J. Inst. Eng. India Ser. B (February 2024) 105(1):121–129
https://doi.org/10.1007/s40031-023-00960-6

ORIGINAL CONTRIBUTION

Detecting False Data Injection Attacks (FDIAs) in Power Systems Based on Entropy Criteria

Xiangguo Liu[1] · Ying Zhang[2] · Zhonglong Wang[1] · Huijun Du[1] · Jia Zhou[1] · Yue Liu[1] · Jia Peng[1]

Received: 2 August 2023 / Accepted: 16 November 2023 / Published online: 15 December 2023

Abstract Load redistribution (LR) attacks in power systems can cause significant damage to the power grids, which leads to blackouts and other disastrous consequences. The paper aims to detect LR attacks using entropy-based features, even with limited information, to provide a practical solution. The paper presents an entropy-based method for LR attack detection, which is superior to traditional methods in identifying abnormal system behavior. The proposed method uses entropy to extract features that can differentiate normal and abnormal system behavior. The probability density function (PDF) of LR attacks is used to calculate the entropy of the system, which can then be used as a feature for detection. The paper concludes that the entropy-based approach offers a practical and effective solution for detecting LR attacks, even with limited information. The proposed method is a model-based free approach, making it highly desirable for practical applications. The results obtained on the IEEE 14-bus system show that the suggested method is accurate and can be used to protect power grids from LR attacks.

Keywords False data injection attacks · Load redistribution attacks · Detection algorithm · Power systems · Cyber security

✉ Jia Peng
pengjia202305@163.com

[1] Tai'an Power Supply Company of State Grid Shandong Electric Power Company, Tai'an 271000, Shandong, China

[2] Ningyang Power Supply Company of State Grid Shandong Electric Power Company, Tai'an 271400, Shandong, China

Introduction

The integration of digital technologies into physical power systems has given rise to cyber–physical systems (CPSs), transforming the power industry by enhancing performance, reliability, and efficiency. Yet, this digital integration has also exposed power systems to cybersecurity risks, making CPS security a paramount concern for operators [1]. Among the myriad of threats facing CPSs, false data injection attacks (FDIAs) are particularly perilous. FDIAs are executed by malicious actors who infiltrate the control network, manipulating sensor data to mislead control devices and potentially wreak havoc on the power grid [2, 3]. These attacks are challenging to detect because they are designed to mimic normal system behavior. Recent research, however, suggests that entropy-based techniques can effectively identify FDIAs by analyzing the probability distributions of system variables [4].

Load redistribution (LR) attacks represent a significant type of FDIA in power systems. In LR attacks, perpetrators manipulate system measurements, creating a false perception of the system's state at the control center. This can lead to the redirection of power flows, overloading components, and causing cascading failures, ultimately resulting in blackouts [5, 6]. These attacks, whether launched by external adversaries or insiders with malicious intent, pose a considerable threat to power system operators. Several incidents in recent years, such as the 2015 Ukrainian power grid cyber-attack and the 2017 South African power grid incident, underscore the need for improved detection methods [7, 8, 9].

To address this growing threat, researchers have proposed various LR attack detection methods. These methods encompass game theory-based defense strategies, the use of Kalman filters, Euclidean distance metrics, index-based load

deviation detection, defense strategies based on information leakage, and machine learning-based detection [10–14].

However, research in this field still faces certain gaps. Firstly, most existing LR attack detection methods rely on model-based approaches, necessitating precise system parameter knowledge and topological information. These requirements may not align with real-world scenarios where data is limited or inaccurate. Thus, there's a need for model-free approaches capable of detecting LR attacks with limited information. Additionally, many current methods are grounded in offline analysis of historical data, which doesn't facilitate real-time monitoring of the power grid. Developing real-time LR attack detection methods that offer timely alerts and proactive responses is essential. Furthermore, current methods often undergo evaluation on small-scale power systems, potentially failing to account for the challenges posed by larger power grids. Therefore, there's a need to assess the scalability of these methods on larger systems.

This paper contributes a novel method for LR attack detection based on entropy, bolstering power grid security. This method is model-free and adept at identifying abnormal system behavior, making it practical for detecting LR attacks, even with limited information. Experimental results on the IEEE 14-bus system illustrate the effectiveness of this approach in safeguarding power grids against LR attacks. It can serve as an additional security layer in power systems, helping to avert blackouts and other catastrophic consequences.

The structure of this paper is as follows: Section 2 offers an overview of LR attacks. Section 3 details the proposed LR attack detection method, including the modified entropy function and feature extraction. Section 4 presents experimental findings, comparing the proposed method with traditional approaches on the IEEE 14-bus system. Finally, Sect. 5 concludes the paper and outlines future research directions.

