Detection of Cyber Attacks on Railway Autotransformer Traction Power Systems

Shantanu Chakrabarty and Biplab Sikdar *Senior Member, IEEE*

***Abstract*—Modern railways are powered by traction power systems (TPS). Thus, the safety and reliability of TPS is crucial for railways, which is a critical infrastructure. TPS, like any other infrastructure, are being automated by means of information and communication technologies (ICT). Similar to smart grids, reactive power compensation and voltage control is important to the reliable operation of TPS. These compensation systems can be broadly controlled or operated in two modes. They are either remotely controlled through ICT channels or by a local closed loop control system monitored remotely. ICT channels, in general, are vulnerable to cyber attacks. This vulnerability renders the reactive power compensation system/voltage control system vulnerable to cyber-attacks. A misuse of the compensation system can hamper the voltage profiles and disrupt the operation of the TPS. The misuse of compensation system thus translates to financial losses and unsafe operation of railways. In this paper, such threats have been identified and investigated in both the modes of operation, in detail. Two detection algorithms are proposed for each mode of operation. The detection approaches proposed in this paper rely on developed detection metrics that are functions of terminal electrical quantities in both the train and the TPS. The effectiveness of these metrics in classification of attacks from normal operation has been established mathematically. The proposed detection methods are computationally inexpensive, easy to implement, and reliable when tested using simulations on an Autotransformer Traction Power System model.**

***Index Terms*—Autotransformer traction power system, cyber-security.**

I. Introduction

Railways, like any other critical infrastructure, must be safe and reliable. Modern railways, in general, are powered by traction power systems. Currently, railways are seeing an increase in penetration of automation, through use of Information and communication technology (ICT). As a result, modern railways are complex cyber-physical systems [1]. The communication standard most prevalent today is Global System for Mobile Communications - Railways [2], [3]. The communication networks for train systems are usually wireless wide area networks [2]–[4]. Several operations related to train and traction power system control are delegated to computers. This shift in operation has made ICT a crucial part of the railway system. Even though the incorporation of ICT has enabled ease of operation and expansion, they leave the railway operation and control vulnerable to cyber-attacks. The exploitation of these vulnerabilities by an adversary could result in financial losses, or worse, could result in loss of lives. Well-known attacks on critical infrastructures [5], [6] usually exploit the vulnerabilities inherent in the ICT. To prevent the adverse effects brought about by such attacks, especially in railway systems, effective protection strategies must be put in place. In other words, the vulnerabilities in the ICT in the railway operation and control must be identified and their exploitation must be prevented.

Among the several components that enable the functioning of railways, Traction Power Systems (TPS) are one of the most important. TPS can be both Direct Current (DC) and Alternating Current (AC), depending on the application. The context of this paper is focussed on AC TPS. In the case of smart grids, voltage control and reactive power compensation is crucial to the safe and reliable operation [7], [8], as voltage outside the safe operational range is not permissible. This is also true in the case of AC TPS [9]. Even in DC grids and TPS, voltage control schemes are employed. In DC systems, the power drawn by the train is regulated when the voltage swells or dips outside the safe operating range [1], [10].

The available literature on security of TPS is limited [1], [11], [12]. In [1] and [12], False Data Injection (FDI) attacks are discussed in the context of DC TPS. These attacks, as the name suggests involve an adversary injecting false feedback data with the intention of forcing a wrong or harmful operation. Such attacks, i.e., FDI attacks have been studied extensively in smart grids [13]–[18]. In the case of smart grids, malicious injection of data must evade alerting Bad Data Detection (BDD) [13], [14]. Several methods have been proposed to address/detect FDI attacks in smart grids. In [15], [17], [18], DC power flow models are employed to model the smart grid. As a result, these methods are designed for system with DC state estimators. However, practical state estimators are AC estimators, based on AC power flow model. There have been works proposed for AC state estimators, considering AC power flow model [19]–[23], using a variety of techniques. In [19], Kullback-Leibler distance (KLD) is employed to capture the dynamics of the measurements. This technique needs historical data to facilitate detection of FDI attacks. A graph theory based approach is proposed in [20] and outlier detection techniques are employed to detect FDI attacks. Incorporation of load forecasting, generation scheduling and synchrophasor data to facilitate detection can be seen in [21]. This method, [21], does not depend on the implementation of ICT. A non-iterative technique to detect FDI attacks is proposed in [22]. In [22], flow measurements (both active and reactive) and

This research was supported in part by Singapore Ministry of Education Academic Research Fund Tier 1 Grants R-263-000-E78-114 and R-263-001-E78-114.

S. Chakrabarty and B. Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583. Email: shantanu1088@gmail.com, bsikdar@nus.edu.sg.

phasor measurements are employed to enable detection of FDI attacks. In [23], ELM-Based OCON Framework is used for FDI attack detection, under AC power flow model. However, it is important to note that BDD is not inherent in TPS [1], especially AC TPS. The possibility of FDI attacks against over-current and squeeze controls, used to control voltages in DC TPS, is explored in [1]. In order to protect the systems from FDI attacks, detection and prevention schemes are also proposed [1]. The impact of signal delay attack, where the timing information related to the voltage measurements is corrupted by the adversary, is studied in [11]. However, attacks where the adversary directly takes over the control action is not addressed in the literature, especially in the case of AC TPS. There are works that consider such attacks in the context of smart grids [24]–[30]. In [24]–[26], attacks involving the disconnection of lines by maliciously tripping circuit breakers (CBs) are considered. In [27], attacks involving injection of false command data are studied in detail. The work in [29] exclusively deals with false command injection attacks in the context of phase shifters, used for active power control. The literature concerning attacks on voltage control, is sparse [28], [30]–[32]. In [31], [32], FDI attacks that result in wrong control action is studied. In [28], attacks involving malicious injection of tap signals to disrupt voltage control in transmission system are studied. In [30], a generalized framework for detection of command injection and FDI attacks is proposed for a transmission system (of a smart grid) that is capable of addressing attacks on voltage control. However, such attacks are not studied in the context of traction TPS. In [33], command injection attacks are studied where the control action is hijacked by the adversary through malicious commands relayed through ICT. However, [33] deals with scenarios where the control is centrally handled by the control centre. In order to have a comprehensive protection strategy, it is necessary to also consider protection under the framework of local closed loop control, in addition to central control framework.

Dynamic thermal ratings (DTR) provides actual current carrying capacity based on real-time operating conditions [34]. DTR usually provide ratings higher than static thermal ratings (STR) [35]. Due to the stochastic nature of loading of transmission systems, DTR is crucial to facilitate efficient and economical use of transmission resources, especially with increasing penetration of renewable sources [36]. DTR system also enables efficient use of underground cables [37]. DTR system, in modern power grids or smart grids, come with a cyber layer, as discussed in [38], [39]. The reliability of this cyber-layer is very important. It is also shown in [38], [39] that a reliable cyber layer of the DTR system improves the overall reliability of the system. As DTR deals with thermal ratings, related to active power, it is not considered in the algorithms developed in the manuscript, as voltage control/reactive power compensation system does not depend on active power. However, the effect of DTR and its cyber layer can be explored in the context of studies involving active power loads, mainly in active power control studies, both in power grids and traction power systems.

In modern railways, Autotransformer (AT) Traction Power Systems (TPS) are widely used [40]. In AT TPS, like AC grids, reactive power compensation system is in place [41] with the objective of either voltage control or loss minimization. This compensation system can be operated by an operator by control signals sent remotely from the control centre [41], i.e., through the ICT systems. Another way of operation is through closed loop control system that adjusts actuation based on the measurements and reference values (desired values). These control mechanisms are inherently prone to cyber-attacks [5], [6]. In AC grids, it is known that reactive power is strongly coupled to voltage (magnitudes) [42]. Thus, any misuse of reactive power compensation results in voltages going out of the safe operational range. This could potentially destabilize the AT TPS, effectively resulting in failure of railway infrastructure. As a result, it is essential to protect this reactive power compensation/voltage control system. This paper is an attempt to identify threats and develop strategies to protect the system from these potential cyber-threats.

