Cyber attacks targeting electronic devices of power systems and countermeasures

Wenjun Bi1, a,∗, Luyu Wang1, a, and Kaifeng Zhang1

Abstract Enhancing the security and reliability of power systems is of great significance to maintaining social stability. The power electronic devices of power systems can be utilized by attackers to launch indirect attacks, which could cause devastating impacts on the power grids. In this paper, load side attacks (LSAs) on relay protection devices is proposed as the first step to analyze the features of the attack. To achieve detection, a relation-based detection network is introduced to distinguish the LSAs from the normal faults.

Keywords: load side attack, relay protection, power electronic device, relation-based detection network

Classification: Power devices and circuits

1. Introduction

With the increasing dependence of power system on intelligent power devices, the number of vulnerable power devices that can be exploited by attackers in power systems is increasing [1, 2, 3, 4]. As the essential components in power systems, relay protections are menaced by malicious attacks. Considering that the relay protection devices are equipped with protection measures (e.g. communication isolation), sophisticated attackers tend to attack vulnerable power electronic devices to make the relay protection device malfunction. At the load side of power systems, distributed generation units, which are distributed in remote areas and equipped with power electronic devices, become potential targets of malicious attacks [5]. The attackers launch attacks on the power electronic devices of distributed generation units, causing the relay protection device to malfunction, and then causing line trip, which has adverse impact on the power grid. The characteristics of this potential attacks need to be analyzed, and the corresponding detection scheme needs to be studied.

In recent years, malicious attacks on power system are emerging. In 2010, Iran’s power station is attacked by Stuxnet virus, and the control of the key equipment of the power station is usurped [6]. The Metcalf sniper attack in California results in 27 days of repair time and over $15 million worth of damage [7]. The Ukraine Electric Grid Hack occurred in 2015 results in several circuit breaker to trip and 225,000 customers to lose power [8]. Attackers can jam the communication channels of power device of power systems using denial of service attacks [9, 10, 11]. Three attack templates against the power electronic devices of High Voltage DC (HVDC) are proposed in [12]. The simulation results show that malicious attacks against power electronic devices are capable of driving power systems into large oscillations or even unstable conditions.

To mitigate malicious attacks on power systems, researchers carry out research works on malicious from aspects including attack models [13], attack templates [14], device vulnerability [15], and countermeasures [16, 17]. The attacker-defender game theoretic models are investigated considering the characteristics of attack methods and defense resources [18, 19, 20, 21]. Notice that attack mitigation methods for different devices of power system are closely related to the characteristics of attack templates.

Though malicious attacks against power systems have been addressed in current literatures, the following aspects should be further studied: 1) Indirect attacks against relay protections should be studied. Sophisticated attackers could launch indirect attacks against relay protections to bypass security defense measures of relay protections. 2) Detection scheme against the aforementioned indirect attacks should be designed. The detection scheme needs to be able to distinguish the malfunction caused by attacks from that caused by faults.

In this paper, we focus on our research on analyzing the characteristics of malicious attacks against relay protections and designing corresponding detection scheme. Load-side attack is discussed to study the characteristics of indirect attacks against relay protections. To mitigate the proposed LSAs, a detection scheme based on measured data is designed.

The main contributions of the paper are as follows:

1) Indirect malicious attacks against relay protections is studied by considering load-side attacks, thus giving a priori knowledge of the characteristics of the potential malicious attacks.

2) A relation-based detection scheme is designed. To extract the features of compromised signals and those of normal signals, a relation network is used. The relation network can score the similarity between the data to be tested and the normal data. Based the score calculated by the relation network, the defender could distinguish the compromised signals from the normal ones.
2. Related work

Up to now, malicious attacks and corresponding countermeasures against malicious attacks are widely investigated in recent literatures. In [22], a supervised learning approach against cyber attacks on demand side of power systems is proposed to achieve attack detection with the aid of the characteristics of the demand side attacks (DSA). Random injection mechanism is proposed to mitigate fault attacks using encryption/decryption circuit [23]. Performance of side channel attack sensor is analyzed to improve the system security [24]. A low-energy prime-field elliptic curve cryptography (ECC) hardware processor is proposed to mitigate the impact of power attacks by analyzing the power dissipation trace [25]. A Markov model-based attack mitigation method is proposed to evaluate the security state of relay protection system using multi-source data of relay protection device [26].