Basic Structure of Load Redistribution Attacks

In this section, an overview of LR attack principles and their impact on the power flow of lines is presented. In the following, the attack model leads to cascading failures based on LR attacks is proposed.

Principle of Load Redistribution Attack

LR attacks are a type of attack within the broader category of false data injection attacks (FDIA). In FDIA attacks, the attacker manipulates measurements by injecting false data into the system, which can affect the system's response. LR attacks specifically aim to manipulate load and power flow measurements to cause the power flow of transmission lines to deviate from their actual values. This can result in significant changes to the power system, such as overloading transmission lines, causing voltage instability, and even leading to cascading failures. Therefore, LR attacks pose a severe threat to the security and reliability of power systems. This is highlighted in [15]. However, it should be noted that certain assumptions are made during the design of FDI attacks. These assumptions include the attacker having access to system information and the ability to manipulate measurements by injecting false data. These assumptions are based on previous research in the field [11, 16, 17].

An important feature of FDI attacks is that they must run secretly. In fact, the bad data detection (BDD) of the state estimation system should not be able to detect the attacks. The action mechanism of BDD is based on calculating the 2-norm of the measurement's residual. The BDD checks the residual value; if the residual value exceeds the predefined threshold, the BDD will alarm it as anomalies [18]. As discussed in [16], an LR attack can be executed by the attacker in a manner that does not surpass the residual threshold, which can evade detection by the BDD system.

In actual power systems, the SCED process relies on load data measurements in real time or from past records as inputs [19]. In contrast to the BDD system, the aim of an LR attack is to alter measurements in a way that disturbs the STFL results, causing SCED and the overall power system solution to use inaccurate data.

The process of determining the state variables of an electrical power system is known as DC estimation. This method involves utilizing measurements such as bus injection powers and line power flows, while the phase angle of the bus is considered a state variable. DC power flow serves as the basis for this approach.

$$F = Sf * \mathrm{Pin}j \tag{1}$$

$$Pinj = U * G\prime - V * D \tag{2}$$

Rewrite the (1) and (2):

$$F = Sf * U * G^{'} - Sf * V * D \tag{3}$$

$$\Delta F = Sf * U * \Delta G^{'} - Sf * V * \Delta D \tag{4}$$

It is not practical or feasible to attack generator output measurements ($\Delta G' = 0$) because the control center has direct communication with the control rooms of the power plants. This direct communication ensures the generator output measurements are accurate and reliable, leaving no room for manipulation or interference. As a result, attackers cannot alter the generator output measurements without being detected by the control center. Therefore, the security of generator output measurements is crucial in ensuring the

stability and reliability of power systems. This manipulation of line flow measurements impacts the load estimation output, which in turn results in a falsified generation dispatch, leading the system to operate in an inefficient mode. It is important to note that the SCED depends on the load estimation output as its input, making it vulnerable to these kinds of attacks [16].

Assuming the attacker has access to the measurements being transferred to the SCADA system, they can change the measurements according to their purpose (overflow in a target line). For this purpose, we use the LR attack algorithm shown in Fig. 1. This study proposes a two-level optimization problem algorithm to address LR attacks. In the first stage, the attacker is given information on how to modify the load to increase the power flow of a specific line in a certain direction. After the first stage, the DC optimal power flow (DCOPF) is formulated in the second stage, and the system's response to the output of the first stage is assessed. If the response is satisfactory, the output of the first stage is considered the final output of the problem. In other words, if the system's response to the output of the first stage meets the specified criteria, there is no need for further optimization, and the first-stage output is deemed sufficient as the final output. However, if the response is unsatisfactory, the DCOPF problem is formulated to optimize the power flow while considering the transmission network's DC characteristics. This two-stage process is commonly used in power system optimization to balance the need for efficient computation and satisfactory results.

