8th International Scientific Conference
Technics and Informatics in Education
Faculty of Technical Sciences, Čačak, Serbia, 18-20th September 2020

Session 3: *Engineerign Education and Practice*

Professional paper
UDC: 620.9:004

Cyber Security of Multi-vector Energy System with Demonstration of Tap Changer Position Estimation

Muchu Qiu[1*], Dragan Ćetenović[1], Vladimir Terzija[1], *Fellow, IEEE*
[1]Department of Electrical & Electronic Engineering, The University of Manchester, UK
[*] muchu.qiu@postgrad.manchester.ac.uk

Abstract: *Multi-vector Energy System is shaped in the progress of optimizing different energy sectors' generation, distribution, transmission, conversion, storage and consumption and finally become an energy integration system. There are many valuable advantages of Multi-vector Energy Systems such as reducing carbon emissions, ensuring the security and reliability of energy supply, increasing renewable energy accommodation and improving the overall energy efficiency. Modern information and communication technology (ICT) and big data analytics are integrated in Multi-vector Energy Systems to satisfy the utilization of distributed energy sectors and the demand of multiple energy consumption. As massive sensors and complicated ICT network are widely applied, Multi-vector Energy System gradually become highly coupling Cyber Physical System (CPS). Therefore, Multi-vector Energy System is confronted with the threat of Cyber-attacks, which endanger the safe operation and information security of the system. In this paper, a typical cyber-attack, False Data Injection Attack (FDIA), is introduced and two cyber-attacks scenarios aimed at transformer tap position are analyzed. To avoid the FDIA from disturbing tap changer position measurement, a tap changer position estimation method is proposed and deployed in OPEN-3000 Energy Management System (EMS). Due to the limited resource, an improved tap changer position estimation method against FDIA is tested and the result is proved applicable.*

Keywords: *cyber-attack, false data injection, ICT, Multi-vector Energy System, state estimation.*

1. INTRODUCTION

Energy systems strongly support the development of society and economy. Energy systems rapidly promote innovation and living standard of modern life as a driving power. In industrial society, traditional fossil fuels including coal, oil, natural gas and others are the most common energy resources worldwide. Also, renewable energies are used more widely since energy industries revolution including wind power, tidal energy, biomass energy, solar energy, etc. Although the current global reserves of fossil fuels are adequate, the world may be faced with future risks such as severe environmental pollution and resource exhaustion since fossil fuels have been large-scale exploited and utilized over hundreds of years. Meanwhile, the categories and reserves of renewable energies are abundant, even more important they are clean and environmental-friendly. So, the prospect of renewable energy is bright.

1.1. Motivations

Existing energy infrastructures have been mostly installed for 20 to 50 years. Plenty of facilities are about to finish their designed lifetime also transmission systems are becoming congested as the energy demand increases. If these infrastructures fail to meet the future requirements, the upgrading is necessary. Besides, other problems push the revolution of the existing systems including restructuring power industry, accommodating more renewable energy, getting rid of the dependence on finite fossil fuels and becoming environmental-friendly.

At present, the research about Multi-vector Energy System are hot issue all over the world. Multi-vector Energy System contains multiple energy carriers including electricity, gas, heat and hydrogen, which are tightly coupled by distributed energy generation. Multi-vector Energy System brings many advantages such as increasing renewable energy accommodation, reducing carbon emissions, improving the overall energy efficiency and ensuring the security and reliability of energy supply.

As the rapid development of ICT technology and sensor technology, Multi-vector Energy System are made possible through high coupling of physical system and cyber systems, and gradually transform into a Cyber Physical System (CPS). This also means the combination of ICT and energy technologies. ICT system provides functions such

as monitoring and controlling meanwhile brings challenges to the cyber security of Multi-vector Energy Systems.

Because ICT infrastructures are situated in an open environment and the coupling mechanism between cyber system and physical system are very complicated, the cyber security gradually become a serious problem. Therefore, the cyber security concerns the safety and reliability of Multi-vector Energy Systems.

