Interactive Visual Analysis on the Attack and Defense Drill of Grid Cyber-physical Systems

攻防演习

Kehe Wu, Jiawei Li, Yayun Zhu, Siwei Miao, Sixun Zhu and Chunjie Zhou

***Abstract*—The open and distributed connection of the power system makes it vulnerable to various potential cyber-attacks, which may lead to power outages and even casualties. Therefore, the construction of attack and defense drill (ADD) platforms for attack mechanism investigation and protection strategy evaluation has become a research hotspot. However, for the massive and heterogeneous security analysis data generated during the drill, it is rare to have a comprehensive and intuitive method to visually and efficiently display the perspective of the attacker and defender. In order to solve this problem, this paper proposes a visual analysis scheme of an ADD framework for a grid cyber-physical system (GCPS) based on the interactive visual analysis method. Specifically, it realizes system weakness discovery based on knowledge visualization, optimization of the detection model and visualization interaction. Finally, the case study on the simulation platform of ADD proves the effectiveness of the proposed method.**

***Index Terms*—Attack and defense drill (ADD), attack path, interactive visual analysis, intrusion detection.**

I. Introduction

UNDER the dual influence of the development of power systems towards automation and intelligence, and the continuous innovation of network attack technology, the safety of power industry control is facing new challenges. The power industrial control system is a complex cyber-physical system (CPS) system that is tightly coupled with the power network and the information network, so there are more threat sources [1]. In 2015, the power grid of Ukrainian was attacked and the supervisory control and data acquisition (SCADA) system was affected [2]; In 2016, Israel's electricity supply system was hit by a cyber-attack that caused a large number of computers to run offline. In 2019, Venezuela had a large-scale blackout nationwide from March 7, causing huge economic losses and social unrest. The occurrence of such incidents is related to many factors, such as the construction level of electric power facilities, human illegal operations and network infiltration attacks. Cyber-attacks often cause the system to lose its visibility and controllability [3] by injecting fake data [4], so that the spread of faults eventually leads to system crashes.

For power systems, in the absence of effective safety protection measures at industrial sites, in order to avoid the occurrence of similar incidents, it is urgent to establish and improve the security simulation verification environment for a grid cyber-physical system (GCPS). By deploying common network attack tasks in the verification environment, it helps operators to discover the security problems existing in the system and carry out security defense technology research and verification. Therefore, it is of great research significance to build GCPS attack and defense drill platforms, and then study network attack and system response defense technology in this environment and further use the research results to guide the GCPS security defense.

During the offensive and defensive exercise, the attacker constantly seeks new opportunities for attack. The defender continuously optimizes the defense methods for the situation presented by the system after the attack. Its purpose is to promote the understanding and mastery of the overall situation knowledge of the system by both sides. At present, many institutions have established GCPS offensive and defensive drill platforms, but most of them are limited to using traditional visualization to display real-time measurement information, such as, displaying the measurement data of the power grid and the state and structure of the system, and providing a friendly interface for users to monitor the operating status of the grid. For different data types, such as low-dimensional, high-dimensional and geographic information system (GIS), a targeted visual representation technology is adopted to express the power flow of nodes [5], such as: using Color-Scale to map the interval range of voltage fluctuations, and displaying real-time power consumption through heat maps [6].

With the technological innovation and the high degree of interaction between the information network and the physical system, the problem of information overload occurs in the power industrial control system, which is manifested in the large amount of data, high degree of information redundancy and low degree of correlation. The operators can not quickly capture the key information and get an accurate understanding of the situation through simple visual representation. How to process and utilize grid data and transform it into effective

Manuscript received September 18, 2020; revised October 20, 2020; accepted November 4, 2020. Date of online publication November 20, 2020; date of current version October 28, 2020. This work was supported by the Science and Technology Project of State Grid Corporation of China (Research on key technologies of integrated electric power network security simulation and verification environment, 521304190004).

K. H. Wu is with School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China.

J. W. Li is with North China Electric Power University, Beijing 102206, China, and the State Grid Beijing Electric Power Company, Beijing 100031, China.

Y. Y. Zhu (corresponding author, e-mail: zhuyayun@epri.sgcc.com.cn; ORCID: https://orcid.org/0000-0002-2934-8831) and S. W. Miao are with China Electric Power Research Institute, Beijing 100192, China.

S. X. Zhu and C. J. Zhou are with School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan 430074, China.

DOI: 10.17775/CSEEJPES.2020.05030

knowledge is one of the difficult problems for users to make analysis and decision. Keim [7] proposed the visualization analysis process model, which realizes the data-knowledge-data conversion process through a visualization process and automatic data analysis process. Sacha [8] proposed a model to explore the process of human knowledge generation, which consists of three-layer nested loop structures of exploration, verification and knowledge generation to constitute the reasoning discovery process of knowledge. Based on the theoretical system of Sacha, the interactive visualization analysis technology proposed in this paper is intended to solve the following problems: 1) Effective presentation of multi-dimensional data. 2) Security analysis models (such as intrusion detection models, situational awareness model [9]) involved in offensive and defensive drills are often regarded as a "black box." Operators can't understand how the detection method works on the data. 3) The multi-domain knowledge in the offensive and defensive exercises is difficult to discover, understand, and disseminate.