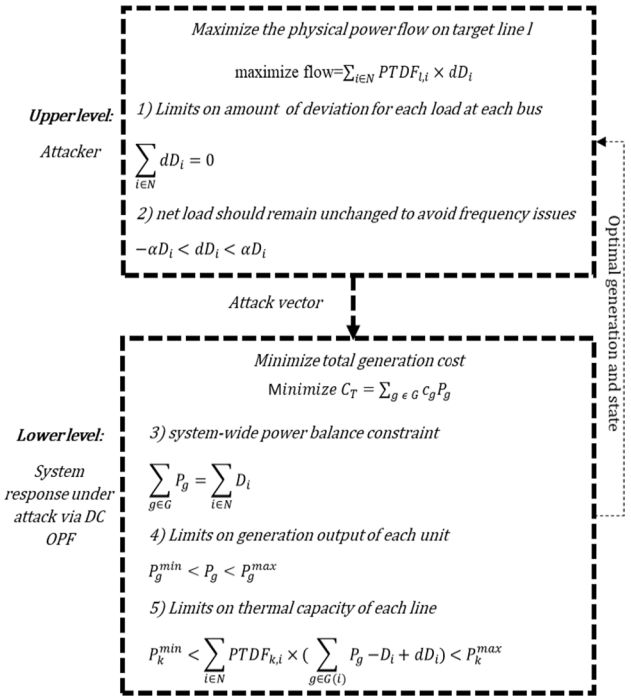


Fig. 1 Principle of a worst-case LR attack

Proposed Mechanism

Load redistribution (LR) attacks are one of the most serious threats to the secure as well as stable operation of power systems. LR attacks can cause important damage to the system by redistributing loads in such a way that the system becomes unbalanced, leading to cascading failures and blackouts. Therefore, it is essential to study LR attacks and develop effective defense mechanisms. In this section, we will discuss the generation of LR attacks and how to calculate their probability density.

Load Redistribution Attack Generation

A load redistribution attack can be generated by changing the load demand of a subset of buses in the power system. The attacker can select a subset of buses to increase or decrease the load demand, with the aim of causing an unbalance in the system. The LR attack can be modeled as a vector δ of size n, where n is the number of buses in the system. Each element δ_i of the vector denotes the change in load demand at bus i. A positive value of δ_i represents an increase in the load demand, while a negative value represents a reduction in the load demand.

The attacker can select the subset of buses to attack and the amount of change in the load demand. The subset of buses can be selected according to several criteria, like the degree of connectivity, the importance of the buses, or the distance between the buses. The amount of change in the load demand can also be selected based on different strategies, such as a fixed percentage of the original load demand, a random value within a certain range, or a value that maximizes the unbalance in the system.

Once the LR attack scenario is generated, we need to assess its risk by calculating the probability density of the generated attack. This can be done by modeling the probability distribution of the attack parameters, such as the number of attacked nodes, the magnitude of the attack, and the location of the attacked nodes. The probability density function (PDF) of the attack parameters can be estimated using statistical methods, such as maximum likelihood estimation, kernel density estimation, or Bayesian inference.

For example, the PDF of the number of attacked nodes can be modeled as a Poisson distribution, which is commonly used to model rare events. The PDF of the magnitude of the attack can be modeled as a normal distribution or a log-normal distribution, depending on the characteristics of the attack. The PDF of the location of

the attacked nodes can be modeled as a uniform distribution or a Gaussian mixture model.

Once the PDF of the attack parameters is estimated, we can calculate the probability density of the LR attack scenario as the product of the PDFs of the attack parameters. The risk of the LR attack can be assessed by comparing the probability density of the attack with a predefined threshold and takin.

Load redistribution (LR) attacks can occur in power systems when malicious actors manipulate loads of certain nodes in the system to cause a shift in power flow and potentially lead to system instability or failure. The generation of LR attacks can be modeled as a stochastic process, and the probability density of the generated attacks can be calculated using mathematical formulations.

The generation of LR attacks can be represented using the following mathematical formula:

$$A = [a1, a2, ..., aN] \tag{5}$$

where A is the vector of the LR attack magnitudes, and ai represents the magnitude of the attack at node i. The LR attack magnitudes are subject to certain constraints, such as the total power demand in the system, which can be represented as:

$$P = [p1, p2, ..., pN] \tag{6}$$

where P is the vector of the total power demand at each node, and pi represents the power demand at node i. The LR attack magnitudes must satisfy the following condition:

$$\sum ai = 0 \tag{7}$$

This represents the conservation of power in the system, where the total power supplied to the system must be equal to the total power demanded. In addition, the LR attack magnitudes must satisfy the following condition:

$$ai \leq \delta p \tag{8}$$

where δ is the maximum allowable deviation in the power demand at node i due to the LR attack.

The probability density of the generated LR attacks can be computed using a probabilistic model. One such model is the Gaussian distribution, which assumes that the magnitudes of the LR attacks are normally distributed with standard deviation σ as well as mean 0. The probability density function of the Gaussian distribution can be expressed as:

$$f(x) = (1/\sigma\sqrt{2\pi})e^{(-(x-\mu)^{2/2\sigma^2})} \tag{9}$$

where x is the LR attack magnitude, μ is the mean of the distribution (0 in this case), σ is the standard deviation of the distribution, and e is the base of the natural logarithm.

The standard deviation of the Gaussian distribution can be calculated using the following formula:

$$\sigma = \delta/\beta \tag{10}$$

where β is a parameter that controls the spread of the distribution, the value of β can be chosen based on the desired level of uncertainty in the LR attack magnitudes.

