smart grid, voltage control and reactive power control are crucial to its safe and reliable operation. Static Var compensators (SVCs) are widely used to achieve these controls in a transmission system, either through centralized control by Energy Management Systems or through local closed loop control systems. In smart grids, the command channels to control SVCs are vulnerable to cyber attacks. In this paper, attack scenarios involving injection of malicious commands to SVCs are studied in detail. Attack models are established for both methods of control. Based on these attack models, two detection algorithms are proposed. The principle behind these algorithms involves the notion that even though an adversary can manipulate the commands and measurements related to SVCs, it is nearly impossible to hide the effect on other state variables and measurements in the system. The algorithms are developed mathematically using electrical quantities, making these schemes independent of the underlying Information and Communication Technologies (ICT) used. The rationale behind the choices made during the development of the algorithms are proven formally. Finally, two algorithms are formally proposed, which are easy to implement and computationally less intensive, when compared to iterative and multi-stage algorithms. These algorithms are then tested on various test-cases on the IEEE 118-bus system and found to be effective.**

***Index Terms*—false command injections, static var compensators, voltage control, reactive control.**

I. Introduction

In a power system, mechanisms pertaining to monitoring and control are crucial for safe and reliable operation. In the traditional paradigm, several of these mechanisms are performed manually, with minimal automation. However, in the case of modern automated power systems, or smart grids, such crucial operations are delegated to computers and automation. In the case of transmission systems, the automated control and operation rely on supervisory control and data acquisition systems (SCADA), which are implemented using appropriate Information and Communication Technology (ICT). Even though these systems enable reliable control and monitoring, they are prone to cyber attacks [1], [2]. As a result, the entire process of monitoring and control of transmission systems is prone to cyber attacks.

In a transmission system, voltage control is crucial for the safe and reliable operation. The voltage control is achieved through manipulation of reactive power flows. There are several devices capable of achieving voltage control, like On-load tap changing transformers (OLTCs), shunt capacitors, etc. However, with the development of Flexible AC Transmission Systems (FACTS) technology [3], [4], devices like Static VAR Compensator (SVC), which use power electronic switches with firing angle control, are widely used for voltage control. SVCs offer faster or near-instantaneous response to control command, when compared to OLTCs. In the context of smart grids, SVCs are either controlled by the operator, by relaying the appropriate firing angle commands through ICT channels, or by employing a closed loop control system. If an adversary has control of these command channels and relays malicious commands, the voltage control and subsequently the transmission grid gets disrupted. Hence, in this work, such attack scenarios are studied in detail and algorithms are developed to detect such attacks.

There has been considerable research on cybersecurity of smart grids. The attack that is well-addressed in the literature is False Data Injection (FDI) Attacks [5], [6]. In a smart grid operation, state estimator plays a significant role in subsequent operation and control decisions. FDI attacks are a class of attacks against state estimators such that the inherent Bad Data Detection (BDD) is evaded. In [5], conditions required to achieve FDI attacks against a DC state estimator are provided. In [6], the conditions required to conduct FDI attacks against a practical AC state estimators are established. In [7], an attack strategy is proposed to attack the state estimator without any knowledge of the Jacobian matrix and distribution of state variables. A strategy to launch FDI attacks by means of a low rank subspace of measurement mapping matrix, $\mathbf{H}$, is presented in [8]. An imperfect FDI attack against AC state estimator is proposed in [9], using forecasting technique based on historical measurement data. In [10], it is shown that FDI attacks against AC state estimators can be launched, with limited information and topological information. A multi-objective FDI attack strategy is presented in [11], where the attack model is represented as a multi-objective optimization problem. In order to mitigate the threats from FDI attacks, several detection schemes have been proposed. Many of these works consider a DC power flow model [12]–[14]. However, practical state estimators are based on AC load flow model. In [15], an online anomaly detection mechanism is proposed to detect FDI attacks, using load forecasting data, Phasor Measurement Units (PMU) data and generation schedules. A graph theory based approach is proposed in [16], in conjunction with outlier detection techniques applied to state estimator results or output. A machine learning based approach, ELM-Based OCON framework, is proposed in [17]. In [18], an efficient cross-silo federated learning scheme is proposed, with strong privacy preservation. The technique developed in [18] is shown

Shantanu Chakrabarty is with NCS Group, Singapore and adjunct with National University of Singapore

Biplab Sikdar is Professor in ECE department, National University of Singapore

to be effective against FDI attacks. In [19], the use of joint dynamic and static state estimation, i.e., weighted least squares and extended Kalman filter is proposed. This joint estimator is used with a cluster partitioning approach to detect FDI attacks. A data driven detection scheme for FDI attacks is proposed in [20], based on a combination of both supervised and unsupervised algorithms.

The literature in case of attacks involving false commands, unlike FDI attacks, is limited. Attacks involving injection of malicious commands are presented in general in [21]–[24]. In [21], [22], coordinated cyber-physical attacks, where the circuit breakers are maliciously tripped are discussed. The implications of the Ukraine attack, which is also a type of coordinated cyber-physical attacks, are discussed in [25]. The confidentiality and integrity of the control process in wide area control of smart grids is discussed in [23]. The work in [24], introduces the concept of false command data injection attacks. It proposes a futuristic hierarchical control, with decentralized local agents. These local agents have their own state estimators and controls. This work is done under the DC power flow model. The available literature on attacks against transmission control is very limited, especially in the context of voltage control. To the best of our knowledge, only [26]–[29] address related problems. In [26], security against cyber attacks directed at the voltage regulation (or control) mechanism is considered. In this work, attacks that maliciously modify sensor data are considered. These malicious data modifications are intended to either suppress transformer tap changes, when needed, or induce unnecessary tap changes, that can potentially result in catastrophic effects. A detection algorithm is proposed that is based on the current and previous voltages of the nodes. In [27], a novel FDI attack is proposed that can potentially disrupt the operation of smart grid equipped with Automatic Voltage Control (AVC). The attack strategy is modeled as a Partial Observable Markov Decision Process (POMDP). In order to solve the POMDP problem, a Q-learning algorithm with nearest sequence memories (NSM) is employed. Furthermore, a detailed analysis of this proposed attack strategy is also proposed. It can be seen that both [26] and [27] deal with attacks on voltage control induced by a FDI attack. In [28], attacks against tap changing transformers are considered in a transmission system. Unlike [26] and [27], here the attacks involving false command injection are considered. In FDI attacks against voltage control, the control action is enforced through falsification of sensor data, or voltage measurements, whereas in command injection attacks, the control action is under attack. In other words, the adversary takes over the commands. This attack is highly catastrophic, as the entire operational range is available to the adversary. In [28], an attack model to launch a stealthy attack against tap changing transformers is proposed. Moreover, a defensive strategy is also proposed to detect such malicious command injections. Though this work handles command injection attacks against voltage control, it does so only in the centralized control mechanism, with a EMS calculating and relaying appropriate commands. The case of local control system based tap changing is not considered. The work in [29] deals with command injection attacks against phase shifters. This work deals with attacks against real power flow control. Usually, in a transmission system, the active power control and voltage control are independent of each other, for most practical purposes.

In this paper, false command injection attacks are studied against SVCs. SVCs, like other devices used for voltage control, are controlled either using a centralized control or by means of a local closed loop control. The issue of false command injection is studied in both these modes of control. In both control mechanisms, stealthy attack strategies are explored and established. Based on the established atack models, two detection algorithms are proposed for each mode of operation. It is clear from the discussion before that protection of command channels are crucial, as an adversary with control to voltage control can severely affect system operation. Thus, such detection mechanisms are a necessity for modern devices like SVCs. The contributions of this paper are as follows:

1) Two detection algorithms are proposed to detect false command injection attacks against SVC in both modes of control. This is the first work to consider such attack scenarios;
2) The developed algorithms are based on strong mathematical validation and tested on the IEEE 118-bus system. The algorithms are
    a) single step,
    b) easy to implement,
    c) computationally less intensive, when compared to multi-stage and iterative algorithms, and
    d) independent of ICT.

When compared with other works that address cyber security of voltage control, the following observations are made: This paper deals with detection of stealthy attacks against the command channels of SVCs, in both centralized operation (EMS or SCADA), and in local control system enabled operation. This paper differs significantly from [26] and [27], because they deal with inducing an incorrect command due to false data injections. However, the work in this manuscript deals with attacks that take over the control command channels. This attack is known to have catastrophic effects. In [28], attacks against transformer taps are considered. These voltage control devices have a different operating principle when compared to SVCs. Tap changers have a set of discrete transformer tap steps that are enabled to control the reactive power flow, where as SVCs are usually power electronic devices that are enabled by changing the firing angle of switches. Furthermore, in [28], the issue of security of local control system enabled operation is not considered. And, in [29], phase shifters are considered, which are active power flow control devices. Hence, the issue of cyber-security SVCs, especially in transmission system control, has not been considered in existing literature. This paper attempts to fill this gap.

The rest of the paper is organized as follows: the necessary background information is presented in Section II-A. The attack scenarios against control of SVC are discussed in Section III. The development of the detection mechanism of false command injecitons in centralized control is presented in Section IV. Similarly, the development of the detection

mechanism in the case of local closed loop control is presented in Section V. The simulation studies are shown in Section VI. Finally, the conclusions are drawn in Section VII.

II. Background

In this section, the necessary background information relevant to this paper is presented. Static VAR Compensators (SVC) are introduced in Section II-A. This is followed by a brief introduction to command injection attacks and their difference from false data injection attacks in Section II-B.

A. Static VAR Compensators and their Applications in Smart Grids

SVCs are employed in transmission networks to regulate voltages (magnitudes) at nodes where they are connected. SVCs essentially contain a reactor (L) which is controlled by means of thyristors, known as Thyristor Controlled Reactors (TCR), connected in parallel with a capacitor (C) [4], [30]. The single-line circuit representation of a SVC, connected to node k of a transmission system, is shown in Figure 1. In Figure 1, the reactors L_{p1} and L_{p2} are employed to limit short-circuit currents. The TCR is controlled by means of firing-angle control, which renders a very high speed of response. SVCs are mainly used in transmission systems to control

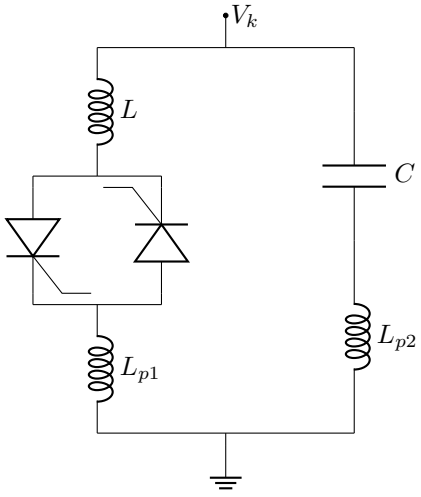


Figure 1: Single-line circuit representation of a SVC connected to node k.

voltages of nodes to specified set points. These devices are also capable of providing reactive power support (i.e., compensation). As discussed before, due to fast response, SVCs can provide dynamic reactive power support in contingency conditions. Additionally, SVCs can also reduce losses, increase transfer capability, and prevent active power losses. Thus, the areas of applications of SVCs in transmission systems are crucial for the safe and reliable operation of the transmission system.