As to the detection schemes against cyber attacks on the charging pile of power systems, a self-learning detection method based on long short-term memory (LSTM) is proposed to extract the unknown malicious behavior characteristics [27]. In [28], an artificial neural network with non-linear auto-regressive exogenous is used to identify the compromised signals in power system state estimation (PSSE). Dual-source data (DSD) of compromised variables are used to detect malicious attacks against remote terminal units of load frequency control systems [29]. Notice that machine learning algorithm plays an important role in the aforementioned detection schemes. The machine-learning-based detection schemes can distinguish the compromised data from the normal ones by extracting particular features of the measured data in power systems.

Although the study on malicious attacks against other critical facilities of power systems has been widely discussed, research on the malicious attacks against protection systems is still in its early stage. In [30], a model of malicious attacks against circuit breakers and relays is presented. In [31], a risk assessment method for evaluating the bus and transmission line protection systems considering the cyber security is discussed.

3. Attack model

As is shown in Fig. 1, line current differential (LCD) relay protection devices, which are increasingly being used for protecting transmission systems, are considered as the potential attack target. Considering the trip conditions of relay protection device and the concealment of attack, attackers could launch indirect attacks on the insulated gate bipolar transistor (IGBT) of distributed generator (DG) to bypass security defense measures of relay protections.

To trip the relay protection devices, the following trip conditions need to be satisfied:

\[
\begin{align*}
    I_{\text{com}} & \geq I_{\text{safe}} = 0.02 \text{p.u.} \\
    |I_1 + I_2 + I_3 + \ldots + I_{\text{com}} + \ldots + I_n| & \geq I_{\text{op}}(I_{\text{res}})
\end{align*}
\]

where \( I_{\text{com}} \) is the current of the compromised line; \( I_{\text{safe}} \) is the safe threshold of the disturbance detector of LCD relay protection; \( I_n \) is the instantaneous sampled value of the current entering the terminal of a line; \( I_{\text{op}}(I_{\text{res}}) \) is the operating current threshold associated with the restraining current \( I_{\text{res}} \). The variables \( I_{\text{com}}, I_{\text{op}}(I_{\text{res}}) \) and \( I_{\text{res}} \) can be expressed as

\[
\begin{align*}
    I_{\text{op}}(I_{\text{res}}) &= I_{\text{d0}} + m_i \times I_{\text{res}}, I_{\text{res}} \leq I_b \\
    I_{\text{op}}(I_{\text{res}}) &= I_{\text{d0}} + n_i \times I_{\text{res}}, I_{\text{res}} \geq I_b \\
    I_{\text{res}} &= |I_1| + |I_2| + |I_3| + \ldots + |I_{\text{com}}| + \ldots + |I_n|
\end{align*}
\]

where \( Z \) is the impedance of the compromised branch; \( u_{\text{VN}}, u_{\text{WN}} \) and \( u_{\text{WN}} \) are the three-phase voltages of the branch; \( I_{\text{d0}}, I_p, m_i \) and \( n_i \) are the parameters of the differential-restricting characteristic. The details of the parameters can be found in [14].

Based on the above analysis, the attacker can launch load-side attacks signals on IGBT modulation wave of distributed photovoltaic (PV) power station considering the relationship between IGBT modulation wave and phase voltage. The on and off status of IGBT are determined by the control signal input to IGBT gate. As a common inverter modulation method, Pulse width modulation (PWM) modulates the bias of IGBT gate by changing the pulse width, and then controls the output voltage of the inverter circuit. The output waveform of PWM is determined by the carrier wave and modulation wave. When an attacker injects a false data signal into the modulation wave signal channel, the modulation wave of PWM will be compromised based on

\[
u_{\text{V_H}}^{\text{com}} = \alpha \sin \omega c t + x_c
\]

where \( u_{\text{V_H}}^{\text{com}} \) is the V-phase modulation wave compromised by attacker; \( \alpha \) is the modulation degree of IGBT; \( \omega c \) is the angular frequency of sinusoidal signal wave. \( x_c \) is the compromised signal input by attacker.