In this paper, two detection algorithms are developed. The first algorithm is developed to detect an intrusion in centrally controlled compensation systems. The second algorithm algorithm, on the other hand, is developed to detect attacks against compensation systems that employ local closed loop control systems. In order to develop these algorithms, various threats are identified in the framework of present AT TPS operation. Based on the identified threats, detection metrics are developed that are functions of terminal electrical quantities. The effectiveness of these detection metrics is established through formal mathematical analysis. The detection metrics are then incorporated to develop two detection algorithms, mentioned above. It is important to note that these algorithms are developed considering attack scenarios that are stealthy (such that the operator does not detect them through existing mechanisms). This is the first paper to address these problems in AT TPS.

The contributions of this paper are as follows:

1) Two algorithms are developed that can detect:
   a) attacks where an adversary injects malicious commands to change the settings of the reactive power compensation system in AC TPS;
   b) attacks where an adversary tampers with the operation of the local closed loop control system used in the locomotive for reactive power compensation.
2) **The developed algorithms are novel** because they:
   a) are computationally inexpensive, as there are no iterative steps involved;
   b) do not require historical data;
   c) are reliable when tested using simulations;
   d) are simple to implement;
   e) rely on electrical parameters information, so it is independent of ICT systems used;
   f) are mathematically proven to be effective;
   g) **are the first to consider such attacks and propose countermeasures against these attacks.**

The paper is organized as follows: The background information relevant to this paper is presented in Section II. The attack scenarios are discussed in Section III. The algorithms

to detect the attack scenarios, discussed in Section III, are developed and proposed in Sections IV and V. The details pertaining to the simulation study are given in Section VI. Finally, the conclusions are drawn in Section VII.

II. Background

In this section, the background concepts relevant to this paper are discussed briefly.

A. Autotransformer Traction Power System

The aspects of the model of AT TPS that are relevant to this paper are presented in this section. The AT TPS, illustrated in Figure 1, has four main components [41], [43]: (i) Traction Substation (TSS), (ii) Autotransformers, (iii) Feeder system that transmits power, and (iv) Electric Train. These components are shown in Figure 1, using their circuit analysis models [41], [43]. The traction substation transformer is represented as an ideal single phase transformer with an AT, whose midpoint is connected to rail, ideally at zero potential. ATs are represented as a voltage sources in series with the leakage impedances. In circuit analysis, the train can be viewed as a constant power or current load. The important physical quantities relevant to the analysis of TPS and the issues discussed in this paper are as follows:

- V_s - Supply voltage from the TSS (usually 25 kV [41]).
- Z_s - Leakage impedance of the substation transformer.
- Z_{AT} - Leakage impedance of the autotransformer.
- $(P_d + jQ_d)$ - Apparent power demand of the train, based on scheduled MW demand of the train and power factor (pf) of the operation.
- m - index denoting m^{th} AT.
- V_{ij} - Voltage at the i^{th} AT, and j is used to denote whether the voltage is seen at catenary (c), rail (r) or feeder (f). For example, V_{mc} denotes voltage at m^{th} AT at the catenary.
- I_{ijk} - Convention of notation for current, where i and j denote the indices of AT and k represents if the current is on the catenary (c), rail (r) or feeder (f). As an example, I_{mnr} denotes current measured or observed between m^{th} and n^{th} ATs in the rail.
- I_{tc} - Current drawn by the train from the catenary.
- $\mathbf{Z_{tx}}$ - 3×3 impedance matrix of the feeder line, usually represented in terms of quantities per unit distance.
- d_{mt} - distance of the train from the m^{th} AT.
- Q_g - Reactive power generation coming from the compensation system.

The system in Figure 1 can be analyzed as a distribution system, using Backward-Forward Sweep (BFS) algorithm [41] or Newton's method [43].

B. Reactive Power Compensation in AC TPS

In case of AC traction, particularly AT TPS, the voltage control is done by the variation of reactive power, similar to the one seen in AC power transmission system. This is mainly because voltages (magnitudes) are strongly coupled with the reactive power. Here, compensators and Pulse Width Modulated (PWM) converters are employed for variation of reactive power or reactive power compensation [41]. These devices are usually operated either by means of control signals sent remotely from the processing center or by means of a closed loop control system. The objectives of reactive power compensating devices can vary from voltage control to minimization of power losses.

III. Attack Model Against reactive power compensation/voltage control system of AT TPS

In order to develop the attack model, it is necessary to consider the possible ways in which the reactive power compensation system is automated in the context of AT TPS. These are discussed in Section III-A. This is immediately followed by a detailed discussion on the vulnerabilities in both these modes of operation in Section III-B.

A. Modes of Operation of Reactive Power Compensation

There are two modes of operation of the reactive power compensation/voltage control of AT TPS. They are as follows:

- The first mode, referred to as Mode 1 for the remainder of this paper, as shown in Figure 2a, involves the control centre. Here, the real-time data related to the trains' positions (d_{mt}), power consumption $\big((P_d + jQ_d)\big)$, and voltage profile (V_{tc}), are received by the control centre. Based on this data, appropriate compensation is determined by the control centre, which is relayed as a command to the compensation system in the AT TPS.
- The second mode, referred to as Mode 2 for the remainder of this paper, on the other hand, involves the use of a closed loop control system present in the train. In this mode, the present value of voltage, V_{tc} is compared to a reference value, V_{tc}^{ref} and the difference, i.e., the error signal is used by the controller to actuate the necessary compensation. This mode is depicted in Figure 2b.

In this paper, the details regarding implementation of these modes of operation are not dealt with. This is because the detection approach is based on the electrical quantities and does not depend on the implementation of the voltage control or reactive power compensation.

B. Vulnerabilities Against the Reactive Power Compensation System

The attack strategy against the AT TPS voltage control system would vary depending on the mode of operation discussed above.

1) Vulnerabilities in Mode 1: In the case of centrally controlled reactive power compensation system, the adversary has two choices. The first one is the corruption or falsification of data, i.e., V_{tc} and $\big(P_d + jQ_d\big)$ in Figure 2a, and positional data, d_{mt}. The falsification eventually misleads the operator to take erratic control actions. Such attacks are broadly known as False Data Injection (FDI) attacks [1]. On the other hand, the adversary could take over the command channel in Figure 2a and use it to relay malicious or false commands. These types of attacks usually have the potential of being high-impact [44].

