A Methodology for Detecting Stealthy Transformer Tap Command Injection Attacks in Smart Grids

Shantanu Chakrabarty and Biplab Sikdar

***Abstract*—On-Load Tap Changing transformers are a widely used voltage regulation device. In the context of modern or smart grids, the control signals, i.e., the tap change commands are sent through SCADA channels. It is well known that the power system SCADA networks are prone to attacks involving injection of false data or commands. While false data injection is well explored in existing literature, attacks involving malicious control signals/commands are relatively unexplored. In this paper, an algorithm is developed to detect a stealthily introduced malicious tap change command through a compromised SCADA channel. This algorithm is based on the observation that a stealthily introduced false data or command masks the true estimation of only a few state variables. This leaves the rest of the state variables to show signs of a change in system state brought about by the attack. Using this observation, an index is formulated based on the ratios of injection or branch currents to voltages of the terminal nodes of the tap changers. This index shows a significant increase when there is a false tap command injection, resulting in easy classification from normal scenarios where there is no attack. The algorithm is computationally light, easy to implement and reliable when tested extensively on several tap changers placed in an IEEE 118-bus system.**

***Index Terms*—Cyber security, stealthy attacks, smart grids**

I. Introduction

On Load Tap Changing transformers (also known as OLTCs) are widely used in power networks to regulate bus/node voltages [1]-[3]. They achieve voltage control by manipulation of reactive power flows, as these two quantities are strongly coupled [2]. The change in tap ratios, in the context of smart grids, are sent as commands through the SCADA channels. Unfortunately, these SCADA channels are vulnerable to cyber attacks [4]-[7]. In light of these threats, this paper is an attempt to detect a stealthily injected malicious tap change command through a compromised SCADA channel.

A. Literature Review

The most widely studied cyber-attacks on power system SCADA is the False Data Injection (FDI) attacks [8]-[21]. In these attacks, the adversary carefully chooses the malicious data so that the Bad Data Detector (BDD) [22] is not triggered.

There are few works concerning attacks on voltage control [16], [17], [19]. However, these essentially consider incorrect control actions due to FDI attacks. The work in [16] considers attacks on the "centralised voltage control scheme" of a distribution system. Here, the sensed voltages are subject to manipulation, resulting in unnecessary change of tap ratios. The detection is achieved by means of the past data related to the behaviour of current values. The attacks considered in [16] cannot be carried out in systems where there is a state estimator with bad data detection because the false data would be filtered out as bad data due to redundant power measurements. Similar limitations of the attack model in [16] can be seen in [17], where it is assumed that the adversary has access to only voltage measurements in a distribution system, but not the power injection measurements. Thus, the detection methods in [16], [17] cannot be applied in the context of transmission systems where there is state estimation with bad data detection. The authors of [19], on the other hand, consider attacks on the "Automatic Voltage Control" handled by the Energy Management Systems (EMS) in transmission networks. In the voltage control system considered in [19], the control parameters are active and reactive power generation which are estimated by solving an optimal power flow problem. In [19], a reinforcement learning based approach is employed to detect the injection of false data to maliciously influence the control mechanism.

As far as false command injection based attacks are concerned, the available literature is sparse [23], [24]. In [21], [23], [24], it is mentioned that the attackers who caused the 2015 Ukraine blackout, had control of the circuit breakers disconnecting various parts of the system. This is an example of attacks by means of malicious commands in the context of a power grid.

B. Motivation

Based on the survey of literature, it can be concluded that the aspect of malicious command injection attacks on power grids is relatively unexplored. The 2015 Ukraine blackout [23] clearly shows the importance of protection against such attacks. This paper is an attempt to address one of these issues. The aim of this paper is to develop a detection algorithm to detect the injection of a false or malicious tap change command relayed through a compromised SCADA channel. The algorithm is designed such that it can detect the presence of such attacks, even if they are carried out stealthily.