1.2. Literature review

Accompanying with the wide application of sensors and information communication technology (ICT) network, conventional energy system becomes a multi-dimensional diversified system, also known as Cyber-Physical System. Firstly, CPS provides various kinds of functions including information processing, real-time monitoring and dynamic controlling to the system operator. Secondly, more cyber security loopholes hidden in the vast information data flow in CPS have been exposed to cyber-attacks. Recently, Cyber-attacks aimed at CPS have resulted in some severe blackouts and cause the alert globally. However, only a few researches are studied on cyber-attacks aimed at CPS worldwide and extensive knowledge about cyber-attacks in concepts, means and scenarios is still in shortage.

Advanced metering infrastructure (AMI), demand response (DR), distribution automation (DA), transmission operation, and many other applications are supported by cyber system and these applications are the main attack targets in cyber-attacks. Cyber-attack scenarios typically exist in energy generation, transmission, distribution and consumption.

The cyber-attacks target at confidentiality, integrity and availability of data [1]. As a typical cyber-attack, false data injection attacks (FDIA) tamper with measurement data to break the integrity of data flow, which are accessible and concealed. These attacks can interfere analysis and decision-making of control center, thereby cause unexpected consequences. These attacks are great threats to system operation safety, for example, attackers injected false data into the Supervisory Control and Data Acquisition (SCADA) system of power grid in Ukraine in 2015. This attack also deleted and altered the data on hard disk, which make system operators lose the control of whole system and the fast recovery ability, therefore cascading failure are spread widely and difficult to recover [2-4].

FDIA frequently utilize the shortcomings of bad data identification in state estimation and maliciously tamper with the measured values of measuring instruments. Then the operator and control center misjudge system state, which could cause mal-operation or operation failure of power system automation devices, thus affecting the safety and stability of the system. As the increasing level of coupling between physical system and cyber system, the attack range of FDIA also expands. In general, attacks aimed at breaking the stability of system or obtain illegal profits by malicious tampering with measurement and control of information and communication equipment can be regarded as FDIA.

On-Load Tap Changing transformer (OLTC) are broadly utilized in electricity systems to control bus or node voltages [5-7]. Voltage control are carried out by changing reactive power flows due to the tight coupling between them [6]. The commands of changing tap changer position are transmitted as action signals through SCADA communication channels. However, cyber-attacks can compromise SCADA channels and inject malicious command of changing tap changer position [8-11].

Only a few researches are studies on the cyber-attacks aimed at voltage control [12-14]. Nevertheless, these incorrect control actions are caused by FDIA basically. The study focuses on the cyber-attacks aimed at 'centralized voltage control scheme' in distribution network [12]. In this study, the voltage measurements are vulnerable to malicious manipulation, leading to needless change of tap changer positions. Through the comparison between historical tap changer position behavior and current measurement, attacks can be detected. However, these attacks [12] cannot succeed in a system with state estimator. Because the bad data detection will filter out the false data injection as bad data based on redundant measurements. The attack model in [13] has the same restrictions with the attack model in [12]. In [13], it is assumed that the attackers have only gained the access of voltage measurements but not the power injection measurements. Hence, these cyber-attacks [12-13] cannot be carried out successfully in transmission networks due to the state estimation with bad data detection. It is discussed that cyber-attacks aimed at Automatic Voltage Control (AVC) software embedded in the Energy Management Systems (EMS) in transmission networks [14]. Given the voltage control system in [14], active and reactive power generation are solved by optimal power flow to be the control parameters. In [15], a false data injection aimed at malicious interfering the control process is detected by a reinforcement learning based approach.

The available literature about cyber-attacks concerning false command injection is lacking [16], [17]. In [16-18], it is reviewed that the attackers in 2015 Ukraine blackout event have gained the control of circuit breakers and disconnected some parts of the power grid. This is an example of cyber-attack caused by malicious commands in power grid.

1.3. Contributions

In this paper, a typical cyber-attack mode, False data injection attack (FDIA), is emphasized. Typical cyber-attack scenarios and some real cases are reviewed.

The original augmented state estimation for tap changer position estimation is improved. In addition, the effects of the improved method on the performances of state estimation and advanced analysis software are studied. The analysis shows that the improved tap changer position estimation method greatly enhances the accuracy and reliability of state estimation. Therefore, the reliability and practicability of power advanced analysis software are also improved.