For the purpose of discussion in this manuscript, the application of node voltage control is considered. In the context of voltage control, the firing angle of the SVC is changed to achieve the required voltage, also known as specified voltage. In this control mechanism, the EMS or control centre both measures and estimates the voltage of the node that is being controlled. Based on the difference between the specified voltage and the measured or estimated voltage, the firing angle of TCR in Figure 1 is updated. Such a control is usually referred to as centralized control. In this paper, the centralized control is referred to as Mode 1 control.

There are several instances where the SVCs are connected at the midpoint of the transmission line. Theoretically, the midpoint of the transmission line is the best location of the compensator [3], [4], as it ideally results in double power transfer capability. In such cases, SVCs are usually controlled using a local closed loop control system. The quantity that is controlled is measured and compared with the reference value (or specified value) and the error is used as the control signal or actuation signal to change the firing angle. In this paper, this type of control is referred to as either local control or Mode 2 control.

B. Command Injection Attacks and False Data Injection Attacks

In order to force or instigate a wrong control action, the adversary has to maliciously tamper or modify the data of one or more measurement devices or sensors. When a measurement(s) is manipulated, one or more state variables (usually, voltage magnitudes and angles at a node or bus) changes. In addition to state variables, other measurements related to these state variables also change. In case these measurements are not changed (rather, manipulated) according to system laws, like power and charge balance, or operating requirements and constraints, the Bad Data Detection (BDD) flags these measurements. As a result, these measurements are taken out of the estimation process or investigated. In order to carry out the injection of false data and evade BDD, all measurements that are a function of the changed state variables must be modified [5], [6]. Such attacks are known as False Data Injection (FDI) attacks. This attack is well-investigated in the literature. Whereas, in the case of malicious command injection based attacks, the adversary directly injects a malicious command, rather than indirectly inducing a wrong command by injecting false measurement data. In other words, the command channels are taken over by the adversary. These attacks are considered to have a very high impact [1] and are referred to as False Command Injection(FCI) Attacks. Usually, when the adversary injects a false command, the effects of this false command, i.e., the control parameter, like SVC firing angle in this context, and the controlled parameter, like the voltage of the node that is being controlled, will deviate from its set or selected value. Such deviations can alert the operator or the EMS. In order to remain hidden from the attention of the operator, it is necessary that the controlled and control parameters are kept close (considering the effect of noise in measurements and observation) to the value selected by the operator. This condition must be achieved while ensuring that the BDD is not triggered using conditions in [6]. Such a command injection attack is referred to as a stealthy FCI attack. The conditions needed to carry out such attacks in the case of SVCs are established in Section III-A.

III. Attack Scenarios

The attack scenarios differ based on the modes of operation of SVC in a transmission system. These modes are already discussed in Section II-A. In both these modes of operation, the effects of attacks on SVCs remain the same, as far as grid operation is concerned. However, the differences in these attacks lie in the mechanism of keeping these attacks hidden from the system operator, both at the substation and the control center.

A. Attacks under centralized control or Mode 1

In the centralized control, the voltages of the nodes, where voltage control is sought, are monitored. Based on the required or specified voltage and the state of the system, adequate setting of SVC (i.e., the firing angle, α) is determined by the EMS or control centre. The command to change the firing angle is relayed by the EMS to the node/substation containing the SVC. In this attack scenario, the adversary can take over this command channel and relay malicious commands. As discussed before in Section I, such malicious commands can result in adverse effects. It is worth noting that in the remainder of the paper, centralized control and Mode 1 are used interchangeably. Such attacks are referred to as False Command Injection (FCI) attacks [28], [29], [31].

In order to execute FCI attack and remain hidden from the attention of the operator or the EMS, the adversary has to atleast hide the change in firing angle (i.e., α) from the operator. For the analysis in this section, consider an SVC placed in a transmission network in Figure 2. Here, the SVC is connected to node k, which is connected to nodes $k_1, \cdots, k_a$. Let the voltage of node k be represented as $\mathbf{V_k} = |V_k| \angle \delta_k$.

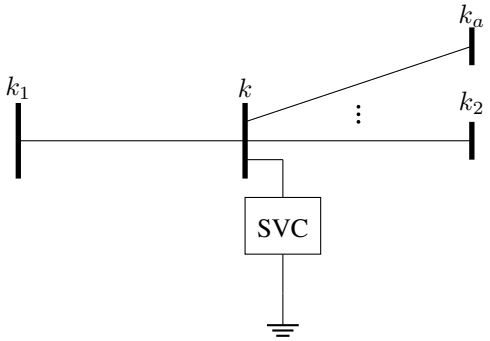


Figure 2: Illustration of the deployment of SVC in a transmission system for voltage control and reactive power support.

SVCs are used for voltage control such that a value of α^{sel} is chosen by the operator or EMS to get a voltage of $|V_k|^{sel}$. When the standard measurement model in (5) is used to estimate the states, due to noisy measurements, the estimated values of α and $|V_k|$, represented as α^{est} and $|V_k|^{est}$, mathematicaly differ from the selected values, i.e, $\alpha^{est} \neq \alpha^{sel}$, and $|V_k|^{est} \neq |V_k|^{sel}$. This relation also holds good when both α and $|V_k|$ are sensed or measured, due their own measurement or sensor noise. Due to noise in measurements, and subsequent deviation in estimation from its true value, we observe that the estimated values and true values are related as

$$\alpha^{est} = (1 \pm \epsilon_\alpha)\alpha^{sel} \tag{1}$$

$$|V_k|^{est} = (1 \pm \epsilon_V)||V_k|^{sel} \tag{2}$$

where, the factors ϵ_α and ϵ_V that govern the deviation of estimated values from true values. Usually, these factors are lower than the maximum error due to noise in the network. For a stealthy FCI attack, the adversary has to ensure that (1) and (2) must hold good. However, for all practical purposes of smart grid operation, this difference does not affect the control action or system overview. In other words, for all practical purposes, due to noise, the estimated or measured values are approximately equal to (or close to) the true values. It is important to note the measurement noise being talked about is the normal or natural errors and noise in measurements, not errors or false data injections.

In the attack scenario under centralized control or Mode 1 operation, the adversary chooses to hide the malicious change in firing angle, α, and the quantity that it controls, i.e., voltage at node k, $|V_k|$. To achieve such an objective, the adversary must ensure that the measured and estimated value of α and $|V_k|$ must appear close to the value selected by the operator (considering measurement error or noise), as discussed above. Consider the power balance equations pertaining to the part of transmission system shown in Figure 2. The power flow between node k and any other node incident at k can be written as

$$\mathbf{S^*_{kk_n}} = \mathbf{y_{km}}|V_k|^2 - \mathbf{y_{km}}\mathbf{V_k}^*\mathbf{V_{k_n}} \ \forall \ n = 1, \cdots, a. \tag{3}$$

Similarly, the power injection at node k be written as

$$\mathbf{S_k} = \sum_{n=1}^{a} \mathbf{S_{kk_n}} + \mathbf{S_{k0}}, \tag{4}$$

where, $\mathbf{S_{k0}}$ is the power injected by the SVC at bus k. As SVC is a reactive power compensation device, $\mathbf{S_{k0}}$ is reactive. SVC either generates or consumes reactive power based on the state of the system and the firing angle, α. The susceptance (magnitude) of SVC as a function of firing angle [30] is given by

$$B_{SVC} = \frac{1}{X_L X_C}\left[X_L - \frac{X_C}{\pi}\Big\{2(\pi - \alpha) + sin(2\alpha)\Big\}\right], \tag{5}$$

and the power injection of SVC, i.e., $\mathbf{S_{k0}}$ can be derived as

$$\mathbf{S_{k0}} = \frac{-j|V_k|^2}{X_L X_C}\left[X_L - \frac{X_C}{\pi}\Big\{2(\pi - \alpha) + sin(2\alpha)\Big\}\right]. \tag{6}$$

Under normal conditions, when there is no cyber attack, the relation between measurements and states can be represented as

$$\mathbf{z^{nor}} = \mathbf{h}(\mathbf{x^{nor}}) + \mathbf{e}, \tag{7}$$

where, the measurements pertaining to flows and injections in (3) and (4) are included in measurement vector $\mathbf{z} \in \mathbb{R}^{n_m}$, the superscript, nor, represents quantities under normal conditions and $\mathbf{e} \sim \mathcal{N}(0, \sigma)$ represents measurement noise. Let the state variable be denoted as $\mathbf{x}^{nor} =$

$\begin{bmatrix} x_1^{nor} & x_2^{nor} & \cdots & x_{k-1}^{nor} & \alpha^{nor} & |V_k|^{nor} & x_{k+2}^{nor} & \cdots & x_{n_s}^{nor} \end{bmatrix}^T$, such that the k^{th} and $(k+1)^{th}$ elements of the state vector, $\mathbf{x} \in \mathbb{R}^{n_s}$, are α^{nor}, and $|V_k|^{nor}$, respectively.

When there is a blatant cyber attack (where there is no effort made by the adversary to hide the intrusion), which results in a malicious change in firing angle, α, the measurement model in (7) can be written as

$$\mathbf{z^b} = \mathbf{h}(\mathbf{x^b}) + \mathbf{e}, \tag{8}$$

where, the superscript, b, represents quantities under a blatant attack. Here, the state vector is of the form, $\mathbf{x}^b = \begin{bmatrix} x_1^b & x_2^b & \cdots & x_{k-1}^b & \alpha^b & |V_k|^b & x_{k+2}^b & \cdots & x_{n_s}^b \end{bmatrix}^T$. Based on principles of power system operation, $\mathbf{x^{nor}}$, $\mathbf{x^b}$, (7) and (8), we get

$$||\mathbf{z^b} - \mathbf{z^{nor}}|| > 0. \tag{9}$$

In order to maliciously change the firing angle and keep this change hidden, the adversary has to ensure that the measured and estimated value of firing angle must remain close to the selected value, i.e., $\alpha^{hid} \approx \alpha^{nor}$. Such an attack is known as stealthy FCI attack [28], [32]. In such attacks, we get

$$\mathbf{z^{hid}} = \mathbf{h}(\mathbf{x^{hid}}) + \mathbf{e}, \tag{10}$$

where, superscript, hid, is used to denote quantities under a stealthy FCI. The state vector takes the form, $\mathbf{x}^{hid} = \begin{bmatrix} x_1^b & x_2^b & \cdots & x_{k-1}^b & \alpha^{nor} & |V_k|^{nor} & x_{k+2}^b & \cdots & x_{n_s}^b \end{bmatrix}^T$.

In order to ensure a stealthy attack, both the attention of the operator and the BDD must be evaded. To achieve this, according to [6], the following quantity,

$$\mathbf{A} = \mathbf{h}(\mathbf{x^{hid}}) - \mathbf{h}(\mathbf{x^b}), \tag{11}$$

must be added to (8). Based on the state vectors, $\mathbf{x}^{hid}$ and $\mathbf{x}^b$, it can be inferred that all entries of $\mathbf{A}$ are zero, except the ones that are functions of either α, $|V_k|$ or both. Moreover, similar to (9), from $\mathbf{x^b}$, $\mathbf{x^{hid}}$, (8) and (10), we get

$$||\mathbf{z^b} + \mathbf{A} - \mathbf{z^{nor}}|| > 0. \tag{12}$$

Hence, it can clearly be stated that in order to carry out a stealthy FCI attack on SVC, all quantities that are functions of either α or $|V_k|$ must be modified. In Figure 2, based on (3), (4), (5) and (6), the derived condition state that apart from α and $|V_k|$, $P_{kk_n} = \Re(\mathbf{S^*_{kk_n}})$ and $Q_{kk_n} = -\Im(\mathbf{S^*_{kk_n}})\ \forall\ n = 1, \cdots a$, and, $P_k = \Re(\mathbf{S^*_k})$ and $Q_k = -\Im(\mathbf{S^*_k})$.

