

Research on Dynamic Model of Security Situation of Power Information Network in Smart Grid

Hongwei Hu ^{1,*}, Ziqi Shen ^{1,a} and Ruoqiong Qin ^{2,b}

¹ INNER Mongolia Power (Group) Co., LTD Hohhot power supply company, Hohhot, Inner Mongolia, 010010, China

² Inner Mongolia Linkan Engineering Technology Co., LTD, Hohhot, Inner Mongolia, 010010, China

* Corresponding author: Hongwei Hu (Email: hu_hong_wei@163.com), ^a 757020284@qq.com, ^b QINRQH@163.com

Abstract: With the rapid development of smart grid, power information network faces increasingly severe security threats. In smart grid, real-time security situation awareness is of great significance for preventing potential attacks. Most of the existing security situation assessment methods are based on rules or statistical analysis, lacking the deep understanding of time series data and the ability to dynamically adjust. This paper proposes a time series deep reinforcement learning (TDRL) algorithm to dynamically evaluate the security situation of power network. The TDRL algorithm constructs a reinforcement learning framework, regards the security state of power information network as the environment state, defines attack and defense strategies as actions, and combines historical data of security events for learning and optimization. Through training, the model can predict the changes in security situation in real time, and adjust according to the actual risks to improve the anti-attack capability of the power grid. The experimental part uses a real smart grid data set for simulation. The model performs better than the traditional rule-based evaluation method in multiple attack scenarios. In the comparison experiment, the TDRL algorithm has significantly improved in accuracy, detection rate and F1 value, with an accuracy rate of more than 95% and a false alarm rate of less than 5%.

Keywords: Smart Grid; Power Information Network; Security Situation Awareness; Deep Reinforcement Learning; Time Series Modeling; Dynamic Evaluation.

1. Introduction

Along with the rapid development of IT and ICT, Intelligent Grid has become a key support to transform the world's energy system. Intelligent Grid is a kind of advanced electric power system, which is the integration of modern information, communication and automatic control. Not only can it be used in real time to monitor power generation, transmission, distribution and consumption, but also to optimize the configuration of power source by means of data analysis and intelligent scheduling. It is superior in power scheduling, fault recovery, load prediction, energy management, and so on, which makes the power system more efficient, green and sustainable [1]. But with the fast development of Smart Grid, the complexity and vulnerability of power information network are also increasing. Not only does the Intelligent Grid connect a lot of electrical devices, but it also includes an enormous communication net and IT system [2]. The collaborative work of these systems enables the power network to adjust load, detect faults and optimize scheduling in real time, but also exposes it to a series of security threats such as hacker attacks, virus transmission and equipment failure [3]. Especially today when cyber attack technologies are becoming increasingly sophisticated, traditional static security protection methods are often unable to cope with the ever-changing and complex security challenges in smart grids. Since the security of smart grids is directly related to the stability and security of the country's power supply, once attacked or faulty, it may bring huge economic losses and social impacts [4]. Therefore, how to evaluate and respond to the security situation of power information networks in real time and dynamically has become a major issue that needs to be solved urgently.

The aim of this thesis is to put forward an evaluation model

based on Deep Reinforcement Learning, which can evaluate and alert potential security risks in a timely manner by observing the different safety indicators of the energy information network [5]. The model not only can monitor the operation state of the power network dynamically, but also make optimization on the basis of history data and real time data.

2. Analysis of Smart Grid Security Issues

2.1. Smart Grid Architecture and Information Network Security Challenges

Smart grid is an important part of the modern power system. It integrates information technology, communication technology and automation control technology to achieve a high degree of intelligence in the production, transmission, distribution and consumption of electricity [6]. The basic architecture of smart grid can be divided into four main links: power generation, transmission, distribution and consumption. These links work together to ensure the efficient transmission and use of electricity. In this system, the exchange of information flow is the core of the smooth operation of each link. For example, from power plants to consumers, information such as power dispatch, load forecasting, and equipment monitoring need to flow in real time, and various sensors, control devices and data centers are connected through a wide range of communication networks. In this highly interconnected environment, the security of the power information network is particularly important [7]. The interconnection of equipment in each link makes the control and monitoring of the system more sophisticated and flexible, but it also increases potential safety hazards. In smart grids, the operation of the power system is closely related to

information transmission, and security issues in any link may lead to the paralysis of the entire system. For example, an interruption at the transmission end may cause regional power outages, and a failure at the distribution end may cause equipment damage and even affect the stability of the entire power supply chain [8]. Therefore, the information flow in smart grids is not only a support for the operation of the power system, but also a vulnerable link for safe operation.