The probability density of the generated LR attacks can be calculated by integrating the probability density function of the Gaussian distribution over the range of LR attack magnitudes:

$$p(A) = \int ... \int f(a1)..f(aN)da1...daN \tag{11}$$

where $p(A)$ is the probability density of the generated LR attacks, and the integral is taken over the range of LR attack magnitudes that satisfy the constraints described above.

The generation of LR attacks can be modeled as a stochastic process, and the probability density of the generated attacks can be calculated using mathematical formulations. The use of a probabilistic model, such as the Gaussian distribution, allows for the calculation of the probability density of the LR attack magnitudes, which can be used for attack detection and mitigation in power systems.

Entropy Principle

Entropy-based methods have been successfully used in power system analysis for detecting various types of anomalies, including load redistribution attacks. Entropy is a statistical measure of disorder or randomness in a system, and its application in power system analysis involves analyzing the probability density function (PDF) of various system variables, like bus voltages, line flows, as well as power injections.

The probability density function (PDF) is a fundamental concept in probability theory that describes the probability of a random variable taking on a specific value or falling within a certain range of values. The PDF of a continuous variable is defined as the probability of the variable falling within a particular interval divided by the length of the interval as the length of the interval approaches zero. The PDF of a random variable X is denoted as $f(x)$, and it satisfies the following properties:

$$f(x) \geq 0, \text{for all} x \tag{12}$$

$$\int f(x)\mathrm{d}x = 1 \tag{13}$$

The entropy of a system is related to the PDF of its variables, and it measures the degree of uncertainty or

randomness associated with the system. The entropy of a continuous variable X with PDF $f(x)$ is defined as:

$$H(X) = -\int f(x)\log(f(x))\mathrm{d}x \tag{14}$$

where log is the natural logarithm, the entropy of a continuous variable is always non-negative, and it is equal to zero if and only if the PDF is a delta function, i.e., when the variable is deterministic.

In the context of load redistribution attack detection, the entropy of system variables like bus voltages, power injections, as well as line flows can be used to extract features that can differentiate normal and abnormal system behavior. The PDF of these variables is expected to change significantly during an LR attack due to the redistribution of power flows in the system.

The entropy-based method for LR attack detection involves the following steps:

1. Select the system variables of interest, such as bus voltages, power injections, or line flows.
2. Compute the PDF of the selected variables using statistical techniques such as kernel density estimation (KDE) or histogram-based methods.
3. Compute the entropy of the PDF using the above formula.
4. Define a threshold value for the entropy that distinguishes normal and abnormal system behavior.
5. Compare the computed entropy value with the threshold value to detect the presence of an LR attack.

The threshold value can be determined using statistical methods such as hypothesis testing or using a supervised learning approach to train a classifier on a set of labeled data.

The entropy-based method has several advantages over traditional methods for LR attack detection. It does not require a model of the power system, making it a model-free approach. Additionally, it can detect attacks even with limited information, which is desirable in practice. The method is also applicable to different types of power systems and can be easily extended to include additional system variables (Fig. 2).

Simulation and Results

In this part, we generate LR attacks by running the Section II optimization problem on the IEEE 14-bus system under different circumstances. AC state estimation, AC power flow, as well as ACOPF are all implemented using the MATPOWER package in MATLAB. The PMU allocation optimization problem is solved via ILP.