The generalized condition to achieve stealthy attacks against SVC can thus be stated as a proposition as follows:

Proposition 1. *Consider a transmission system with n_{svc} SVCs used to control the voltage magnitudes of certain buses or nodes. Let the indices of these buses whose voltages are being controlled be represented by the set C such that $\overline{\overline{C}} = n_{svc}$. The voltages are controlled by a change in the firing angles of these SVCs, denoted as $\alpha_k\ \forall\ k = 1, \cdots, n_{svc}$. In order to launch a stealthy FCI attack on all the SVCs in the transmission system, α_k and $|V_m|$ and all the measurements that are functions of α_k and $|V_m|$ must be modified, $\forall$ $k = 1, \cdots, n_{svc}$ and $m \in C$.*

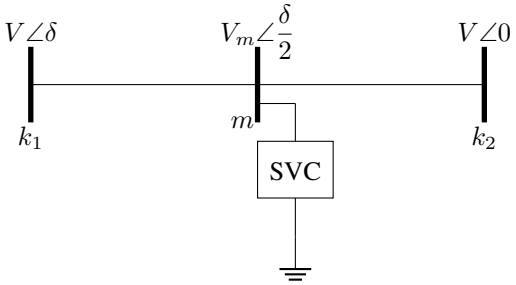


Figure 3: SVC connected to the midpoint of a symmetric lossless transmission line.

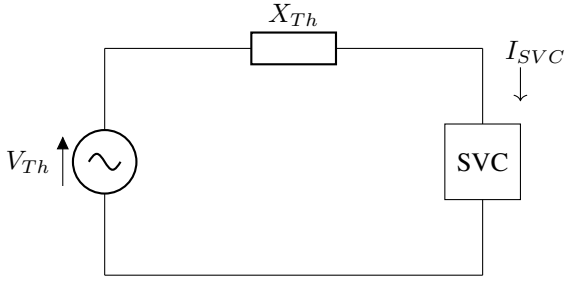


Figure 4: The Thevenin's equivalent circuit at node m of the system in Figure 3.

B. Attacks under local control systems or Mode 2

As discussed before in Section II-A, SVCs are also controlled using local closed loop control systems [4]. From (5), it is clear that the admittance is a function of firing angle. Hence, determination of appropriate admittance and consequently, the required change in firing angle of thyristors in Figure 1 is necessary to carry out voltage control. Consider a SVC place at the midpoint of a symmetric line in Figure 3. The Thevenin's equivalent circuit at the SVC in Figure 3 is shown in Figure 4. In Figure 4, the Thevenin's voltage is given by $V_{Th} = \dfrac{V cos(\frac{\delta}{2})}{cos(\frac{\theta}{2})}$, and the Thevenin's equivalent reactance is given by $Z_{Th} = \dfrac{Z_n}{2} tan(\frac{\theta}{2})$ [4]. Z_n in V_{Th} is the surge impedance or the natural impedance of the line between nodes k_1 and k_2 in Figure 3 and $\theta = \beta l = 2\pi f\sqrt{lc}$ in the expression of Z_{Th}, where l and c are the inductance and capacitance per unit length and f is the frequency of the supply voltage, usually 50 or 60 Hz. β is commonly known as the phase constant.

From Figure 4, the voltage at the SVC or at the midpoint is

$$V_{SVC} = V_{Th} - X_{Th} I_{SVC}, \tag{13}$$

which represents the system characteristics.

The $V - I$ (Voltage-Current) characteristics of the SVC and the system characteristics in (13) are drawn in Figure 5. From Figure 5, we get

$$V_{SVC} = V_{ref} + I_{SVC} X_S, \tag{14}$$

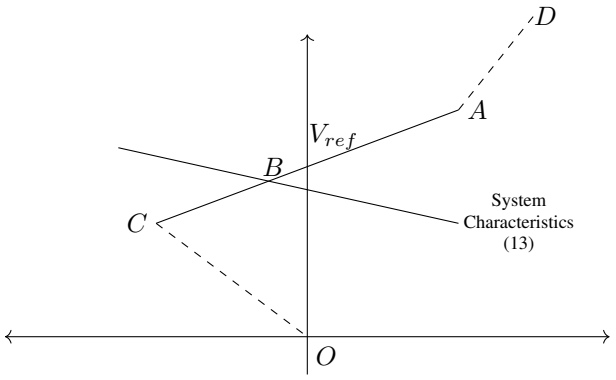


Figure 5: SVC and system $V-I$ characteristics.

where, V_{ref} represents the voltage at $I_{SVC}=0$, and X_S is the slope of line ABC. The intersection point of (13) and (14) is represented by point B, indicative of the operating point. The compensation is done by means of variation of the SVC admittance. Based on the convention that SVC current is positive when the circuit is inductive, we get

$$I_{SVC} = -B_{SVC}V_{SVC}. \tag{15}$$

From (5), it is clear that the admittance is a function of the firing angle. Hence, determination of appropriate admittance and consequently, the required change in firing angle of thyristors in Figure 1 is necessary to carry out voltage control. The voltage is controlled dynamically, based on the value of V_{SVC}, by means of a control system shown in Figure 6. Here, $H_M(s)$ is a low pass filter of either order 1 or 2, $\dfrac{k_R}{(1+sT_R)}$ represents voltage regulator, with $k_R = \dfrac{1}{X_s}$ and $T_R = \dfrac{K_I}{k_R}$ (K_I is integrator gain), T_d is transport delay due to discrete nature of firing pulses and T_b represents average delay from the time of delivering the order or command.

The method of control in Figure 6 is not immune to cyber-attacks [33]–[36]. There are several ways in which a control system can be compromised [33]. The attacks aimed at disruption of these control systems can potentially affect the sensor or feedback signals, the control signals, or the control unit itself. A local closed loop control systems is usually implemented using closed loop control modules [37], which are specialized Programmable Logic Controllers (PLCs). This module is usually a system with two components (nodes), i.e., process and the controller, that interact with each other through sensor data and control inputs. Such configurations are vulnerable to cyber attacks [38], [39], for instance, Denial of Service (DoS) and Man-in-the-Middle attacks (MiTM) [39]. A MiTM attack can disrupt both the feedback signal and the control signals. For the control system in Figure 6, two possible attacks can be inferred, based on the above discussion. They are as follows:

- Falsification of the voltage (magnitude) that is fed back to the control system, i.e., V_{SVC};
- Falsification of the actuation command to change the firing angle in Figure 1, i.e., B_{SVC} in Figure 6.

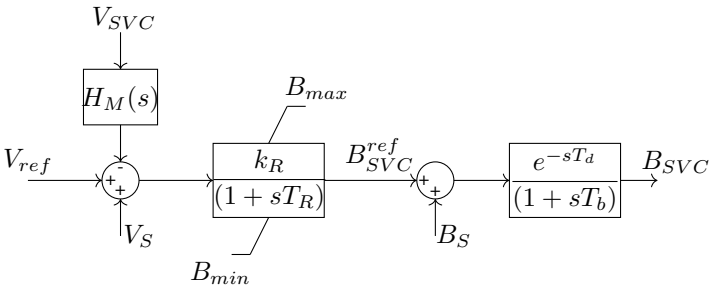


Figure 6: The control system representation of voltage control in SVC.

These attacks can result in scenarios where the design of the control system is exploited to force voltages that are outside the acceptable limits. These attack scenarios are further discussed in detail in Section V.

IV. Detection Mechanisms to prevent cyber-attacks against SVCs in Mode 1 operation or centralized control

In this section, a detection algorithm is proposed to mitigate attacks stated in Proposition 1, in Section III-A. The detection metrics, represented as a function of state variables, are developed in Section IV-A. The mathematical justification for the applicability of the developed metrics is presented in Section IV-B. The detection algorithm is finally presented in Section IV-C.

A. Detection Metrics

From Figure 2, the apparent power flow from node k to any node k_n, incident at k (i.e., $k_n \in k$), given by (3), is rewritten as

$$\mathbf{S^*_{kk_n}} = \mathbf{y_{km}}|V_k|^2 - \mathbf{y_{km}}\mathbf{V_k}^*\mathbf{V_{k_n}} \ \ \forall \ n = 1, \cdots, a.$$

In voltage control at node k, $|V_k|$ is regulated at its specified value, under normal conditions (i.e., $|V_k|^n$) and falsified to represent this specified value. Dividing (3) by $|V_k|^2$, we get

$$\begin{aligned}\frac{\mathbf{S^*_{kk_n}}}{|V_k|^2} &= \mathbf{y_{kk_n}}\Big(1 - \frac{\mathbf{V_{kk_n}}}{\mathbf{V_k}}\Big) \\ &= \mathbf{y_{kk_n}}\Big(1 - \frac{|V_{k_n}|}{|V_k|}e^{j(\delta_{k_n}-\delta_k)}\Big) \ \ \forall \ n = 1, \cdots, a. \end{aligned} \tag{16}$$

The power injected by the SVC, i.e., $\mathbf{S_{k0}}$ is given by (6). Dividing (6) by $|V_k|^2$ and taking the conjugate, we get

$$\frac{\mathbf{S^*_{k0}}}{|V_k|^2} = \frac{j}{X_L X_C}\left[X_L - \frac{X_C}{\pi}\Big\{2(\pi-\alpha_k)+sin(2\alpha_k)\Big\}\right]. \tag{17}$$

The power injection at the SVC bus (or node), i.e., node k, is given by (4). Dividing $\mathbf{S_k}^*$ by $|V_k|^2$, we get

$$\begin{aligned}\frac{\mathbf{S^*_k}}{|V_k|^2} &= \sum_{n=1}^{a}\mathbf{y_{kk_n}}\Big(1 - \frac{\mathbf{V_{kk_n}}}{\mathbf{V_k}}\Big) \\ &+ \frac{j}{X_L X_C}\left[X_L - \frac{X_C}{\pi}\Big\{2(\pi-\alpha_k)+sin(2\alpha_k)\Big\}\right]. \end{aligned} \tag{18}$$

We define the magnitude of the quantities in (16) and (18) as follows:

$$\gamma_{kk_n} = \left|\frac{\mathbf{S^*_{kk_n}}}{|V_k|^2}\right| = \left|\frac{\mathbf{S_{kk_n}}}{|V_k|^2}\right| \ \forall\ n = 1, \cdots, a; \tag{19}$$

$$\gamma_k = \left|\frac{\mathbf{S^*_k}}{|V_k|^2}\right| = \left|\frac{\mathbf{S_k}}{|V_k|^2}\right|. \tag{20}$$

As discussed in Section III-A, the value of firing angle α_k is determined by the operator or EMS depending on the generation-load pattern and the required voltage, $|V_k|^n$ (using notation introduced in Section III-A). The values of γ_{kk_n} and γ_k can be determined using (16) and (18), respectively, and recorded every time the firing angle is determined and relayed. These recorded values are denoted by $\gamma^{ref}_{kk_n}$ and γ^{ref}_k, respectively.