The requirement for measurements configuration is more redundant and falsified tap changer position measurement is difficult to pass bad data identification module. The difficulty of breaking the reliability and security of power system is increased.

2. TRANSFORMER TAP CHANGER POSITION ATTACK SCENARIOS

The difference between cyber-attacks aimed at transformer tap changer control and FDIA lies in the attack targets. The control command is the main attack target in the former attacks but measurements in FDIA. Cyber-attacks aimed at tap changer control can be launched stealthily. In order to hide the malicious change in tap changer position, it is essential for the attacker to make the estimated and measured tap changer position consistent and its control parameters, that is, the bus voltage perform similar to the set values due to noise of measurements. This can be achieved by a selective injection of false data [19].

As the one line diagram shown in Figure 1, the tap ratio k can be varied by changing tap changer position, thereby control the voltage of bus i (Vi). Two cases of cyber-attacks aimed at transformer tap changer control are analyzed next.

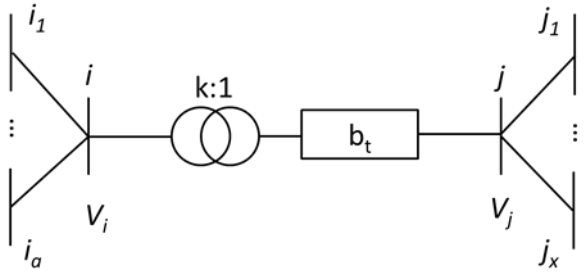

Figure 1. *An OLTC transformer simplified model with surrounding nodes.*

2.1. Case 1: Concealing Malicious change in tap changer position (tap ratio)

There are some steps to hide a malicious change in tap changer position (tap ratio). In the first place, attackers must tamper the measuring instruments relaying tap ratio messages. Secondly, only tampering with the tap ratio alone is not adequate to hide the attacks from bad data detection in EMS because adjacent measurements have quantitative relation with tap ratio k, which reveal true tap changer position. During bad data detection in state estimation, false tap changer position can be identified and submitted to notify system operator. Therefore, for the stealth of cyber-attacks, the listed measurements must be tampered synergistically:

- Active and reactive power injections of nodes i and j.
- Active and reactive power flows between nodes i and j.

2.2. Case 2: Concealing Malicious Change in Tap Changer Position and Related Bus Voltage

It is recognized that if attackers maliciously change the tap changer position, the bus voltage V_i will also change. If the bus voltage V_i is seriously deviated from its normal settings, detection procedure will be triggered. Hence, measurements having quantitative relation with both tap ratio k and bus voltage V_i must be tampered simultaneously to keep the cyber-attack fully concealed. In this situation, estimated and measured values of tap ratio k and bus voltage V_i can be kept consistent with the values derived from EMS. The following measurements must be altered in addition:

- The voltage measurement of bus i (V_i).
- Active and reactive power injections of nodes connected to node i.
- Active and reactive power flows between node i and adjacent nodes.

There are some common points between a concealed malicious attack aimed at tap changer position and an FDIA. The effects of attack in Case 1 are not obvious or even unobserved while tap changers coordinate with other parameters to fulfill certain goal such as minimizing reactive power loss. But when tap changers are regulated to maintain system voltages, the attack in Case 2 is qualified to stay concealed.

3. PROPOSED TAP CHANGER POSITION ESTIMATION

3.1. Original Estimation Method

The augmented state estimation method is commonly used to estimate transformer tap changer position. In augmented state estimation method, the parameters to be estimated are taken as parameter state variables, together with the original node state variables (node voltage vectors). Increasing the dimension of the state variables will decrease the redundancy of original measurements as well as the estimation accuracy. So, a more redundant measurement configuration is proposed to ensure the estimability of parameter

state variables. The measurement function of the power system can be written as

$$z = h(x) + v \tag{1}$$

z- m dimension measurement vector

x- n dimension state variable vector

v- m dimension measurement error vector

h(x)- m dimension nonlinear function vector, mathematical model of the system representing the relation between actual values of measurement and state variables.