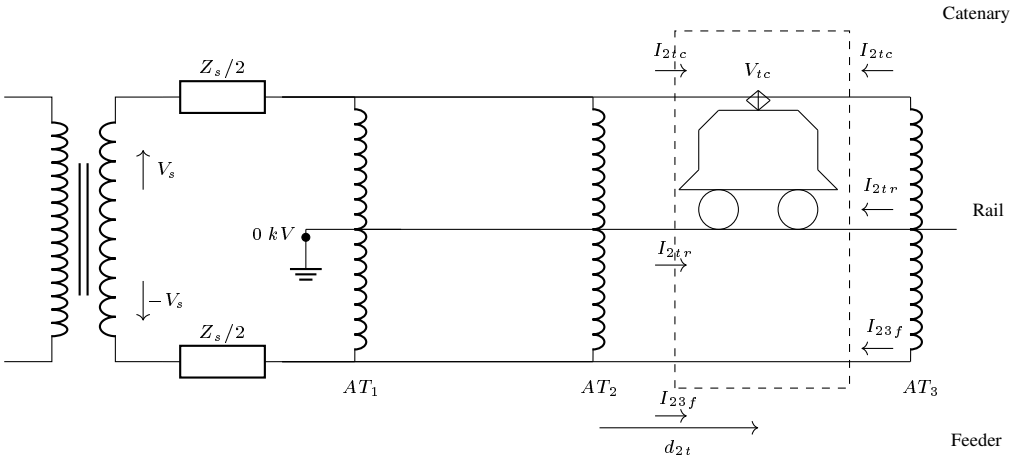
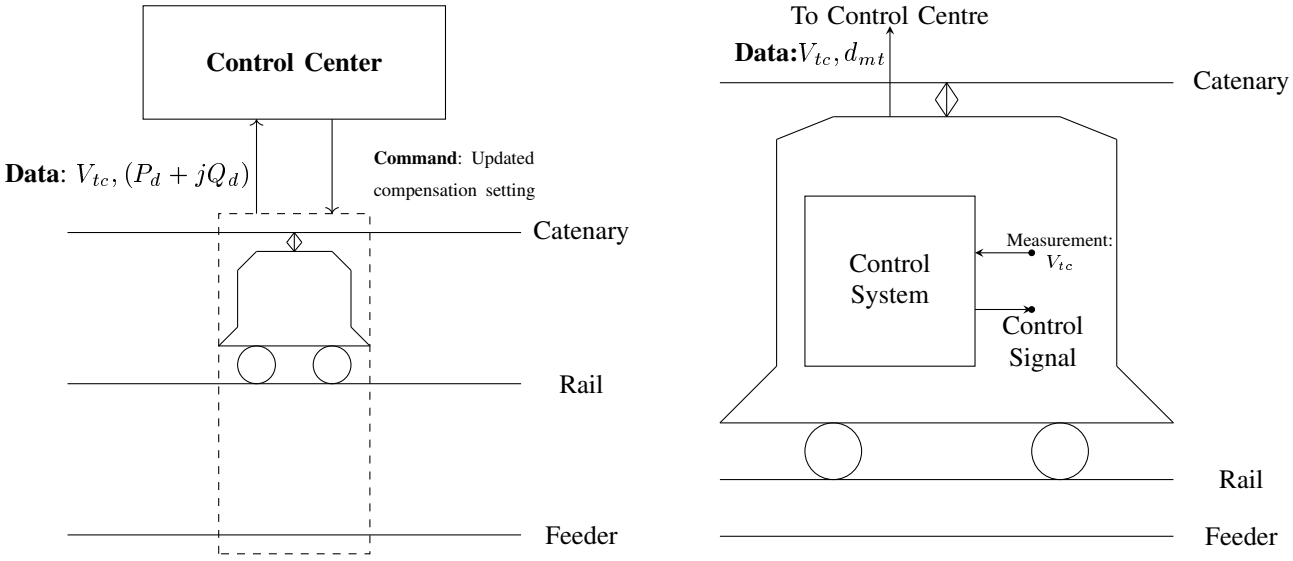


Fig. 1: Autotransformer Traction Power System (AT TPS).



(a) Centrally Controlled compensation system

(b) Local Closed loop Control System

Fig. 2: Modes of Control in Reactive power compensation/Voltage control system in AT TPS.

The network diagram in Figure 3 represents the communication of both measurements and control commands in the SCADA environment. It can be seen that in Mode 1 operation, the data pertaining to load and present voltage values from the train and its voltage control/reactive power compensation are relayed to the control centre. The control centre estimates the appropriate amount of compensation and relays it to the train's compensation system. In the case of FDI attacks [1], the data channel, marked in Figure 3 are affected or attacked. Similarly, if the adversary chooses to attack the command channels, instead of data channels in Figure 3, then it results in False Command Injection (FCI) attacks. The command channels can be attacked before commands are relayed to the train SCADA system or at the train ICT channels, as shown in Figure 3, marked by "×". Hence, as far as SCADA networks are concerned, the command channels can be attacked in a way similar to the way data channels are attacked in FDI attacks [1], [13]. However, the impact of attacks on command channels is very high when compared to attacks on data channels [44]. Whenever falsification of data is involved in centrally controlled mechanisms (reactive power compensation system in this context), the adversary has to usually inject a false data close to the operating point (or previous data points). This is because data quality checks can detect a wide variation in measurement data. However, in the case of attacks where an adversary has control over the commands, the entire control range is available.

2) Vulnerabilities in Mode 2: In this case, the adversary attacks the closed loop control system in Figure 2b. Such closed loop control systems are known to be vulnerable [45]–[47]. These systems can be targeted using a wide array of attacks [45]. These attacks are launched with the objective of disruption of the control process intended by the operator. The attacks disrupt either of the three components of the control system, i.e., the sensor (to force wrong control signal), the control signal, or the control unit itself.

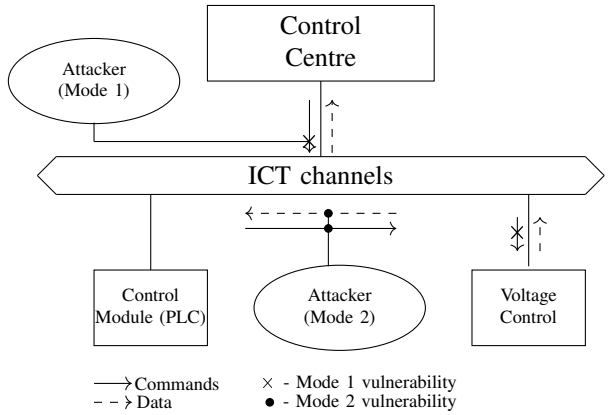


Fig. 3: Network diagram showing the vulnerabilities of voltage control/reactive power compensation system in both Mode 1 and Mode 2 operations.

The local closed loop control system is implemented using closed loop control modules, like [48], which acts as a specialized programmable logic controller (PLC). This creates a system with two components (nodes), i.e., process and the controller, in the system that interact with each other through sensor data and control inputs, as shown in the network diagram of Figure 3. Such a configuration is vulnerable to cyber attacks [49], [50], like Denial of Service (DoS) and Man-in-the-Middle (MiTM) attacks [50]. For instance, a MiTM attack can be launched to corrupt the measurement values and consequently the commands relayed to the compensation system. The points of vulnerability are appropriately marked in Figure 3. In Figure 2b, the adversary can falsify the feedback value, i.e., V_{tc} in the context of voltage control. This leads to erratic commands resulting in voltage profiles that are detrimental to the TPS and train operation. In order to have comprehensive protection, it is also necessary to consider scenarios where the actuation commands of the control systems are tampered with.

In order to ensure the reliable and safe operation of both train and TPS in the purview of automation, it is thus necessary to address these vulnerabilities. In this paper, detection strategies are proposed against the following attacks. They are as follows:

(i) Falsification of commands issued to the compensation or voltage control system in Mode 1 operation.
(ii) Falsification of V_{tc} in the voltage control system in Mode 2 operation, shown in Figure 2b.
(iii) Falsification of actuation command in the locally controlled reactive power compensation system.

IV. Scheme for Detection of Attacks on Reactive Power Compensation Mechanism in Mode 1 Operation

A. Parameters Used as Classifiers

In order to develop the parameters that can be used as classifiers, the train in Figures 1 and 2a is viewed as a six terminal network as shown below in Figure 4. In order to develop detection parameters that are independent of ICT used in the implementation, it is essential to represent them as

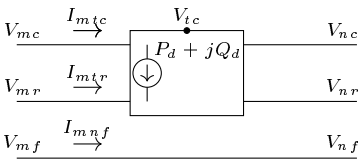


Fig. 4: Representation of the train between two ATs as a six terminal network.

a function of the terminal electrical quantities that can be practically measured and monitored by the operator in the control centre.

The current flow in the catenary from the m^{th} AT to the train can be expressed as

$$I_{mtc} = \frac{(V_{mc} - V_{tc})}{(Z_c d_{mt})}, \tag{1}$$

where, Z_c is the impedance of the catenary per unit distance, which can be obtained from $\mathbf{Z_{tx}}$ defined in Section II-A and d_{mt} is the distance of the train from the m^{th} AT. When (1) is divided by V_{mc}, we get

$$\frac{I_{mtc}}{V_{mc}} = \frac{(|V_{mc}|\angle\delta_{mc} - |V_{tc}|\angle\delta_{tc})}{(Z_c d_{mt} V_{mc})}. \tag{2}$$

In (2), the quantities in the right hand side is represented by phasors, where, δ is used to represent voltage angles.

