Proceedings Paper:
Xia, M, Du, D, Fei, M et al. (1 more author) (2021) Impact Analysis of False Data Injection Attack on Smart Grid State Estimation Under Random Packet Losses. In: Communications in Computer and Information Science. LSMS 2020, ICSEE 2020: Recent Featured Applications of Artificial Intelligence Methods. LSMS 2020 and ICSEE 2020 Workshops, 25 Oct 2020, Hangzhou, China. Springer , pp. 61-75. ISBN 978-981-33-6377-9

https://doi.org/10.1007/978-981-33-6378-6_5

Impact Analysis of False Data Injection Attack on Smart Grid State Estimation under Random Packet Losses

Meng Xia[1], Dajun Du[1], Minrui Fei*[1], and Kang Li[2]

[1] Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai
[2] School of Electronic and Electrical Engineering, University of Leeds, Leeds; LS2 9JT, United Kingdom

Abstract. Supervisory control and data acquisition (SCADA) system has been widely used in traditional power systems for operation and control. As increasingly more ICT technologies are deployed to improve the smartness of the power grid, cyber security is becoming an important issue in the development of smart grids, for example, false data injection attack (FDIA) poses a serious threat. The paper analyzes the impact of false data injection attack on smart grid state estimation under random packet losses. First, a measurement model of power grids under random packet loss is established, and an attack vector range that can fool the attack detector is acquired. Then, a mean square error matrix of weighted least squares estimation is proposed, taking into account potential false data injection attacks. A IEEE-14 nodes system is used to evaluate the performance of the weighted least squares state estimation under three different scenarios, namely false data injection attack only, random packet loss only, and under both random packet loss and false data injection attack.

Keywords: False data injection attack · Random packet losses · Weighted least squares estimation · Smart grid

1 Introduction

Modern power systems transmit electricity from generators to users via large-scale transmission and distribution networks. To ensure safe and reliable operation of the system, increasingly more ICT technologies are introduced into the power systems to improve the smartness [1]. However, the introduction of modern communication networks not only facilitates information interaction and wide-area system monitoring, protection and control of power grids but also makes it vulnerable to network invasion [2] [3]. In recent years, cyber-attacks on power grids around the world have been viewed as a principal threat, not just a conceptual one.

For example, Iran's Blushehr nuclear power plant was attacked by the Stuxnet virus in 2010, which caused the delay of power generation and seriously

damaged Iran's industrial facilities [4]. The transmission lines in Ukraine were continuously tripped in 2015, while the information system was implanted with malicious software, which blocked the system restart [5]. In 2019, several cities in Venezuela including its capital city Caracas plunged into darkness, and power outages affected 21 of the country's 23 states. According to the media reports, the direct cause of the power failure was a cyber-attack on the country's largest hydropower station. Soon after, several transformer explosions occurred in the federal district of Caracas, causing another power failure [6].

The power system control center collects measurement data from different power devices and components through the supervisory control and provide instructions back to the system [7]. State estimation is a key functionality in real-time power system monitoring and supervisory control. By analyzing the data collected by the SCADA systems, the current operating state of the power grids can be estimated while bad data and anomalies in the collected measurements can be eliminated.

However, state estimation can be vulnerable to cyber-attack in the open network environment. The false data injection attack (FDIA) against the state estimator in the SCADA system was investigated by Liu et al in 2009 [8], and it was found that existing bad data detection methods relying on Chi-square detector may not work in response to some false data injection attacks. An experienced attacker can deliberately design the attack vector such that these attacks can bypass the Chi-square detector. Once the sensor is successfully hacked, the tampered measurement will spread in the network, resulting in system performance degradation or even instability [9].

In the research area of false data injection attack, some researchers aim to identify the vulnerability of the system and build the attack models[10] [11] [12] [13], and this helps to improve the understanding of the attack mechanism in order to design a better defense system. For example, a linear spoofing attack strategy and the corresponding feasibility constraints are demonstrated where fake data can be effectively designed to cause system failure [10]. In [11], the potential impact of unobservable attacks is investigated, and the least measurable attack strategy is proposed. Under the fully measurable model and partially measurable model, the existence conditions of unobservable subspace attacks are derived, based on which two attack strategies are proposed in [12]. The first strategy directly affects the system state by hiding attack vectors in the system subspace, and the second strategy misleads the bad data detection mechanism. Meanwhile, other researchers focus on the detection and defense of the system in the presence of attacks [14][15][16][17][18][19]. For example, both active detection and estimation-based detection are proposed in [14]. In the active detection method, a reasonable excitation signal is designed to be superimposed on the control signals, which improves the detectability of attacks on the actuator attack. The other method estimates the value of the attack by using the unknown input observer. In [15], a FDIA attack detection mechanism based on the increments of analytic measurements in the micro-grid environment was proposed.