In conventional state estimation, state variables are voltage (u_i) of all busbars and voltage phase angle (θ_i) of all nodes except slack bus node in the same electrical island. That is x=(u_1, θ_1, u_2, θ_2 … u_n) (n is slack bus, θ_n=0). Equation (1) can be rewritten as

$$z = \begin{bmatrix} h_1(u_{11}\theta_{11}u_{12}\theta_{12}\ldots u_{1n}) \\ h_2(u_{21}\theta_{21}u_{22}\theta_{22}\ldots u_{2n}) \\ \ldots \\ h_m(u_{m1}\theta_{m1}u_{m2}\theta_{m2}\ldots u_{mn}) \end{bmatrix} + v \tag{2}$$

In augmented state estimation, the unknown parameter P is considered as state variable (parameter state variable), equation (2) is reformed as below

$$z = \begin{bmatrix} h_1(u_{11}\theta_{11}u_{12}\theta_{12}\ldots u_{1n}P) \\ h_2(u_{21}\theta_{21}u_{22}\theta_{22}\ldots u_{2n}P) \\ \ldots \\ h_m(u_{m1}\theta_{m1}u_{m2}\theta_{m2}\ldots u_{mn}P) \end{bmatrix} + v \tag{3}$$

As long as the configuration of measurements satisfies the requirements of estimability, parameter state variables can be multiple. The optimal solution of the augmented state variables vector can be solved by weighted least square estimation method. The iteration equation of the weighted least square method is

$$H_a^T R^{-1} H_a \Delta x_a = H_a^T R^{-1} \Delta Z \tag{4}$$

H_a is augmented Jacobian matrix, its elements can be figured by equation below

$$H_{aij}(x_a) = \frac{\partial h_i(x_a)}{\partial x_{aj}} \tag{5}$$

The difference between augmented state estimation and conventional state estimation is the augmentation of dimensions of state variable vector, meaning the augmentation of row in Jacobian matrix. Given a start condition $x_a^{(k)}$, follow the equation below

$$\Delta Z^{(k)} = Z - h\left(x_a^{(k)}\right) \tag{6}$$

Substitute the value of $\Delta Z^{(k)}$ into (4). Corresponding $\Delta x_a^{(k)}$ can be resolved.

$$x_a^{(k+1)} = x_a^{(k)} + \Delta x_a^{(k)} \tag{7}$$

Follow the equations above, state variables can be iterated until convergence. k is the number of iterations.

3.2. Improved Tap Changer Position Estimation Method

OLTC transformer is modelled as Pi-equivalent circuit [20], similar to transmission lines. In Pi-equivalent circuit, the shunt and series admittances are functions of tap ratio k. The simplified model of OLTC transformer in Figure 1 can be represented by a Pi-equivalent model in Figure 2. In the Pi-equivalent model, the equivalent admittances are shown as below

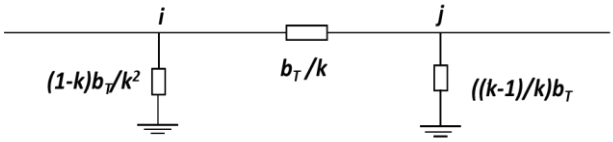

Figure 2. *Pi-equivalent model of OLTC transformer.*

$$P_i = \sum_{j=1}^{n} U_i U_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{8}$$

$$Q_i = \sum_{j=1}^{n} U_i U_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \tag{9}$$

The power flow from node *i* to node *j* is

$$P_{ij} = -\frac{1}{k} U_i U_j b_T \sin\theta_{ij} \tag{10}$$

$$Q_{ij} = -\frac{1}{k^2} U_i^2 b_T + \frac{1}{k} U_i U_j b_T \cos\theta_{ij} \tag{11}$$

The power flow from node *j* to node *i* is

$$P_{ji} = \frac{1}{k} U_i U_j b_T \sin\theta_{ij} \tag{12}$$

$$Q_{ji} = -U_j^2 b_T + \frac{1}{k} U_i U_j b_T \cos\theta_{ij} \tag{13}$$

According to the principle of augmented state estimation, *K* is considered as parameter state variable. Also, elements in Jacobian matrix are shown as below due to the principle of fast decoupled state estimation.