This paper conducts research on the application of visual analysis technology in the environment of the attack and defense drill of GCPS, and aims to promote the comprehension of data, analysis of models, and dissemination of knowledge in the process of attack and defense. The main contributions of this paper are as follows: 1) A visual framework for the offensive and defensive drills is proposed, and the visual analysis tasks of both the attackers and the defenders are clarified; 2) In view of the exploit form of attack, text mining the information of the vulnerability database to obtain the vulnerability knowledge entity matching the current host, through the expression of vulnerability of heuristic knowledge to obtain parallel vulnerabilities, and further the correlation between the vulnerabilities knowledge entities is discovered. Finally, it identifies the attack chain by exploiting the vulnerability relationship, in order to promote the attackers to quickly locate the weak links in order to determine the feasibility of the attack. 3) This paper visually optimize the defense intrusion detection model [10] construction process to achieve the purpose of understanding, diagnosing, refining the model [11] and discovering and enhancing knowledge during the analysis [12]. In addition, it can strengthen the defender's perception of the attack, discover abnormal behavior in time and identify the attack type.

The rest of this paper is organized as follows. Section II defines the GCPS visual framework for attack and defense drills and describes the visual tasks of the attacker and defender. In section III, the specific steps of exploiting and expressing vulnerability knowledge by the attacker are described in detail. In section IV, the steps for the defender to optimize the intrusion detection model based on the visual interaction technology are introduced. Section V introduces the specific content of the visualization of vulnerability knowledge and model interaction optimization experiments implemented on the offense and defense exercise platform. Finally, section VI summarizes the full text study.

II. Interactive Visual Analysis Method

The interactive visual analysis method uses visual representation as the interface of human-computer interaction, and directly presents complex and abstract information. Through visual interaction means, expert knowledge is fed back into the system to realize dynamic feedback analysis of humans in the loop. Based on user feedback information, the layout of the view is adjusted and parameters are modified to capture the potential laws of the data, so as to improve the ability of users to mine and perceive the information. The following describes the visual representation, visual interaction methods, and interactive visual analysis process.

A. Visual Representation

Visual representation aims at transforming massive data into views to reflect the distribution characteristics, statistical laws and essential meanings of the data. Visual representation is an important basis for visual analysis and information discovery. Inspiring display views that meet the use's psychological expectations can assist in further analysis.

According to the types of view elements, the visual representation technology can be divided into view representation methods based on graphics technology, pixel-oriented technology, geometric technology, icon technology and hierarchical technology [13]

B. Visual Interaction

According to the requirements of the analysis task, users adjust and modify the view elements to achieve the purpose of reintegrating the view information. Through efficient visual interaction means, it is easier for users to find and locate valid information, and to achieve the goals of information mining, analysis and optimization.

As shown in Fig. 1, in the series of processes of transforming raw data into visual views, interactive operations act on three processes: data transformation, visual mapping and view transformation [14].

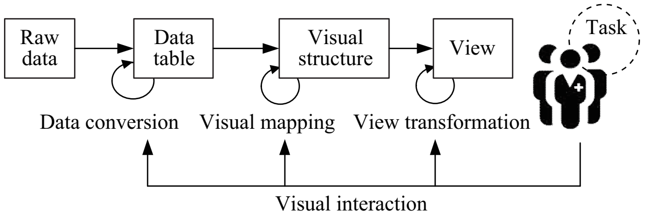


Fig. 1. The diagram of visual interaction.

Common interaction technologies include Select, Explore, Reconfigure, Encode, Abstract/Elaborate, Focus + Context, Filter, and Connect [15], [16].

C. Visual Analysis

Based on the derived theoretical system of Sacha [8], this paper proposes an interactive visual analysis method, with the specific structure as shown in the Fig. 2.

The interactive visual analysis process allows users to explore data distribution patterns on the one hand, and allows users to build and refine automatic data analysis models [17] through interactive operations on the other. Different from the traditional visual interaction, this process integrates the required expert knowledge in the field of analysis information. By feedback and decision-making of the analysis process, highly interactive analysis of humans in the loop is realized [18]. In traditional visual technology, operators only provide some limited supervision, such as: data selection and modified algorithm parameters. Based on the visual interaction technology, it is possible to unpack the model and realize the intervention of the operator in the execution process of the model. The specific performance is to introduce the use's subjective consciousness in the analysis process [19], to judge and evaluate the effect of the model and provide feedback to the analysis loop, and to build the user's trust in the model [20]. Aiming at the problem that multi-domain knowledge is difficult to discover, understand, and disseminate, a heuristic visualization of knowledge is proposed. Through selecting appropriate visual representation techniques for knowledge entities and expressing their attributes, it helps operators accurately discover and acquire knowledge, and also promote the dissemination and innovation of knowledge in this field, such as a word cloud graph expressing text attributes in knowledge, and a knowledge graph expressing logical attributes between entities.

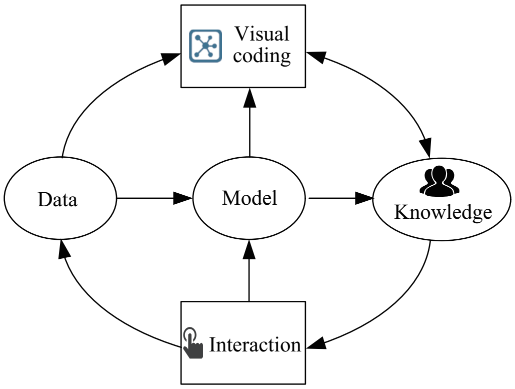


Fig. 2. Interactive visual analysis method.

III. Visual Framework for ADD

A. Component of ADD

Different from the power information security ADD field that only researches network offensive and defensive technologies, the ADD visualization framework proposed in this paper increases the attention to the physical layer, and considers the perception of attacks and the recovery response strategy to the system's failure disturbance. The framework is shown in Fig. 3. The simulation platform of the grid-cyber physical system serves as the supporting environment for offensive and defensive tasks. On this support environment, attack injection and protection verification will be carried out.

Supporting Environment: Provide an environment for system operation and policy deployment, in order to reproduce the attack and defense scenarios in combination with virtualization technology. Core functions include: user management, drill task matching, scenario configuration and security tool support.