The detection metric is formulated as the Manhattan distance between sets, $\{\{\gamma_{kk_n} : n = 1, \cdots, a\}, \gamma_k\}$ and $\{\{\gamma^{ref}_{kk_n} : n = 1, \cdots, a\}, \gamma^{ref}_k\}$, given by

$$\Gamma_k = \sum_{n=1}^{a} |\gamma_{kk_n} - \gamma^{ref}_{kk_n}| + |\gamma_k - \gamma^{ref}_k|. \tag{21}$$

It is clear from (21) that under ideal conditions, in absence of noise in measurements, the value of Γ_k is 0, when there is no cyber attack or malicious change in α_k. Thus, a non-zero value under ideal conditions is indicative of a malicious change or cyber-attack. This is established mathematically in Section IV-B.

B. Mathematical analysis and justification of using Γ_k as detection metric

In order to establish the effectiveness of a detection algorithm that incorporates Γ_k in (21), it is essential to establish the applicability of Γ_k as a classifier for attacks. The applicability of Γ_k as a detection metric is established mathematically in this section through Propositions 2 and 3.

Proposition 2. *Let Γ^{nor}_k (with superscript, nor) correspond to the value of Γ_k in (21) under normal conditions, when there is no cyber attack. Similarly, let Γ^{hid}_k (with superscript, hid) correspond to the value of Γ_k estimated under a stealthy cyber-attack proposed in Proposition 1. Under ideal conditions, with noiseless measurements, $\Gamma^{nor}_k = 0$ and $\Gamma^{hid}_k > 0$.*

Proof. Under normal conditions, in absence of cyber attacks, with noiseless measurements, it can be directly inferred that

$$\gamma^{nor}_{kk_n} = \gamma^{ref}_{kk_n} \ \forall\ n = 1, \cdots, a, \text{and}$$
$$\gamma^{nor}_k = \gamma^{ref}_k.$$

Hence, $\Gamma^{nor}_k = 0$.

When a stealthy cyber-attack in Proposition 1 is carried out, the adversary ensures that the state variables, α_k and $|V_k|$ remain close to their specified values, α^{ref}_k and $|V_k|^{ref}$, respectively. As there are no noise in measurements, we get

$$\alpha^{hid}_k = \alpha^{nor}_k = \alpha^{ref}_k, \text{and}$$
$$|V_k|^{hid} = |V_k|^{nor} = |V_k|^{ref}.$$

Also, other state variables in (16) and (18) remain at the values, caused by the stealthy attack in Proposition 1. Using the same notations of Section III-A, the other state variables in (16) and (18) are given by $|V_{k_n}|^b$ and $\delta^b_{k_n}$, $\forall\ n = 1, \cdots, a$.

It is worth noting that $\mathbf{y_{kk_n}}\ \forall\ n = 1, \cdots, a$ remain unchanged due to cyber-attack. So, representing (16) as

$$\frac{\mathbf{S^*_{kk_n}}}{|V_k|^2} = \mathbf{y_{kk_n}}\beta_{\mathbf{kk_n}}, \tag{22}$$

$$\implies \left|\frac{\mathbf{S^*_{kk_n}}}{|V_k|^2}\right| = |\mathbf{y_{kk_n}}||\beta_{\mathbf{kk_n}}|, \forall\ n = 1, \cdots, a, \tag{23}$$

such that, further analysis is only performed on the term, $\beta_{\mathbf{kk_n}}\ \forall\ n = 1, \cdots, a$.

When a stealthy cyber-attack, proposed in Proposition 1 is carried out, we have

$$|\beta_{\mathbf{kk_n}}|^{hid} = \Bigg[2 + \frac{(|V_{k_n}|^{hid})^2}{(|V_k|^n)^2} - 2\frac{|V_{k_n}|^{hid}}{|V_k|^n}\big(cos(\delta^{hid}_{k_n} - \delta^{hid}_k) + sin(\delta^{hid}_{k_n} - \delta^{hid}_k)\big)\Bigg]^{\frac{1}{2}}. \tag{24}$$

Similarly, during the selection of α_k to meet the specified voltage $|V_k|^{sp}$, we get

$$|\beta_{\mathbf{kk_n}}|^{ref} = \Bigg[2 + \frac{(|V_{k_n}|^{ref})^2}{(|V_k|^{ref})^2} - 2\frac{|V_{k_n}|^{ref}}{|V_k|^{ref}}\big(cos(\delta^{ref}_{k_n} - \delta^{ref}_k) + sin(\delta^{ref}_{k_n} - \delta^{ref}_k)\big)\Bigg]^{\frac{1}{2}}. \tag{25}$$

As discussed before, we have

$$|V_{k_n}|^{hid} \neq |V_{k_n}|^{ref}, \text{and}$$
$$\delta^{hid}_{k_n} \neq \delta^{ref}_{k_n}, \forall\ n = 1, \cdots, a.$$

Thus, from (24) and (25), we can infer that

$$|\beta_{\mathbf{kk_n}}|^{hid} \neq |\beta_{\mathbf{kk_n}}|^{ref}$$
$$\implies \gamma^{hid}_{kk_n} \neq \gamma^{ref}_{k_n},$$
$$\implies |\gamma^{hid}_{kk_n} - \gamma^{ref}_{kk_n}| > 0, \forall\ n = 1, \cdots, a. \tag{26}$$

The steps used to establish (26) can be similarly applied to establish

$$|\gamma^{hid}_k - \gamma^{ref}_k| > 0, \forall\ n = 1, \cdots, a. \tag{27}$$

From (21), (26) and (27), we can write

$$\Gamma^{hid}_k > 0.$$

Hence proved. □

Proposition 3. *Using the notations in Section III-A and Proposition 2, under the presence of noise in measurements, it can be stated that $\Gamma^{hid}_k > 0$.*

Proof. The measurement model pertaining to quantities in Γ_k in (21), when estimated by the EMS during selection of firing angle, α_k, can be written as

$$\begin{bmatrix} P^{ref}_{kk_1} \\ \vdots \\ P^{ref}_{kk_n} \\ Q^{ref}_{kk_1} \\ \vdots \\ Q^{ref}_{kk_n} \\ P^{ref}_{k} \\ Q^{ref}_{k} \end{bmatrix} = \begin{bmatrix} h^{Re}_{kk_1}(\mathbf{x^{nor}}) \\ \vdots \\ h^{Re}_{kk_n}(\mathbf{x^{nor}}) \\ h^{Im}_{kk_1}(\mathbf{x^{nor}}) \\ \vdots \\ h^{Im}_{kk_n}(\mathbf{x^{nor}}) \\ h^{Re}_{k}(\mathbf{x^{nor}}) \\ h^{Im}_{k}(\mathbf{x^{nor}}) \end{bmatrix} + \mathbf{e_{\Gamma_k}}, \tag{28}$$

where the noise vector, $\mathbf{e_{\Gamma_k}} \sim \mathcal{N}(0,1)$.

Under a blatant attack, where a malicious command changes the firing angle, α_k, and the attack is not hidden from the operator and EMS, the measurement model is written as

$$\begin{bmatrix} P^{b}_{kk_1} \\ \vdots \\ P^{b}_{kk_n} \\ Q^{b}_{kk_1} \\ \vdots \\ Q^{b}_{kk_n} \\ P^{b}_{k} \\ Q^{b}_{k} \end{bmatrix} = \begin{bmatrix} h^{Re}_{kk_1}(\mathbf{x^{b}}) \\ \vdots \\ h^{Re}_{kk_n}(\mathbf{x^{b}}) \\ h^{Im}_{kk_1}(\mathbf{x^{b}}) \\ \vdots \\ h^{Im}_{kk_n}(\mathbf{x^{b}}) \\ h^{Re}_{k}(\mathbf{x^{b}}) \\ h^{Im}_{k}(\mathbf{x^{b}}) \end{bmatrix} + \mathbf{e_{\Gamma_k}}. \tag{29}$$

From the conditions to carry out stealthy command injection attack established in Section III-A and Proposition 1,

$$\zeta_{\mathbf{k}} = \begin{bmatrix} h^{Re}_{kk_1}(\mathbf{x^{hid}}) \\ \vdots \\ h^{Re}_{kk_n}(\mathbf{x^{hid}}) \\ h^{Im}_{kk_1}(\mathbf{x^{hid}}) \\ \vdots \\ h^{Im}_{kk_n}(\mathbf{x^{hid}}) \\ h^{Re}_{k}(\mathbf{x^{hid}}) \\ h^{Im}_{k}(\mathbf{x^{hid}}) \end{bmatrix} - \begin{bmatrix} h^{Re}_{kk_1}(\mathbf{x^{b}}) \\ \vdots \\ h^{Re}_{kk_n}(\mathbf{x^{b}}) \\ h^{Im}_{kk_1}(\mathbf{x^{b}}) \\ \vdots \\ h^{Im}_{kk_n}(\mathbf{x^{b}}) \\ h^{Re}_{k}(\mathbf{x^{b}}) \\ h^{Im}_{k}(\mathbf{x^{b}}) \end{bmatrix}, \tag{30}$$

must be added to (29).

Adding $\zeta_{\mathbf{k}}$ in (30) to (29), we get

$$\begin{bmatrix} P^{b}_{kk_1} \\ \vdots \\ P^{b}_{kk_n} \\ Q^{b}_{kk_1} \\ \vdots \\ Q^{b}_{kk_n} \\ P^{b}_{k} \\ Q^{b}_{k} \end{bmatrix} + \zeta_{\mathbf{k}} = \begin{bmatrix} h^{Re}_{kk_1}(\mathbf{x^{hid}}) \\ \vdots \\ h^{Re}_{kk_n}(\mathbf{x^{hid}}) \\ h^{Im}_{kk_1}(\mathbf{x^{hid}}) \\ \vdots \\ h^{Im}_{kk_n}(\mathbf{x^{hid}}) \\ h^{Re}_{k}(\mathbf{x^{hid}}) \\ h^{Im}_{k}(\mathbf{x^{hid}}) \end{bmatrix} + \mathbf{e_{\Gamma_k}}. \tag{31}$$

It can be seen from the measurement model in (31) that the system states and consequently measurements have changed from their normal values. From (12), we get

$$\left\| \begin{bmatrix} P^{b}_{kk_1} \\ \vdots \\ P^{b}_{kk_n} \\ Q^{b}_{kk_1} \\ \vdots \\ Q^{b}_{kk_n} \\ P^{b}_{k} \\ Q^{b}_{k} \end{bmatrix} + \zeta_{\mathbf{k}} - \begin{bmatrix} P^{ref}_{kk_1} \\ \vdots \\ P^{ref}_{kk_n} \\ Q^{ref}_{kk_1} \\ \vdots \\ Q^{ref}_{kk_n} \\ P^{ref}_{k} \\ Q^{ref}_{k} \end{bmatrix} \right\| > 0$$

$$\implies \left\| \begin{bmatrix} P^{hid}_{kk_1} \\ \vdots \\ P^{hid}_{kk_n} \\ Q^{hid}_{kk_1} \\ \vdots \\ Q^{hid}_{kk_n} \\ P^{hid}_{k} \\ Q^{hid}_{k} \end{bmatrix} - \begin{bmatrix} P^{ref}_{kk_1} \\ \vdots \\ P^{ref}_{kk_n} \\ Q^{ref}_{kk_1} \\ \vdots \\ Q^{ref}_{kk_n} \\ P^{ref}_{k} \\ Q^{ref}_{k} \end{bmatrix} \right\| > 0. \tag{32}$$

Thus, from (16), (18), (19), (20) and (32), it can be inferred that:

$$\mathbf{\Gamma^{hid}_k} > 0.$$

Hence proved. □

Hence, it can be seen that in presence noisy measurements, the detection metric is capable of classifying a stealthy attack proposed in Proposition 1.