$$\frac{\partial V_i}{\partial K} = 0 \tag{14}$$

$$\frac{\partial P_i}{\partial K} = 0 \tag{15}$$

$$\frac{\partial P_j}{\partial K} = 0 \tag{16}$$

$$\frac{\partial Q_i}{\partial K} = \frac{U_i}{k^2} b_T \left(\frac{2U_i}{k} - U_j \right) \quad (17)$$

$$\frac{\partial Q_j}{\partial K} = -\frac{1}{k^2} U_i U_j b_T \quad (18)$$

$$\frac{\partial P_{ij}}{\partial K} = 0 \quad (19)$$

$$\frac{\partial P_{ji}}{\partial K} = 0 \quad (20)$$

$$\frac{\partial Q_j}{\partial K} = \frac{1}{k^2} U_i b_T \left(\frac{2U_i}{k} - U_j \right) \quad (21)$$

$$\frac{\partial Q_{ji}}{\partial K} = -\frac{U_i U_j}{k^2} b_T \quad (22)$$

The gain matrix in the weighted least square estimation is written as below.

$$H^T R^{-1} H = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \quad (23)$$

$$A = U_0^4 \left[(-B_a)^T R_a^{-1} (-B_a) \right] \quad (24)$$

$$B = U_0^4 \left[(-B_r)^T R_r^{-1} (-B_r) \right] \quad (25)$$

$$\frac{\partial h_a}{\partial \theta} = -U_0^2 B_a \quad (26)$$

$$\frac{\partial h_r}{\partial U} = -U_0^2 B_r \quad (27)$$

From (14) to (22), parameter state variable K has no influence on P-θ type Jacobian matrix B_a, B_a is still a constant matrix. Therefore, only Q-V type Jacobian matrix B_r need to be reformed each iteration. Compared to augmented state estimation, the simplified method in fast decoupled state estimation is adopted with faster computing speed and less storage usage and higher convergence precision.

Due to the increase of state variables in matrix B_r, measurements configuration is required to be more redundant, that is, reactive power flows and voltage magnitudes must be measured on primary and secondary side of the estimated transformer.

After estimating the value of K, the estimated tap changer position can be examined by the range of transformer tap changer position, tap changer position of rated voltage and step of tap changer.

4. PERFORMANCE EVALUATION

4.1. Current Situation of Tap changer position Estimation

Table 1 shows the tap changer position estimation comparison between artificial pseudo tap changer positions and estimated tap changer positions before applying improved tap changer position estimation method. The tap changer positions in column 'Artificial Pseudo Tap changer position' are collected by verification of on-site operators and set pseudo measurement manually. The tap changer positions in column 'Estimated Tap changer position' are estimated by state estimation method before improvement. From the comparison, the accuracy of original tap changer position estimation is proved to be not ideal.

Table 1. *Comparison between artificial pseudo tap changer positions and estimated tap changer positions.*

Station ID	Voltage Type (High-Mid-Low winding)	Artificial Pseudo Tap Position	Estimated Tap Postion
TWA	13.8kV/4.16kV	2	3
TWA	13.8kV/4.16kV	2	3
DAS	34.5kV/1kV	3	4
DAS	34.5kV/1kV	3	4
BOT	230kV/69kV/13.8kV	9	11
BOT	230kV/69kV/13.8kV	9	11
BOT	230kV/69kV/13.8kV	9	11
BAY	69kV/13.8kV	2	3
BAY	69kV/13.8kV	2	3
BNG	69kV/13.8kV	2	3
BNG	69kV/13.8kV	3	2
MLL	69kV/13.8kV	3	2
MLL	69kV/13.8kV	3	2
ANG	115kV/13.8kV/13.8kV	5	6
ANG	115kV/13.8kV/13.8kV	5	6
ANG	115kV/13.8kV/13.8kV	5	6
BAN	115kV/69kV/13.8kV	8	9
BAN	115kV/69kV/13.8kV	8	9
BAN	115kV/69kV/13.8kV	8	9
CLR	115kV/13.8kV	2	3
CLR	115kV/13.8kV	2	3
CUR	115kV/69kV/13.8kV	2	3
CUR	115kV/69kV/13.8kV	11	9
CUR	115kV/69kV/13.8kV	11	9

4.2. Test Substation Details

YUCI substation, with one line diagram shown in Figure 3, is taken as an example.

