Detection of Cyber Attacks on Railway Autotransformer Traction Power Systems

Shantanu Chakrabarty
Department of Electrical and Computer Engineering
National University of Singapore
Singapore
shantanu@nus.edu.sg

Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—The safe and reliable operation of traction power systems that power railways are crucial to the uninterrupted functioning of this critical public infrastructure. In modern times, traction power systems and railways, in general, are seeing increasing penetration of information and communication technologies (ICT). Traction power systems, like smart grids, have reactive power compensation mechanisms which are controlled remotely through ICT channels. ICT channels are inherently vulnerable to cyber attacks, rendering reactive power compensation mechanisms vulnerable. Malicious reactive power settings through a cyber attack can either hamper the voltage profiles of the traction power system or disrupt the efficient operation, resulting in losses and unsafe operation. In this paper, such attack scenarios are investigated in detail and a methodology is developed to detect such attacks. The proposed methodology is based on detection metrics that are a function of electrical quantities in both train and traction power systems. The effectiveness of these metrics to classify attacks from normal scenarios is justified along with implementation details. The proposed detection method is 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

Like any other critical infrastructure, railways need to function safely and reliably. Modern railway systems are complex cyber-physical systems [1]. Several operations like train control and traction power system control, which were traditionally done manually, are increasingly being delegated to computers. Thus, a very important part of modern railways is the information and communication technology (ICT). This modernization of railways enables convenience and expansion. However, ICTs are inherently vulnerable to cyber-attacks. Any adversary with sufficient motivation and know-how can breach these systems to cause human harm and financial losses. Attacks on critical infrastructures [2], [3] are examples of exploitation of inherent vulnerabilities in ICT. Thus, effective protection strategies must be developed to prevent and detect attacks that exploit vulnerabilities of ICT embedded in critical infrastructure, especially railways.

Modern railways have several components that enable its smooth functioning. One of the most important components is the Traction Power System (TPS). This paper is centered around cyber-security of TPS. A major concern for the safe and reliable operation of an AC grid (even smart grids) is the control of reactive power, or equivalently, voltage [4], [5]. In AC TPS, voltage and reactive power control is crucial for safe operation of the grid, as voltages outside the safe range cannot be permitted [6]. Voltage control can also be seen in DC power grids, where schemes have been developed to regulate the power drawn by the train when the voltage dips or swells beyond safe values [1], [7].

The Autotransformer (AT) Traction Power Systems (TPS) is widely used to power modern railways [8]. In AT TPS, a reactive power compensation system is implemented [9] where the objective can be either voltage control or loss minimization. This compensation system is operated by the operator by sending signals remotely [9], i.e., through the ICT systems. These systems are inherently vulnerable to cyber attacks [2], [3]. It is well-known that in AC supply systems, voltages are strongly coupled to reactive power [10]. Thus, a misuse of this compensation system can push the voltages outside the safe range of operation, potentially destabilizing the TPS. Thus, protection of this system against cyber-attacks is extremely important. This paper is focused on the development of a mechanism that is capable of detecting attacks against reactive power compensation in AC TPS.

The literature on cyber security of traction power systems is sparse [1], [11], [12]. The works in [1] and [12] are centered around False Data Injection (FDI) attacks in the context of DC TPS. FDI attacks are well-investigated under the purview of smart grid security [13]–[16]. In smart grids, the malicious changes caused by cyber-attacks must pass through Bad Data Detection (BDD) [13], [14]. *However, BDD is not inherently present in railway systems [12], especially AC TPS.* In [1], FDI attack strategies against overcurrent and squeeze controls (used to control voltages) are studied and detection and prevention schemes are proposed to protect DC TPS against FDI attacks. In [11], the impact of signal delay attack (where the timing information of voltage measurements is maliciously corrupted) on voltage control is studied. However, attacks where the adversary takes over the command channels are not investigated. An adversary with access to supervisory control can have a severe impact [17].

978-1-6654-4319-7/21/$31.00 ©2021 IEEE.

This paper is focused on the study of attacks where the adversary takes over supervisory control (control of commands) of the reactive power compensation system in AT TPS. As discussed above, a misuse of reactive power compensation can have adverse effects. Furthermore, an adversary with access to supervisory control of reactive power compensation has the entire range of control available to him/her. In this paper, the threat model and attack scenarios are established. This is followed by the development of an algorithm to detect such attacks, even if they are carried out stealthily (such that the operator does not detect them through existing mechanisms). This is the first paper to address the problem of cyber attacks on AT TPS.