C. Detection algorithm

The proposed detection algorithm is based on the application of detection metric, Γ_k in (21). Based on Propositions 2 and 3 and their proofs, it is clear to see that there are no iterative steps needed to carry out the detection algorithm. Thus, the algorithm is simple to implement. The steps of the proposed algorithm are presented in Algorithm 1.

Algorithm 1: Proposed algorithm for detection of false command injection attacks against SVC in Mode 1 operation or centralized control.

Data: The reference values, $\gamma^{ref}_{kk_n} \ \forall \ k = 1, \cdots, a$, γ^{ref}_{k} and the predefined threshold T_h
Output: Trigger
Calculate Γ_k using (21);
if $\Gamma_k > T_h$ **then**
    Trigger = 1;
    A stealthy attack is detected against SVC.;
else
    Trigger = 0;
    go back to step 1;

An estimation of the computational effort for Algorithm IV-C, is provided in terms of number of floating point operations). Without any loss of generality, we consider any

operation ($+, -, \times, /, >, <, \sqrt{a}$) on real numbers as 1 floating point operation [40]. It is worth noting that floating point operations can also be calculated in terms of complex operations. However, real operations are considered in this context. As an example, a complex multiplication of two numbers involves 1 complex operation, but 6 real operations. Hence, in this context, a complex multiplication is considered to have a computational effort of 6 floating point operations. The real and reactive power components in $\mathbf{S^*_{kk_n}}$, and $|\mathbf{S^*_{kk_n}}|$, are available from the state estimator at the EMS. Hence, the computational effort to estimate γ_{kk_n} in (19), is 1 floating point operation, as it essentially involves a division operation. Similarly, from the expressions of γ_k, it can be inferred that the computational effort to estimate γ_k is 1 floating point operation. Now, the computational effort to estimate $|\gamma_{kk_n} - \gamma^{ref}_{kk_n}|$ is 3 floating point operations (1 for subtraction and 2 for modulus or absolute number, considering 1 floating point operation for comparison, and 1 floating point operation for sign change by multiplication with -1). Similarly, the computational effort to estimate γ_{kk_n} is 1 floating point operation, and to estimate $|\gamma_k - \gamma^{ref}_k|$, it is 3 floating point operations. Hence, the total computational effort to calculate for one SVC is given by $4(a+1)$. For the comparison with the threshold value, we need to account for 1 floating point operation. For n_{svc} SVCs, we have $(4a+5)n_{svc}$. As this algorithm is one-step algorithm, where Γ_k is estimated for every window, and compared with the threshold value for every observation window, the computational effort remains constant. As an example, let us consider a SVC placed at node k. Usually, in a transmission system, each node is usually connected to $2-3$ nodes, thus, $a \approx 3$. So, for a SVC at node k, we can execute Algorithm 1 with only 17 floating point operations. This results in lower computational effort, when compared to algorithms involving iterative computations and multiple stages.

From the system measurement models in (7) and estimation algorithms, it can be inferred that at any given instance, the exact value of state variables cannot be estimated. Furthermore, the exact value of measurements cannot be obtained. This is mainly due to noisy measurements and other practical aspects of a transmission system. Hence, when a adversary introduces changes in the firing angle that are very small, the changes introduced in the system measurements can be in the order or close to the order of measurement noise and estimation errors. In other words, there are cases where the minimum values of Γ_k in case of attack scenarios is less than the maximum values of Γ_k in normal scenarios. It is worth noting that in practical transmission system operation, any change in system operating conditions that introduces changes in measurements, in the order of noise or error, does not cause any disruption in system operation. Hence, theoretically or mathematically, it can be stated that the developed Algorithm 1 cannot capture changes reliably in all observation windows for very small malicious change in firing angle. However, from a practical standpoint, this limitation does not affect the efficacy of the algorithm. This is mainly because system noise is a universal phenomenon, in all transmission systems. It is also worth noting that the noise varies from system to system and sensitivities of various quantities to a change in system state also varies across different transmission system. Hence, a threshold to classify the attack and normal scenarios is needed. This is discussed in Section VI-A, with discussions on efficacy of the developed Algorithm 1. However, when there is an appreciable change (usually, above the order of noise), the detection metric, Γ_k in (21) reliably classifies all the attacks from normal scenario, as seen in Figure 8.

V. Detection mechanism to mitigate cyber-attacks against SVCs in Mode 2 operation

In this section, another detection algorithm is proposed for attacks against Mode 2 operation, discussed in Section III-B. The approach is based on development of detection metrics, which are a function of electrical quantities. These metrics are developed in Section V-A. These metrics are justified mathematically in Section V-B. Finally, the detection algorithm is proposed in Section V-C.

A. Detection Metrics

The closed loop control system, used to enable SVCs to dynamically control voltages, is already presented in Figure 6, and the following relation holds good:

$$B_{min} \leq \left[V_{ref} + V_S - V_{SVC} H_M(s)\right] \frac{k_R}{(1+sT_R)} = B^{ref}_{SVC} \leq B_{max}. \quad (33)$$

From Figure 6, it can be deduced that

$$B_{SVC} = \frac{e^{-sT_d}}{(1+sT_b)} B^{ref}_{SVC}. \quad (34)$$

From (33) and (34), it is clear that a malicious tampering of either the feedback measurement, V_{SVC}, or the actuation signal, B^{ref}_{SVC}, can result in voltages and reactive power profile that are not acceptable.

Consider a SVC placed at the mid-point of a transmission line, for mid-point regulation. Let $\mathbf{y_{k_1k_2}} (= \dfrac{1}{\mathbf{z_{k_1k_2}}})$ be the line admittance, $\mathbf{y_{SVC}}$ be the effective admittance of the SVC and $\mathbf{y_{k_1o}}$ and $\mathbf{y_{k_2o}}$ be the line charging admittances. The Star-Delta representation of this network, for the purpose of analysis is shown in Figure 7. The equivalent admittances in the delta network in Figure 7b are as follows:

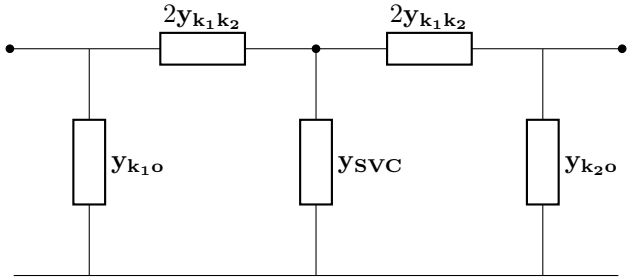
$$\mathbf{y_{k_1d}} = \mathbf{y_{k_2d}} = \frac{2\mathbf{y_{k_1k_2}}\mathbf{y_{SVC}}}{(\mathbf{y_{SVC}} + 4\mathbf{y_{k_1k_2}})},$$
$$\mathbf{y_{Sd}} = \frac{4\mathbf{y_{k_1k_2}}^2}{(4\mathbf{y_{k_1k_2}} + \mathbf{y_{SVC}})}. \quad (35)$$

Application of Kirchoff's Current Law (KCL) at node m in Figure 7a, results in

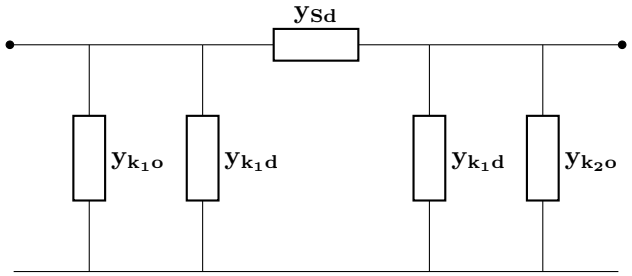
$$\mathbf{V_m} = \frac{2\mathbf{y_{k_1k_2}}(\mathbf{V_{k_1}} + \mathbf{V_{k_2}})}{(4\mathbf{y_{k_1k_2}} + \mathbf{y_{SVC}})}. \quad (36)$$

From (36), it can be seen that measurements from two PMUs, placed at buses k_1 and k_2, can be used to estimate the magnitude of $\mathbf{V_m}$. Similarly, the current flowing from node k_1 towards k_2, through the transmission line, in Figure 7b, can be expressed as

$$\mathbf{I_{k_1k_2}} = \mathbf{V_{k_1}}(\mathbf{y_{k_1d}} + \mathbf{y_{Sd}}) - \mathbf{V_{k_2}}\mathbf{y_{Sd}}, \quad (37)$$



(a) Star Connection



(b) Delta Connection

Figure 7: Equivalent circuit representations of SVC connected to the mid-point of a transmission line.

and similarly, the current flowing from node k_2 towards k_1, can be expressed as

$$\mathbf{I_{k_2k_1}} = \mathbf{V_{k_2}}(\mathbf{y_{k_2d}} + \mathbf{y_{Sd}}) - \mathbf{V_{k_1}}\mathbf{y_{Sd}}. \tag{38}$$

Application of KVL in Figure 7a results in

$$\begin{aligned}\mathbf{V_m} &= \mathbf{V_{k_1}} - 0.5\mathbf{I_{k_1k_2}}\mathbf{z_{k_1k_2}} \\ &= \mathbf{V_{k_2}} - 0.5\mathbf{I_{k_2k_1}}\mathbf{z_{k_1k_2}}.\end{aligned} \tag{39}$$

From (39), it can be seen that with PMUs at buses k_1 and k_2 measuring the quantities, $\mathbf{V_{k_1}}$, $\mathbf{I_{k_1k_2}}$, $\mathbf{V_{k_2}}$ and $\mathbf{I_{k_2k_1}}$, the magnitude of voltage at the midpoint, i.e., $\mathbf{V_m} = |V_m|\angle\delta_m$, can be estimated.

The detection metric in this mode of operation is formulated for both the cases in (36) and (39) as follows:

- When phasor measurements pertaining to voltages at k_1 and k_2 are used to estimate $\mathbf{V_m}$, the detection metric can be formulated as

$$\rho_m = \left| \left| \frac{2\mathbf{y_{k_1k_2}}(\mathbf{V_{k_1}} + \mathbf{V_{k_2}})}{(4\mathbf{y_{k_1k_2}} + \mathbf{y_{SVC}})} \right| - V_m^{meas} \right|. \tag{40}$$

- When phasor measurements, $\mathbf{V_{k_1}}$, $\mathbf{I_{k_1k_2}}$, $\mathbf{V_{k_2}}$ and $\mathbf{I_{k_2k_1}}$ are available, the detection metric can be formulated as

$$\begin{aligned}\psi_m = &\left| \left| (\mathbf{V_{k_1}} - 0.5\mathbf{I_{k_1k_2}}\mathbf{z_{k_1k_2}}) \right| - V_m^{meas} \right| \\ &+ \left| \left| (\mathbf{V_{k_2}} - 0.5\mathbf{I_{k_2k_1}}\mathbf{z_{k_1k_2}}) \right| - V_m^{meas} \right|.\end{aligned} \tag{41}$$

In both (40) and (41), V_m^{meas} is the measured voltage at the midpoint, available to control system as feedback signal. These detection metrics, in (40) and (41), will be the basis for the detection algorithm to detect attacks presented in Section III-B. In order to launch such attacks and stay hidden from the operator, it is necessary that the adversary ensures that the measured voltage at SVC, i.e., V_m^{meas} remains close to their rated or selected or reference values. For reference, such attacks are referred to as stealthy attacks. The detection algorithm is designed to detect such attacks.