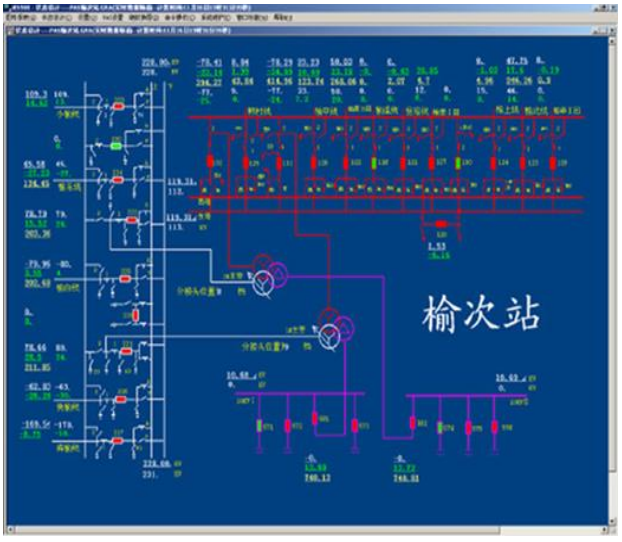

Figure 3. *One Line Diagram of YUCI substation.*

SE sections using original tap changer position estimation and the improved tap changer position estimation are both calculated and saved based on same SCADA section. The redistribution of SE power flow is used to verify which tap changer position estimation has more consistency with the actual tap changer position and higher state estimation eligible ratio at the same time. Thus, the rationality and practicability of the improved tap changer estimation method are verified.

At first, some basic topology and devices parameters in YUCI substation are introduced. The highest voltage level in YUCI substation is 220kV. The 220kV and 121kV busbar connection is double-busbar (DB). For 220kV side, 221 is the 220kV circuit breaker of 1# transformer, 222 is the 220kV circuit breaker of 2# transformer, 230 is the bypass circuit breaker and 220 is the bus-tie circuit breaker. For 121kV side, 131 is the 121kV circuit breaker of 1# transformer, 132 is the 121kV circuit breaker of 2# transformer, 130 is the bypass circuit breaker and 120 is the bus-tie circuit breaker.

The parameters of two transformers in YUCI substation are shown as below.

Table 2. *The parameters of two transformers in YUCI substation.*

	Rated Capacity (MW)			Rated Voltage (kV)		
	H	M	L	H	M	L
1# TR	150	150	150	220	121	10.5
2# TR	150	150	150	220	121	10.5
	Percentage of short-circuit voltage			Short-circuit loss		
	H-M	H-L	M-L	H-M	H-L	M-L
1# TR	13.4	23	7.53	628	783.6	535.6
2# TR	13.5	23.3	7.69	626	793.5	522.1
	OLTC	Min Tap	Max Tap	Nom Tap	Tap Step	Connnection
1# TR	Y	1	19	10	1.06	Y0-Y0-△
2# TR	Y	1	19	10	1.06	Y0-Y0-△

4.3. Comparison of SE Power Flow Sections

Two separated state estimation calculation are respectively conducted using original tap changer position estimation and the improved tap changer position estimation based on the same SCADA historical section. The diagram and data sheet of power flow in YUCI substation are saved and compared as it is given in Table 3.

Due to the wrong tap changer position estimation, state estimator gives the ineligible point statistics in YUCI station. As shown in Table 4, the active and reactive power flow distribution of state estimation is interfered by the wrong tap changer position estimation.

It can be concluded from Table 3 that two methods are adopted using the same SCADA section at the same time and the actual power flow remains unchanged. While the estimated value of tap changer position is different, power flows are redistributed. Comparison of estimated tap changer position using two methods is shown in Table 5. It can be seen that improved tap changer position estimation method is more consistent with actual tap changer position and substation measurement error is less. Therefore, the state estimation power flow section in YUCI substation is more consistent with the actual situation.