Based on the relationship between modulation signal and IGBT on-off control signal, the on-status time period of the compromised IGBT can be expressed as

\[
\delta_V = \frac{T_c}{2}(1 + \alpha \sin \omega_c t_D + x_c)
\]

where \( T_c \) is the period of carrier wave. \( t_D \) is the time when the carrier wave reaches the negative peak.

The off-status time period of the compromised IGBT can be expressed as

\[
\delta^0_V = \frac{1}{2}(T_c - \delta) = \frac{T_c}{4}(1 - \alpha \sin \omega_c t_D)
\]

It can be seen that the on-off time of IGBT can be controlled by false data injection signal \( x_c \).
Based on the relationship between modulation wave and phase voltage, $u_{VN}$ can be expressed as

$$u_{VN} = \frac{U_d}{4} \left( \alpha \sin \omega_t t + \frac{2}{3} x_c \right)$$  \hspace{1cm} (8)

where $U_d$ is the Voltage of distributed generator before inverter. Therefore, the trip conditions can be rewritten as

$$\left\{ \frac{U_d}{4Z} \left( \alpha \sin \omega_t t + \frac{2}{3} x_c \right) + \frac{u_{VN} + u_{WN}}{Z} \geq I_{safe} \right\}$$

$$\left\{ I_1 + I_2 + I_3 + \cdots + I_n \leq I_{max}(I_{max}) \right\}$$

$$+ u_{VN} + u_{WN} + \cdots + I_n \leq I_{max}(I_{max})$$  \hspace{1cm} (9)

Based on the proposed attack method, attackers can meet the trip conditions by injecting the compromised signal $x_c$.

4. Relation-based detection scheme against indirect attacks on relay protection

In this section, a relation-based detection network is used to extract the features which can be used to distinguish the compromised signals from the normal ones. The core idea of the proposed detection network can be summarized as follows:

- Based on the features of the deep learning network, the characteristics of signal samples can be mined automatically by comparing the compromised signals and the normal signals.
- Considering the features of the siamese network architecture, the training target of the proposed detection network is to exploit the difference between the compromised data and the normal data.

The details of the proposed detection network is shown in Fig. 2.

As is shown in Fig. 2, the inputs of the relation-based detection network are compromised data vector $u_{V}^c$, normal data vector $u_{V}^n$ and query data vector $u_{V}^q$. The data vector is the time series data of one phase voltage $u_{VN}$. The compromised data set is generated based on the attack template proposed in Section 3. The historical data of phase voltage $u_{VN}$ is generated based on the attack template $u_{V}^c$. The attack parameter $x_c$ is randomly generated considering the value range of $x_c$. The value of attack parameter $x_c$ is based on the amplitude $\alpha$ of modulation wave $u_{V}$.

The detailed parameters can be found in [32]. 1000 compromised data are generated based on the attack model proposed in Section 3. The value of attack parameter $x_c$ is based on the amplitude $\alpha$ of modulation wave $u_{V}$. The attack parameter $x_c$ is randomly generated considering the value range of $x_c$. The value of attack parameter $x_c$ can be expressed as $x_c \in [0.1% \alpha, 100% \alpha]$. 1000 normal data are randomly selected from 2000 normal data as part of sample set. The remaining normal data are used as query data. True positive (TP), True negative (TN), False positive (FP) and False negative (FN) are used to quantify the relationship between the features of the input data vector. The input-output relationship of the detection network can be expressed as

$$\xi_{s,q} = \Psi \left( \Phi \left( \varphi \left( u_{V}^c \right), \varphi \left( u_{V}^q \right) \right) \right)$$  \hspace{1cm} (10)

During the training process, the mean square error (MSE) is used as the detection criteria to guide the training process. The detection criteria $\mathbf{T}$ can be expressed as

$$\mathbf{T} = \left\{ \sum \xi_{s,q} = 1 \right\}$$

$$\text{if } l_s \text{ is equal to } l_q$$

$$\sum \xi_{s,q} = 0$$

$$\text{if } l_s \text{ is not equal to } l_q$$  \hspace{1cm} (11)

where $l_s$ and $l_q$ are the labels for data in sample set and data in query set, respectively.