B. Mathematical justification of using ρ_m and ψ_m as detection metrics

In order to develop a detection algorithm that uses ρ_m and ψ_m, in (40) and (41), respectively, it is necessary to prove their effectiveness mathematically. This is done through Proposition 4 as follows:

Proposition 4. *Let ρ_m^{nor} and ψ_m^{nor} (with superscript, nor) be the values of ρ_m and ψ_m, when there is no cyber-attack. Similarly, let ρ_m^{hid} and ψ_m^{hid} (with superscript, hid) be the values of ρ_m and ψ_m, under a stealthy cyber-attack. Under ideal conditions, when there is no noise in measurements, it can be stated that $\rho_m^{nor} = \psi_m^{nor} = 0$. Similarly, under stealthy attacks and ideal measurements, when either the feedback signal, V_m^{meas}, or actuation signal to change the firing angle is maliciously modified, it can be stated that $\rho_m^{hid} > 0$ and $\psi_m^{hid} > 0$.*

Proof. When there is no cyber-attack, it can be clearly inferred from (36) and (40) that $\rho_m = 0$, and $\psi_m = 0$.

Consider a malicious change in feedback measurement, V_m^{meas}, to say, $V_m^{meas,hid}$ (similarly, the value of V_m^{meas} under normal conditions is denoted by $V_m^{meas,nor}$). The KCL in Figure 7a would still result in true relation in (36), as

$$\mathbf{V_m^{nor}} = \frac{2\mathbf{y_{k_1k_2}}(\mathbf{V_{k_1}^{nor}} + \mathbf{V_{k_2}^{nor}})}{(4\mathbf{y_{k_1k_2}} + \mathbf{y_{SVC}})}, \tag{42}$$

using notations defined above. As (42) represents the true relationship, from (40), it can be seen that

$$\rho_m^{hid} = |V_m^{meas,nor} - V_m^{meas,hid}| > 0. \tag{43}$$

Under this cyber-attack, when KVL is applied in Figure 7a, the true relationship still exists as

$$\begin{aligned}\mathbf{V_m^{nor}} &= \mathbf{V_{k_1}^{nor}} - 0.5\mathbf{I_{k_1k_2}^{nor}}\mathbf{z_{k_1k_2}} \\ &= \mathbf{V_{k_2}^{nor}} - 0.5\mathbf{I_{k_2k_1}^{nor}}\mathbf{z_{k_1k_2}}.\end{aligned} \tag{44}$$

Even in (44), the true values of quantities still hold good. From (41), it can be seen again that

$$\psi_m^{hid} = 2 \times |V_m^{meas,nor} - V_m^{meas,hid}| > 0. \tag{45}$$

Consider the attack where the adversary manipulates the control signal, to change the firing angle. Even in this attack scenario, to remain hidden from the operator, the feedback measurement, V_m^{meas}, must remain close to its normal value, i.e, $V_m^{meas,nor}$. Under this attack scenario, KCL in Figure 7a would reflect true relation resulting from the malicious change in firing angle, i.e,

$$\mathbf{V_m^{hid}} = \frac{2\mathbf{y_{k_1k_2}}(\mathbf{V_{k_1}^{hid}} + \mathbf{V_{k_2}^{hid}})}{(4\mathbf{y_{k_1k_2}} + \mathbf{y_{SVC}})}, \tag{46}$$

using notations defined above. From (40) and (46), it can be seen that

$$\rho_m^{hid} = |V_m^{meas,nor} - V_m^{meas,hid}| > 0. \tag{47}$$

Similarly, under this attack, when KVL is applied in Figure 7a, the equation would reflect quantities that result due to the malicious change in firing angle command. Thus, we get

$$\begin{aligned} \mathbf{V_m^{hid}} &= \mathbf{V_{k_1}^{hid}} - 0.5\mathbf{I_{k_1k_2}^{hid}}\mathbf{z_{k_1k_2}} \\ &= \mathbf{V_{k_2}^{hid}} - 0.5\mathbf{I_{k_2k_1}^{hid}}\mathbf{z_{k_1k_2}}. \end{aligned} \tag{48}$$

From (41), it can be inferred that

$$\psi_m^{hid} = 2 \times |V_m^{meas,nor} - V_m^{meas,hid}| > 0. \tag{49}$$

Hence Proved. □

Remark 1. *In order to beat the detection metric, ρ_m, in* (40)*, for every SVC, the adversary has to manipulate the phasors $\mathbf{V_{k_1}}$ and $\mathbf{V_{k_2}}$, and the measurements which are a function of these phasors (according to [6] and Proposition 1). Similarly, to beat the detection metric, ψ_m, in* (41)*, for every phasor, the adversary has to manipulate $\mathbf{V_{k_1}}$, $\mathbf{V_{k_2}}$, $\mathbf{I_{k_1k_2}}$, $\mathbf{I_{k_2k_1}}$, and all the functions of phasors $\mathbf{V_{k_1}}$ and $\mathbf{V_{k_2}}$.*

C. Algorithm

The detection algorithm based on detection metrics in (40) *and* (41) *is similar to Algorithm 1.* Even in this case, the detection metrics are calculated at an observation windows and if any significant deviation, governed by a predefined thresholds, is observed, the attack gets detected. The steps are given in Algorithm 2. Using similar method to compute the computational effort as in case of Algorithm 1, the computational effort of Algorithm 2, when (40) is used as detection metric, is $2+2+6+2+2+6+1+4+1+2 = 28$ floating point operations. Similarly, when (41) is used as detection metric, it is $2 \times (6+2+2+4+1+2)+1 = 35$ floating point operations. Even here, it can be stated that the computational effort needed is in general significantly lower than algorithms that have multiple stages or involve iterative computations.

There are instances where a substation or a operator could potentially need to apply the detection metrics and techniques in both Algorithm 1 and Algorithm 2. This could be due to the application of multiple SVCs in a region, with different modes of control. In other words, there may be situations where some SVCs are in Mode 1 control and some in Mode 2 control. For such cases, a unified algorithm is presented as Algorithm 3. This algorithm essentially integrates both Algorithms 1 and 2, with a step to classify which detection metrics to use, depending on whether the SVC is in Mode 1 control or Mode 2 control.

Algorithm 2: Proposed algorithm for detection of attacks, in Section III-B, against SVC in Mode 2 operation.

Data: The phasor measurements, $\mathbf{V_{k_1}}$, $\mathbf{V_{k_2}}$, $\mathbf{I_{k_1k_2}}$, and $\mathbf{I_{k_2k_1}}$, and predefined thresholds, T_{h_1} and T_{h_2}
Output: Trigger

```
Calculate ρ_m using (40);
Calculate ψ_m using (41);
if ρ_m > T_{h_1} then
    Trigger = 1;
    A stealthy attack is detected against SVC.;
else
    Trigger = 0;
    go back to step 1;
if ψ_m > T_{h_2} then
    Trigger = 1;
    A stealthy attack is detected against SVC.;
else
    Trigger = 0;
    go back to step 1;
```

Algorithm 3: Unified detection algorithm for detection of attacks against both Mode 1 and Mode 2 operations of SVC

Data: The phasor measurements, $\mathbf{V_{k_1}}$, $\mathbf{V_{k_2}}$, $\mathbf{I_{k_1k_2}}$, and $\mathbf{I_{k_2k_1}}$, the reference values, $\gamma_{kk_n}^{ref}$ $\forall$ $k = 1, \cdots, a$, γ_k^{ref} and the predefined thresholds T_h, T_{h_1} and T_{h_2}.
Output: Trigger

```
Set M_d ← 1, for SVCs under Mode 1 or centralized control, and M_d ← 2, for SVCs Mode 2 or local control system based control;
if M_d == 1 then
    Calculate Γ_k using (21);
    if Γ_k > T_h then
        Trigger = 1;
        A stealthy attack is detected against SVC.;
    else
        Trigger = 0;
        go back to step 1;
if M_d == 2 then
    Calculate ρ_m using (40);
    Calculate ψ_m using (41);
    if ρ_m > T_{h_1} then
        Trigger = 1;
        A stealthy attack is detected against SVC.;
    else
        Trigger = 0;
        go back to step 1;
    if ψ_m > T_{h_2} then
        Trigger = 1;
        A stealthy attack is detected against SVC.;
    else
        Trigger = 0;
        go back to step 1;
```

Even in Algorithm 2, like Algorithm 1, if a small change is introduced by the adversary, this algorithm will not be able to detect such changes. This is mainly because the system measurements, PMUs and sensors are noisy. Hence, if a small

S.No	RB[1]	V^{sp2}	α^{sp3}
1	22	1.0253	2.44
2	37	0.9903	2.52
3	48	1.0332	2.355
4	75	0.9750	2.62
5	94	1.0018	2.441
6	117	1.0190	2.36

[1] Regulated bus ;
[2] Specified Voltage;
[3] Required firing angle.

Table I: The location of SVCs, regulated buses and the specified voltages at these regulated buses.

S.No.	Normal	Attacks, Γ_k^{min2}			
	Γ_k^{max1}	$\Delta\alpha^{sel}=0.1$	$\Delta\alpha^{sel}=0.3$	$\Delta\alpha^{sel}=0.5$	$\Delta\alpha^{sel}=0.7$
1	0.0234	0.2299	0.4988	0.5749	3.0558
2	0.0412	0.0497	0.1165	0.1416	1.0433
3	0.0211	0.0893	0.2496	0.3280	0.3440
4	0.0478	0.0618	0.3426	0.7428	1.0600
5	0.0312	0.1679	0.4024	0.4889	0.4942
6	0.0176	0.0587	0.1711	0.2283	0.2443

[1] Maximum value of Γ_k;
[2] Minimum value of Γ_k.

Table II: The values of Γ_k under normal and a few attack scenarios in Mode 1 or centralized operation.

change is introduced by the adversary, the changes in the detection metrics could be less appreciable, due to noise and other practical considerations. As a result this algorithm is not very adept at detecting such small changes. It should be pointed out that this limitation does not affect the practical application of this algorithm. This is because adversaries introduce attacks to disrupt the system, i.e., cause significant changes, and for an appreciable change in the system, the changes introduced must be greater than that perceived due to the effects of noise.