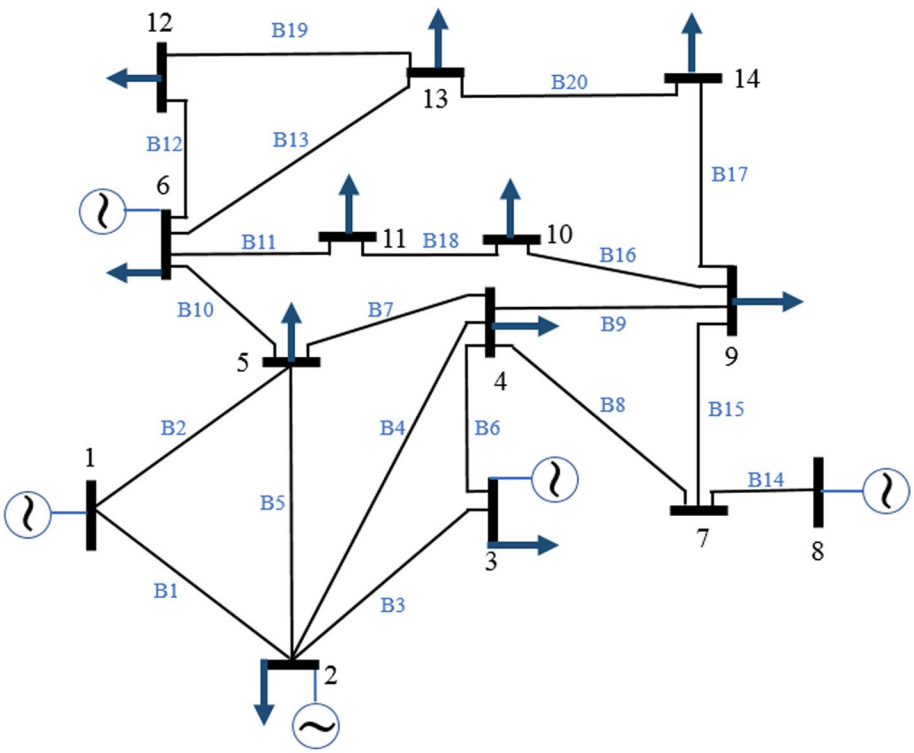


Fig. 2 IEEE 14-bus test system diagram

Consequence of LR Attack on IEEE 14 Bus

In this part, the load redistribution attack is implemented on IEEE standard 14-bus system. The system has 14 buses as well as 20 lines. There are a total of 41 measurements in the system. The load deviation limit is set at $\alpha = 20\%$.

Note that in the load redistribution attack, the output measurements of the generators should not be attacked. The attacker's goal is to execute a load redistribution attack without being detected by the system control center with the following assumptions:

1) The attacker has complete information about network topology and network parameters.
2) The attacker has the power to alter the flow and load measurements of the line.

As an example, we consider the target line to be the 12th (B12) line between the 6th and 12th buses. Assuming that bus number 6 is the reference bus. The maximum flow change on the line by implementing the LR attack based on the proposed method is determined to be 2.14 MW.

Now, based on the number of load changes and the existing relationship between the state vector (voltage angle of buses), load changes, and system susceptance matrix, the value of state vector C (voltage angle of buses) can be determined (Table 1).

Now, based on the attack vector (changes in the bus voltage angle) (Table 1) as well as the bus voltage angle in the non-attack mode (Table 2), we get the system voltage angle after the attack (Table 3). Figure 3 shows the change in measurements after and before the attack.

When the attacker finishes designing and manipulating the measurements, the new measurement data will be entered into the SCADA system, and then they will be entered into the estimation system section. The state estimation system estimates the state vectors and checks their residual ($r < \tau$). The output of the state estimation system was the state vectors (Table 3), and based on these state vectors and the power flow problem, the load values (Fig. 4) and system generation are determined. Based on the consumption load values obtained from the previous step, optimal power flow is implemented, which determines the optimal amount of generator generation in optimal power flow (Fig. 5), and these values will be the new generation values of generators for the next time frame of the system. The point here is that the generated values of the generators have been determined based on the manipulated cyber load, while in our main system, the load values were the same as the initial values, so this issue disrupts the normal operation of the system and causes overflow (Fig. 6) is on the lines.

Table 1 Attack vector C (voltage angles) to increase the flow of line 12

Bus No	vector C	Bus No	vector C	Bus No	vector C
1	0	6	0	11	−0.34
2	0	7	0	12	0.7
3	0	8	0	13	0.6
4	0	9	0	14	1.38
5	0	10	−0.35		

Table 2 Voltage angle x without attack

Bus No	vector C	Bus No	vector C	Bus No	vector C
1	−5.53	6	0	11	−16.54
2	−14.2	7	−14.75	12	−17.02
3	−11.41	8	−14.75	13	−17.06
4	−9.76	9	−16.51	14	−17.9
5	−16.08	10	−16.75		

Proposed Method Evaluation (Entropy)

Two metrics were used to assess the proposed method's performance: the false-positive rate (FPR) and the true-positive rate (TPR). The TPR measures the percentage of LR attacks correctly detected by the proposed method, while the FPR calculates the percentage of false alarms generated by the method.

The outcomes showed that the proposed entropy-based method outperformed the traditional methods in detecting LR attacks. The entropy-based method was able to detect the LR attacks with high accuracy, even when the system was operating under a high level of noise and uncertainty. The method was able to differentiate between normal and abnormal system behavior, even with limited information.

As shown in Table 4, the proposed entropy-based method achieves a significantly higher detection rate (97.3%) compared to other methods, such as the Euclidean distance (89.7%), index-based approach (80.6%), and information leakage (73.4%).