The magnitude of the ratio in (2) is defined as

$$D_{mc} = \left|\frac{I_{mtc}}{V_{mc}}\right|. \tag{3}$$

Similarly, for the n^{th} AT and feeder, using notational conventions defined in Section II, we get

$$D_{nc} = \left|\frac{I_{ntc}}{V_{mc}}\right|, \tag{4}$$

and,

$$D_{mnf} = \left|\frac{I_{mnf}}{V_{mf}}\right|. \tag{5}$$

The parameters defined in (3), (4) and (5) can be arranged in a vector defined as

$$\mathbf{\Gamma} = \begin{bmatrix} D_{mc} & D_{nc} & D_{mnf} \end{bmatrix}^T. \tag{6}$$

The elements of $\mathbf{D}$ are estimated by the operator/control center when the upcoming settings for reactive power compensation system are chosen. The parameters estimated during the command selection, denoted by D_{mc}^{ref}, D_{nc}^{ref} and D_{mnf}, respectively, are arranged in the vector, $\mathbf{D}^{ref}$, across the section of TPS between two ATs. The comparison of $\mathbf{D}$ when compared to $\mathbf{D}^{ref}$ is the basis of the detection algorithm proposed in this paper. Hence, the detection metric can be defined as

$$\Gamma_{cen} = ||\mathbf{D} - \mathbf{D}^{ref}||_1. \tag{7}$$

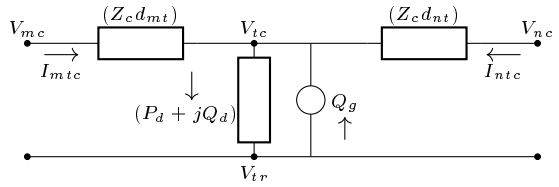


Fig. 5: Circuit diagram of train and reactive power compensation system between two ATs.

B. Practical Realization of the Detection Metric, DM

Based on the developed detection metric, Γ, in Section IV-A, there are two ways to realize its application for practical purposes. They are as follows:

- *Use of Phasor Measurements Units (PMUs):* Based on (2), a PMU placed at m^{th} AT terminal that provides the phasor, V_{mc}, would be sufficient to enable the calculation of D_{mc}. The voltage of the train, V_{tc}, is monitored by the operator. In case of an attack, V_{tc} used in (2) would be the one falsified by the adversary (usually at the value intended by the operator before the cyber attack). This is because the operator cannot know about the attack in advance and hence has to rely on the available measurements. However, it will be shown that this does not affect the detection.
- *Use of Voltage and Current Meters:* Based on (3), the use of current and voltage meters at m^{th} AT that provides the magnitudes of the current flowing out of the AT and voltage at the AT would enable the calculation of D_{mc}. In this case, the falsification of measurements does not affect the calculation of D_{mc}.

C. Justification for the Choice of Detection Metric

The justification of the use of detection parameters from (3)-(5) can be formally proven by means of the following Propositions.

Proposition 1. *Let the value of D_{mc} calculated during the selection of reactive power compensation command be D_{mc}^{ref}. During an attack involving malicious operation of reactive power compensation mechanism, let the value of D_{mc} observed by means of a PMU at m^{th} AT be D_{mc}^{p}. Then, for any TPS operation with noiseless measurements, the following relation holds good:*

$$|D_{mc}^{p} - D_{mc}^{ref}| > 0.$$

Proof. Under normal conditions, the operator selects a value of reactive power generation, Q_g^{sel}, based on $(P_d + jQ_d)$ and V_{tc}. For convenience, the circuit diagram of train and reactive power compensation system across two ATs is shown in Figure 5. The effective load of the train as seen by the TPS can be written as

$$S_d^{nor} = P_d + j(Q_d - Q_g^{sel}) \tag{8}$$

where, the superscript, nor, represents quantities under normal operation, in absence of a cyber-attack.

The current drawn by the train can be written as

$$I_{tc}^{nor} = \frac{P_d + j(Q_d - Q_g^{sel})}{(V_{tc} - V_{tr})}. \tag{9}$$

It is known that $|V_{tr}| \ll |V_{tc}|$, as rails are ideally close to zero potential [40], [41]. For the purpose of analysis, V_{tr} is thus neglected.

From Figure 5, we can see that $I_{tc} = I_{mtc} + I_{ntc}$. Under normal conditions, with noiseless measurements, based on definition in (3), we get

$$D_{mc}^{ref} = \eta_1 \left(\frac{\sqrt{P_d^2 + (Q_d - (Q_g^{sel}))^2}}{|V_{tc}|^{nor} |V_{mc}|^{nor}} \right), \tag{10}$$

where, $\eta_1 = \dfrac{I_{mtc}}{I_{tc}}$. Under a cyber-attack on reactive power compensation system, an adversary maliciously injects Q_g^{att}, where the superscript, att, is used to denote quantities under a cyber attack. When PMUs are used, it is important to note that from the perspective of the operator and detection mechanism using (2), the train voltages do not change, i.e., $V_{tc}^{att} = V_{tc}^{nor}$, as discussed in Section IV-B.

Performing an analysis similar to (8)-(10), based on discussion in Sections III and IV-B, we get

$$D_{mc}^{p} = \eta_1 \left(\frac{\sqrt{P_d^2 + (Q_d - (Q_g^{att}))^2}}{|V_{tc}|^{nor} |V_{mc}|^{att}} \right). \tag{11}$$

By comparing (10) and (11), we observe that:

- $\sqrt{P_d^2 + (Q_d - (Q_g^{sel}))^2} \neq \sqrt{P_d^2 + (Q_d - (Q_g^{att}))^2}$.
- $|V_{mc}|^{att} \neq |V_{mc}|^{nor}$, as a change in reactive power appreciably affects voltage magnitudes of connected nodes, due to their strong coupling (also discussed before).

Based on these observations, it can thus be concluded that

$$|D_{mc}^{p} - D_{mc}^{ref}| > 0.$$

Hence proved. □

Proposition 2. *Similar to Proposition 1, let the value of D_{mc} observed by means of voltage and current meters at the m^{th} AT be D_{mc}^{mag}. Then, for any TPS operation with noiseless measurements, the following relation holds good:*

$$|D_{mc}^{mag} - D_{mc}^{ref}| > 0.$$

Proof. For the purpose of this proof, notations used in the proof of Proposition 1 are used. Under normal conditions, D_{mc} would follow (10). However, the difference in this case, as opposed to that seen in Proposition 1, would be in the value of D_{mc} under a cyber attack.

When current and voltage meters are used to measure I_{mtc} and $|V_{mc}|$, the values of these quantities as seen by the detection method would be based on their true values, as none of these quantities are directly affected due to attack. As a result, the values of $|V_{tc}|$ used in the calculation of D_{mc}, to model the calculation made using I_{mtc} and $|V_{mc}|$ measurements, must be the value changed due to an attack, i.e., V_{mc}^{att}, and $V_{mc}^{att} \neq V_{mc}^{nor}$.

The expression for D_{mc}^{mag}, under a cyber-attack can be written similar to (11) as

$$D_{mc}^{mag} = \eta_1 \left(\frac{\sqrt{P_d^2 + (Q_d - (Q_g^{att}))^2}}{|V_{tc}|^{att} |V_{mc}|^{att}} \right). \tag{12}$$

The comparison of (10) and (12) yields:

- $\sqrt{P_d^2 + (Q_d - (Q_g^{sel}))^2} \neq \sqrt{P_d^2 + (Q_d - (Q_g^{att}))^2}$.
- $V_{tc}^{att} \neq V_{tc}^{nor}$.
- $V_{mc}^{att} \neq V_{mc}^{nor}$.

Hence, we get

$$|D_{mc}^{mag} - D_{mc}^{ref}| > 0.$$

□

Proposition 3. *The conditions stated in Propositions 1 and 2 hold good even in presence of measurement errors and noise.*

Proof. The measurements relevant to the calculation of D_{mc}^{mag}, under normal conditions, using current and voltage meters to calculate the magnitudes of I_{mtc} and V_{mc}, can be written in matrix form as

$$\begin{bmatrix} |I_{mtc}|^{nor} \\ |V_{mc}|^{nor} \end{bmatrix} = \begin{bmatrix} h_I(T^{nor}) \\ |V_{mc}|^{nor-t} \end{bmatrix} + \begin{bmatrix} e_I \\ e_V \end{bmatrix} \tag{13}$$

where, T is the set $\{P_d, (Q_d - Q_g), |V_{mc}|, |V_{tc}|, \delta_{mc}, \delta_{tc}\}$, the superscript, nor, denotes quantities under normal conditions, the superscript, $nor - t$, represents true value (without noise) under normal conditions, $h_I(\cdot)$ denotes "function of", and $\begin{bmatrix} e_I & e_V \end{bmatrix}^T \sim \mathcal{N}(0, \sigma)$.