VI. Simulation Results

In order to test the effectiveness of the developed algorithms, simulation studies are performed on the IEEE 118-bus system [41]. Tests are carried out separately for both Algorithms 1 and 2. In order to test Algorithm 1, it is necessary to create a baseline of normal operation, where there is no cyber attack. This baseline case, or normal scenario is followed by several attack scenarios, where the attack strategy established in Proposition 1 is implemented. For the purpose of convenience, in this section, certain notions are introduced to consolidate results. Let $\alpha^{\mathbf{sel}}$ represent the selected firing angle by the operator. Similarly, let $|\mathbf{V^{svc}}|^{sel}$ denote the vectors containing the regulated bus voltages. For the purpose of simulation studies, the adversary introduces a deviation of firing angle, given by $\pm\Delta\alpha^{mal} \times \mathbf{U}$, where $\mathbf{U}$ is a vector containing all entries as 1, while ensuring that the conditions established in Proposition 1 holds good. It is worth emphasizing that a detailed analysis is performed to analyze this method for any potential limitations and practical considerations. Furthermore, this is a first effort to address command injection in the context of SVCs. For the purpose of testing, $\Delta\alpha^{mal}$ is varied in steps of $0.025\ rad$, from 0 rad (normal condition) to $0.8\ rad$. Thus, there are 33 distinct attack scenarios considered here. For every attack scenario, the firing angle is changed by $\Delta\alpha^{mal}$, and the conditions in Proposition 1 must be carried out to ensure that for an operator, the estimated and measured values of firing angles and voltages follows (1) and (2).

These test-cases are run for six SVCs, placed at six buses to control voltages. The data pertaining to the location of these SVCs are in Table I. Each of these six SVCs in Table I is modelled according to the circuit diagram in Figure 1, with inductive reactance, $X_L = 0.288\,pu$, and capacitive reactance, $X_C = 1.07\,pu$ [30]. Each of the 33 cases is run for 200 times, to account for the effect of noise in measurements. The measurement noise is considered to follow the standard Gaussian distribution, with $\sigma = 1\%$ for power measurements, and $\sigma = 0.3\%$ for voltage measurements [42], [43]. In Case 1, when there is no cyber-attack, the firing angle of the all the SVCs are chosen such that the bus voltages at the regulated buses reflect (approximately, due to measurement noise) the specified voltages in Table I. In Cases 2 to 5, the firing angles of all SVCs are changed by the stated values. In these attack scenarios, the stealthy attack proposed in Proposition 1 is carried out, such that the adversary ensures that the measured and estimated values of firing angles and regulated bus voltages are close to the values in Table I. The values of the detection metric, Γ_k, for some of the cases are presented in Table II.

From the values on Γ_k recorded in Table II, it can be seen that the minimum values of Γ_k under attack scenarios in Cases 2 to 5 are greater than the maximum values of Γ_k under normal scenarios, even when the change in firing angle, i.e., $\Delta\alpha^{sel}$, is as small as 0.1 rad. For other values of $\Delta\alpha^{sel}$, it is seen that the minimum values of Γ_k is significantly higher than the maximum values seen in normal conditions. It can thus be inferred that the detection metric, Γ_k, is effective in classifying attacks from normal scenarios, in practical scenarios where it is expected that a deviation will be much higher than $0.1\ rad$, to cause any appreciable effects.

Subsequently, the observed values of detection metric, Γ_k in (21), denoted by Γ^{obs} in this section, for all the 33 are recorded. In the case of normal scenario, when there is no cyber-attack, i.e., $\Delta\alpha^{sel} = 0$, the maximum values are recorded as observed values of Γ_k, i.e., Γ^{obs}, whereas in all attack scenarios, the minimum values of Γ_k are recorded under Γ^{obs}. The purpose of recording maximum values in normal condition, as opposed to minimum values in attack scenarios, is to give a clear idea of the range of values of $\Delta\alpha^{mal}$, for which the detection metrics clearly classify the attack. A plot of all these recorded values of detection metric w.r.t. the malicious deviation in firing angle is presented in Figure 8. It is interesting to note that in Figure 8, the values of Γ^{obs} decrease in general (when compared to values recorded under normal conditions) when the malicious phase shift is small, for instance $0.025\ rad$. This is because the values of Γ^{obs} recorded under normal conditions are the maximum values obtained, as opposed to the values of Γ^{obs} under attacks, which are minimum values. Due to the nature of measurement noise, for small values of malicious firing angle change, there are instances where the maximum values of detection metric, Γ_k obtained in normal conditions can be greater than the

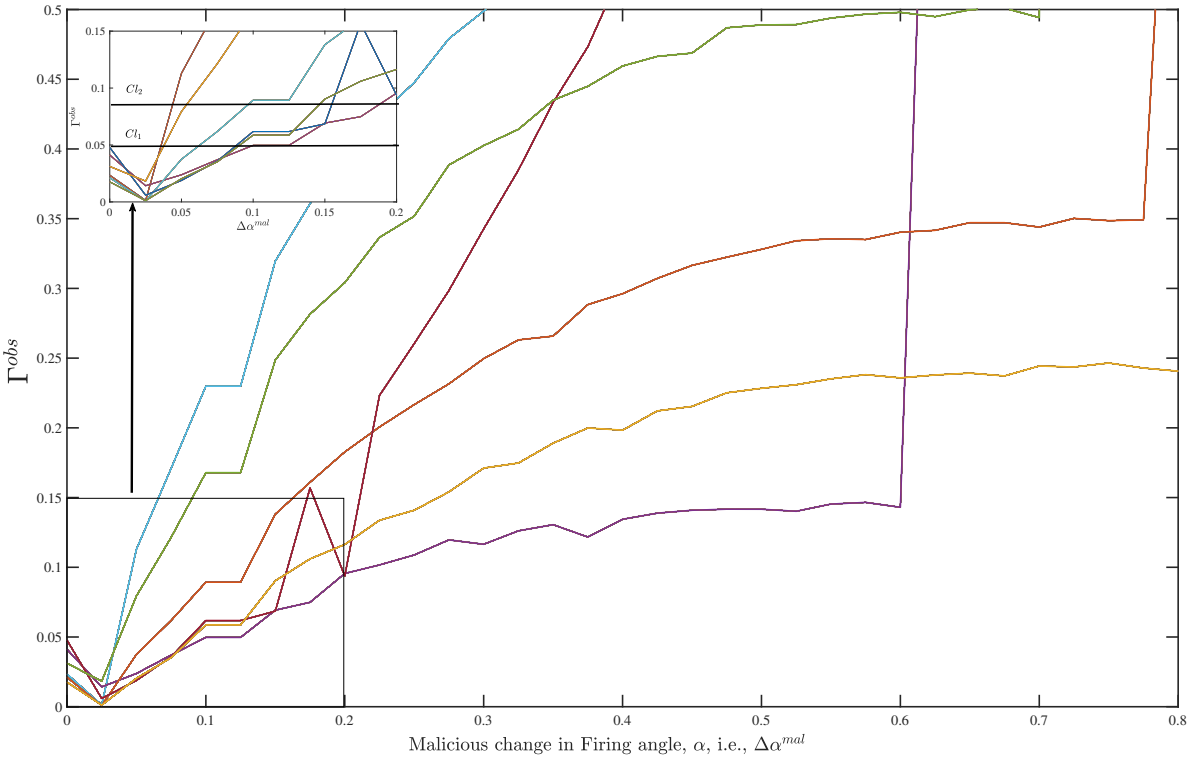


Figure 8: A plot of the observed values of detection metric, i.e., Γ^{obs}, using (21) for all the 33 cases w.r.t. the malicious firing angle deviation, α^{sel}.

minimum values of Γ_k under attack. These observations are in agreement with the predictions made using mathematical analysis in Section IV-C.

In order to quantify the effectiveness of the developed method in detecting FCI attacks, it is necessary to consider some important statistical parameters, viz., false positives (FP), which indicates the number of cases where the detection algorithm falsely detects an FCI attack under normal condition, false negatives (FN), which indicates the number of cases where the detection algorithm fails to detect an attack scenario, true negatives (TN), which indicates the number of cases where the detection algorithm correctly detects the absence of an FCI attack, true positives (TP), which indicates the number of cases where the detection algorithm detects the presence of an FCI attack correctly, accuracy, given by the relation, $\frac{(TP+TN)}{(TP+TN+FP+FN)}$, precision, given by the relation, $\frac{TP}{(TP+FP)}$, and recall, given by the relation, $\frac{TP}{(TP+FN)}$ [44]. Furthermore, these parameters can also be used to compare the efficacy of the developed algorithms when compared with state-of-the-art technique discussed further in Section VI-B.

To test the effectiveness of detection metrics, ψ_m and ρ_m, for Mode 2 operation, four SVCs are considered to be placed at the midpoint of transmission lines. The location of these SVCs are given in Table IIIa.

To test the effectiveness of Algorithm 2, the following test cases are considered:

- *Case 1:* Normal condition, when there is no cyber-attack.
- *Case 2:* When the measured or feedback voltage is incremented in steps of 0.05 pu, i.e., $V_m^{meas} = V_m^{sp} + a_1 \times 0.05 \ , \forall \ a_1 = \{1, 2\}$.
- *Case 3:* When the actuation command or firing angle is changed in steps of 0.2 rad, i.e., $\alpha_m = \alpha_m^{sp} + a_2 \times 0.2, \ \forall \ a_2 = \{1, 2\}$.

Even in these test-cases, the effects of noisy measurements are considered and simulations are run for 200 times. The PMUs measurement noise is considered to have a Gaussian distribution with maximum allowable error, such that $\sigma = 0.01$ pu for voltage measurements and $\sigma = 0.01$ radians for angle measurements [45]. The values of detection metrics, ψ_m and ρ_m, in Cases 1, 2 and 3, are tabulated in Table IIIb. From the values of detection metrics recorded, it can be clearly inferred that the minimum values of ρ_m and ψ_m under attack scenarios, i.e., Cases 2 and 3, are higher than the maximum values of ρ_m and ψ_m under normal scenario, i.e., Case 1. Hence, it can be seen the detection metrics, Γ_k, for centralized or Mode 1 control, and, ρ_m and ψ_m, for Mode 2 or local control system based control, are effective in classification of attacks from normal scenarios.

S.No	Line[1]	FB[2]	TB[3]
1	16	11	13
2	29	22	23
3	52	37	39
4	73	52	53

[1] Line or branch number ;
[2] From bus of the line;
[3] To bus of the line.

(a) The location of SVCs used for mid-point voltage and reactive power regulation.

S.No.	Case 1		Case2				Case 3			
			$a_1 = 1$		$a_1 = 2$		$a_2 = 1$		$a_2 = 2$	
	ρ_m^{max1}	ψ_m^{max1}	ρ_m^{min2}	ψ_m^{min2}	ρ_m^{min2}	ψ_m^{min2}	ρ_m^{min2}	ψ_m^{min2}	ρ_m^{min2}	ψ_m^{min2}
1	0.0116	0.0234	0.0399	0.0796	0.0882	0.1763	0.0175	0.0350	0.0396	0.0744
2	0.0092	0.0214	0.0391	0.0783	0.0910	0.1817	0.0442	0.0882	0.0843	0.1695
3	0.0095	0.0280	0.0414	0.0819	0.0872	0.1741	0.0140	0.0281	0.0303	0.0609
4	0.0122	0.0246	0.0403	0.0799	0.0911	0.1826	0.0621	0.1245	0.1162	0.2328

[1] Maximum values ;
[2] Minimum values.

(b) The values of ρ_m and ψ_m under both normal and attack scenarios in Mode 2 or local control system based control.

Table III: The test conditions and the values of detection metrics under normal and attack scenarios.