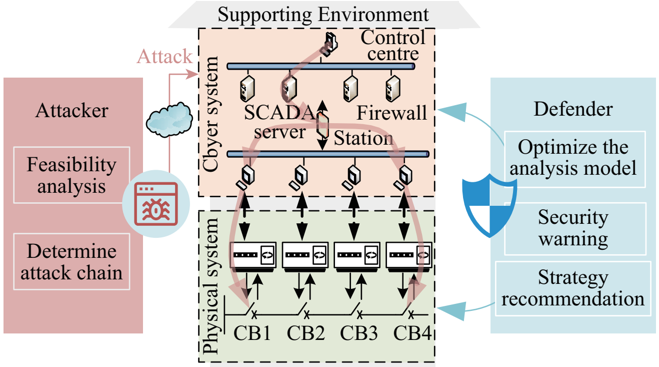


Fig. 3. The visual framework for GCPS attack and defense drill.

Attacker: Vulnerability analysis of industrial control systems are performed in the simulation environment. The simulation experiment is carried out based on the vulnerability information of the system, which aims to provide attack examples for analyzing the behavior characteristics of the attacker and the system security protection strategy. Attackers primarily adopt denial-of-service attacks, man-in-the-middle attacks, false data injection attacks (FDIA) and other attack strategies.

Defender: Based on the real-time perception of the system status, users conduct the research and verification of the industrial control safety protection strategy. The defense methods primarily consider defense methods such as intrusion detection, fault location, and security assessment.

B. Visual Tasks for ADD

Visual analysis of Cognitive understanding tasks require expert guidance during the ADD process.

The network attack of the industrial control system is divided into three stages: attack preparation stage, attack implementation stage and attack aftercare stage. In this paper, the task of visual analysis from the perspective of the attacker primarily focuses on the first two stages. In the stage of attack preparation, the attacker analyzes and evaluates the scanned vulnerability information to enhance the user's understanding of the distribution of vulnerability of the system, and further determines the attack feasibility and attack method according to the analysis results. In the attack implementation stage, the attack chain is constructed based on the knowledge of exploit. The specific core functions include: building a vulnerability information database; digging through the weak links of specific objects to find timely security vulnerabilities; discovering the correlation between various independent vulnerabilities based on vulnerability scan results. The visual analysis method proposed by the defender in this paper focuses on optimizing the analysis model of security detection, security monitoring, and security protection tasks, such as intrusion detection model, attack identification model, and the protection strategy matching model. Furthermore, the visual display of the warning function and defense strategy recommendation function is realized, and the operators can quickly and accurately respond to the attack through the friendly human-computer interaction interface. The specific core functions include: The Cyber layer monitors the network traffic in real time and perceives the network attack behavior; The Physical layer carries out all-round monitoring on the system equipment and senses the occurrence of fault from the change trend of the running state; Determining the type of attack based on the warning information. Blocking attacks and recovering the system based on the defense strategy matched in the security strategy database.

IV. Attack Path Generation Based on Knowledge Visualization

In the GCPS offensive and defense drill, the attacker primarily carries out network attacks against the information layer, with the purpose of destroying the security targets of confidentiality, integrity, availability in the network. The specific content of the network attack in the GCPS system is to use vulnerabilities or security flaws in the system to illegally obtain system permissions or attack on system resources, so that the attacker can track communication behavior or obtain modified transmission content, eventually causing the GCPS system to not work properly and provide high-quality services. More specifically, the attacker monitors and probes the target, obtains the network environment and information security status of the information layer. Based on the network information, the attacker can further detect the specific information of the physical layer industrial control equipment. Through the above process, attackers can obtain network topology information, host information in the physical system, identify services provided by the target host, and also existing vulnerabilities.

The foundation of launching a successful attack is to discover and exploit the vulnerabilities of the target host. Exploiting multiple vulnerabilities can ensure the concealment and success probability of the attack. Therefore, the task of interactive visual analysis of attackers primarily focuses on the analysis and utilization of security vulnerability knowledge.

The attacker focuses on discovering the weak links of the system in the preparation stage of the attack. In order to enhance the attackers' understanding of the nature of system vulnerabilities and make reasonable use of vulnerabilities to find injection points and attack paths of the system, a visual analysis scheme for mining system vulnerability knowledge is proposed. The implementation flow is shown in the Fig. 4.

A. Vulnerability Collection: Anomaly Cause Analysis

The research on vulnerability information is used to extract vulnerability knowledge entities, including: Multi-source vulnerability information is organized and combined first, and then its format is standardized to build a vulnerability database for power industry control systems. Automatic vulnerability classification technology is researched based on vulnerability semantic analysis. Based on the TF-IDF method, the features of the vulnerability attributes are obtained from the text topic which aims to determine the causes of the vulnerability and construct the feature vector space, further extract the necessary services and conditions to constitute the knowledge entity of the vulnerability attack. Attackers can evaluate the importance of features, feedback the knowledge of vulnerability corpus to delete useless words, then adjust the weight of keywords to realize the visual interaction in the analysis process.

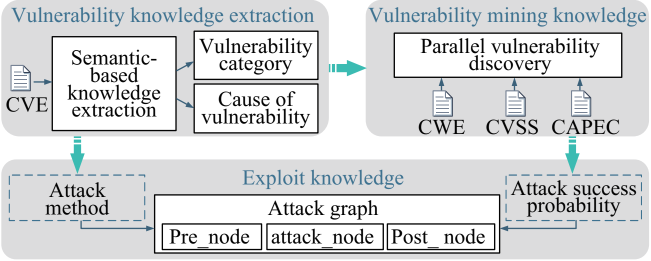

Vulnerability knowledge extraction
CVE
Semantic-based knowledge extraction
Vulnerability category
Cause of vulnerability
Vulnerability mining knowledge
Parallel vulnerability discovery
CWE
CVSS
CAPEC
Attack method
Exploit knowledge
Attack graph
Pre_node
attack_node
Post_node
Attack success probability

Fig. 4. The visualization process of GCPS vulnerability knowledge.