When there is a cyber-attack, we observe that

$$\begin{bmatrix} |I_{mtc}|^{att} \\ |V_{mc}|^{att} \end{bmatrix} = \begin{bmatrix} h_I(T^{att}) \\ |V_{mc}|^{att-t} \end{bmatrix} + \begin{bmatrix} e_I \\ e_V \end{bmatrix} \tag{14}$$

where, the superscript, att, denotes under attack conditions. Even though the adversary hides the changes in P_d, $(Q_d - Q_g)$, $|V_{tc}|$ and δ_{mc}, the set T^{att} would only contain true values as the current meter placed at m^{th} AT can measure I_{mtc} that results from a true change in the variables contained in the set, T. As a result, it can be inferred that, $T^{att} = \{P_d, (Q_d - Q_g^{att}), |V_{mc}|^{att}, |V_{tc}|^{att}, \delta_{mc}^{att}, \delta_{tc}^{att}\}$. Hence, based on relation between measurements and variables and using notations defined in Proposition 2, it can be inferred that

$$\left|\left| \begin{bmatrix} |I_{mtc}|^{mag} \\ |V_{mc}|^{mag} \end{bmatrix} - \begin{bmatrix} |I_{mtc}|^{nor} \\ |V_{mc}|^{nor} \end{bmatrix} \right|\right|_1 > 0. \tag{15}$$

Based on the definition in (3) and the proven relation in (15), we can see that $|D_{mc}^{mag} - D_{mc}^{ref}| > 0$ holds good in presence of noise.

Using similar analysis and arguments in the proofs of Propositions 1 and 2, it can be shown that $|D_{mc}^{p} - D_{mc}^{ref}| > 0$ holds good in presence of noise. Hence, the conditions in Propositions 1 and 2 hold good in presence of noise. □

The propositions 1, 2 and 3 can be extended to other parameters defined in (4) and (5). The direct consequence of these propositions is that that the $\mathcal{L} - 1$ norm of $(\mathbf{D} - \mathbf{D}^{ref})$ is greater than zero.

Based on the definition of the index D_{mc} in (3), there are two quantities involved, V_{mc} and I_{mtc}. Let us consider the case when voltage and current meters are used to realize the detection metric, D_{mc}. From Figures 1, 4 and 5, it can be seen that V_{mc} is the voltage of the leading autotransformer (AT) (m^{th} AT) of the autotransformer section where the train is at the instant of measurement. Similarly, I_{mtc} is the current drawn from the m^{th} AT. It is important to note that the measurement quantity V_{mc} changes depending on the AT section housing the train at the instant of measurement. Similarly, I_{mtc} varies depending on both the AT section and also on the distance of the train from the leading or trailing AT in the AT section. Hence, in order to beat the detection algorithm based on D_{mc}, the attacker has to manipulate the values of V_{mc} at all the ATs in the traction line from the starting to the destination of the train. Moreover, the values of I_{mtc} also have to be manipulated continuously at every instant depending on both the AT section is housing the train and the distance of the train from the leading AT in that section. In order to beat this detection approach, the adversary has to falsify the PMU and meter data at every AT as the train passes through. As railway networks are spread across large distances, this practically implies that the adversary has to take over the entire system and control centre. However, though such controls are theoretically possible, it is not practically likely [44].

D. The Algorithm

The steps of the proposed algorithm are presented in Algorithm 1. This algorithm basically involves monitoring of Γ_{cen} defined in (7). If the value of Γ_{cen} exceeds a threshold, Th_{cen}, an attack on the reactive power compensation is detected. The calculation of Γ_{cen} depends on equipment placed in TPS to monitor the system (as discussed in Section IV-B).

The variation in D_{mc} from its normal value in both (2) and (3), are dependant on the sensitivities of several electrical quantities in (2) and (3) on a malicious change in compensation command. In power grids and traction power systems, it is well-known that the sensitivities of electrical quantities due to the variation (both normal and malicious) of dependant electrical quantities vary significantly, when compared to each other. This is a well-known phenomenon. So, sensitivities are usually calculated individually for every node or line [51]. Hence, the analysis or operation based on this is done empirically for the system where the study is done. As a result, the threshold in Algorithm 1 must be determined by the operator, based on the system where it is deployed.

Algorithm 1: Proposed algorithm to detect attacks on TPS reactive power compensation system

Data: Vector, $\mathbf{D}^{ref}$ and the predefined threshold, Th_{cen}.
Output: Tr

```
Calculate Γ_cen using (7);
if Γ_cen > Th_cen then
    Tr = 1;
    An attack on reactive power compensation system
      is detected;
    For safety, stop the train and investigate the extent
      of attack;
else
    Tr = 0;
    go back to step 1;
```

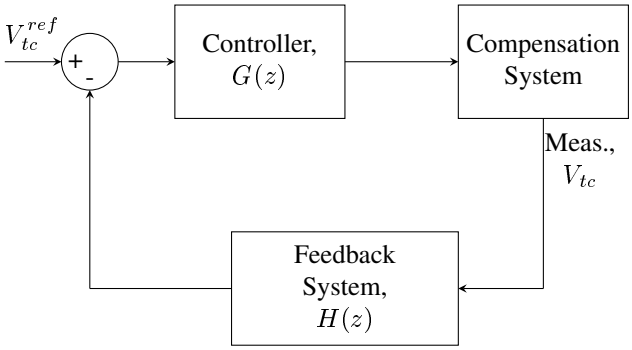


Fig. 6: Internal Closed Loop Control

V. Scheme for Detection of Attacks on Reactive Power Compensation Mechanism in Mode 2 Operation

Similar to the approach developed in Section IV, the approach to detect attacks against compensation systems controlled using a local closed loop control is based on the electrical quantities of the AT terminals in Figure 1.

A. Parameters used as classifiers

An abstraction of the closed loop control system is shown in Figure 6. It is worth noting that this is a general mathematical representation of the control system without any details of implementation. This is because the approach is based on the terminal electrical quantities which does not depend on these details.

Let $V_{tc}^{(k-1)}$ represent the measured value of the train voltage, where the superscript, $(k-1)$, represents the snapshot of measurement (discrete) at $(k-1)^{th}$ window. Let the reference signal, indicative of the scheduled or desired value of the train voltage, be represented using V_{tc}^{ref}, where the superscript, ref, indicates reference or selected value. Based on the comparison of feedback signal (based on measurement, $V_{tc}^{(k-1)}$), and reference signal, V_{tc}^{ref}, the voltage gets adjusted to V_{tc}^{k} at the next window.

Mathematically, the error signal, $E(z)$ as received by the controller can be written as

$$E(z) = V_{tc}^{ref}(z) - V_{tc}^{k-1}H(z). \tag{16}$$

The controller, on the other hand, sends the actuation signal, $A(z)$, to the compensation system, given by

$$A(z) = \big(V_{tc}^{ref}(z) - V_{tc}^{k-1}H(z)\big)G(z). \tag{17}$$

The adversary can tamper or inject a malicious feedback signal, i.e., tamper the value of V_{tc}^{k-1}, forcing the control system to take an erratic control action. In order to develop the detection metrics, the circuit diagram of Figure 5 is considered again. When looked into the network from the m^{th} and n^{th} AT sections, the Kirchoff's Voltage Law (KVL) governs

$$V_{mc} = I_{mtc}Z_c d_{mt} + V_{tc} - V_{tr}, \tag{18}$$

and,

$$V_{nc} = I_{ntc}Z_c d_{nt} + V_{tc} - V_{tr}, \tag{19}$$

respectively. In the subsequent analysis, V_{tr} is set to zero as rails are ideally at zero potential. Similarly, the mutual coupling between the catenary, rail and feeder is neglected. However, they are not neglected in the simulation studies in Section VI. With these simplifications applied to (18) and (19), we get

$$\begin{aligned} V_{tc} &= V_{mc} - I_{mtc}Z_c d_{mt} \\ &= V_{nc} - I_{ntc}Z_c d_{nt}. \end{aligned} \tag{20}$$

Based on (20), a detection metric is formulated as

$$\Gamma_{ctr} = \sum_{l \in t} |V_{lc} - I_{ltc}Z_c d_{lt} - V_{tc}|, \tag{21}$$

where, $l \in t$ indicates the AT section inside which the train is currently positioned. It can be clearly inferred that the value of Γ_{ctr} under normal conditions (when there is no cyber-attack) must be close to 0, i.e., $\Gamma_{ctr} \approx 0$.