Most existing researches are based on the analysis of the acquired measurements, but the impact of data communication is not considered. The FDIA in smart grid applications is an attack that reduces the integrity of data acquired by the system. In the existing communication technology, data transmitted through the network is often in the form of packets[20]. Most existing approaches construct the attack model and detect the attack using acquired measurements and the estimation of measurements [10]-[18]. However, in addition to potential F-DIA, the data transmitted through the network may also be affected by network characteristics such as data losses during the transmission phase. This paper investigates the data injection attack on power system state estimation considering data losses in communication. The main contributions are as follows:

- A DC (direct current) model of the system under data injection attack is deduced, taking into account the random packet losses.
- The mechanism of weighted least squares state estimation and bad data detection are analyzed and an undetected range of attack vectors is derived.
- Based on the established DC measurement model, the mean square error matrix of state estimation under the FDIA is analyzed.

The remainder of the paper is organized as follows. The transmission model of sensor measurements in the power grids under random packet loss is discussed in Section 2. Section 3 analyses the effects of random packet loss and data injection attacks on weighted least squares estimation, and the range of attack vectors is also studied. Simulation results are presented in Section 4, and the weighted least squares state estimation results under three different cases are compared.

2 Problem Formulation

2.1 Data Transmission Model

The SCADA system in the power grids collects sampled measurements from sensors through the communication network However, due to limitations of the communication technology, data may get lost during the transmission. Figure 1 illustrates the whole process from data sampling and transmission to state estimation.

As shown in Figure 1, at time instant t_{k-1}, the measurement device samples and transmit the sensor measurements to the network in the form of packets. Due to network induced delays, after the transmission delay d_{k-1}, the SCADA system will receive the sampled measurements at time instant $t_{k-1}+d_{k-1}$. Further, some data may be lost during the transmission process, such as the data at time instant t_k shown in Figure 1. Once the SCADA system obtains the measurements, the estimator can receives the data after the computing time delay of c_{k-1}. Power grids are typical complex cyber-physical systems with numerous sensors, and all sensor data will go through the similar process as shown in Figure 1 when they are transmitted to the SCADA system.

Define the measurements received by the SCADA system at sampling instant k as z_k, $z_k \in R^m$, and if there exists data packet losses, two popular compensated

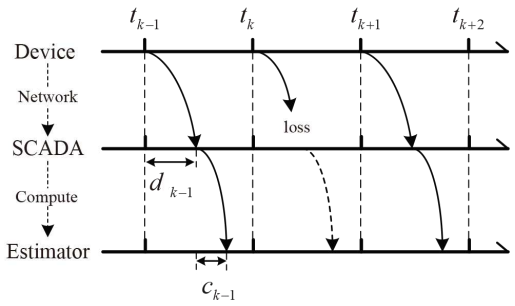

Fig. 1. The data sampling, transmission and state estimation process.

methods are often adopted. One is to directly replace the lost data with 0 [21]. Another is to replace the lost data with the previous sampled data. This paper adopts the first method, i.e., the loss packet is set as 0. For random packet losses, the received measurements can be expressed by

$$z_{lk} = \lambda_k z_k, \tag{1}$$

where $\lambda_k \in R^{m \times m}$ is a diagonal matrix whose diagonal elements are either 1 or 0. When a measurement is lost, its corresponding value is set to 0.

2.2 Power Grid Measurement Model

When the system is subject to a false data injection attack, the measurement process of the grids is shown in Figure 2. When a sensor device samples measurements, it may be invaded by an attacker by deception, and false data are injected. Next, the sensor transmits the corrupted data to the SCADA over the network. When random packet loss is not considered at the sampling instant k, the AC measurement model can be described as

$$z_k = h(x_k) + v_k, \tag{2}$$

where z_k is denoted as the measurement vector, x_k is the system state vector, v_k is the Gaussian measurement noise, and $h(x_k)$ is the functional dependency between measurements and state variables.