The integrated management and cause analysis of vulnerability information provides a reference for the discovery, classification and early warning analysis of unknown vulnerabilities.

B. Vulnerability Mining: Parallel Vulnerability Discovery

Based on the common attack pattern enumeration and classification (CAPEC) attack pattern description, common weakness enumeration (CWE) vulnerability description and vulnerability database information description, the attacker can minimize vulnerabilities in the system that meet the user's expected attack purpose. Attackers often combine different vulnerabilities to achieve the same attack purpose and effect through different attack paths [21].

The similarity calculation is carried out for the vector of vulnerability sets that map CAPEC, CWE and common vulnerabilities and exposures (CVE) relationships. In this paper, the calculation results of the similarity between vulnerabilities are presented in a heuristic view, based on which implicit parallel link patterns and rules in vulnerability data can be mined.

The cosine similarity calculation method is used to measure the degree of correlation between vulnerable individuals. The specific calculation formula is:

$$\begin{aligned} s &= \text{similarity} < \boldsymbol{v}_i, \boldsymbol{v}_j > \\ &= \frac{\sum\limits_{i=1}^{n}(x_i y_i)}{\sqrt{\sum\limits_{i=1}^{n}(x_i)^2}\sqrt{\sum\limits_{i=1}^{n}(y_i)^2}} = \frac{\boldsymbol{v}_i\boldsymbol{v}_j}{\|\boldsymbol{v}_j\| \times \|\boldsymbol{v}_j\|} \end{aligned} \quad (1)$$

where $\boldsymbol{v}_i$ is the feature vector of vulnerability i, and $\boldsymbol{v}_j$ is the feature vector of vulnerability j; x_i is the term frequency–inverse document frequency (TF-IDF) value of word i in the feature dictionary. y_i is the TF-IDF value of word j in the feature dictionary.

Key parameters in parallel vulnerability discovery are adjusted by user interaction, including cosine similarity threshold, vulnerability correlation view tension coefficient, etc. Whether the threshold value is satisfied or not is the criterion for judging the parallel vulnerability. And the tension coefficient is a decisive parameter that determines the degree of correlation between the data in the view. The adjustment of the tension coefficient can solve the problem of visual confusion caused by the complex degree of correlation.

C. Vulnerability Exploitation: Attack Path Expression

Attackers can make use of different types of vulnerabilities to generate multiple different attack paths, thus posing a threat to the target host. This paper proposes a method for generating a host threat penetration attack graph based on the knowledge map, which reflects the exploitation relationship of vulnerabilities and shows the possible attack paths.

Construct a threat penetration attack graph between any two hosts in the network as shown in Fig. 5. The AG_{k+1}. AG_k represents the attack graph of the attack step of the kth step. The precondition node is represented by $< Host, privilege >$, and expressed with a hexagon shape in attack graph, to reflect the permissions an attacker needs to satisfy in order to penetrate the host. The attack node is expressed with a rectangle, and its data structure is represented by the triplet form of entity, attribute and attribute value. The triple structure $< CVE\_ID, Service, Probability >$ includes the vulnerability exploited by the attack, the host service to be utilized, and the feasibility of the attack. The post node includes $< Target, privilege >$ and its representation in the attack graph is an ellipse, which represents the effect achieved by penetrating the target host. In the above representation, the specific services and permissions of the exploit are obtained through semantic knowledge extraction of the vulnerability database, and the feasibility of the attack is calculated based on the CVSS 3.0 specification parameter calculation.

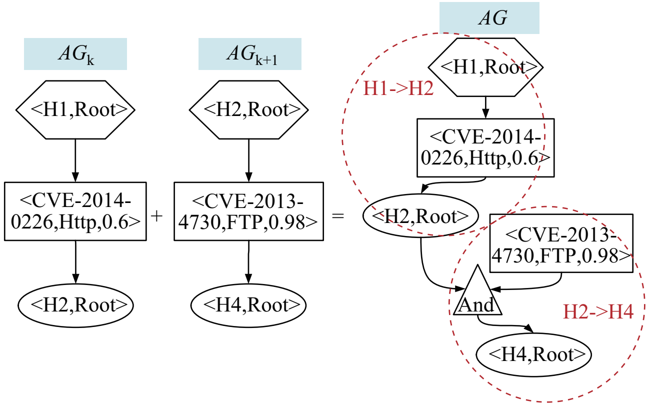


Fig. 5. The threat penetration attack graph merge process.

The attacker can scan the network topology information and construct the threat penetration attack graph between two hosts in the network. Based on the connection mode of the host in the network, determine whether the post node in AG_{k+1} matches the precondition in AG_k. If satisfied, the sub-attack graphs can be combined into a complete global attack graph. In the merge process, connection nodes, including "And" and "Or," are introduced to reflect the logical relationship between different sub-attack graphs; the connection nodes are represented by triangles. The sub-attack graph shows the specific situation of vulnerability exploitation, and the global attack graph shows the diversity of attack paths, which can be further inferred to obtain the optimal attack path. The attack graph merge process is shown in Fig. 5.