C. Contributions

In this paper, an algorithm is developed to detect the injection of malicious tap change commands. Based on the review of literature, this is the first paper which considers this class of attacks. The developed algorithm is shown to have the following features:

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

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

- Easy to implement.
- Computationally inexpensive.
- Accurate.

The organization of the paper is as follows: An overview of the background information regarding state estimation and bad data detection is presented in Section II. The various attack scenarios involving stealthy injection of malicious tap change commands are discussed in Section III. The proposed algorithm and its development are discussed in Section IV. The simulation results validating the applicability and accuracy of the proposed algorithm are presented in Section V. Finally, conclusions are drawn in Section VI.

II. Background

A. State estimation

The measurements, when expressed as a function of state variables can be written as

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

Here, z_i is the i^{th} measurement, $h_i(\mathbf{x})$ is the function which relates h_i with the state variables. and e_i is the measurement error with zero mean and a variance of σ_i^2. The weighted least square estimation [22] involves minimising

$$J(\mathbf{x}) = \frac{1}{2}\sum_{i=1}^{m}\left[\frac{z_i - h_i(\mathbf{x})}{\sigma_i}\right]^2 \tag{2}$$

subject to the basic equality constraints of node power balance. To find $\mathbf{x}$ that minimises $J(\mathbf{x})$, it is necessary to solve

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

according to the first order optimality condition.

When Taylor series expansion of the first order derivative of $J(\mathbf{x})$ is obtained and terms above order 1 are neglected, the following iterative process is obtained.

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

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

where, $G = H^T R^{-1} H$ is the gain matrix, R is a diagonal matrix with measurement variances as entries and H is the Jacobian matrix. The transformer taps can be augmented as state variables and measurements (if available) to this formulation of state estimation [25].

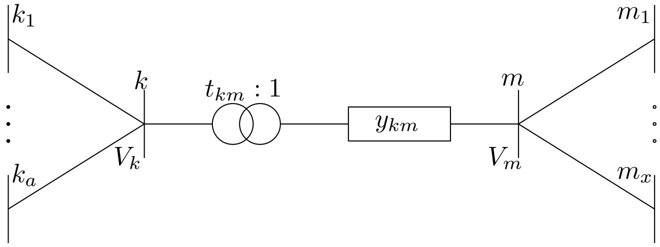
B. Bad Data Detection

Bad data detection is the mechanism to detect faulty and infeasible measurements (according to principles of power system operation). The most commonly used bad data detection technique is based on χ^2 testing [22]. The first step is to determine the measurement residual

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

Then, a threshold, T is found using the error distribution of measurements and χ^2 test. If it is found that $||r||_2 > T$, then EMS is notified of the presence of bad data.

Figure 1. A tap changing transformer with other nodes in its vicinity



III. Transformer Tap Setting Attack Scenarios

The attack on transformer tap control is essentially different from FDI attacks. In this attack, the control command is tampered, unlike measurements in FDI attacks. This attack on tap control can be carried out openly or stealthily. In the context of this paper, stealthy attacks are considered as the attack model. To hide any malicious change in tap values, it is necessary for the attacker to ensure that the estimated and measured values of tap and the parameter it controls, i.e., the bus voltage appear close (as measurements are noisy) to the selected values. This can be achieved by a selective injection of false data [15].

Consider the one line diagram in Figure 1. Here, a tap ratio t_{km} is varied to achieve control of the voltage of the bus k, i.e, V_k. There are two possibilities or cases of stealthy attacks.