If the ground admittance and branch conductance are ignored and assume that the voltage phase difference between two nodes is negligible, the voltage amplitude of the nodes is close to unit quantity 1. The DC measurement model can be used to approximate AC measurement model. The DC measurement model can be expressed as

$$z_k = Hx_k + v_k, \tag{3}$$

where H is the steady-state functional dependency between measurements and state variables.

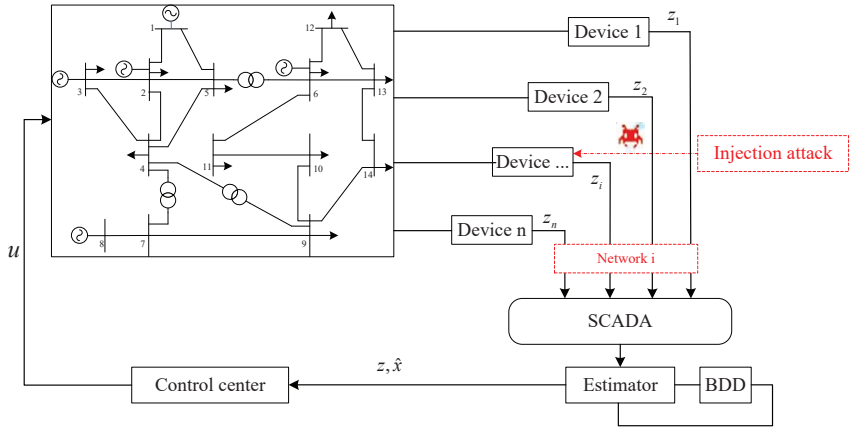

Fig. 2. The power grid measurement process subject to false data injection attack.

When only random packet loss is considered, at the sampling instant k, the DC measurement model can be expressed as

$$z_{lk} = \lambda_k(Hx_k + v_k). \tag{4}$$

When only a data injection attack is considered and assume that the injected value is $a_k$and $a_k \in R^m$. If a_k is nonzero, the corresponding measurement is tampered. Then the measurement contains the attack vector a_k, which can be expressed as

$$z_{ak} = z_k + a_k, \tag{5}$$

where a_k is the attack vector injected to measurement.

When random packet loss is considered, the measurement function can be expressed as

$$z_{lak} = \lambda_k z_{ak}. \tag{6}$$

Eqn (6) is the measurement model under the false data injection attack which considers both the influence of random packet loss and data injection attack on the measurements of the grid.

3 Analysis of Weighted Least Squares Estimation

State estimation is used for monitoring the operating state of the grid and to remove bad data, and the weighted least square method is a popular state estimation method. The false data injection attack aims to mislead the state estimation, and it is necessary to have a detailed analysis of the state estimator. According to the weighted least squares estimation, the objective function can be expressed as

$$\min J\left(x_k\right) = \left(z_k - Hx_k\right)^T W(z_k - Hx_k), \tag{7}$$

where W is the weighted matrix. The estimation of the system state can be expressed as

$$\hat{x}_k = (H^T W H^T)^{-1} H^T W z_k. \tag{8}$$

Define $\hat{z}_k = H\hat{x}_k$ as the state estimation of the system, and the residual between the real and the measurement estimation is defined as r_k, and r_k can be expressed as

$$r_k = z_k - \hat{z}_k. \tag{9}$$

According to the Chi-square detector, 2-norm of the residual must be less than the threshold to consider that there is no bad data, i.e.,

$$\|r_k\|_2 \leq \tau, \tag{10}$$

where τ is the threshold of the Chi-square detector, which can be obtained by checking the Chi-square distribution table. When there is only a false data injection attack, the injected increment must meet certain conditions in order not to be detected. According to (8), for a given a_k, the state estimation can be expressed as

$$\hat{x}_{ak} = (H^T W H^T)^{-1} H^T W z_{ak}, \tag{11}$$

where $\hat{x}_{ak}$ the corrupted estimation due to FDIA. The estimate of the measurement is $\hat{z}_{ak} = H\hat{x}_{ak}$, and the residuals can be expressed as

$$\begin{aligned} r_{ak} &= z_{ak} - \hat{z}_{ak} = z_k + a_k - (H\hat{x}_k + H\big(H^T W H\big)^{-1} H^T W a_k) \\ &= (I - H\big(H^T W H\big)^{-1} H^T W)(z_k + a_k). \end{aligned} \tag{12}$$