5. Simulation and analysis

5.1 Experimental setup

The IEEE standard two-area 4-unit 9-bus system is used to illustrate the effectiveness of the proposed detection network. The detailed parameters can be found in [32]. 1000 compromised data are generated based on the attack model proposed in Section 3. The value of attack parameter $x_c$ is based on the amplitude $\alpha$ of modulation wave $u_{V}$. The attack parameter $x_c$ is randomly generated considering the value range of $x_c$. The value of attack parameter $x_c$ can be expressed as $x_c \in [0.1% \alpha, 100% \alpha]$. 1000 normal data are randomly selected from 2000 normal data as part of sample set. The remaining normal data are used as query data. True positive (TP), True negative (TN), False positive (FP) and False negative (FN) are used to calculate the simulation results.

To evaluate the performance of the proposed detection scheme, the following indexes are used:

1) The accuracy of the detection scheme:

$$Ac = \frac{TP + TN}{TP + TN + TP + FN + FN}$$  \hspace{1cm} (12)

2) The probability of detecting correctly

$$P_{dc} = \frac{TP}{TP + FN}$$  \hspace{1cm} (13)

3) Success ratio:

$$SR = \frac{TP}{TP + FP}$$  \hspace{1cm} (14)

4) Probability of identifying normal cases:

$$P_{inc} = \frac{TN}{TN + FP}$$  \hspace{1cm} (15)

5.2 Simulation results

To illustrate the effectiveness of the proposed indirect attacks against LCDR, the risk coefficient of zero-sequence current, which can be expressed as $R_c = |I_{2s}|/|I_{safe}|$, is used to evaluate the trip risk of LCDR. $I_{2s}$ is the zero sequence current of the line that the defender is concerned about.

As is shown in Fig. 3, the magnitude zero-sequence current rapidly exceeds the safe value after the IGBT being attacked. It can be learned that the proposed indirect attack could make the remote power system relay protection device trip by attacking the distributed generation, resulting
Fig. 3  Risk coefficient of zero-sequence current.

Fig. 4  Performance of different detection method.

in the loss of power of the compromised node and power imbalance of power systems.

To illustrate the effectiveness of the proposed relation-based network (RN), three state-of-the-art data-driven detection methods are adopted. Based on multiple parameter adjustments, the optimal parameters of each method are obtained:

- Support vector machine (SVM) method. The linear kernel is used. The cost is set to 0.334;
- Multi layer perception (MLP) method. Two hidden layers are used. There are 64 neurons in each hidden layer;
- Particle swarm optimization (PSO) method. The learning factors are set to 1.45. The inertia factor is set to 0.8.

The simulation results are shown in Fig. 4. From the simulation results, it can be learned that the proposed detection scheme can identify the compromised effectively considering the four performance indexes. The proposed relation-based method can have high recall rate ($P_{dc}$) and precision rate ($SR$) at the same time. In terms of precision, high precision rate can reduce the occurrence of misjudged cases. As to recall, higher precision can identify more attack cases. Compared with the proposed method, the comprehensive performance of the SVM method, MLP method or PSO method is poor. The advantages of the proposed algorithm mainly come from the fact that the algorithm focuses on exploiting the differences between normal data and abnormal data, while other traditional algorithms focus on exploiting the characteristics of the data itself. When the traditional algorithm learns the common features of normal data and abnormal data, it has a negative impact on the accuracy of the algorithm.

To test the detection performance under noisy environment, we add three types of noise in the sample signals: Gaussian noise (GN), non-stationary noise (NSN) and random walk model (RWM). Safe signal-to-noise (SNR), which can be defined as the minimum SNR that makes the accuracy rate reach the set threshold $T_a$, is used to evaluate the performance of the proposed detection method. The simulation results can be found in Fig. 5.