The contributions of this paper are as follows:

1) An algorithm is developed that can detect attacks where an adversary injects malicious commands to change the settings of the reactive power compensation system in AC TPS.
2) The developed algorithm
   a) is computationally inexpensive, as there are no iterative steps involved.
   b) does not require historical data.
   c) is reliable when tested using simulations.
   d) is simple to implement.
   e) relies on electrical parameters information, so it is independent of ICT systems used.
   f) is first to consider such attacks and propose countermeasures against such 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 algorithm to detect the attack scenarios, discussed in Section III, is developed and proposed in Section IV. The details pertaining to the simulation study are given in Section V. Finally, the conclusions are drawn in Section VI.

II. Background

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

A. Autotransformer Traction Power System

In this section, aspects of the model of AT TPS that are relevant to this paper are presented. The AT TPS has four main components [9], [18]: (i) Traction Substation (TSS), (ii) Autotransformers (ATs), (iii) Feeder system that transmits power, and (iv) Electric Train. These components are shown in Figure 1, using their circuit analysis models [9], [18]. The traction substation (TSS) transformer is represented as an ideal single phase transformer with an AT, whose midpoint is connected to rail at zero potential (ideally). ATs are represented as a voltage sources in series with the leakage impedances. 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 [9]).

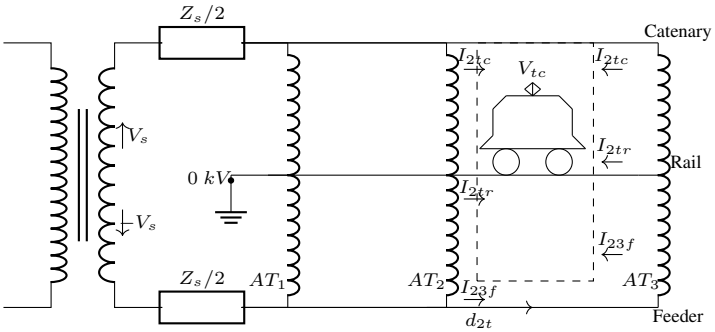

Fig. 1: Autotransformer Traction Power System (AT TPS).

- 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 [9] or Newton's method [18].

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 [9]. These devices are usually operated by means of control signals sent remotely from the processing center. The objectives of reactive power compensating devices can vary from voltage control to minimization of power losses.

III. Threat Model

In the operation of reactive power compensation of AT TPS, illustrated using Figure 2, the real-time data regarding the trains' positions and power consumption profiles (i.e., V_{tc} and $(P_d + jQ_d)$) are necessary for the control center to determine

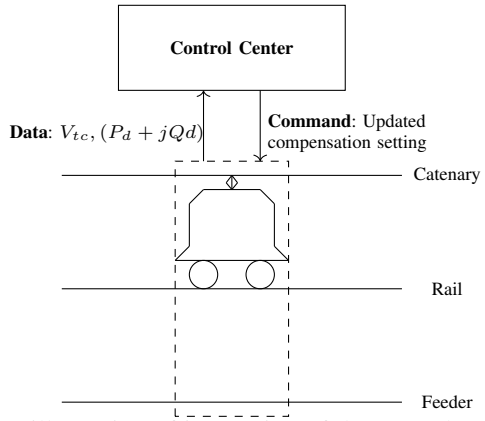

Fig. 2: An illustration of interaction of the control center with train and TPS for reactive power compensation.

the compensation required. Once the control action (adequate compensation) is determined, updated command is relayed to the compensators, either placed in the TPS or inside the train.

In order to attack this mechanism and hinder the safe operation of the TPS, an attacker has two choices. They are as follows:

- The first choice is that the attacker corrupts V_{tc} and $(P_d + jQ_d)$) in Figure 2 and the positional data of the train, eventually misleading the operator to take erratic control actions, also broadly known as False Data Injection (FDI) attacks [1].
- The other choice for the attacker is to attack command channel, shown in Figure 2, through which updated reactive power compensation setting is relayed. An attack of this nature is considered to have a very high impact [17]. In case of attacks involving injection of false data, usually an attacker has to inject data around the true measurement observed in previous windows [1], as data quality checks can detect a wide variation in measurements. However, in case of attacks where the command channels are attacked, the entire control range is available to the adversary. **The paper is focussed on such attacks on reactive power compensation commands.**

The attack model considered in this paper is as follows: The adversary relays a false setting to the reactive power compensation system and falsifies the feedback data (voltages and power consumption profile) using values selected by the operator which does not raise any alarm. The rest of the paper deals with the algorithm proposed to detect such attacks.