A. Case 1: When only the malicious change in tap ratio is hidden

In order to hide a malicious change in t_{km}, firstly, the measurement device relaying tap ratio information must be tampered. However, this action alone cannot hide the attack as power measurements which are a function of tap ratio, t_{km} reveal their true value during state estimation and can be used to notify EMS of faulty tap setting information. So, for a stealthy attack, the following measurements must also be tampered:

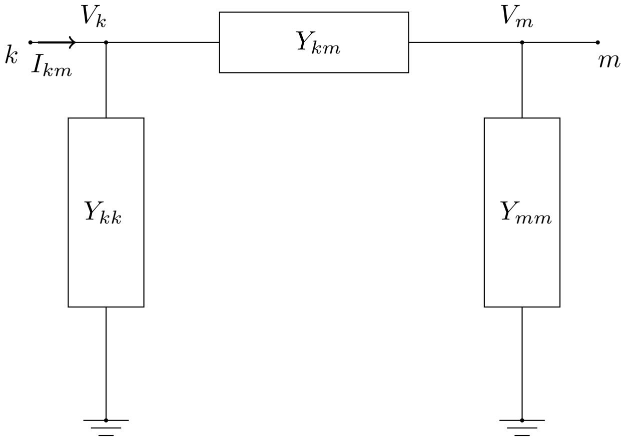
(i) Active and reactive power injections of nodes k and m.
(ii) Active and reactive power flows between nodes k and m.

B. Case 2: When changes in both tap ratio and regulated bus voltage are hidden

It is worth noting that a malicious change in tap ratio, even if it is hidden, changes the bus voltage V_k. If there is significant deviation of V_k from its scheduled value, an investigation will be launched. Thus, for an attack to remain completely hidden, measurements which are function of both t_{km} and V_k must be tampered. This ensures that both the estimation and measurement of t_{km} and V_k remain close to the values selected by the EMS. The additional measurements which must be altered are listed as follows:

(i) Voltage measurement at bus k.
(ii) Active and reactive power injections of buses connected to k.
(iii) Active and reactive power flows between k and the other buses connected to it.

Figure 2. Equivalent π-network representation of a tap changing transformer



It can be seen that the effort required to carry out a stealthy malicious tap injection attack is similar to a FDI attack. The attack in Case 1 remains stealthy when tap is used along with other parameters to achieve certain objective (for example, minimization of reactive power loss) as its effects cannot be readily observed. However, when taps are used to maintain voltages, the attack in Case 2 is required in order to remain stealthy.

IV. Scheme for Detection of Transformer tap Setting Attack

A. Transformer tap equivalent circuit

Transformer taps are modelled as a π-network [26], like a transmission line. In case of taps, the series and shunt admittances are a function of the tap ratios. The transformer tap in Figure 1 can be represented by an equivalent π-network in Figure 2. In the π-network, the equivalent admittances are

$$Y_{km} = t_{km} y_{km} \tag{7}$$

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

$$Y_{mm} = y_{km}(1 - t_{km}). \tag{9}$$

B. The quantity used as a classifier

The apparent power flow between k and m, S_{km} can be expressed as

$$S_{km} = V_k I_{km}^*. \tag{10}$$

(10) can be rearranged as

$$I_{km} = \frac{S_{km}^*}{V_k^*} \implies \frac{I_{km}}{V_k} = \frac{S_{km}^*}{|V_k|^2} \tag{11}$$

Let $\left(\dfrac{I_{km}}{V_k}\right)$ in (11) be denoted as YY_{km}.

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

$$YY_{mk} = \frac{I_{mk}}{V_m} = \frac{S_{mk}^*}{|V_m|^2}, \tag{12}$$

The quantities YY_{km} and YY_{mk} are the admittances seen by the current flowing between nodes k and m. Performing similar steps on the apparent power injections of buses k and m, we get

$$YY_k = \frac{I_k}{V_k} = \frac{S_k^*}{|V_k|^2} \tag{13}$$

$$YY_m = \frac{I_m}{V_m} = \frac{S_m^*}{|V_m|^2}. \tag{14}$$

The values of YY_{km}, YY_{mk}, YY_k and YY_m are determined when the tap is selected by the EMS. Let the values of YY_{km}, YY_{mk}, YY_k and YY_m estimated during tap selection be YY_{km}^{ref}, YY_{mk}^{ref}, YY_k^{ref} and YY_m^{ref}, respectively. These values, estimated during tap selection are referred to as “reference values”.