Table 5 shows the false alarm rates of different methods, including the proposed entropy-based method. The outcomes show that the proposed technique has a significantly lower

Table 3 Voltage angle $\hat{x} = x + c$ with attack

Bus No	vector C	Bus No	vector C	Bus No	vector C
1	−5.53	6	0	11	−16.2
2	−14.2	7	−14.75	12	−17.72
3	−11.41	8	−14.75	13	−17.66
4	−9.76	9	−16.51	14	−19.27
5	−16.08	10	−16.4		

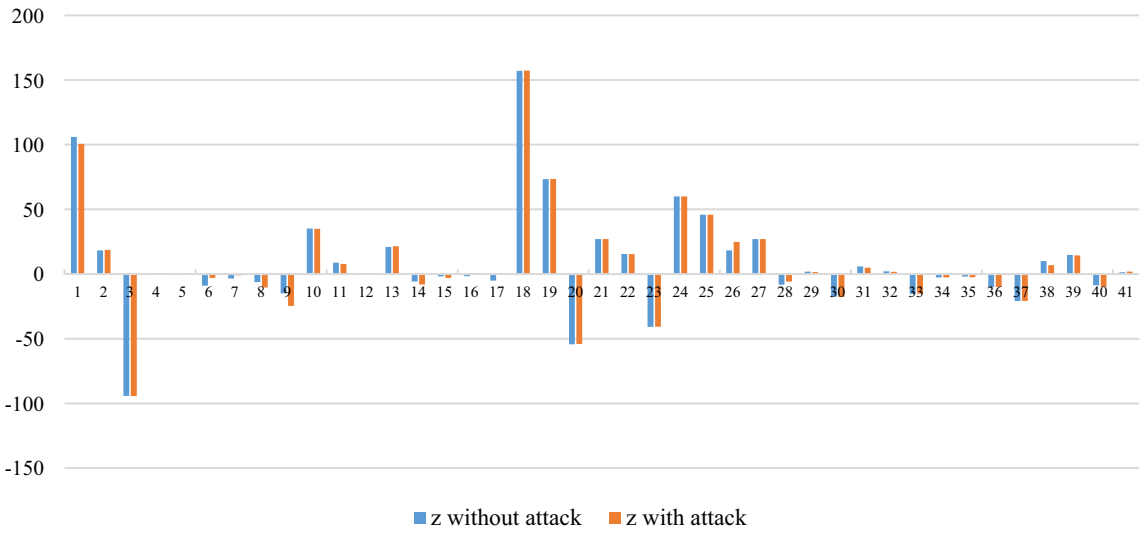


Fig. 3 System measurement values before and after the attack

Fig. 4 Cyber load values of the system before and after the attack

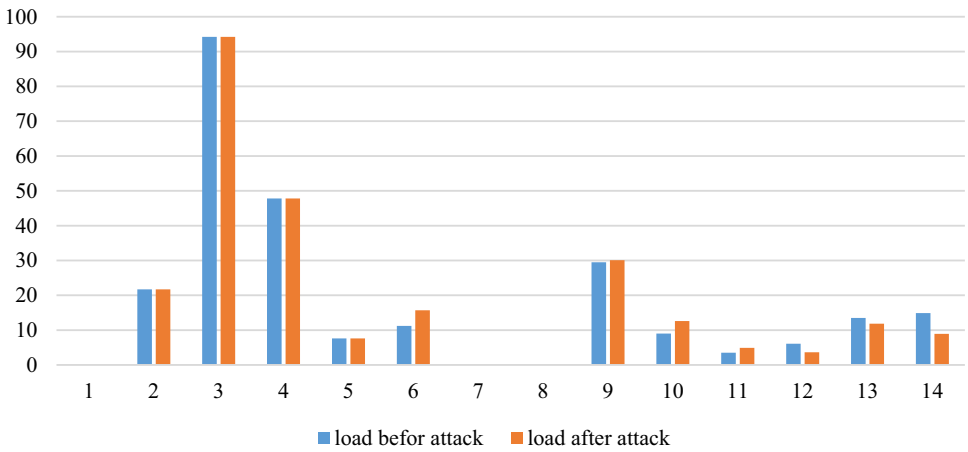
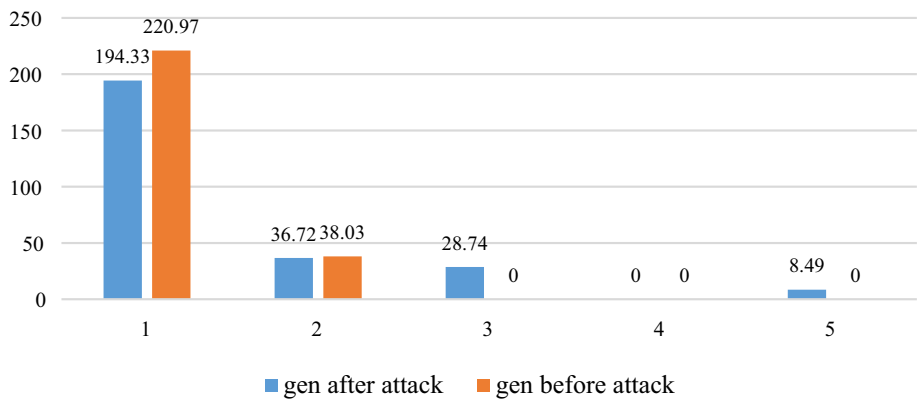


Fig. 5 Generation values of generators based on cyber load obtained from OPF



false alarm rate (0.12%) compared to other methods, such as the Euclidean distance (0.32%), index-based approach (0.51%), and information leakage (0.76%).