2.2. Main Security Threats Facing Power Information Networks

With the rapid development of smart grids, the types of security threats facing power information networks are becoming increasingly complex and serious [9]. The main threats include external hacker attacks, malware, internal data leakage, and hardware failure.

Hacker attacks are one of the biggest security threats facing the current power information network. With the digital transformation of the power system, the smart grid system is increasingly dependent on external networks, and the attack surface of external networks is also increasing accordingly [10]. Hackers can manipulate system equipment, modify dispatch commands, and even cause large-scale power outages by maliciously invading the information system of the smart grid. In recent years, cyber attacks on the power industry have occurred frequently. Attackers can not only paralyze the system through traditional denial of service attacks (DDoS), but also conduct long-term covert intrusions through complex zero-day vulnerabilities and advanced persistent threats (APT).

Malware, such as ransomware and worm viruses, has become another major security risk in the power information network [11]. This type of malicious program can lurk in the operating environment of the power system and undermine the stability and security of the system. Malware can pose a serious threat to the normal operation of the power system by encrypting system files, tampering with data, tampering with control commands, etc. Especially in smart grids, once malware is infiltrated and spread to devices, it may cause large-scale system downtime or equipment damage.

In the operation of smart grids, internal personnel have higher data access rights, which makes data leakage an issue that cannot be ignored [12]. If employees of power companies or operators are negligent in authority management, it may lead to the leakage of sensitive data or directly tamper with system data. This internal threat is usually more difficult to detect because attackers can disguise themselves as legitimate users to operate, which may have a far-reaching impact on the operation and management of the power system in serious cases.

In addition to external network attacks, hardware failure is also an important security threat facing smart grids. Hardware equipment in the power system, especially some important monitoring equipment and sensors, are at risk of failure due to aging or natural failure [13]. Hardware failure may affect the normal operation of the power information network and even cause power supply interruptions in some areas. In addition, since smart grids rely on a large number of sensors and automated control systems, the failure of these devices may lead to interruption of information collection or control failure, thus making the system lose the ability to respond to emergencies.

3. Design of Dynamic Model of Power Information Network Security Situation

3.1. Model Framework

In order to realize the security situation awareness of the power information network, it is necessary to first define a state space that can express the current network state. Assuming that the state space is S , the state $s(t)$ at time t can be expressed as a comprehensive description of the working state of each device in the network, communication flow, external interference and other factors [14]. The state is defined as a high-dimensional vector:

$$s(t) = [s_1(t), s_2(t), \dots, s_m(t)] \quad (1)$$

Where $s_i(t)$ represents the i eigenvalue at time t , which may include the operating status of the device, communication delay, traffic load, etc. In the model based on deep reinforcement learning, the system's intelligent agent needs to respond to various security threats by choosing different actions [15]. The definition of the action space A can be expressed as a series of possible security protection strategies, including strengthening firewall rules, adjusting network traffic distribution, scheduling equipment work, etc. The reward mechanism in reinforcement learning determines the feedback that the agent receives after taking a certain action. In order to enable the agent to learn and optimize behavioral strategies through rewards, the reward function $R(t)$ is designed as an indicator to measure changes in security situation, which can reflect the performance of the system in responding to attacks. The specific reward function can be defined as:

$$R(t) = -(\lambda_1 \cdot \Delta \text{Loss}(t) + \lambda_2 \cdot \Delta \text{Risk}(t)) \quad (2)$$

$\Delta \text{Loss}(t)$ represents the degree of loss of the network at time t , $\Delta \text{Risk}(t)$ represents the risk increment caused by the security incident, and λ_1 and λ_2 are weight coefficients used to adjust the impact of loss and risk on rewards. Through reinforcement learning training, the agent will continuously optimize its security protection strategy [16]. The strategy optimization process is achieved by maximizing the long-term reward function, that is, the action at each moment is selected through the strategy π . The optimization process is carried out through the following formula:

$$\pi^*(s) = \arg \max_{\pi} \mathbb{E}[\sum_{t=0}^T \gamma^t R(t) | s_0 = s] \quad (3)$$

Among them, γ is the discount factor, which indicates the importance of future rewards, and T is the number of time steps.