In order to quantify the change observed in YY_{km} when compared to its reference value, the following index is defined:

$$YYD_1 = \Big| |YY_{km}| - |YY_{km}^{ref}| \Big| \tag{15}$$

Similar indices can be defined for the other three quantities as follows:

$$YYD_2 = \Big| |YY_{mk}| - |YY_{mk}^{ref}| \Big| \tag{16}$$

$$YYD_3 = \Big| |YY_k| - |YY_k^{ref}| \Big| \tag{17}$$

$$YYD_4 = \Big| |YY_m| - |YY_m^{ref}| \Big|. \tag{18}$$

C. Justification

Whenever there is a hidden attack, the values of indices defined in Equations (15) to (18) increase significantly compared to the values seen during normal conditions, when there is no attack. The reason for such an observation can be easily explained using index YY_{km} as an example, as shown below.

The current flow between node k and node m in Figure 2 can be written as

$$I_{km} = Y_{kk} V_k + Y_{km}(V_k - V_m). \tag{19}$$

Using (7) and (8), (19) can be expressed as

$$I_{km} = t_{km}^2 y_{km} V_k + y_{km} V_m. \tag{20}$$

Dividing both sides by V_k,

$$YY_{km} = \frac{I_{km}}{V_k} = t_{km}^2 y_{km} + y_{km}\Big(\frac{V_m}{V_k}\Big). \tag{21}$$

YY_{km} can be further expanded as

$$YY_{km} = t_{km}^2 y_{km} |V_k|^2 - t_{km} |y_{km}| |V_m| |V_k| e^{j(\delta_m - \delta_k + \theta_{km})} \tag{22}$$

where $y_{km} = |y_{km}| \angle \theta_{km}$, $V_k = |V_k| \angle \delta_k$ and $V_m = |V_m| \angle \delta_m$.

As discussed in Section III, the adversary only needs to ensure that the state variables $|V_k|$ and t_{km} remain close to their selected values, i.e., these variables remain unchanged from the values seen when there is no cyber-attack. The other state variables remain unaffected, i.e., their estimated and measured values change due to the hidden attack. This causes the absolute value of YY_{km} to change significantly from the values seen during normal operation (where YY_{km} is close to YY_{km}^{ref}). This results in a significantly higher value of the index YYD_1 when there is a cyber-attack. Similarly, the increase in the other three indices can also be explained.

D. Complete Formulation of the Classifier

In order to detect the attack, an index is formulated. If this index exceeds certain threshold value, then it is declared that the tap control is under attack. This index is formulated by adding the individual indices defined in Equations (15) to (18). Thus, the single index or quantity which can be used to formulate the algorithm is as follows:

$$YYD = \sum_{i=1}^{4} YYD_i. \tag{23}$$

It can be seen that this classifier is fairly simple to implement with few additional lines of code at EMS for each of the taps.

E. The Algorithm

The steps of the proposed algorithm are given in Algorithm 1. This algorithm involves comparison of the index YYD in (23) with a predefined threshold, Th. The selection of this predefined threshold, Th is discussed in Section V-A.

Algorithm 1: The algorithm of the developed method to detect hidden false transformer tap command injections

```
Data: The reference values $YY_{km}^{ref}$, $YY_{mk}^{ref}$, $YY_{k}^{ref}$
      and $YY_{m}^{ref}$ and the predefined Threshold $Th$
Output: Trig
1 Calculate $YYD$ using (23);
2 if $YYD > Th$ then
3     Trig = 1;
4     The presence of a false tap command is detected;
5 else
6     Trig = 0;
7     go back to step 1;
```

V. Simulation Results

The algorithm developed to detect the presence of an attack on tap settings is tested on a 118-bus system [27]. In this system, six tap changing transformers are placed and their details are given in Table I. The tap ratios are assumed to vary between 0.9 and 1.1 in steps of 0.025 (i.e., 2.5% of the winding).