V. Optimization of Intrusion Detection Model Based on Visual Interaction

A. Intrusion Detection Framework Based on Visualization Technology

The first step of the defender is to detect system attacks, which is to detect system anomalies in time through intrusion detection. The optimization of the intrusion detection model based on the interactive visual analysis method is primarily reflected in the model construction process. During the process, by introducing expert experience in the field of data analysis and emphasizing human subjective initiative, the entire process of data-analysis-assessment is displayed and interacted to open the model's "black box" mode.

According to the display and interaction requirements in the process of grid intrusion detection model construction, a grid intrusion detection framework based on visualization technology is proposed, as shown in Fig. 6.

The attack perception of GCPS is divided into two parts: offline modeling and online detection. Offline modeling primarily uses anomaly-based intrusion detection modeling methods and visualization methods to realize the modeling and iterative optimization of the power grid historical data. Until the expected evaluation index is reached, the intrusion detection model is completed. The established intrusion detection model can be used in online detection to timely identify abnormal behaviors in real-time data of the power grid and find attack threats.

The optimization effect of the interactive visual analysis method on the model is reflected in the offline modeling process, which is primarily carried out from three aspects: data domain, feature domain and algorithm domain. Through the guided interactive behavior of these three parts, the user's model construction experience and data cognitive understanding are fed back into the analysis process.

B. Visual Optimization of Intrusion Detection Based on Support Vector Machine (SVM)

According to the proposed intrusion detection model visualization framework and the training steps of the SVM algorithm, a specific intrusion detection implementation method based on the SVM algorithm for visual analysis is proposed. This method consists of three steps, as shown in Fig. 7. Fig. 7 shows the main interactive contents and the data transformation forms in the process of constructing the intrusion detection model.

1) Data Domain

Understand its distribution process through the classification of multi-source data of the GCPS. Furthermore, form a normative data set through data cleaning, data integration, data transformation and numerical processing.

2) Feature Domain

Based on random forest and information gain, the visual interaction method is combined with the expert knowledge of the analyst to realize the features selection of phasor measurement unit (PMU) data. By optimizing the projection mapping of the high-dimensional sample space based on the

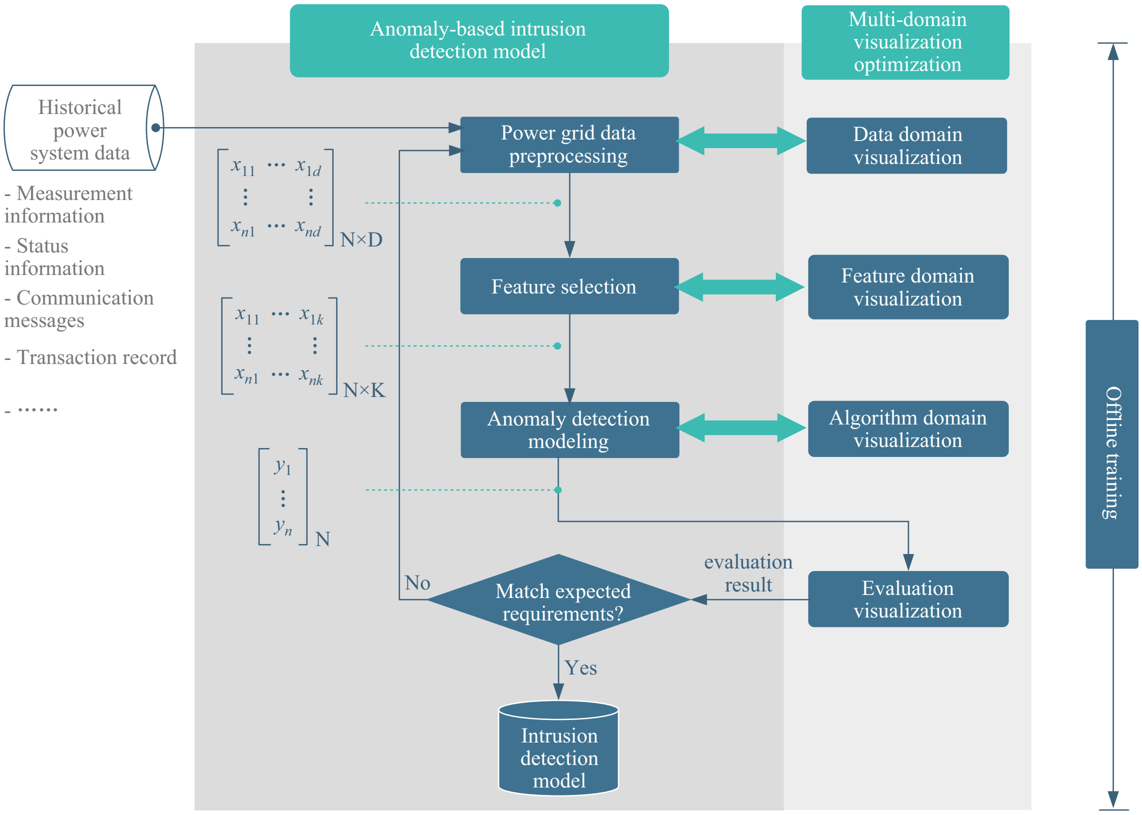

Anomaly-based intrusion detection model
Multi-domain visualization optimization
Historical power system data
- Measurement information
- Status information
- Communication messages
- Transaction record
- ......
$x_{11} \cdots x_{1d}$
$x_{n1} \cdots x_{nd}$
N×D
$x_{11} \cdots x_{1k}$
$x_{n1} \cdots x_{nk}$
N×K
y_1
y_n
N
Power grid data preprocessing
Data domain visualization
Feature selection
Feature domain visualization
Anomaly detection modeling
Algorithm domain visualization
evaluation result
Evaluation visualization
No
Match expected requirements?
Yes
Intrusion detection model
Offline training

Fig. 6. The optimization framework of GCPS detection model based on visual interaction.