To evade the detector, Eqn (13) must be satisfied, that is

$$\|r_{ak}\|_2 \leq \tau. \tag{13}$$

Let $B = (I - H\big(H^T W H\big)^{-1} H^T W)$, Eq. (13) can be re-written as

$$\|B(z_k + a_k)\|_2 \leq \tau. \tag{14}$$

According to the compatibility

$$\|B(z_k + a_k)\|_2 \leq \|B\|_2 \|(z_k + a_k)\|_2, \tag{15}$$

when $\|B\|_2\|(z_k + a_k)\|_2 \leq \tau$ hold, the Eq. (14) will be hold, where $\|B\|_2 = \sqrt{\eta_{\max}(B^T B)}$ is the induced norm and $\eta_{\max}(B^T B)$ is the maximum eigenvalue of the matrix $B^T B$.

Therefore,

$$\|(z_k + a_k)\|_2 \leq \frac{\tau}{\|B\|_2}. \tag{16}$$

Remark 1. Inequality (16) represents a subset of the attack vector which will not trigger an alarm from the bad data detector.

Corollary 1. *Eqn (17) is the non-detectable spoofing range of the attack vector.*

$$\|a_k\|_2 \leq \frac{\tau}{\|B\|_2} - \|z_k\|_2. \tag{17}$$

According to the triangle inequality, it's easy to prove Corollary 1 is true. The specific derivation is given as follows.

According to the triangle inequality of vector 2- norm,

$$\|(z_k + a_k)\|_2 \leq \|z_k\|_2 + \|a_k\|_2, \tag{18}$$

when $\|z_k\|_2 + \|a_k\|_2 \leq \frac{\tau}{\|B\|_2}$ hold, the Eqn (16) will be hold. So Eqn (17) is a safe range of the attack vector.

When packets are randomly lost, the integrity of the collected data by SCADA is destroyed. However, due to the redundancy of data in data acquisition of the power grids, the effect of the loss of a small number of measurements may small. To study the effect of data injection attack on the performance of state estimation under random packet losses, the mean square error (MSE) of weighted least squares state estimation under random packet losses is derived.

Suppose that the state vector x_k, the attack vector a_k, and the noise v_k obey the Gaussian distribution where the mean value is $\mu_{x_k} = 0$, and the variance is R_{x_k}, R_{a_k}, R_v. When there is random packet loss, the measurement model of the system is shown by Eqn (6). Combined Eqn (11) with Eqn (6), the state estimation of the system can be expressed as

$$\begin{aligned} &\hat{x}_{lak} = ((\lambda_k H)^T W \lambda_k H)^{-1} (\lambda_k H)^T W (z_k + a_k) \\ &= (H^T \lambda_k W H)^{-1} H^T \lambda_k W (z_k + a_k). \end{aligned} \tag{19}$$

When the system state estimation residual is defined as $\varepsilon_{x_k} = \hat{x}_{lak} - x_k$, ε_{x_k} can be expressed as

$$\begin{aligned} &\varepsilon_{x_k} = (H^T \lambda_k W H)^{-1} H^T \lambda_k W (z_k + a_k) - x_k \\ &= (H^T \lambda_k W H)^{-1} H^T \lambda_k W (H x_k + v_k + a_k) - x_k \\ &= (H^T \lambda_k W H)^{-1} H^T \lambda_k W (v_k + a_k) \end{aligned} \tag{20}$$

When there is random packet losses and data injection attack, the mean square error matrix of system state estimation is

$$\begin{aligned} &R_{\varepsilon_{x_k}} = E\{\varepsilon_{x_k} \varepsilon_{x_k}^T\} = (H^T \lambda_k W H)^{-1} \\ &+ (H^T \lambda_k W H)^{-1} H^T \lambda_k W R_{a_k} \lambda_k W H (H^T \lambda_k W H)^{-1}. \end{aligned} \tag{21}$$

Let $B_k = (H^T \lambda_k W H)$, $R_{\varepsilon_{x_k}}$ can be expressed as

$$R_{\varepsilon_{x_k}} = {B_k}^{-1} + {B_k}^{-1} H^T \lambda_k W R_{a_k} \lambda_k W H {B_k}^{-1}. \tag{22}$$

Ideally, when there is no packet losses and data injection attacks, $\lambda_k = I$, $a_k = 0$. Then the mean square error matrix of the weighted least squares state estimation is

$$R_{\varepsilon_{x_k}} = (H^T W H)^{-1}. \tag{23}$$

Comparing Eqn (22) and (23), it can be found that the existence of random packet losses will not only affect the state estimation, but also affect the effect of data injection attack.