The selected tap value (using [1]) and the regulated bus voltages are given in Table II. In order to test the developed algorithm, stealthy attacks have to be created such that the measurements and the estimated values of the tap settings and regulated bus voltages read values in close vicinity to the ones given in Table II. Thus, measurements which are related to the tap values and regulated bus voltages are manipulated as discussed in Section III. Using these principles of stealthy attacks, three sets of stealthy attacks are designed as test cases. They are:

- **Case 1:** When the adversary changes the tap settings by two or more than two steps.
- **Case 2:** When the tap settings are changed by just one setting.
- **Case 3:** When the tap settings are changed by just one setting and the load changes. As a representative of the effects of load changes, two cases are considered:
  - **Case 3a:** When load is increased by 10%.
  - **Case 3b:** When load is decreased by 10%.

The measurement errors or noise is considered to be 1% for power measurements and 0.3% for voltage measurements [28], [29]. Thus, in order to study the variation of the developed index YYD due to noise, in every case(including the case when there is no attack), the simulations are run for 200 times.

The accuracy of the developed algorithm is tabulated in Table III. It can be seen that that the algorithm detects the attack in all the cases. To further establish the results shown in Table III, the necessary statistical parameters, i.e., mean, minimum, maximum and standard deviation are recorded for all the cases in tables IV to VIII. From the values in these tables, it is clear that the minimum values of YYD observed in all the attacks (as seen in Tables V to VIII) are significantly higher than the maximum values of YYD observed when there is no attack (as seen in Table IV).

Another important aspect to note is that the reference values of indices in the calculation of index YYD can be prone to errors. Logically, if the reference values are erratic, then the selected tap ratio would not meet the specified voltage. When there is no false tap command, this would be indicated by the estimated and measured voltages of the regulated buses. This

Table I
DETAILS OF THE LOCATION AND REGULATED BUSES OF THE TRANSFORMER TAPS CONSIDERED

Tap number	FB[1]	TB[2]	RB[3]
1	11	13	11
2	30	17	30
3	38	37	38
4	64	61	64
5	96	97	96
6	114	115	114

[1] From Bus
[2] To Bus
[3] Regulated Bus

Table II
THE SPECIFIED VOLTAGES OF THE REGULATED BUSES AND THE TAP SETTINGS REQUIRED TO ACHIEVE IT

Tap number	RB[1]	V^{sp}[2]	t_{km}^{sp}[3]
1	11	0.9836	1.025
2	30	0.9934	1.025
3	38	0.9729	1.05
4	64	0.9875	1.025
5	96	0.9882	1.025
6	114	0.95	1.025

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

Table III
ACCURACY OF THE DEVELOPED METHOD ACROSS ALL THE CASES

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

Table IV
The mean, minimum, maximum and standard deviation of the computed YYD values when there is no attack

Tap number	Mean	Minimum	Maximum	Standard Deviation
1	0.0136	0.0016	0.0404	0.0075
2	0.0198	0.0047	0.0452	0.0084
3	0.026	0.0058	0.0621	0.0111
4	0.0241	0.0043	0.0621	0.0111
5	0.0170	0.001	0.0482	0.0093
6	0.0170	0.0021	0.0426	0.0074

Table V
The mean, minimum, maximum and standard deviation of the computed YYD values when tap ratio is manipulated by 0.05(Case 1)

Tap number	Mean	Minimum	Maximum	Standard Deviation
1	0.5969	0.5812	0.6156	0.0067
2	1.28	1.2512	1.3121	0.0130
3	1.1267	1.0697	1.1802	0.0180
4	0.749	0.7279	0.7916	0.0118
5	0.6236	0.5689	0.6776	0.0201
6	8.0305	7.961	8.1037	0.027

Table VI
The mean, minimum, maximum and standard deviation of the computed YYD values when tap ratio is manipulated by 0.025(Case 2)

Tap number	Mean	Minimum	Maximum	Standard Deviation
1	0.5365	0.5126	0.5646	0.0112
2	0.3631	0.3226	0.4002	0.0134
3	0.3434	0.3070	0.3858	0.0155
4	0.3793	0.3520	0.4128	0.0117
5	0.2237	0.2	0.2599	0.0106
6	3.6154	3.5664	3.6612	0.0165