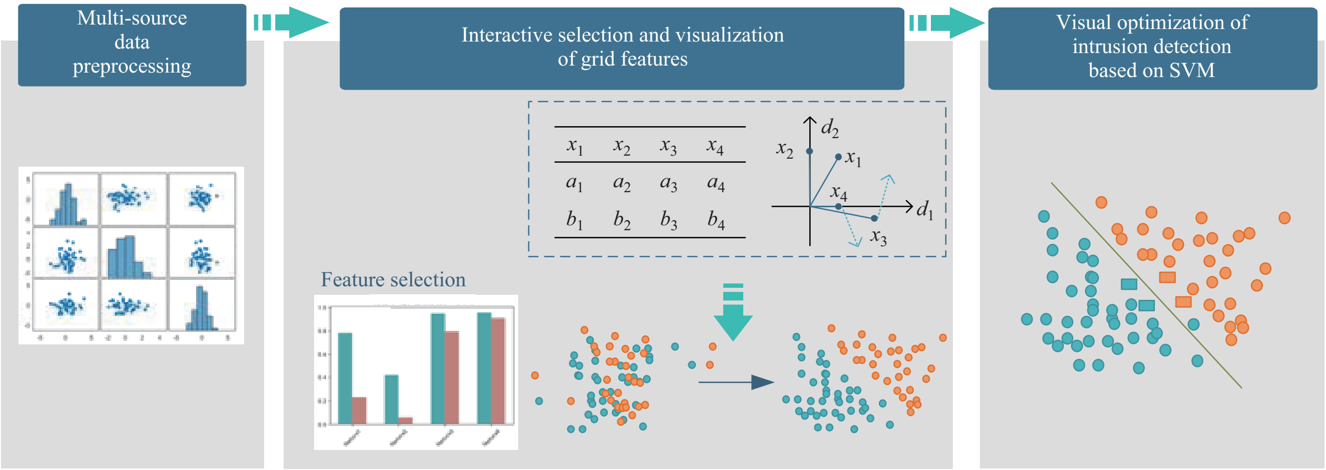

Multi-source data preprocessing
Interactive selection and visualization of grid features
Visual optimization of intrusion detection based on SVM
x_1 x_2 x_3 x_4
a_1 a_2 a_3 a_4
b_1 b_2 b_3 b_4
d_2
d_1
x_1
x_2
x_3
x_4
Feature selection

Fig. 7. The implementation process of intrusion detection based on the SVM algorithm.

knowledge of the modeler, a two-dimensional sample set with explicit data distribution is obtained.

3) Algorithm Domain

Explain the SVM through showing support vector and separation hyperplane in the classification process. Provide suggestions for selecting or adjusting kernel functions, penalty factors, and support vectors to achieve higher precision detection. Provide manual annotation selection for data items such as false positives and false negatives, and realize feedback iterative learning of the model.

VI. Case Study

The visual framework proposed in this paper is verified by conducting an experiment of ADD on the test platform. The function of the experiment is to implement specific network attack means to infiltrate the cyber layer control system, and then affect the operation of the physical equipment. The contents of visualization include the representation of vulnerability knowledge to help attackers exploit. It also includes visual optimization of the intrusion detection model, based on which defenders can monitor the physical layer to detect whether equipment deviates from normal operating conditions.

A. Experiment Setup

According to [22], [23], the specific structure of the GCPS test platform is shown in Fig. 8. The cyber layer simulates the actual wide area network (WAN) environment and realizes the information flow transmission functions between the sub-station and the control center, such as measurement data and instruction transmission. On the physical layer, an IEEE 4-bus 3-generate system is selected for simulation to observe the impact of safety events such as breaker tripping. Attack methods include: false data injection attacks and distributed denial of service (DDoS) attacks. Attacks affect the control center and sub-stations, further affecting the running state of the physical system, or induce operators to make wrong decisions.

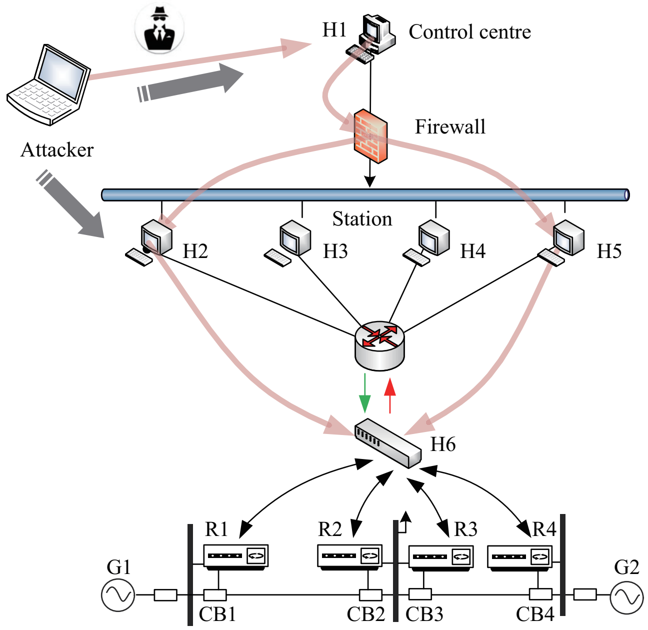


Fig. 8. The structure of the GCPS test platform.

The attacker sorts out the network vulnerability information and constructs the local vulnerability database. The specific data set structure is shown in Table I.