IV. Scheme for Detection of Attacks on Reactive Power Compensation Mechanism

A. Parameters used as classifiers

In order to develop the parameters that can be used as classifiers, the train in Figures 1 and 2 is viewed as a six terminal network as shown below in Figure 3. It is intended to express the detection parameters as a function of the terminal electrical quantities that can be practically measured and monitored by the operator in the control center.

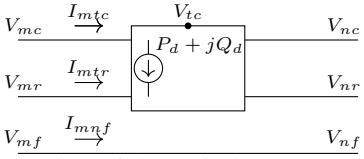

Fig. 3: Representation of the train between two ATs as a six terminal network.

The current flow in the catenary from the m^{th} AT to the train can be written 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 (this information is also included in $\mathbf{Z_{tx}}$) and d_{mt} is the distance of the train from the m^{th} AT. Now, dividing (1) by V_{mc} and using phasor representations in the right hand side, we get

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

where, δ represents 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

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

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

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

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

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

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

B. Practical Realization of the Detection Metric, DM

Based on the developed detection metric, DM, 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

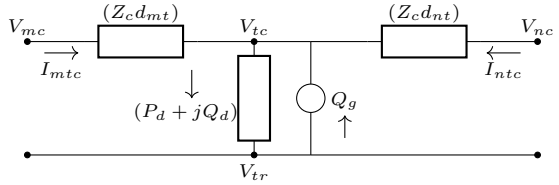

Fig. 4: Circuit diagram of train and reactive power compensation system between two ATs.

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 of 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 4. The effective load of the train as seen by the TPS can be written as

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

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 [8], [9]. For the purpose of analysis, V_{tr} is thus neglected.

From Figure 4, 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 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 normal 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.

In order to beat this 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 center. However, though such controls are theoretically possible, it is not practically likely [17].

D. The Algorithm

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

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

Data: Vector, $\mathbf{D}^{ref}$ and the predefined Threshold, Th.
Output: Tr

```
Calculate DM using (7);
if DM > Th then
    Tr = 1;
    An attack on reactive power compensation system
      is detected;
else
    Tr = 0;
    go back to step 1;
```

V. Results and Discussion

The developed algorithm is tested on a AT TPS [9] with layout given in Figure 1. The impedance parameters are available in [9]. The train is modeled as a constant power load. In this section, it is considered that the train contains Pulse Width Modulated (PWM) converters that can also provide reactive power support [9]. The extent of reactive power compensation is controlled by the operator by relaying the command to the train, depending on the requirement. In order to study the effectiveness of the developed algorithm, it is essential to first establish the normal condition (or the condition intended by the operator). For the purpose of analysis of the system, various values (measurements) are generated using a load flow algorithm. In this paper, the Backward-Forward Sweep (BFS) algorithm is used [9]. 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 [19]. To account for the effect of noise in the performance of the algorithm, the algorithm is run for 100 times for each case. Important statistical parameters, viz., mean, maximum and minimum values and standard deviation, are noted. The results are first obtained using voltage and current magnitude measurements at the ATs. These results are tabulated in Table I. Then, the results 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. The attack scenarios are represented using a set of malicious reactive power injections, Q_g in Tables II and I and include both generation and absorption.

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

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 DM 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 DM under both normal and attack scenarios using PMU measurements

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, 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 threshold chosen are as follows:

- $Th = 35$, when voltage and current magnitudes are measured using meters.
- $Th = 75$, 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 has been carried out taking that into account.

VI. Conclusions

In this paper, issues pertaining to malicious command injection in reactive power compensation system of an AT TPS are studied. Various attack scenarios are investigated and based on the results, an algorithm is developed to detect such attacks. The algorithm uses detection metrics that are functions of electrical parameters of the AT TPS and the train. Theoretical justifications for the applicability of these detection metrics for the separation of attacks from normal scenarios are presented. The proposed algorithm is a simple, one step algorithm that is computationally inexpensive. The proposed algorithm is found to be reliable when investigated using simulation studies. It is important to note that this is first paper to address cyber attacks on AT TPS in railway systems.

Acknowledgment

This work is supported in part by Ministry of Education, Singapore under Academic Research Funds R-263-000-E78-114 and R-263-001-E78-114.

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] 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.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] 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

[10] 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.

[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] 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.

[18] 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

[19] 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.