4 Simulation Study

To assess the impact of data injection attack under random packet losses on smart grid state estimation, IEEE-14 node system is used in the simulation experiments, as shown in Figure 3. IEEE-14 node system has 54 measurements, where 1-14 are the measurements of the active power of the bus, 15-34 are the measurements of branch power of the incoming node, and 35-54 are the measurements of branch power of the outgoing node. Assuming that the noise of each measurement obeys the Gaussian distribution, i.e., $v_i \tilde{} N(0, 0.02^2)$, where $i = 1, 2, \cdots, 54$. Considering the phase angle of the reference bus $\delta_1 = 0$, it is only necessary to estimate the state quantity of the other 13 nodes, and $H \in R^{54\times 13}$.

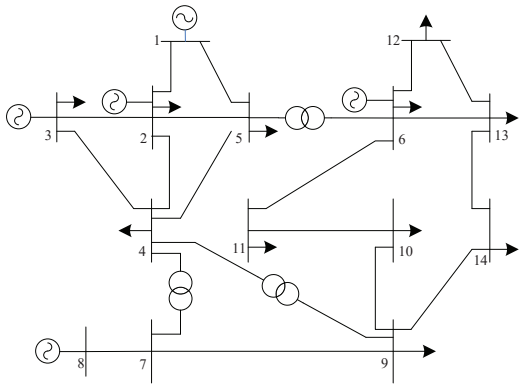

Fig. 3. The power grids measurement process.

Firstly, node 1 is selected as the reference node, and the state truth value and the measurement truth value are obtained by 100 power flow calculations. It is assumed that the white noise obeys the Gaussian distribution $(0, 0.02^2)$ and the measurement error covariance matrix is constant.

Performance index: From Eqn (23) under ideal conditions, when there is no data injection attack and transmission packet losses, the mean square error matrix of system state estimation is $R_{\varepsilon_{x_k}} = (H^T W H)^{-1}$. In order to measure the state estimation performance, Eqn (24) is used as the performance index.

$$\text{Performance}=\frac{\|(xreal-\hat{x})(xreal-\hat{x})'\|_F}{\left\|(H^T W H)^{-1}\right\|_F}, \tag{24}$$

where $xreal$ is system status truth value, $\hat{x}$ is the estimation, and $\|\|_F$ is frobenius norm of matrix.

When there only exist data injection attacks, while Eqn (17) is satisfied, three different attacks are randomly selected, where one measurement is tampered in

a_{88}, five measurements are tampered in a_{41}, and ten measurements tampered in a_{55}. The dimension of each non-zero in the attack vector was randomly selected in $[-(\frac{\tau}{\|B\|_2} - \|z_k\|_2)/p, (\frac{\tau}{\|B\|_2} - \|z_k\|_2)/p]$, where p is the number of the tampered devices. The details of the attack vector are shown in Table 1. The estimated results are also illustrated in Figure 4.

Table 1. Details of the attack vector in data injection attack only

Attack		Details									
a_{88}	Index	52									
	Value	37.97									
a_{41}	Index	4		15		43		44		45	
	Value	0.84		-6.05		9.47		8.44		-8.57	
a_{55}	Index	11	12	16	25	29	47	48	50	51	54
	Value	-5.06	-1.18	-1.01	-3.22	-3.59	-0.1	0.17	-0.04	-2.17	-5.25

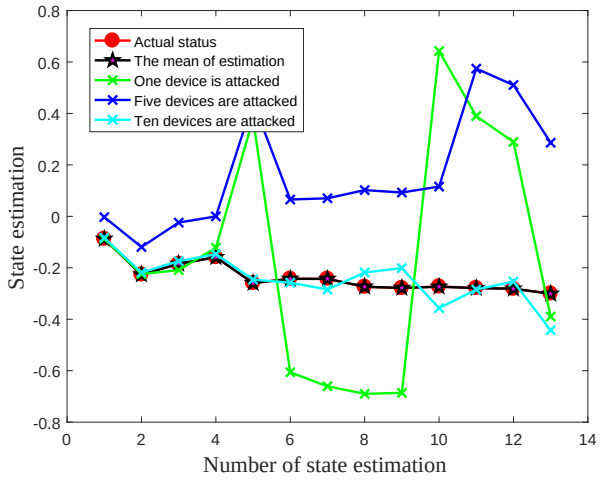

Fig. 4. State estimation under only data injection attack.