TABLE I
DATA STRUCTURE OF VULNERABILITY DATABASE

Name	Type	Implication
Id	Object ID	Unique number of the vulnerability
createTime	Date	When the vulnerability was created
processtime	Date	Time to process the vulnerability
description	String	Specific description of the vulnerability text
userId	Object ID	User ID who processed the vulnerability
processState	Boolean	Processing status

The physical layer components include generator G1, G2, intelligent electronic devices (IEDs) R1–R4, respectively control breaker CB1–CB4. The two transmission lines run from CB1 to CB2 and CB3 to CB4. The physical system dataset contains a total of 128 features. The system dataset contains a total of 128 features, and the data comes from 4 PMUs. The specific data content is shown in Table II. Each PMU contains 29 measurement types, that is, a total of 116 measurement columns. After the PMU measurement column, there are always 12 columns of features including Control panel logs, Snort alarms, and PMU/Relay logs. The last column is the label for an attack or no attack.

B. Experimental Results of the Attack Process

Before injecting an attack, the attacker first summarizes the vulnerability information in a certain period of time to find out the main causes and exploitation methods of the vulnerability in the network security.

The Nightingale rose diagram is used to demonstrate the distribution of threat caused by the vulnerability after statistical analysis. Through the form of word cloud, the specific details of the vulnerability feature vector space are displayed. The weight of feature semantics reflects the importance of this field in the process of vulnerability information analysis, which is shown in Fig. 9.

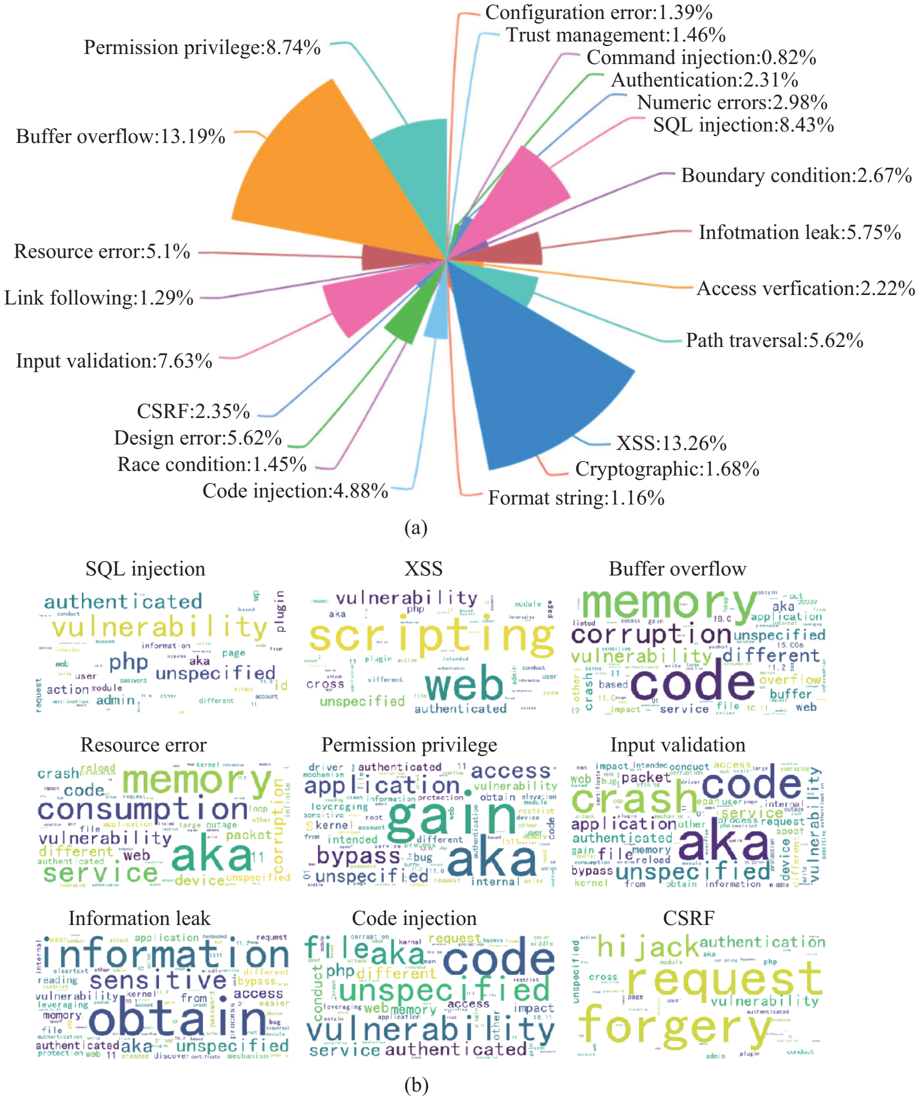
Figure 9(a) shows that the number of vulnerabilities in the Buffer overflow category are heavily weighted. As can be seen from Fig. 9(b), the extracted features of this category are {memory, code, corruption, crash}. The vulnerability knowledge entity extracted by semantic analysis is used to construct the data structure of the attack graph.

TABLE II
DATA STRUCTURE OF VULNERABILITY DATABASE

Feature	Description
PA1:VH – PA3: VH	Phase A-Phase C voltage phase angle
PM1: V – PM3: V	Phase A-Phase C voltage amplitude
PA4:IH – PA6: IH	Phase A-Phase C current phase angle
PM4: I – PM6: I	Phase A-Phase C current amplitude
PA7:VH – PA9: VH	Positive sequence - Negative sequence - Zero sequence voltage phase angle
PM7: V – PM9: V	Positive sequence - Negative sequence - Zero sequence voltage amplitude
PA10: VH – PA12: VH	Positive sequence - Negative sequence - Zero sequence current phase angle
PM10: V – PM12: V	Positive sequence - Negative sequence - Zero sequence current amplitude
F	Relay frequency
DF	Relay frequency increment
PA: Z	Relay impedance
PA: ZH	Relay impedance wiring angle
S	Relay status

The similarity between vulnerabilities is calculated and the results are expressed in the form of a heat map. The size of the specific value is reflected by the color mapping, as shown in Fig. 10. The heuristic representation of the interactive radiant layout is used to assist the attacker to form a cognition of the overall distribution and similarity of vulnerabilities, as shown in Fig. 11. The radiation pattern is composed of an outer loop and an inner arc: the outer loop is used to represent specific vulnerability information, the arc connects the vulnerabilities, and the color depth and density of the inner arc indicate similarity. The attacker finds the degree of correlation between the data by interactively adjusting the tension coefficient of the arc, and reads the details of the data through a focus + detailed interaction to highlight the lines of the selected data. The discovery of parallel vulnerability provides more path choices for attacks to target the host.