Table 3. *Comparison of power flows using two tap changer position estimation.*

	SCADA data	SE data	
		Original Tap Changer Position Estimation	Improved Tap Changer Position Estimation
1# TR Tap Position	4	8	4
2# TR Tap Position	4	8	4
223	76+j3	76.1+j3.5	74.5+j2.35
230	0+j0	0+j0	0+j0
224	-19-j18	-18.9-j17.5	-18.2-j18.5
222	64+j12	64.3+j8.42	65.9+j9.19
225	-79+j25	-78.5+j25.4	-78.5+j25.4
220	0+j0	0+j0	0+j0
221	66+j12	64.9+j5.32	65.4+j6.5
226	58-j50	58.04-j41.67	52.3-j41.34
227	-166+j14	-165.9+j16.4	-163.1+j16.5
132	-63-j15	-63.9-j15.6	-63.9-j15.6
125	9+j0	8.86+j1.03	8.82+j1.22
131	-63-j15	-64.6-j13.1	-65.1-j14.9
128	6+j0	6.02+j0.45	5.97+j0.94
122	52+j16	52.8+j15.8	52.4+j17
126	0+j0	0.01-j0.01	0.01-j0.01
121	0+j0	0.01-j0.38	0.01-j0.41
127	12+j0	11.2+j0.01	12.4+j0.26
130	0+j0	0+j0	0+j0
124	9+j2	0.01-j0.91	0.01-j0.98
123	49+j13	49.7+j12.9	50.3+j14.1
129	0+j0	0.01-j0.17	0.01-j0.18
220kV 1# Bus Voltage	231kV	231kV	231kV
220kV 2# Bus Voltage	233kV	231kV	231kV
110kV 1# Bus Voltage	111.97kV	116kV	115.84kV
110kV 2# Bus Voltage	112.22kV	115kV	116.09kV

Table 4. *Ineligible Data Statistics in YUCI Station.*

SE Ineligible Measurements	Measurement Points
Ineligible P measurement	Line: YUQIAN I, Error: -8.63, Standard Error: 7.57
Bad Data P measurement	Line: YUBEI, Error: 11.77, Standard Error: 10.33
Ineligible P measurement	Line: YUCI 124, Error: 9.00, Standard Error: 7.89
Ineligible Q measurement	Transformer 2# 121kV winding, Error: -6.1, Standard Error: 5.35
Ineligible V measurement	110kV 1# Busbar Voltage, Error: -3.85, Standard Error: 2.92
Ineligible Q measurement	Transformer 1# 121kV winding, Error: 5.46, Standard Error: 4.79

Table 5. *Comparison of Estimated Tap Changer Position Using Two Methods.*

	Actual Tap Position (1#/2#)	Estimated Tap Position (1#/2#)	Substation Measurement Error Statistics
Original Tap Changer Position Estimation Method	4/4	8/8	4.166%
Improved Tap Changer Position Estimation Method	4/4	4/4	2.012%

4.4. The Impacts on Performance of Power Advanced Software

Then, an important index of state estimation, System Eligible Ratio, is introduced to judge the influence of different tap position estimation methods on state estimation. System Eligible Ratio is calculated by equation as below.

$$\text{System Eligible Ratio} = \frac{Eligible\ Points}{Total\ Measurement\ Points} * 100\%$$

System Eligible Ration reflects the performance of state estimator. A higher System Eligible Ration means the state estimation power flow section is more consistent with the actual power flow.

The upper section in Figure 4 shows the comparison of the SE daily eligible ratio curves using two

different tap changer position estimation methods. The red curve shows the SE daily eligible ratio curve using improved tap changer position estimation method. The blue curve shows the SE daily eligible ratio curve using original tap changer position estimation method. The SE daily eligible ratio is raised from 90% (blue curve) to around 95% (red curve), also SE calculation keep convergent all day, which greatly improves the performance of the state estimation module.