Table VII
The mean, minimum, maximum and standard deviation of the computed YYD values when tap ratio is manipulated by 0.025 and the load is increased by 10%(Case 3a)

Tap number	Mean	Minimum	Maximum	Standard Deviation
1	0.5636	0.5312	0.5964	0.0131
2	0.5183	0.4857	0.5481	0.0123
3	0.7027	0.6471	0.7507	0.0167
4	0.7512	0.7084	0.7947	0.0165
5	0.3824	0.3527	0.4070	0.0092
6	3.3530	3.29	3.4136	0.0203

Table VIII
The mean, minimum, maximum and standard deviation of the computed YYD values when tap ratio is manipulated by 0.025 and the load is decreased by 10%(Case 3b)

Tap number	Mean	Minimum	Maximum	Standard Deviation
1	0.5130	0.4863	0.554	0.0125
2	0.7925	0.7615	0.8314	0.0131
3	1.0206	0.9761	1.0757	0.0167
4	0.3946	0.3428	0.4421	0.0173
5	0.2434	0.2130	0.2935	0.0135
6	3.8509	3.7979	3.887	0.0188

would prompt the EMS to select a new ratio if the deviation in voltages are significant enough (in the order of voltage change that can be caused by one step increment/decrement of tap). In case of an attack, the index YYD would anyway show a significant increase indicating the presence of a false tap command injection.

A. Threshold Selection

Based on the observed values of the index YYD in all the cases(Tables IV, V, VI, VII, VIII), the threshold, Th chosen is 0.15 as this threshold can classify the false injection even when the tap change is as small as 0.025.

VI. Conclusion

The aim of this paper was to develop an algorithm to detect stealthily injected malicious tap change commands. In order to achieve this goal, various stealthy attack models were studied. An algorithm was then developed to detect such attacks. It is worth noting that an algorithm which detects a stealthy attacks can easily detect any other attack which involve lesser sophistication. The algorithm involved four indices based on ratios of the injection or branch currents to the voltages of terminal nodes of tap changing transformers for each tap. These indices were combined into one single index to result in a classifier, making this algorithm simple to implement. The proposed algorithm was subjected to extensive testing across several taps placed in a 118-bus system and was found to be accurate. The algorithm detected a false command in all the cases. It is important to note that this paper is the first to consider such attacks on transformer tap control and propose a detection scheme.

References

[1] N. M. Peterson and W. S. Meyer, *Automatic Adjustment of Transformer and Phase Shifter Taps in Newton Power Flow*, IEEE. Trans. Power App and Syst., Vol. PAS-90, No. 1, 1971.

[2] B. Stott and O. Alsac, *Fast Decoupled Load Flow Method*, IEEE Trans. on Power App. and Syst., Vol. PAS-93, No. 3, pp. 859-869, 1974.

[3] Stott, B.: 'Review of Load flow calculation methods', Proc. IEEE, Vol. 62, no. 7, pp.916-929, 1974.

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, *SCADA security in the light of Cyber-Warfare*, Computers and Security, Vol. 31, No. 4, pp. 418-436, 2012.

[5] V. M. Igure, S. A. Laughter, R. D. Williams, *Security issues in SCADA networks*, Computers and Security, Vol. 25, No. 7, pp. 498-506, 2006.

[6] C. Ten, C. Liu and G. Manimaran, *Vulnerability assessment of Cyber security for SCADA systems*, IEEE Trans. Power Syst., Vol. 23, No. 4, pp. 1836-1846, 2008.

[7] G. N. Ericson, *Cyber-security and Power system communications - Essential parts of a smart grid infrastructure*, IEEE Trans. Power Del., Vol. 25, No. 3, July 2010.

[8] O. Kosut, L. Jia, R. J. Thomas and L. Tong, *Malicious Data Attacks on the Smart Grid*, IEEE Trans. on Smart Grid, Vol. 2, No. 4, pp. 645-658, 2011.