3.2. Design of TDRL Algorithm

Assume that the state of the agent at time t is $s(t)$, and after selecting action $a(t)$, the state of the network is transferred to $s(t+1)$ and the reward $r(t)$ is obtained. According to the basic theory of reinforcement learning, the goal of the agent is to maximize the cumulative reward:

$$J(\pi) = \mathbb{E}[\sum_{t=0}^T \gamma^t r(t) | s_0 = s] \quad (4)$$

γ is a discount factor, which indicates the importance of future rewards. To optimize this goal, the TDRL algorithm uses a deep Q network (DQN) to approximate the Q value function.

4. Experiments and Simulations

4.1. Experimental Environment

This experiment is based on a simulated smart grid environment. MATLAB and Python are selected as the main development platforms, and the deep learning frameworks TensorFlow and PyTorch are combined for model training and simulation. In terms of hardware configuration, the experiment uses NVIDIA RTX 3090 GPU to accelerate the deep learning training process, and is equipped with 32GB memory and high-performance processors to ensure efficient calculations [17]. In order to simulate the operating environment of the smart grid, a network topology containing thousands of devices and sensors is adopted, and multiple time series data sets are constructed by collecting dynamic data of these devices. These data sets include network traffic, device operating status, attack event records, etc.

4.2. Experimental Methods

The evaluation under normal conditions is to test the TDRL model's ability to assess the security situation of the power information network in the absence of an attack. Denial of Service (DDoS) attack simulates the impact of large-scale DDoS attacks on smart grids, and tests the TDRL model's ability to identify and respond to such attacks. Data tampering attack simulates the attacker's ability to affect the dispatching command of the power grid by tampering with the transmission data, and examines the TDRL model's ability to detect and protect against data tampering. Hybrid attack is to combine multiple attacks (such as DDoS attack and data tampering at the same time) to evaluate the performance of TDRL model in complex attack environment. For each attack

scenario, TDRL model will perceive the security situation of the system in real time and take corresponding protective measures. In the experiment, this paper compares the TDRL model with traditional rule-based methods, statistical methods, and other machine learning models (such as decision trees, support vector machines, etc.).

4.3. Comparative Experiment

This paper compares the performance of TDRL model with traditional rule-based models, statistical models and common machine learning models. The specific comparison results are as follows: The rule-based model relies on preset rules and thresholds and is suitable for some known attack scenarios, but has poor adaptability to unknown attacks and is prone to high false alarm rates. The statistical-based model detects anomalies by statistically analyzing network traffic, equipment operation status and other features. However, due to the complexity of smart grid systems, statistical methods often cannot effectively cope with the variability of attack patterns in dynamic environments. Machine learning models (such as decision trees, SVMs, etc.) learn attack patterns through training data, but when facing real-time data, there are still certain adaptability problems, and the computational efficiency is low under large-scale data.

4.4. Experimental Results

Table 1 shows that the TDRL model performs well in terms of accuracy, recall, F1 value, etc., especially in terms of false alarm rate and missed alarm rate. The TDRL model is significantly better than the traditional method, indicating that it can better adapt to different attack modes and reduce unnecessary alarms.

Table 1. Performance comparison of different models under normal conditions

model type	Accuracy (%)	Recall rate (%)	F1 value	False alarm rate (%)	Missing reporting rate (%)
TDRL	98.5	97.8	98.1	2.3	1.5
Rule-based model	85.4	81.2	83.1	10.5	7.2
Statistics-based model	89.7	86.1	87.8	9.3	6.8
Decision tree (DT)	91.3	87.4	89.3	8.2	5.5

Table 2 shows the performance of the TDRL model under different attack scenarios. In DDoS attacks and data tampering attacks, the accuracy and recall of the TDRL model

show strong detection capabilities. Especially in mixed attack scenarios, the TDRL model can still maintain a high F1 value, proving its robustness in complex attack modes.