As is shown in Fig. 5, it can be learned that the safe SNR decreases as the threshold $T_a$ increases under noisy environment. In order to maintain the high performance of the detection method, it is necessary to ensure that the data source contains less noise.

In practical applications, two complex conditions may occur: 1) The proportion of positive and negative samples that defenders can obtain is very different. 2) There is noise in the data obtained by the defender. We further compare the performance of the detection methods in these two conditions. The results are shown in Fig. 6 and Fig. 7.

In Fig. 6, four ratios between negative samples and positive samples are selected as 1:1, 1:2, 1:5 and 1:10. It can be seen that although the different proportion of positive and negative samples will affect the performance of the proposed method, its stability is always better than other methods. The performance degradation of the method is due to the reduction of negative samples, resulting in less key features that the method can mine. When the test sample does not have these untapped features, the proposed method is difficult to distinguish whether the sample comes from the compromised system.

Four noisy environment cases considering the noisy index SNR are shown in Fig. 7. It can be learned that the low SNR has little impact on the performance of the detection methods. When the noise increases further, the performance of the detection algorithm decreases rapidly. This is because some features in the sample are gradually annihilated by noise. Although the performance of the proposed detection method still has advantages, its advantages are not as great as those in low noise environment. This is because the main sample features mined by the proposed method may be annihilated in a high noise environment.

6. Conclusion

In this paper, we discuss a potential indirect attack against
This work was supported by Key Laboratory of Measurement and Control of CSE, School of Automation, Southeast University.

Acknowledgments

This work was supported by Key Laboratory of Measurement and Control of CSE, School of Automation, Southeast University.

References

[1] J. Wang and D. Shi: “Cyber-attacks related to intelligent electronic devices and their countermeasures: A review,” 2018 53rd International Universities Power Engineering Conference (UPEC) (2018) (DOI: 10.1109/upec.2018.8542059).

[2] J. Hong and C.C. Liu: “Intelligent electronic devices with collaborative intrusion detection systems,” IEEE Trans. Smart Grid 10 (2019) 271 (DOI: 10.1109/tsg.2017.2737826).

[3] M. Bahrami, et al.: “Reliability evaluation of power grids considering integrity attacks against substation protective IEDs,” IEEE Trans. Ind. Inform. 16 (2020) 1035 (DOI: 10.1109/tii.2019.2926557).

[4] T.S. Ustun, et al.: “A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard,” IEEE Access 7 (2019) 156044 (DOI: 10.1109/access.2019.2948117).

[5] M. Amin, et al.: “CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review,” IEEE Access 9 (2021) 38571 (DOI: 10.1109/access.2021.3063229).

[6] S. Kim, et al.: “Cyber attack taxonomy for digital environment in nuclear power plants,” Nuclear Engineering and Technology 52 (2019) 995 (DOI: 10.1016/j.net.2019.11.001).

[7] Y. Zha, et al.: “Coordinated attacks against substations and transmission lines in power grids,” IEEE Global Communications Conference (2015) (DOI: 10.1109/glocom.2014.7036882).

[8] D.U. Case: “Analysis of the cyber attack on the Ukrainian power grid,” Electricity Information Sharing and Analysis Center (E-ISAC) 388 (2016).

[9] G.K. Befekadu, et al.: “Risk-sensitive control under markov modulated denial-of-service (DoS) attack strategies,” IEEE Trans. Autom. Control 60 (2015) 3299 (DOI: 10.1109/tac.2015.2416926).

[10] J. Qin, et al.: “Optimal denial-of-service attack scheduling with energy constraint,” IEEE Trans. Autom. Control 63 (2018) 1648 (DOI: 10.1109/tac.2017.2756259).

[11] C.D. Persis and P. Tesi: “Input-to-state stabilizing control under denial-of-service,” IEEE Trans. Autom. Control 60 (2015) 2930 (DOI: 10.1109/tac.2015.2416924).

[12] R. Fan, et al.: “Impact of cyber attacks on high voltage DC transmission damping control,” Energies 11 (2018) 1046 (DOI: 10.3390/en11051046).