B. Practical Implementation

From (21), the estimation of the metric requires the estimation or measurement of phasors, $V_{mc}\angle\delta_{mc}$, $V_{nc}\angle\delta_{nc}$, $I_{mtc}\angle\delta_{mtc}$ and $I_{ntc}\angle\delta_{ntc}$. This can be achieved by the following ways:

- The placement of PMUs at the AT sections. This would ensure that the phasor measurements required to estimate Γ_{ctr} in (21), would always be available . Such measurements could be used to estimate Γ_{ctr} before the execution of control action, as shown in Figure 7. It is worth noting that this additional block in the control system need not be implemented locally in the train.
- Another approach would be to use the outcome of a real time analysis of the system using the power flow studies, if there is any. In other words, use the estimated values of the phasors (using power flow analysis [41], [43]). However, in this implementation, the block used to represent detection action in Figure 7 is done at the control centre.

C. Justification for the use of the detection metric

In order to justify the use of the detection metric in (21) to classify cyber-attacks from normal operation, it is necessary to validate its effectiveness mathematically.

Proposition 4. *Under ideal conditions, when there is no noise in PMU measurements, under a cyber-attack involving malicious tampering V_{tc}^{k-1} in Figure 6, it can be stated that*

$$\begin{aligned} \Gamma_{ctr}^{nor} &= 0, \\ \Gamma_{ctr}^{att} &> 0, \end{aligned}$$

at the k^{th} window, based on measurements from the $(k-1)^{th}$ window. Here, the superscripts, nor and att denote values under normal conditions and cyber-attack, respectively.

Proof. When there is no cyber-attack, i.e., normal conditions, based on (18), (19) and (20), it can easily be seen that

$$\Gamma_{ctr}^{nor} = 0. \tag{22}$$

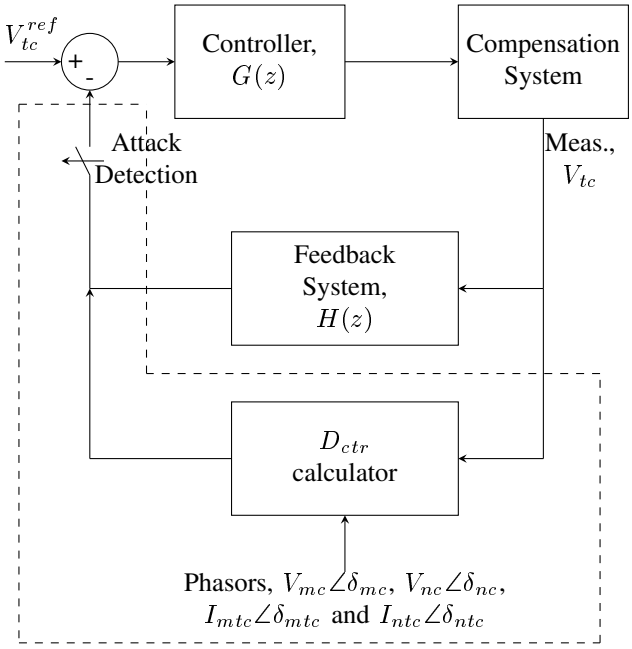


Fig. 7: Detection approach in the closed loop control

Let $V_{tc}^{k-1,nor}$ be the train voltage under normal conditions. In the case of a cyber-attack, the value of V_{tc}^{k-1} is falsified by the adversary to force a wrong control action, and this voltage is denoted by $V_{tc}^{k-1,att}$. From (20), even under a cyber-attack, it can be stated that

$$\begin{aligned} V_{mc}^{nor} &= V_{tc}^{k-1,nor} + I_{mtc}^{nor} d_{mt} Z_c, \\ V_{nc}^{nor} &= V_{tc}^{k-1,nor} + I_{ntc}^{nor} d_{nt} Z_c. \end{aligned} \tag{23}$$

Effectively, from (21) and (23), we get

$$\begin{aligned} \Gamma_{ctr}^{att} &= 2 \times |V_{tc}^{k-1,nor} - V_{tc}^{k-1,att}| \\ &> 0. \end{aligned} \tag{24}$$

Hence proved. □

In other words, if the phasor measurements of $V_{mc}\angle\delta_{mc}$, $V_{nc}\angle\delta_{nc}$, $I_{mtc}\angle\delta_{mtc}$ and $I_{ntc}\angle\delta_{ntc}$ are employed, in absence of measurement noise, the detection metric ideally captures the difference by which the adversary tampered the voltage measurement.

Proposition 5. *Under a cyber-attack involving malicious injection of actuation signal in locally controlled voltage control/reactive power compensation system, the conditions stated in Proposition 4 still hold good.*

Proof. In an attack involving malicious injection of false actuation signal, the adversary falsifies the actuation signal to the compensation system. In order to keep the malicious commands hidden, the adversary ensures the measurement feedback, i.e., V_{tc}^{k-1}, in the context of voltage control, appear or read close to the selected value (according to V_{tc}^{ref}), at $V_{tc}^{k-1,nor}$.

When the adversary injects a false actuation signal causing the train voltage to change to $V_{tc}^{k,att}$, instead of the selected V_{tc}^{nor}, when seen from the m^{th} and n^{th} AT, KVL governs that

$$\begin{aligned} V_{mc}^{att} &= V_{tc}^{k-1,att} + I_{mtc}^{att} d_{mt} Z_c, \\ V_{nc}^{att} &= V_{tc}^{k-1,att} + I_{ntc}^{att} d_{nt} Z_c. \end{aligned} \tag{25}$$

It is worth noting that V_{mc}, V_{nc}, I_{mtc} and I_{ntc} change based on the malicious changes made by the adversary. However, the train voltage measured or fed back remains at $V_{tc}^{k-1,nor}$, i.e., the value selected by the operator.

From (21) and (25), we get

$$\begin{aligned} \Gamma_{ctr}^{att} &= 2 \times |V_{tc}^{k-1,att} - V_{tc}^{k-1,nor}| \\ &> 0. \end{aligned} \tag{26}$$

□

Even in Mode 2 operation, in order to beat the detection metric in (21), the adversary has to falsify the phasors at every AT section.

D. The Algorithm

The steps in the proposed algorithm for detection of cyber-attacks in Mode 2 operation are given in Algorithm 2.

Algorithm 2: Proposed algorithm to detect attacks on TPS reactive power compensation system in Mode 2 Operation

Data: Available voltage measurement, V_{tc}^{k-1} and the predefined threshold, Th_{ctr}.
Output: Tr

```
Calculate Γ_ctr using (21);
if Γ_ctr > Th_ctr then
    Tr = 1;
    An attack on reactive power compensation system is detected;
    For safety, stop the train and investigate the extent of attack;
else
    Tr = 0;
    go back to step 1;
```

As an interesting exercise, consider the detection metric in (21). For the mathematical analysis of this paper, it is considered that the train is between the m^{th} and n^{th} ATs. So, l in (21) takes the values m and n. Based on the implementation of Algorithm 2, PMUs are used to measure the quantities V_{mc}, V_{nc}, $(I_{ltc} Z_c d_{lt})$ and V_{tc}. Based on the proof of Propositions 4 and 5, in an ideal measuring system without noise, the exact value of manipulation in V_{tc} gets captured by Γ_{ctr}. Thus, a threshold of zero would work. In the case of noisy measurements, the effect of maximum noise has to be considered. Let $|\Delta M|$ denote absolute value of maximum noise in magnitudes (for all the measured quantities). Similarly, let $\Delta\delta$ be the maximum noise in the angle measurements for the measured quantities. Let the true values of V_{mc}, V_{nc}, $I_{ltc} Z_c d_{lt}$ and V_{tc}, both magnitudes and angles, be represented with a superscript,

$true$. Let Γ_{ctr}^{max} be the value of Γ_{ctr} obtained with maximum possible noise in all measurements.