According to Figure 4, the data injection attack has a great impact on the survivability of system state estimation. However, with the increase of attack dimensions, the impact of the attack on the estimation decreases gradually if the attack vector remains non-detectable by satisfying Eqn (16).

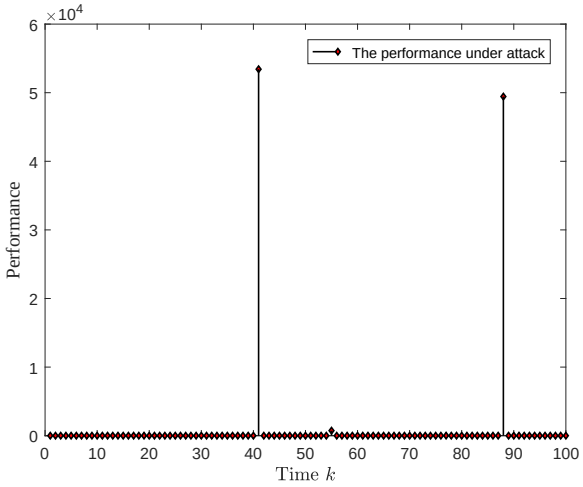

Fig. 5. Estimation performance under only data injection attack.

The performance index is also illustrated in Figure 5. This is a result from the attack vector limited by Eqn (17). The more dimensions of the attack, the lower the amplitude of each dimension in the attack vector will become.

In the packet loss only scenario, three packet loss rates are randomly selected, which are 2%, 5% and 10% respectively. The specific information of random packet losses is shown in Table 2, and the estimation results are illustrated in Figure 6.

Table 2. Details of the packet loss due to random packet loss only

Probability	Time	Index
2%	66	2
5%	99	16,28,48
10%	62	3,5,7,8,39

As show in Figures 6 and 7, a small amount of random data packet loss in the data transmission of the sensor does not have significant impact on the system state estimation. This is due to the existence of the measurement redundancy of the power system, which guarantees the safety and reliability of power system state estimation.

Furthermore, comparing Figure 4 with Figure 6, it is clear that the data injection attack has a greater impact on the system state estimation. Again, the performance indexes as shown in Figures 5 and 7 are not in the same order of magnitude.

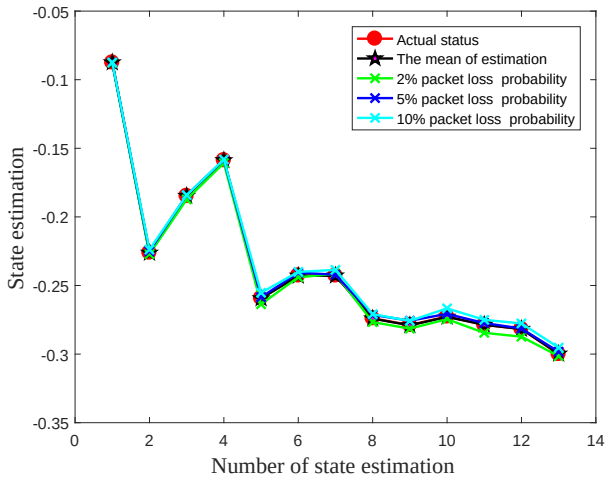

Fig. 6. State estimation under random packet loss scenario.

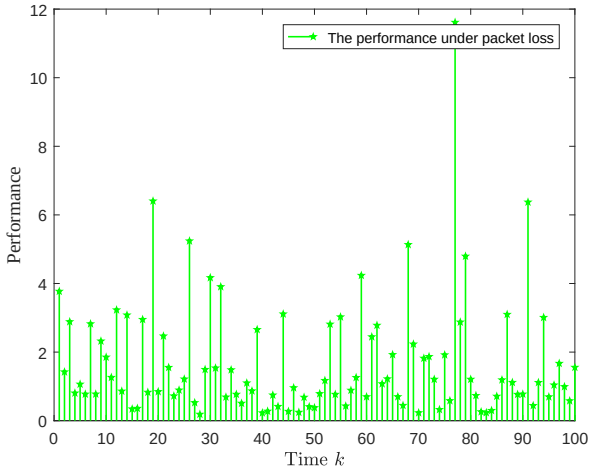

Fig. 7. Estimation performance in random packet loss only scenario.