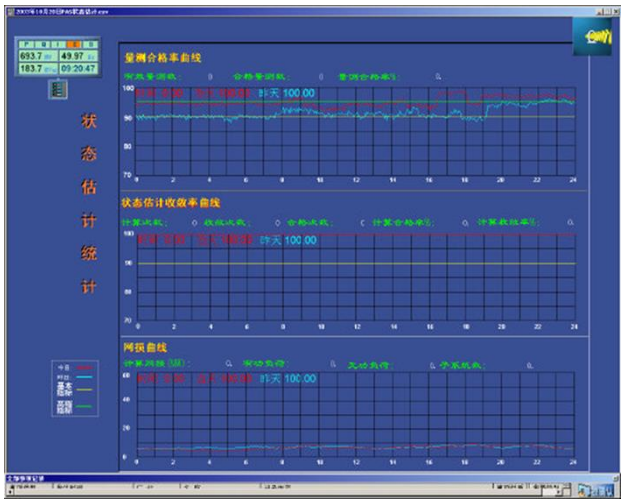

Figure 4. *SE daily eligible ratio curve.*

Table 6 shows the SE calculation statistics using two tap changer position estimation methods based on the same SCADA daily section. When eligible ratio >= 90%, the result of this state estimation calculation is considered qualified to be used by other advanced power software, such as Dispatching Power Flow, Contingency Analysis.

Table 6. *SE calculation statistics using two tap changer position estimations.*

	Eligible Measurement Points	Daily Eligible Ratio (%)	Number of Calculation	Number of Convergence	Number of Qualification	Qualification ratio (%)
Original Method	411	90.73	4265	4265	3967	93.01
Improved Method	428	95.86	4302	4302	4089	95.05

State estimation is calculated based on SCADA real-time telemetry and status in order to obtain a relatively accurate and complete run mode. At the same time, SE verifies SCADA measurements and puts forward the possible abnormal measurement points. The power flow sections of state estimation can be used by power advanced analysis software in real-time mode and historical mode. For example, Dispatcher Power Flow (DPF) can simulate the change of operation mode based on specific SE section and replay the failure situation. Besides, Contingency Analysis can help system operators to find the potential risks if one component is outage resulting in overload or load shedding, which is also simulated based on specific SE section. In summary, improved tap changer can increase the accuracy and reliability of state estimation and other advanced analysis software based on SE to meet the goal of safety and economy, improve the voltage quality and reduce the network loss in power system.

5. CONCLUSION

The process of tap changer position estimation is introduced, and the effect of the improved method is analyzed. The example proves that the improved tap changer position method is more consistent with the actual tap changer position, which is practical. The impact of improved transformer tap changer position estimation method on the performance of the state estimation and other power advanced software. The analysis shows that improved method has greatly enhanced the performance of each module.

The requirement for measurements configuration is more redundant in improved tap changer position estimation method, that is, reactive power flow and voltage magnitude must be measured on primary and secondary side of the estimated transformer. False tap changer position measurement is difficult to pass bad data identification module because this tap changer position needs to be consistent with reactive power flow and voltage magnitude. Therefore, cyber-attackers have to gain access to more relevant measurement at the same time to implement FDIA. The difficulty of breaking the reliability and security of power system is increased.

ACKNOWLEDGEMENTS

This study is the result of Supergen Energy Networks Hub project. The authors hereby express sincere gratitude for the support.

REFERENCES

[1] *Tang Yi, Chen Qian, Li Meng-Ya, Wang Qi, Ni Ming, Liang Yun. Overview on cyber-attacks against cyber physical power system. Automation of Electric Power Systems, 2016, 40(17): 59i69*

[2] *Liang G Q, Weller S R, Zhao J H, Luo F J, Dong Z Y. The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Transactions on Power Systems, 2017, 32(4):3317-3318*

[3] *Li Zhong-Wei, Tong Wei-Ming, Jin Xian-Ji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel. Automation of Electric Power Systems, 2016, 40(8):147-151*

[4] *Zhao Jun-Hua, Liang Gao-Qi, Wen Fu-Shuan, Dong Zhao-Yang. Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks. Automation of Electric Power Systems, 2016, 40(7): 149i151*

[5] *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.*

[6] *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.*

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

[8] *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.*

[9] *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.*

[10] *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.*

[11] *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.*

[12] *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.*

[13] *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.*

[14] *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.*

[15] *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.*

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

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

[18] *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.*

[19] *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.*

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