A. Threshold Selection

The selected threshold varies depending on the system conditions, and the sensitivities of the quantities in (21), (40) and (41) to changes in the state variables due to malicious commands. As discussed before, due to noisy measurements and subsequent estimations, it is necessary to consider the effect of noise, in choosing a threshold. If changes in firing angle, α_k, or any state variable causes a change in system measurements that is within the order of measurement noise, then it is not possible to observe the change, both for the operator and also any algorithm that leverages on these changes, including state estimators. From the variation of the detection metric, Γ_k, w.r.t to a malicious change in firing angle, α_k, i.e., $\Delta\alpha^{sel}$, in Figure 8, the threshold can be estimated to reliably classify attacks from normal scenarios. In the plot, two thresholds are shown as Cl_1, and Cl_2. The threshold, $Cl_1 = 0.04$, which is approximately equal to the maximum value of Γ_k, under normal condition. Another threshold $Cl_2 = 0.08$, is considered which is indicative of the practical considerations, like the effects of noise, the malicious change in α_k required to actually cause an attack in practice, as firing angles have a wide range of operation, and transmission systems usually remain unaffected by small changes in state variables, as discussed before in Section VI. A statistical analysis is performed on the $6 \times 200 \times 33 = 39600$ cases, and the results are shown in Table IV, where false and true positives, false and true negatives, accuracy, precision, and recall [44], defined earlier, are recorded. These values are recorded considering two potential thresholds, $Cl_1 = 0.04$ and $Cl_2 = 0.08$. It can be seen from Table IV that when a lower value of threshold is chosen, close to the order of variations introduced due to measurement noise, there are few false positives. However, when a higher value of threshold is chosen, there are more false negatives. This is because the variations in detection metrics introduced due to very small changes in firing angle are likely to be smaller than the threshold chosen. When $Th_1 = Cl_1 = 0.04$ is chosen as the threshold, it leads to better accuracy, as seen in Table IV, because several attack scenarios involving a very small change in firing angles get classified as attacks. Moreover, some of the attack scenarios, involving $\Delta\alpha^{sel} = \{0.025, 0, 05, 0, 075, 0.1, 0.125\}$, provide an interesting insight in some of the limitations of the algorithm, when a sufficiently higher value of threshold is chosen. However, in practical scenarios, i.e., realistic attack scenarios (that can cause disruption), a $Th_1 = Cl_2 = 0.08$ or even $Th_1 = 0.1$ is adequate. This is because an attacker is likely to introduce changes that are sufficiently larger than the variations caused due to measurement noise.

Parameters	$Cl_1 = 0.04$	$Cl_2 = 0.08$
False negatives	1787	3380
False positives	2	0
True negatives	1198	1200
True positives	36613	35020
Accuracy	95.48 %	91.46 %
Precision	99.99 %	100 %
Recall	95.35 %	91.2 %

Table IV: Statistical analysis of the performance of the proposed algorithm, in classifying attacks, from normal scenarios.

In Mode 2 operation, based on (40) and (41), thresholds that are greater than the maximum errors obtained in estimation of ρ_m and ψ_m under noisy measurements, are sufficient. Based on observed values of ρ_m and ψ_m in Table IIIb, the thresholds of $T_{h_1} = 0.03$ and $T_{h_2} = 0.06$, would be sufficient to separate attack from normal scenarios. Here, any classifier that considers the issue of noise in feedback signal is capable of classification of attacks from normal scenario. In other words, any threshold higher than the maximum variations in evaluation of detection metrics in (40) and (41), caused due to measurement noise, can reliably classify attack from normal scenarios, unlike in the case of Algorithm 1.

B. Comparison with state-of-the art technique

It is worth noting that this is the first paper to handle the problem of command injection attacks in SVCs. Hence, it is not possible to directly compare this work with any existing technique. Hence, the algorithm in [28], which have been developed for attacks involving transformer taps, has been modified to handle attacks against SVCs. This modified algorithm is run for the same attack scenarios discussed above. Even in this study, as stated earlier, statistical parameters, like false positives, false negatives, true positives, true negatives, accuracy, precision, and recall [44], introduced earlier, are recorded for both the proposed algorithm and the Modified algorithm in [28]. The values obtained for both these algorithms are given in Table V. From Table V, it can be observed that the false negatives obtained in Modified [28] is significantly higher than that seen in the proposed algorithm. Similarly, the number of true positives obtained in the proposed method is higher than that seen in Modified [28]. Due to these differences, it is seen that the accuracy and recall of the proposed method

is significantly better than that seen in Modified [28]. Hence,

Parameters	Proposed	Modified [28]
False negatives	3380	7193
False positives	0	0
True negatives	1200	1200
True positives	35020	31207
Accuracy	91.46 %	81.84 %
Precision	100 %	100 %
Recall	91.2 %	81.27 %

Table V: Comparison of the proposed algorithm with [28], adapted to handle SVCs, instead of tap-changers.

it can be seen that the proposed algorithm performs better in terms of classifying attack scenarios from normal scenarios.

VII. Conclusion

In this paper, detection algorithms are proposed to mitigate attacks that involve injection of false commands against SVCs. The attack models are developed in both modes of control of SVCs, such that the attacks evade both the operator and BDD. Based on these attack models, detection metrics are formulated to enable the separation of attacks from normal scenarios. The ability of the formulated metrics to do the same is validated through formal mathematical proofs. These metrics work on the principle that even though the adversary can hide the measurements and state variables of the SVC, it is not feasible for the adversary to hide the effect of stealthy attacks on other state variables and measurements in the system. These detection metrics that are formulated and validated mathematically, are used to develop two detection algorithms to detect the stealthy attacks. The detection algorithms are easy to implement, computationally less intensive, when compared to multi-stage and iterative algorithms and independent of ICT used for automation. These detection algorithms are then tested on the IEEE 118-bus system and found to be effective in practical scenarios, with non-ideal measurements. This work is the first effort to explore such attacks against SVCs, which is a device under the class of FACTS devices.

Acknowledgement

This work was supported in part by Ministry of Education, Singapore under the Tier 2 grant MOE-T2EP20121-0011.

References

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

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

[3] L. G. N Hingorani, *Understanding FACTS: Concepts and Technology of Flexible AC Transmission Systems*, ser. Power Engineering. Wiley-IEEE Press, 2000.

[4] K. R. Padiyar, *FACTS Controllers in Power Transmission and Distribution*, ser. Power Engineering. New-Age International Publishers, 2016.

[5] 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

[6] 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, 2012.

[7] Z.-H. Yu and W.-L. 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, 2015.

[8] D. Mukherjee, "Data-driven false data injection attack: A low-rank approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2479–2482, 2022.

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

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

[11] K.-D. Lu and Z.-G. Wu, "Multi-objective false data injection attacks of cyber–physical power systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 9, pp. 3924–3928, 2022.

[12] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26 022–26 033, 2017.

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

[14] 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, 2013.

[15] 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, 2018.

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

[17] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing elm-based ocon framework," *IEEE Access*, vol. 7, pp. 31 762–31 773, 2019.

[18] H.-Y. Tran, J. Hu, X. Yin, and H. R. Pota, "An efficient privacy-enhancing cross-silo federated learning and applications for false data injection attack detection in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2538–2552, 2023.

[19] P. Hu, W. Gao, Y. Li, F. Hua, L. Qiao, and G. Zhang, "Detection of false data injection attacks in smart grid based on joint dynamic and static state estimation," *IEEE Access*, vol. 11, pp. 45 028–45 038, 2023.

[20] A. Parizad and C. J. Hatziadoniu, "A real-time multistage false data detection method based on deep learning and semisupervised scoring algorithms," *IEEE Systems Journal*, vol. 17, no. 2, pp. 1753–1764, 2023.

[21] 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, 2017.

[22] Z. Zhang, S. Huang, Y. Chen, B. Li, and S. Mei, "Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game," *IEEE Transactions on Power Systems*, vol. 37, no. 1, pp. 530–542, 2022.

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

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

[25] 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, 2017.

[26] 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, 2016.

[27] 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, 2019.

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

[29] ——, "Detection of malicious command injection attacks on phase shifter control in power systems," *IEEE Transactions on Power Systems*, vol. 36, no. 1, pp. 271–280, 2021.
[30] H. A.-P. C. A.-C. Enrique Acha, Claudio R. Fuerte-Esquivel, *FACTS: Modelling and Simulation in Power Networks*, ser. Power Engineering. John Wiley and Sons, 2004.
[31] B. Li, "Detection of false data injection attacks in smart grid cyber-physical systems," 2019.
[32] S. Chakrabarty and B. Sikdar, "Unified detection of attacks involving injection of false control commands and measurements in transmission systems of smart grids," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1598–1610, 2022.
[33] F. Khorrami, P. Krishnamurthy, and R. Karri, "Cybersecurity for control systems: A process-aware perspective," *IEEE Design and Test*, vol. 33, no. 5, pp. 75–83, 2016.
[34] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, and F. Khorrami, "Machine learning-based defense against process-aware attacks on industrial control systems," in *2016 IEEE International Test Conference (ITC)*, 2016, pp. 1–10.
[35] S. Pequito, F. Khorrami, P. Krishnamurthy, and G. J. Pappas, "Analysis and design of actuation–sensing–communication interconnection structures toward secured/resilient lti closed-loop systems," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 667–678, 2019.
[36] K. Paridari, N. O'Mahony, A. El-Din Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 113–128, 2018.
[37] Siements, *SIMATICS7-300FM 355 closed-loop control module*, 2011.
[38] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, and T. Cruz, "Elegant: Security of critical infrastructures with digital twins," *IEEE Access*, vol. 9, pp. 107 574–107 588, 2021.
[39] O. Eigner, P. Kreimel, and P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," in *2016 International Conference on Software Security and Assurance (ICSSA)*, 2016, pp. 64–69.
[40] W. Ford, "Chapter 9 - algorithms," in *Numerical Linear Algebra with Applications*, W. Ford, Ed. Boston: Academic Press, 2015, pp. 163–179. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780123944351000090
[41] U. of Washington. (1999) Power system test case archive. [Online]. Available: http://www.ee.washington.edu/research/pstca/
[42] 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.
[43] "IEEE standard for scada and automation systems," *IEEE STD C37.1-2007 (Revision of IEEE STD C37.1-1994)*, pp. 1–143, May 2008.
[44] H. Dalianis, *Evaluation Metrics and Evaluation*. Cham: Springer International Publishing, 2018, pp. 45–53. [Online]. Available: https://doi.org/10.1007/978-3-319-78503-5_6
[45] "Ieee standard for synchrophasor measurements for power systems," *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–61, 2011.

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 Senior Research Scientist in NCS Pte. Ltd., Singapore and Adjunct Senior Research Fellow in National University of Singapore. His areas of interest include power system analysis, smart grid cyber-security, IoT Security, and 5G networks and critical infrastructure cyber-security.

Biplab Sikdar (Senior Member, IEEE) is a Professor in the Department of Electrical and Computer Engineering at the National University of Singapore, where he also serves as the Head of the Department of Electrical and Computer Engineering and the director of the Cisco-NUS Corporate Research Laboratory. He 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 the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was an Assistant Professor from 2001-2007 and Associate Professor from 2007-2013 in the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute. He is a recipient of the NSF CAREER award, the Tan Chin Tuan fellowship from NTU Singapore, the Japan Society for Promotion of Science fellowship, and the Leiv Eiriksson fellowship from the Research Council of Norway. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He has served as an Associate Editor for the IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, and IEEE Internet of Things Journal and is an IEEE COMSOC and VTS Distinguished Lecturer and ACM Distinguished Speaker.