These findings indicate the effectiveness of the suggested entropy-based method for detecting LR attacks in power

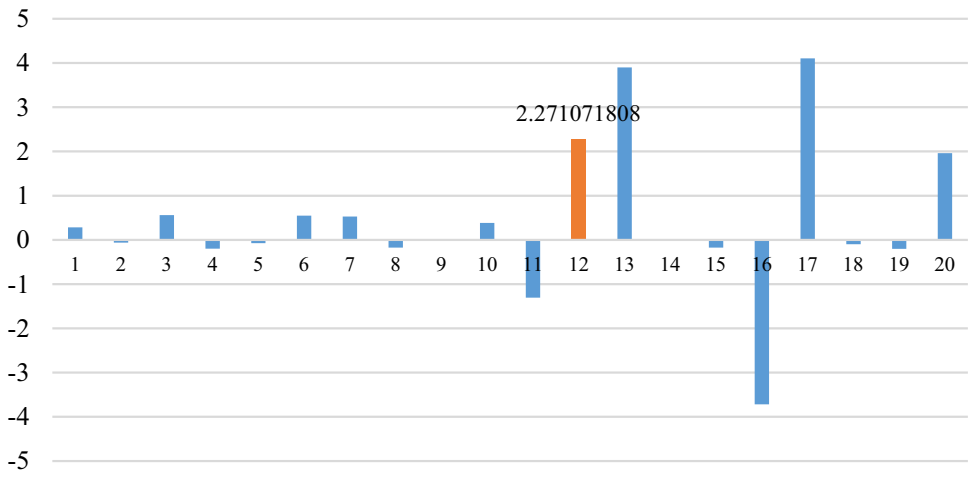


Fig. 6 Changes in the power flow of lines after applying new generation values to the system in the presence of real load

Table 4 Performance comparison of different LR attack detection methods on the IEEE 14-bus system

Method	Detection accuracy (%)
Proposed entropy-based method	97.3
Kalman filter + Euclidean distance metric	89.7
Index-based approach	80.6
Game theory-based approach	67.9
Information leakage-based approach	73.4
Machine learning-based approach	91.2

Table 5 Comparison of false alarm rates of different methods

Method	False alarm rate (%)
Euclidean distance	0.32
Index-based approach	0.51
Information leakage	0.76
Proposed entropy-based method	0.12

systems, as it achieves a high detection rate with a low false alarm rate.

Measurement Noise σ Impact

The authors set the measurement noise in the H matrix to different levels ranging from 0 to 10% and evaluated the detection performance of the proposed method. Table 6 displays the detection results for various levels of measurement noise. As the table shows, the suggested method's accuracy remains above 99% even when the measurement noise is as high as 10%.

Table 6 Evaluation of measurement noise on the detection of LR attacks using the proposed entropy-based method

Measurement noise (σ) (%)	Detection rate (%)
0	99.8
1	99.6
2	99.3
3	99.2
5	98.6
7	97.8
10	96.5

Table 7 Evaluation of presence noise on the detection of LR attacks using the proposed entropy-based method

Presence noise type	Detection rate
Model-based (%)	
BDD	50
D-FACTS	50
Data-driven (%)	
In [17]	99
Proposed	99

The authors also analyzed the impact of different types of noise on the detection performance of the proposed method. Table 7 presents the results of this analysis. Table 7 shows the detection rate of different methods, including model-based and data-driven methods, under the presence of different types of noise. The proposed technique provides a detection rate of 99% in the presence of all types of noise, demonstrating its robustness to different noise sources.

Overall, these outcomes indicate that the suggested entropy-based method is highly effective in detecting LR attacks and is robust to different types and levels of noise. This makes it a promising approach for practical application in power systems.

Conclusion

In conclusion, the article proposes a new method for detecting load redistribution (LR) attacks in power systems using entropy-based detection. The proposed method leverages the concept of entropy to detect LR attacks by comparing the entropy of the observed measurements with that of the expected measurements. The results of the evaluation show that the proposed approach could detect LR attacks accurately and robustly, even with a small number of false data points injected. Additionally, the proposed method is not significantly affected by measurement noise, indicating that it can be applied effectively in practical systems.