Considering maximum noise for both magnitude and angle measurements all the PMUs, the algebraic analysis of (21) yields,

$$\Gamma_{ctr}^{max} = \sum_{l\in t} \Big| (|V_{lc}|^{true} - \Delta M)e^{j(\delta_{lc}^{true}+\Delta\delta)} - (Z_c|I_{ltc}|^{true} + \Delta M)e^{j(\delta_{ltc}+\Delta\delta)} - (|V_{tc}|^{true} + \Delta M)e^{j(\delta_{tc}^{true}+\Delta\delta)} \Big|.$$

Rearranging, we get

$$\Gamma_{ctr}^{max} = \sum_{l\in t} \Big| \Big(|V_{lc}|^{true} e^{j\delta_{lc}^{true}} - Z_c|I_{ltc}|^{true} e^{j\delta_{ltc}^{true}} - |V_{tc}|^{true} e^{j\delta_{tc}^{true}} \Big) - \big(\Delta M e^{j\delta_{lc}^{true}} + \Delta M e^{j\delta_{ltc}^{true}} + \Delta M e^{j\delta_{tc}^{true}} \big) \Big|.$$

Hence, it can be seen from the derivation of Γ_{ctr}^{max} that theoretically a threshold of $6\times|\Delta M|$ (as a train can physically be between two ATs in Figure 1) can facilitate separation of attack from normal scenarios. However, based on discussion in Section IV-D regarding selection of Th_{cen}, the empirical approach can also be taken, depending on operator discretion.

VI. Results and Discussion

The developed algorithm is tested on a AT TPS, with the layout given in Figure 1, by means of simulation studies. The details regarding the AT TPS network, mainly the impedance profile, is available in [41]. In order to accurately represent the voltage and current profile of any electrical system, such as transmission systems, a power flow algorithm is needed. In the case of power transmission networks, algorithms like Newton's power flow [52] and Fast Decoupled Load Flow (FDLF) [42] give the voltage and current profile in the network, for a given generation-load pattern. Even in AT TPS, power flow algorithm must be run under both normal and attack scenarios to accurately represent the system operation. In the case of this paper, the Backward-Forward Sweep algorithm [41] is employed. Following usual practice in traction system computations, the train is modelled as a constant power load which is subject to a change in location in the network. The voltage control/reactive power compensation system is present in the train. In the simulation studies, modern Pulse Width Modulated (PWM) converters, capable of providing reactive power support are considered [41].

In Mode 1 operation, the extent of reactive power compensation required is controlled by the operator by relaying the command to the train. On the other hand, in Mode 2 operation, this adjustment, more specifically, voltage control adjustment, is performed autonomously by a control system. In this case, data pertaining to voltages and position of the locomotive are relayed to the control centre. In order to study the effectiveness of the developed algorithms, it is essential to first establish the normal condition (or the condition intended by the operator). The conditions during the normal operation of TPS are as follows:

- $P_d = 2MW$.
- $cos(\phi)$ = 0.7.
- $Q_g = 0.5$ MVAR (instructed by the operator).

In order to study the practical application of any algorithm, it is necessary to consider noise in measurements. The noise is modeled as a zero-mean Gaussian noise. The voltage and current meters have noise with $\sigma = 0.3\%$. On the other hand, voltage magnitude coming from the PMUs have $\sigma = 0.0001$ pu, whereas the angles have $\sigma = 0.001$ degrees [53]. To take the effect of noise on the performance of the algorithm into account, the algorithms are run for 100 times for each case. Important statistical parameters, viz., mean, maximum and minimum values and standard deviation, are noted.

It is important to note that voltages cannot be directly controlled in AC systems. However, they can be controlled using manipulation of reactive power, by increasing generation (positive Q_g) or decreasing generation (negative Q_g). The attack model used in Mode 1 basically involves the adversary injecting a false or malicious value of compensation command, i.e., malicious change in Q_g and subsequently hiding its effects by falsifying V_{tc} measurements. Whereas in Mode 2 operation, the attack model involves injection of wrong compensation command (control signal), i.e., maliciously change Q_g and falsify the value of V_{tc} observed by the operator.

The results are first obtained for the Mode 1 operation to test the effectiveness of Algorithm 1. Algorithm 1 can be implemented using two practical implementations, as discussed in Section IV-B. The first implementation is done using voltage and current magnitude measurements at the ATs. The results pertaining to this implementation are tabulated in Table I. Then, the results pertaining to implementation using PMU measurements are tabulated in Table II. The attacks usually involve an adversary launching a command to change the reactive power profile from the rated or selected values. As it is well-known that reactive power and voltages are strongly coupled, this malicious change also translates as change in voltages from the desired values. The attack scenarios are represented using a set of malicious reactive power injections, Q_g, in Tables I and II and include both generation and absorption.

Q_g (MVAR)	Statistical parameters			
	maximum	minimum	mean	Std. Dev.
0.5 (Normal)	19.185	0.5786	6.1099	4.3027
0.75	87.5475	44.1493	64.3421	8.3841
1	152.6512	105.6585	127.9286	8.5109
2	317.9699	255.8835	285.1978	13.4976
5	289.8798	269.3807	279.3995	3.8715
8	600.647	592.879	597.004	1.468
0	136.1866	112.6576	123.9458	5.0736
-1	334.5631	314.2343	325.235	4.069
-2	473.046	460.1412	467.128	2.369
-5	695.78	690.697	693.222	0.9555
-8	798.3677	794.98	796.6433	0.6436

TABLE I: Maximum and minimum values, mean and standard deviation of Γ_{cen} under both normal and attack scenarios using voltage and current measurements

Q_g (MVAR)	Statistical parameters			
	maximum	minimum	mean	Std. Dev.
0.5 (Normal)	41.9795	1.2497	14.7272	8.9539
0.75	176.23	125.113	154.561	10.4669
1	289.5215	251.4768	269.65	7.97
2	529.4339	505.5363	519.5976	4.5678
5	712.08	708.9159	710.5326	0.6488
8	828.163	826.5813	827.3758	0.2764
0	507.4846	330.504	403.002	29.9347
-1	188.3251	161.4878	177.4649	5.1984
-2	575.9679	554.4414	566.94	3.6809
-5	823.885	820.104	822.0967	0.7285
-8	814.1807	811.2916	812.6552	0.6403

TABLE II: Maximum and minimum values, mean and standard deviation of Γ_{cen} under both normal and attack scenarios using PMU measurements

Q_g ($MVAR$)	V_{tc} (KV)	Statistical parameters			
		maximum	minimum	mean	Std. Dev.
0.5	24.34	80.9	62.02	70.822	3.5917
0.75	24.39	39.24	22.13	29.31	3.2
1	24.43	134.01	115.01	125.64	3.77
2	24.62	524.88	505.56	515.59	3.97
5	25.10	1686.7	1669.0	1679.4	3.7
8	25.7	2835.1	2819.6	2828.5	3.1
0	24.25	277.47	256.31	267.92	3.589
-1	24.06	670.36	645.65	661.37	3.74
-2	23.87	1067.2	1039.6	1056.37	3.5
-5	23.31	2262.0	2243.5	2253.6	3.5
-8	22.7	3474.6	3453.1	3464.8	3.4

TABLE III: Maximum and minimum values, mean and standard deviation of Γ_{ctr} under both normal and attack scenarios using PMU measurements in Mode 2 operation

From Table I, it can be seen that the minimum values observed during an attack are greater than the maximum values observed under normal conditions. This holds good even when the change in reactive power generation is changed by 0.25 MVAR. Same observations can be made regarding values seen in Table II. However, it is interesting to note that the threshold, Th_{cen}, would differ depending on the type of monitoring system used. In case of measurements using PMUs, the threshold is higher. Based on the data in Tables I and II, the thresholds chosen are as follows:

- $Th_{cen} = 35$, when voltage and current magnitudes are measured using meters.
- $Th_{cen} = 75$, when PMUs are used.