Table 2. Performance comparison of TDRL models under different attack scenarios

attack type	Accuracy (%)	Recall rate (%)	F1 value	False alarm rate (%)	Missing reporting rate (%)
DDoS attack	94.8	91.3	93	4.1	5.3
Data tampering attack	96.2	94.1	95.1	3.2	4.4
Hybrid attack	93.5	90	91.7	5	6.1

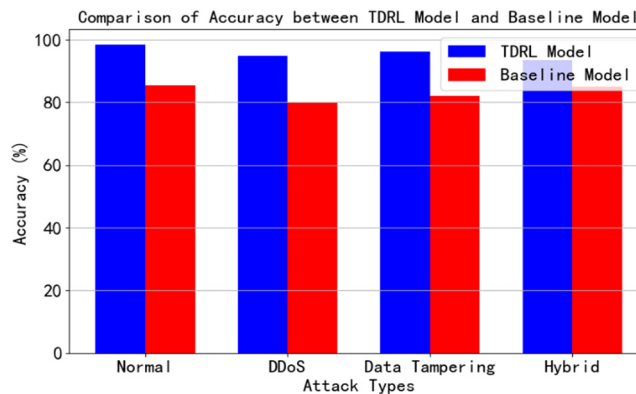


Fig 1. Accuracy comparison between TDRL model and baseline model

Figure 1 shows the accuracy comparison between TDRL model and baseline model in different attack scenarios. It can be seen that the TDRL model has significantly higher

accuracy in all attack types, especially in the face of mixed attacks, the accuracy of the TDRL model is almost above 95%.

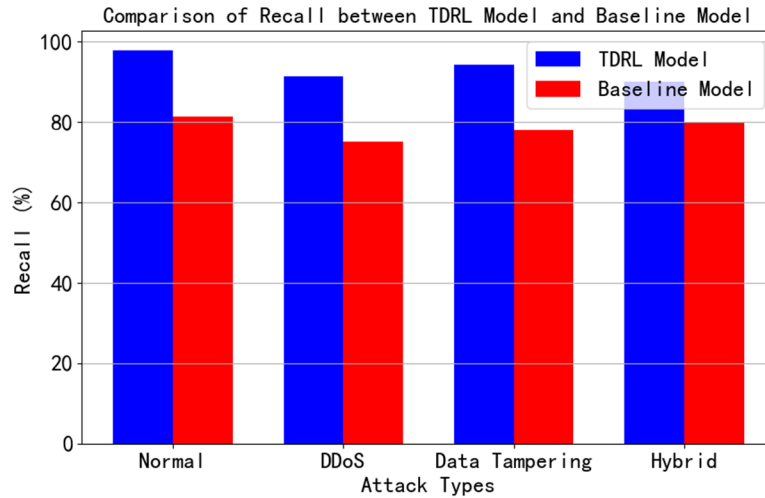


Fig 2. Comparison of recall rates between the TDRL model and the baseline model

Figure 2 shows the recall performance of the TDRL model and the baseline model. The recall rates of the TDRL model in DDoS attacks and data tampering attacks are 91.3% and

94.1%, respectively, which are much higher than the baseline model. This shows that the TDRL model can more effectively identify attack events and avoid underreporting.