When both packet losses and data injection attacks are presented, 5% packet loss rate and 5 dimensions attacked are simulated.

Three scenarios, including random packet losses and data injection attack are not coincidences, some coincident, and all occurred coincidently are analyzed. The specific information of random packet loss and attack vectors are listed in Table 3, and the estimation results are illustrated in Figure 8. It can be seen that

Table 3. The details of the packet loss and attack vectors

Time	Attack and packet loss		Details					Common index
44	a_{44}	Index	9	15	24	30	49	No
		Value	-9.33	-7.28	-6.88	-3.79	-9.67	
	Packet loss index		7,20,22					
92	a_{92}	Index	2	14	30	44	46	30,44
		Value	6.37	-6.40	0.94	9.84	-6.14	
	Packet loss index		21,30,44					
53	a_{53}	Index	12	24	28	48	53	12,48,53
		Value	-2.19	-8.03	5.65	8.68	-1.45	
	Packet loss index		12,48,53					

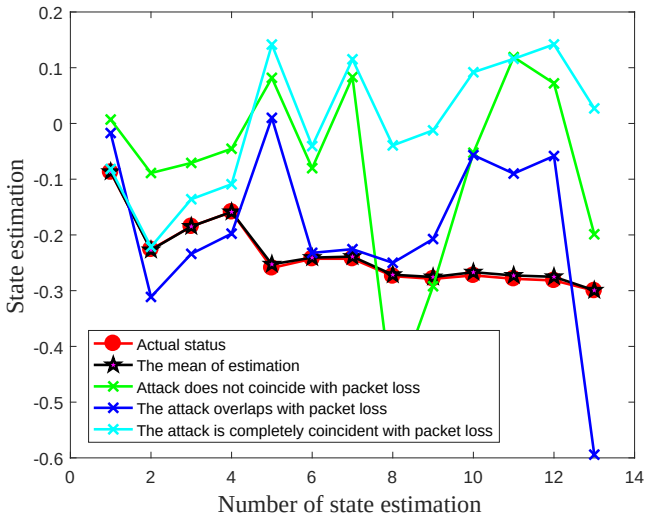

Fig. 8. State estimation under both random packet loss and data injection attack.

notification of data injection attack and random packet loss will have a great impact on system state estimation results.

As shown in Figure 9, when the random packet losses occur coincidently with the attack, and the estimation performance is better than the non-overlap, but the impact of the attack vector itself is greater.

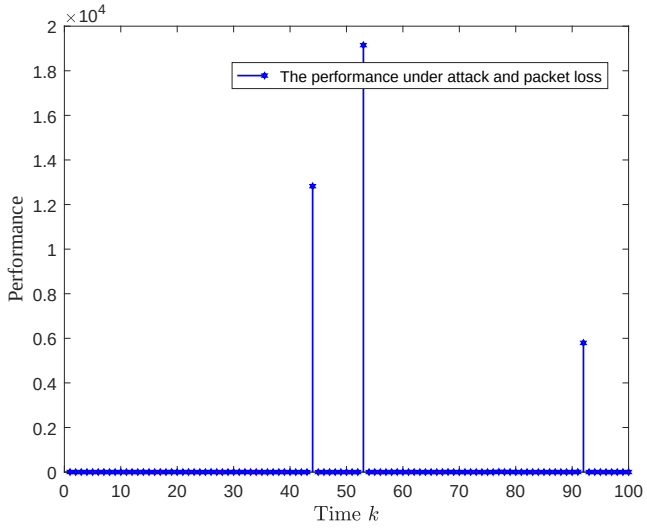

Fig. 9. Estimation performance under both random packet loss and data injection attack.

5 Conclusions

This paper has analyzed the impact of false data injection attacks on smart grid state estimation under random packet losses. Firstly, the measurement model of power grid under random packet losses is established, and an attack vector range that can escape the detector is derived. Then, the weighted least squares estimation is analyzed, and a non-detectable range of attack vectors in the data injection attack is derived. It is proved that as long as the attack vectors are selected in the derived range, the existing "bad data" detection device will not respond. Further, considering the false data injection attack, the mean square error matrix of the weighted least squares estimation is provided. Finally, simulation experiments on a IEEE-14 node system is used to compare the effects of data injection attack, random packet loss, and simultaneous random packet loss and data injection attack on the system state estimation.