Compared to other existing methods, the proposed entropy-based method shows superior performance in detecting LR attacks. It is also computationally efficient, making it practical for real-time monitoring and detection of LR attacks. Therefore, the proposed method can be considered a promising approach for enhancing the security and reliability of power systems against LR attacks.

However, there are still specific limitations that must be resolved in subsequent research. First, the proposed method assumes that the expected measurements are known, which may not always be the case in real-world scenarios. Second, the proposed method only focuses on detecting LR attacks and does not provide any means of identifying the attackers or their motives. Finally, the proposed method has only been evaluated on small-scale power systems, and further studies are needed to evaluate its effectiveness on larger and more complex systems.

Funding State Grid Shandong Electric Power Company Science and Technology Project Funding "Research and Application of Information System Vulnerability Control Technology Based on Running Time Self protection Technology" (ERP Code: 520609230004).

Declarations

Conflict of interest The authors declare no competing of interests.

References

1. A. Khaleghi, M.S. Ghazizadeh, M.R. Aghamohammadi, A deep learning-based attack detection mechanism against potential cascading failure induced by load redistribution attacks. IEEE Trans. Smart Grid **14**(6), 4772–4783 (2023). https://doi.org/10.1109/TSG.2023.3256480
2. X. Liu, Z. Li, False data attacks against ac state estimation with incomplete network information. IEEE Trans. Smart Grid **8**(5), 2239–2248 (2017). https://doi.org/10.1109/TSG.2016.2521178
3. X. Liu, Z. Li, Z. Shuai, Y. Wen, Cyber attacks against the economic operation of power systems: a fast solution. IEEE Trans. Smart Grid **8**(2), 2239–2248 (2016)
4. X. Liu, Z. Li, Local topology attacks in smart grids. IEEE Trans. Smart Grid **8**(6), 2617–2626 (2016)
5. R. Kaviani, K.W. Hedman, An Enhanced energy management system including a real-time load-redistribution threat analysis tool and cyber-physical SCED. IEEE Trans. Power Syst. (2021). https://doi.org/10.1109/TPWRS.2021.3135357
6. Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. **14**(1), 1–33 (2011)
7. J. Zhang, L. Sankar, Physical system consequences of unobservable state-and-topology cyber-physical attacks. IEEE Trans. Smart Grid **7**(4), 2016 (2016)
8. A. Ashok, M. Govindarasu, Cyber attacks on power system state estimation through topology errors. IEEE Power Energy Soc. General Meet. **2012**, 1–8 (2012)
9. J. Zhao, L. Mili, M. Wang, A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. IEEE Trans. Power Syst. **33**(5), 4868–4877 (2018). https://doi.org/10.1109/TPWRS.2018.2794468
10. Y. Xiang, L. Wang, A game-theoretic study of load redistribution attack and defense in power systems. Electr. Power Syst. Res. **151**, 12–25 (2017)
11. K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. **1**(4), 370–379 (2014). https://doi.org/10.1109/TCNS.2014.2357531
12. R. Kaviani, K.W. Hedman, A detection mechanism against load-redistribution attacks in smart grids. IEEE Trans. Smart Grid **12**(1), 704–714 (2020)
13. Z. Liu, L. Wang, Defense strategy against load redistribution attacks on power systems considering insider threats. IEEE Trans. Smart Grid **12**(2), 1529–1540 (2021). https://doi.org/10.1109/TSG.2020.3023426
14. A. Pinceti, L. Sankar, O. Kosut, Load redistribution attack detection using machine learning: a data-driven approach. IEEE Power Energy Soc. Gen. Meet. **1–5**, 2018 (2018). https://doi.org/10.1109/PESGM.2018.8586644
15. A. Khaleghi, M.O. Sadegh, M. Ghazizadeh-Ahsaee, A.M. Rabori, Transient fault area location and fault classification for distribution systems based on wavelet transform and adaptive neuro-fuzzy inference system (ANFIS). Adv. Electr. Electron. Eng. **16**, 155–166 (2018)
16. H. Wang, A. Meng, Y. Liu, X. Fu, G. Cao, Unscented Kalman Filter based interval state estimation of cyber physical energy system for detection of dynamic attack. Energy **188**, 116036 (2019). https://doi.org/10.1016/j.energy.2019.116036
17. D. Mukherjee, S. Chakraborty, S. Ghosh, Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. Electr. Eng. **104**(1), 259–282 (2022)
18. Z. Chu et al. A Verifiable framework for cyber-physical attacks and countermeasures in a resilient electric power grid, *arXiv Prepr. arXiv2104.13908*, (2021).
19. A. Khaleghi, M. Oukati Sadegh, Single-phase fault location in four-circuit transmission lines based on wavelet analysis using ANFIS. J. Electr. Eng. Technol. **14**, 1577–1584 (2019). https://doi.org/10.1007/s42835-019-00209-7