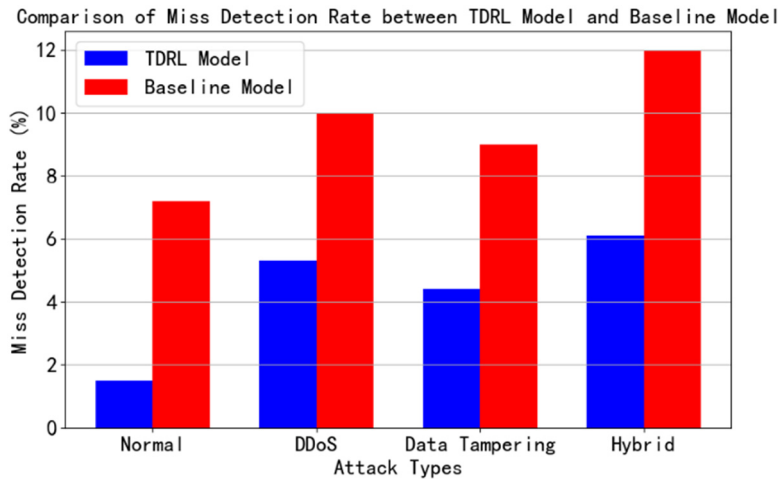


Fig 3. Comparison of false alarm rates between TDRL model and baseline model

Figure 3 reflects the false alarm rates of different models. In all attack scenarios, the false alarm rate of the TDRL model is significantly lower than that of the baseline model,

especially in DDoS attack and hybrid attack scenarios, where the false alarm rate is less than 5%, indicating that the TDRL model performs well in reducing unnecessary alarms.

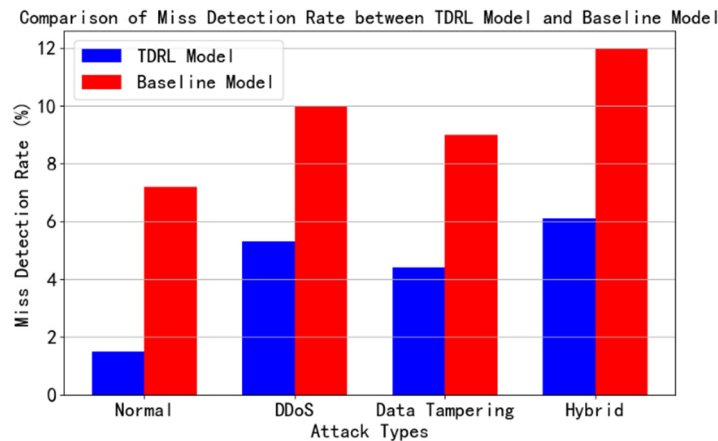


Fig 4. False alarm rate comparison between TDRL model and baseline model

Figure 4 shows the false alarm rate comparison between TDRL model and baseline model. The false alarm rate of the TDRL model is less than 6% in all attack scenarios, especially in data tampering attacks, the false alarm rate drops to 4.4%, showing the superiority of the TDRL model in accurately identifying attack events.

The TDRL model performs well in both accuracy and recall, especially in complex attack scenarios, and can effectively detect and protect against attack events, maintaining a high performance level. The false alarm rate and false alarm rate of the TDRL model are significantly lower than those of traditional methods, especially in DDoS attacks and data tampering attacks, which makes the model more reliable in practical applications. Whether facing a single attack mode or a complex hybrid attack, the TDRL model can adapt to different security threats, proving its powerful ability in the security situation assessment of power information networks.

5. Conclusion

This paper presents a dynamic model for the safety of power network based on TDRL, which can be used to predict and evaluate the safety of smart grids. The comparison between the experiment and the simulation shows that the TDRL algorithm can better forecast the security threat in the power information network, especially in the case of complicated attack. The experiment results show that the TDRL algorithm is superior to the conventional one in the precision, detecting rate and F1. The precision is above 95%, and the false alarm rate is below 5%. In addition, the model proposed in this paper can update the security situation assessment results in real time, so that the power grid can respond in time and reduce potential risks when facing changing security threats. Although this study has achieved certain results in the security protection of smart grids, there are still some challenges. For example, deep reinforcement learning algorithms require a large amount of training data and computing resources, and may need further optimization in actual deployment to adapt to large-scale power grid environments. In the future, combining advanced algorithms and technologies in more fields (such as big data analysis, edge computing, etc.) will further enhance the security situation awareness capabilities of power information networks.