[9] Y. Liu, P. Ning and M. K. Reitner, *False data injection attacks against state estimation in electric power grids*, ACM Trans. on Information and Syst. Security, Vol. 14, No. 1, Article 13, May 2011.

[10] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, *Smart Grid Data Integrity Attacks*, IEEE Trans. on Smart Grid, Vol. 4, No. 3, 2013.

[11] D. B. Rawat and C. Bajracharya, *Detection of false data injection attacks in smart grid communication systems*, IEEE Signal Proc. Letters, Vol. 22, No. 10, 2015.

[12] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu and X. Du, *Achieving efficient detection against false data injection attacks in smart grid*, IEEE Access, Vol. 5, pp. 13787-13798, 2017.

[13] R. J. R. Kumar and B. Sikdar, *Efficient detection of false data injection attacks on AC State estimation in smart grids*, IEEE Conference on Communications and Network Security(CNS), 2017.

[14] G. Chaojun, P. Jirutitijaroen and M. Motani, *Detecting False Data Injection Attacks in AC State Estimation*, IEEE Trans. on Smart Grids, Vol. 6, No. 5, pp. 2476-2483, 2015.

[15] G. Hug and J. A. Giampapa, *Vulnerability assessment of AC state estimation with respect to false data injection Cyber-attacks*, IEEE Trans. on Smart Grid, Vol. 3, No. 3, pp. 1362-1370, 2012.

[16] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda and Y. Hayashi, *Detection of cyber attacks against voltage control in Distributed power grids with PVs*, IEEE Trans. on Smart Grid, Vol. 7, No. 4, July 2016.

[17] A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. B. Bobba, A. Valdes, *Security of smart distribution grids: Data integrity attacks on integrated Volt/VAR control and countermeasures*, American Control Conference, 2014.

[18] Z-H. Yu and W-L. Chin, *Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid*, IEEE Trans. on Smart Grid, Vol. 6, No. 3, pp. 1219-1226, 2015.

[19] 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 Trans. on Smart Grid, Vol 10, No. 2, pp. 2158-2169, 2019.

[20] K. Manandhar, X. Cao, F. Hu and Y. Liu, *Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter*, IEEE Trans. on Control of Net. Syst., Vol. 1, No. 4, pp. 370-379, 2014.

[21] L. Che, X. Liu, Z. Li and Y. Wen, *False Data Injection Attacks Induced Sequential Outages in Power Systems*, IEEE Trans. on Power Syst., Vol. 34, No. 2, pp. 1513-1523, 2019.

[22] A. Monticelli, *Electric Power System State Estimation*, Proc. of the IEEE, Vol. 88, No. 2, 2000.

[23] Electricity Information Sharing and Analysis Center, *TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid: Defence Use Case*, 2016.

[24] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, *The 2015 Ukraine Blackout: Implications for False Data Injection Attacks*, IEEE Trans. on Power Syst., Vol. 32, No. 4, pp. 3317-3318, 2017.

[25] P. A. Texeira, S. R. Brammer, W. L. Rutz, W. C. Merritt and J. L. Salmonsen, *State Estimation of Voltage and Phase-Shift Transformer Settings*, IEEE Trans. on Power. Syst., Vol. 7, No. 3, 1992.

[26] L. V. Barboza, H. H. Zurn and R. Salgado, *Load Tap Changing Transformers: A Modelling Reminder*, IEEE Power Engg. Rev., 2001.

[27] University of Washington(1999): ‘Power System Test Case Archive’, Available http://www.ee.washington.edu/research/pstca/.

[28] Y. Wang, W. Xu and J. Shen, *Online Tracking of Transmission-Line Parameters Using SCADA Data*, IEEE Trans. on Power Delivery, Vol. 31, No. 2, pp. 674-682, 2016.

[29] IEEE Standard for SCADA and Automation Systems, IEEE Standard C37. 1-2007 (revision of IEEE Standard C37. 1-1994), 2008.