[13] Y. Liu, et al.: “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security (TISSEC) 14 (2011) 1 (DOI: 10.1145/1952982.1952985)

[14] S. Sridhar and M. Govindarasu: “Model-based attack detection and mitigation for automatic generation control,” IEEE Trans. Smart Grid 5 (2014) 580 (DOI: 10.1109/tsg.2014.2298195).

[15] A. Ameli, et al.: “Development of a cyber-resilient line current differential relay,” IEEE Trans. Ind. Inform. 15 (2018) 305 (DOI: 10.1109/tii.2018.2831198).

[16] C. Chen, et al.: “Novel detection scheme design considering cyber attacks on load frequency control,” IEEE Trans. Ind. Inform. 14 (2017) 1932 (DOI: 10.1109/tii.2017.2765313).

[17] W. Bi, et al.: “Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis,” IEEE Syst. J. 13 (2019) 2859 (DOI: 10.1109/jsyst.2019.2911869).

[18] A.J. Holmgren, et al.: “Evaluating strategies for defending electric power networks against antagonistic attacks,” IEEE Trans. Power Syst. 22 (2007) 76 (DOI: 10.1109/tpwrs.2006.889080).

[19] P. Capanera and M.P. Scappare: “Optimal allocation of protective resources in shortest-path networks,” Transportation Science 45 (2011) 64 (DOI: 10.1287/trsc.1100.0340).

[20] Z.Y. Yue, et al.: “Markov game analysis for attack-defense of power networks under possible misinformation,” IEEE Trans. Power Syst. 28 (2012) 1676 (DOI: 10.1109/tppw.2012.2226480).

[21] A. Sanjab and W. Saad: “Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective,” IEEE Trans. Smart Grid 7 (2016) 2038 (DOI: 10.1109/tsg.2016.2550218).

[22] K. Hatalis, et al.: “Modeling and detection of future cyber-enabled DSM data attacks,” Energies 13 (2020) 4331 (DOI: 10.3390/en13174331).
[23] J. Zhang, et al.: “Against fault attacks based on random infection mechanism,” IEICE Electron. Express 13 (2016) 20160872 (DOI: 10.1587/elex.13.20160872).

[24] M. Nagata, et al.: “Protecting cryptographic integrated circuits with side-channel information,” IEICE Electron. Express 14 (2017) 20162005 (DOI: 10.1587/elex.14.20162005).

[25] H.R. Ahmadi, et al.: “A power-optimized low-energy elliptic-curve crypto-processor,” IEICE Electron. Express 7 (2010) 1752 (DOI: 10.1587/elex.7.1752).

[26] D. Nan, et al.: “Risk assessment of smart substation relay protection system based on Markov model and risk transfer network,” Energies 13 (2020) 1777 (DOI: 10.3390/en13071777).

[27] Y.Y. Zhang, et al.: “A self-learning detection method of sybil attack based on LSTM for electric vehicles,” Energies 13 (2020) 1382 (DOI: 10.3390/en13061382).

[28] M. Ganjkhani, et al.: “A novel detection algorithm to identify false data injection attacks on power system state estimation,” Energies 12 (2019) 2209 (DOI: 10.3390/en12112209).

[29] W. Bi, et al.: “Cyber attack detection scheme for a load frequency control system based on dual-source data of compromized variables,” Applied Sciences 11 (2021) 1584 (DOI: 10.3390/app11041584).

[30] S. Liu, et al.: “A framework for modeling cyber-physical switching attacks in smart grid,” IEEE Trans. Emerg. Topics Comput. 1 (2013) 273 (DOI: 10.1109/tetc.2013.2296440).

[31] X. Liu, et al.: “Power system risk assessment in cyber attacks considering the role of protection systems,” IEEE Trans. Smart Grid 8 (2016) 572 (DOI: 10.1109/tsg.2016.2545683).

[32] C. Huang, et al.: “Robust load frequency controller design based on a new strict model,” Electric Power Components and Systems 41 (2013) 1075 (DOI: 10.1080/15325008.2013.809824).