It is worth emphasizing again that in these AT TPS, Bad Data Detection (BDD) is not inherently present. So, an adversary has to just corrupt the data regarding the power consumption and voltage of train to hide the injection of malicious compensation command. The attacks demonstrated in this section have been carried out taking that into account.

In order to validate the effectiveness of Algorithm 2, the testing conditions stated above are used again. In order to test the algorithm, the normal condition is same as above, where the operator chooses to inject 0.5 MVAR of reactive power to ensure that that the train voltage, i.e., V_{tc} remains in close vicinity of 24.34 KV. As it is well known that the reactive power is strongly coupled to voltages, the changes in Q_g made due to various attack scenarios also cause changes in voltages. For all scenarios, both normal condition and attacks, the detection metric, Γ_{ctr}, is calculated. As the PMU measurements are noisy, important statistical parameters are recorded. The results of this study are presented in Table III. It is important to note that in the attack scenarios studied here, which are stealthy attacks, the measured or observed values of voltages available to the operator are the normal or selected value of 24.34 KV. From Table III, it is seen that when the voltages are maliciously changed to 24.43 KV and 24.25 KV, the minimum value of Γ_{ctr} observed under a cyber-attack is greater than the maximum value of Γ_{ctr} under a normal operation. Thus, it can be concluded that a malicious change of voltage by 0.9 KV and upwards can be detected by Algorithm 2. Even in Mode 2 operation, a threshold, Th_{ctr}, must be selected similar to Th_{cen}. Based on results in Table III, $Th_{ctr} = 100$ is adequate to classify attacks from a normal scenario.

VII. Conclusions

In this paper, issues pertaining to malicious operation of reactive power compensation system/voltage control of an AT TPS are studied. This study included two broad types of attacks depending on the mode of control of the compensation system. In the first attack, which is in the context of a centrally controlled compensation system, command injection attacks are studied. Then, attacks against a local closed loop control system based operation are studied. In both these modes of operation, detection metrics are developed such that they are functions of terminal electrical quantities. Such a development of detection metrics enables the algorithms that use them to be independent of the ICT used. The effectiveness of these metrics are established mathematically using five propositions that are formally stated and proven. Subsequently the algorithms used for detection are proposed. These algorithms, when tested in a railway system using simulations, were found to be reliable. Moreover, the algorithms proposed do not include iterative steps and are easy to implement through placement of additional measurements or in some systems, using existing measurements.

References

[1] S. Lakshminarayana, Z. Teo, R. Tan, D. K. Y. Yau, and P. Arboleya, "On false data injection attacks against railway traction power systems," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016, pp. 383–394.

[2] H. Li, W. Mei, H. Zhao, Z. Huang, C. Zhang, and Z. Zhang, "Energy conscious management for smart metro traction power supply system with 4g communication loop," *Energy Reports*, vol. 7, pp. 798–807, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484721000858

[3] I. Ahmad, W. Chen, and K. Chang, "Lte-railway user priority-based cooperative resource allocation schemes for coexisting public safety and railway networks," *IEEE Access*, vol. 5, pp. 7985–8000, 2017.

[4] Siements, *Reliable rugged communications solution for Spanish railway*, 2018.

[5] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 4490–4494.

[6] 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.

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

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

[9] D. Z. Morris Brenna, Federica Foiadelli, *Electrical Railway Transportation Systems*, ser. Electric Power Systems. John Wiley & Sons, Ltd, 2018.

[10] P. Arboleya, B. Mohamed, C. González-Morán, and I. El-Sayed, "Bfs algorithm for voltage-constrained meshed dc traction networks with nonsmooth voltage-dependent loads and generators," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1526–1536, 2016.

[11] H. H. Nguyen, R. Tan, and D. K. Y. Yau, "Impact of signal delay attack on voltage control for electrified railways," in *TENCON 2015 - 2015 IEEE Region 10 Conference*, 2015, pp. 1–3.

[12] S. Lakshminarayana, T. Z. Teng, R. Tan, and D. K. Y. Yau, "Modeling and detecting false data injection attacks against railway traction power systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 4, Aug. 2018. [Online]. Available: https://doi.org/10.1145/3226030

[13] 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

[14] 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.

[15] 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.

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

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

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

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

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

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

[22] 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.

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

[24] 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.

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

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

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

[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, Nov 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, Jan 2021.

[30] ——, "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, Mar 2022.

[31] 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.

[32] 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.

[33] S. Chakrabarty and B. Sikdar, "Detection of cyber attacks on railway autotransformer traction power systems," in *2021 IEEE 2nd International Conference on Smart Technologies for Power, Energy and Control (STPEC)*, 2021, pp. 1–6.

[34] S. Karimi, P. Musilek, and A. M. Knight, "Dynamic thermal rating of transmission lines: A review," *Renewable and Sustainable Energy Reviews*, vol. 91, pp. 600–612, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032118302119

[35] C.-M. Lai and J. Teh, "Comprehensive review of the dynamic thermal rating system for sustainable electrical power systems," *Energy Reports*, vol. 8, pp. 3263–3288, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235248472200333X

[36] S. H. H. Kazmi, N. Viafora, T. S. Sørensen, T. H. Olesen, B. C. Pal, and J. Holbøll, "Offshore windfarm design optimization using dynamic rating for transmission components," *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 1820–1830, 2022.

[37] P.-Y. Wang, H. Ma, G. Liu, Z.-Z. Han, D.-M. Guo, T. Xu, and L.-Y. Kang, "Dynamic thermal analysis of high-voltage power cable insulation for cable dynamic thermal rating," *IEEE Access*, vol. 7, pp. 56 095–56 106, 2019.

[38] B. Jimada-Ojuolape and J. Teh, "Composite reliability impacts of synchrophasor-based dtr and sips cyber–physical systems," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3927–3938, 2022.

[39] ——, "Impacts of communication network availability on synchrophasor-based dtr and sips reliability," *IEEE Systems Journal*, pp. 1–12, 2021.

[40] Z. Fei, T. Konefal, and R. Armstrong, "Ac railway electrification systems — an emc perspective," *IEEE Electromagnetic Compatibility Magazine*, vol. 8, no. 4, pp. 62–69, 2019.

[41] S. Raygani, "Load flow analysis and future development study for an ac electric railway," *IET Electrical Systems in Transportation*, vol. 2, pp. 139–147(8), September 2012. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-est.2011.0052

[42] 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.

[43] K. Mongkoldee and T. Kulworawanichpong, "Current-based newton-raphson power flow calculation for at-fed railway power supply systems," *International Journal of Electrical Power and Energy Systems*, vol. 98, pp. 11–22, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014206151731267X

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] Siements, *SIMATICS7-300FM 355 closed-loop control module*, 2011.

[49] 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.

[50] 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.

[51] 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.

[52] W. F. Tinney and C. E. Hart, "Power flow solution by newton's method," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-86, no. 11, pp. 1449–1460, 1967.

[53] V. Murugesan, *Error Detection and Error Correction for PMU Data as Applied to Power System State Estimators*, ser. M.S. Thesis. Arizona State University, 2013.

Shantanu Chakrabarty is currently working as Senior Research Scientist in NCS Pte. Ltd., Singapore, and as Adjunct Senior Research Fellow in School of Computing (SoC), National University of Singapore. Previously, he worked as Research Fellow in Department of Electrical and Computer Engineering, National University of Singapore. He received B.E. degree in electrical engineering from the University College of Engineering (Autonomous), Osmania University, in 2010, and M.E. and Ph.D. degrees in electrical engineering from the Indian Institute of Science, Bengaluru, in 2012 and 2018, respectively. His areas of interest include power system analysis, smart grid cybersecurity, critical infrastructure cybersecurity, robotics security and internet of things (IoT) 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 the 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 for IoT and cyber physical systems. 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* and the *IEEE Transactions on Mobile Computing* and currently serves on the editorial board of *IEEE Internet of Things Journal*.