Acknowledgement

Supported by Natural Science Foundation of China (No. 61633016, 61533010), Key Project of Science and Technology Commission of Shanghai Municipality (No. 19510750300, 19500712300, 16010500300), Industrial Internet Innovation and Development Project(TC190H3WL).

References

1. Yan, J., Guo, F., Wen, C.: False data injection against state estimation in power systems with multiple cooperative attackers. ISA Transactions **101**(10) (2020) 225–233
2. Sahoo, S., Dragicevic, T., Blaabjerg, F.: Cyber security in control of grid-tied power electronic converterschallenges and vulnerabilities. IEEE Journal of Emerging and Selected Topics in Power Electronics **15** (2019) 1–15
3. Shu, J., Guo, Z., Han, B.: A bilevel optimization model for power network spurious data injection attack. Automation of Electric Power Systems **43**(10) (2019) 95–101
4. Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y.: A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid **8**(4) (2017) 1630–1638
5. Liang, G., Weller, S.R., Zhao, J., Luo, F., Dong, Z.Y.: The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems **32**(4) (2017) 3317–3318
6. Gong, X.: Analysis of the situation of the power outage in venezuela and recommendations for the safety of critical infrastructure. Journal of information technology and network security **38**(04) (2019) 1–2+14
7. Upadhyay, D., Sampalli, S.: Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security **89** (2020) 101666
8. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. Acm Transactions on Information & System Security **14**(1) (2011) 1–33
9. Li, L., Yang, H., Xia, Y., Yang, H.: Event-based distributed state estimation for linear systems under unknown input and false data injection attack. Signal Processing **170** (2020) 107423
10. Guo, Z., Shi, D., Johansson, K., Shi, L.: Optimal linear cyber-attack on remote state estimation. IEEE Transactions on Control of Network Systems **4** (2016) 4–13
11. Zhao, Y., Goldsmith, A., Vincent Poor, H.: Minimum sparsity of unobservable power network attacks. IEEE Transactions on Automatic Control **62**(7) (2017) 3354–3368
12. Kim, J., Lang, T., Thomas, R.J.: Subspace methods for data attack on state estimation: A data driven approach. IEEE Transactions on Signal Processing **63**(5) (2015) 1102–1114
13. Zhong, H., Du, D., Li, C., Li, X.: A novel sparse false data injection attack method in smart grids with incomplete power network information. Complexity **2018** 1–16
14. Muniraj, D., Farhood, M.: Detection and mitigation of actuator attacks on small unmanned aircraft systems. Control Engineering Practice **83** (2019) 188 – 202
15. huaye, P., peng Chen, hongtao, S., mingjin, Y.: Incremental detection mechanism of microgrid under false data injection attack. Information and Control **48**(5) (2019) 522–527
16. Chen, R., Li, X., Zhong, H., Fei, M.: A novel online detection method of data injection attack against dynamic state estimation in smart grid. Neurocomputing **344** (2019) 73 – 81
17. Du, D., Chen, R., Li, X., Wu, L., Zhou, P., Fei, M.: Malicious data deception attacks against power systems: A new case and its detection method. Transactions of the Institute of Measurement and Control **41**(6) (2019) 1590–1599

18. Du, D., Li, X., Li, W., Chen, R., Fei, M., Wu, L.: ADMM-Based Distributed State Estimation of Smart Grid Under Data Deception and Denial of Service Attacks. IEEE Transactions on System Man Cybernetics-Systems **49**(8) (2019) 1698–1711
19. Xia, M., Du, D., Fei, M., Li, X., Yang, T.: A Novel Sparse Attack Vector Construction Method for False Data Injection in Smart Grids. Energies **13**(11) (2020)
20. Aghanoori, N., Masoum, M.A., Abu-Siada, A., Islam, S.: Enhancement of microgrid operation by considering the cascaded impact of communication delay on system stability and power management. International Journal of Electrical Power & Energy Systems **120** (2020) 105964
21. Ding, D., Han, Q.L., Xiang, Y., Ge, X., Zhang, X.M.: A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing **275** (2018) 1674 – 1683