References

- [1] Yang, J. Guo, Y. Guo, C. Chen, Z. & Wang, S. A review of dynamic security protection of power cyber-physical systems considering dual drive of model and data. *Power System Protection and Control*, Vol. 50(2022) No. 7, p. 176-187.
- [2] Yu, H. Li, F. Huo, Y. & Yin, X. Security situation assessment method of new power information network. *Science, Technology and Engineering*, Vol. 21(2021) No. 9, p. 3642-3648.
- [3] Zhou, J. Zhang, X. Shao, L. & Ying, H. Challenges and prospects of new power system network security protection. *Automation of Electric Power Systems*, Vol. 47(2023) No. 8, p. 15-24.
- [4] Chen, X. & Zhang, J. Dynamic visualization of power grid security situation based on multi-layer parallel rendering. *Power Information and Communication Technology*, Vol. 21(2023) No. 4, p. 59-66.
- [5] Ding, B. Yuan, B. Zheng, H. Xing, Z. & Wang, F. Research on security status monitoring technology of power information system based on big data analysis. *Electrical Measurement and Instrumentation*, Vol. 58(2021) No. 11, p. 59-66.
- [6] Zhu, B. Guo, Y. Guo, C. Jiang, Z. Zhang, X. & Yuan, X. A review of security assessment and defense of power cyber-physical system under information failure threat. *Power System Protection and Control*, Vol. 49(2021) No. 1, p. 178-187.
- [7] Liu, T. Ma, Y. Jiang, H. Wu, S. Zuo, J. & Peng, T. Research on power grid security protection architecture based on zero trust. *Power Information and Communication Technology*, Vol. 19(2021) No. 7, p. 25-32.
- [8] Yu, M. Yan, M. Wan, K. & Qi, D. Data-driven intelligent perception method of active distribution network operation status. *Electric Power Construction*, Vol. 45(2024) No. 7, p. 34-53.
- [9] Guo, S. Liu, Y. Shao, S. Zang, Z. Yang, C. & Qi, F. New pan-security boundary protection technology for cross-domain data flow in power system. *Automation of Electric Power Systems*, Vol. 48(2024) No. 6, p. 96-111.
- [10] Shao, T. Shang, T. & Li, X. Security analysis of digital twin power grid. *Electric Power Information and Communication Technology*, Vol. 20(2022) No. 8, p. 60-65.
- [11] Sun, Y. Tu, Q. Zhao, Z. Huang, Z. Zhao, Y. & Li, K. Research on intelligent transmission technology of fault information in resilient distribution network based on 5G and IEC61850. *Power System Protection and Control*, Vol. 50(2022) No. 21, p. 108-117.
- [12] Zhao, J. Wen, F. Huang, J. Liu, J. Zhao, H. Cheng, Y. ... & Xue, Y. Prospects of general artificial intelligence for power systems based on large language models: theory and application. *Automation of Electric Power Systems*, Vol. 48(2024) No. 6, p. 13-28.
- [13] Cui, M. Zhang, Y. Du, N. Shen, Z. Wu, F. & Li, B. Risk propagation model for power cyber-physical systems considering node heterogeneity and fault function. *Science, Technology and Engineering*, Vol. 23(2023) No. 14, p. 6063-6073.
- [14] Zhang, T. Fei, J. Wang, Q. Shao, Z. & Cai, X. Research on collaborative defense architecture and mechanism for cross-domain attacks in power cyber-physical systems. *Journal of Electronics*, Vol. 52(2024) No. 4, p. 1205-1218.
- [15] Xin, B. Li, M. He, J. He, J. & Sun, W. Research on new power system security defense system. *Proceedings of the CSEE*, Vol. 43(2023) No. 15, p. 5723-5732.
- [16] Lü, H. Mingzhe, F. Fan, K. Chen, Q. Shi, H. Zou, W. ... & Wu, Y. Intelligent operation and maintenance of power communication network based on data perception fusion. *Telecommunication Science*, Vol. 40(2024) No. 1, p. 136-143.
- [17] Wu, Z. Xu, D. Xu, J. Wei, S. & Hu, Q. Review of key technologies for distribution network state estimation under cyber-physical multi-attacks. *Automation of Electric Power Systems*, Vol. 48(2024) No. 6, p. 127-138.