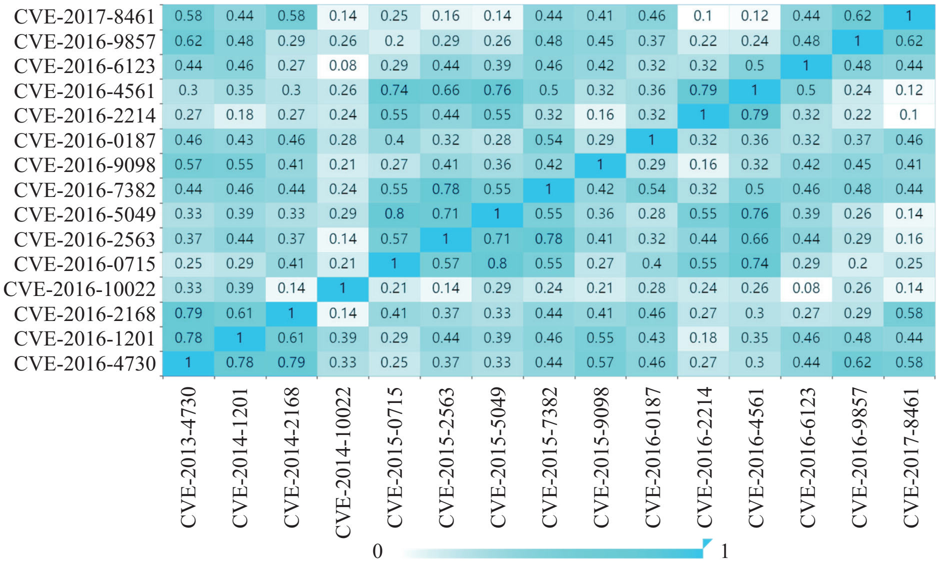
The attacker penetrated the H1 host and combined multiple



(a)

(b)

Fig. 9. Cause and feature distribution of vulnerabilities. (a) Nightingale rose diagram. (b) Word cloud graph.



	CVE-2013-4730	CVE-2014-1201	CVE-2014-2168	CVE-2014-10022	CVE-2015-0715	CVE-2015-2563	CVE-2015-5049	CVE-2015-7382	CVE-2015-9098	CVE-2016-0187	CVE-2016-2214	CVE-2016-4561	CVE-2016-6123	CVE-2016-9857	CVE-2017-8461
CVE-2017-8461	0.58	0.44	0.58	0.14	0.25	0.16	0.14	0.44	0.41	0.46	0.1	0.12	0.44	0.62	1
CVE-2016-9857	0.62	0.48	0.29	0.26	0.2	0.29	0.26	0.48	0.45	0.37	0.22	0.24	0.48	1	0.62
CVE-2016-6123	0.44	0.46	0.27	0.08	0.29	0.44	0.39	0.46	0.42	0.32	0.32	0.5	1	0.48	0.44
CVE-2016-4561	0.3	0.35	0.3	0.26	0.74	0.66	0.76	0.5	0.32	0.36	0.79	1	0.5	0.24	0.12
CVE-2016-2214	0.27	0.18	0.27	0.24	0.55	0.44	0.55	0.32	0.16	0.32	1	0.79	0.32	0.22	0.1
CVE-2016-0187	0.46	0.43	0.46	0.28	0.4	0.32	0.28	0.54	0.29	1	0.32	0.36	0.32	0.37	0.46
CVE-2016-9098	0.57	0.55	0.41	0.21	0.27	0.41	0.36	0.42	1	0.29	0.16	0.32	0.42	0.45	0.41
CVE-2016-7382	0.44	0.46	0.44	0.24	0.55	0.78	0.55	1	0.42	0.54	0.32	0.5	0.46	0.48	0.44
CVE-2016-5049	0.33	0.39	0.33	0.29	0.8	0.71	1	0.55	0.36	0.28	0.55	0.76	0.39	0.26	0.14
CVE-2016-2563	0.37	0.44	0.37	0.14	0.57	1	0.71	0.78	0.41	0.32	0.44	0.66	0.44	0.29	0.16
CVE-2016-0715	0.25	0.29	0.41	0.21	1	0.57	0.8	0.55	0.27	0.4	0.55	0.74	0.29	0.2	0.25
CVE-2016-10022	0.33	0.39	0.14	1	0.21	0.14	0.29	0.24	0.21	0.28	0.24	0.26	0.08	0.26	0.14
CVE-2016-2168	0.79	0.61	1	0.14	0.41	0.37	0.33	0.44	0.41	0.46	0.27	0.3	0.27	0.29	0.58
CVE-2016-1201	0.78	1	0.61	0.39	0.29	0.44	0.39	0.46	0.55	0.43	0.18	0.35	0.46	0.48	0.44
CVE-2016-4730	1	0.78	0.79	0.33	0.25	0.37	0.33	0.44	0.57	0.46	0.27	0.3	0.44	0.62	0.58

Fig. 10. The heat map of vulnerability similarity calculation results.

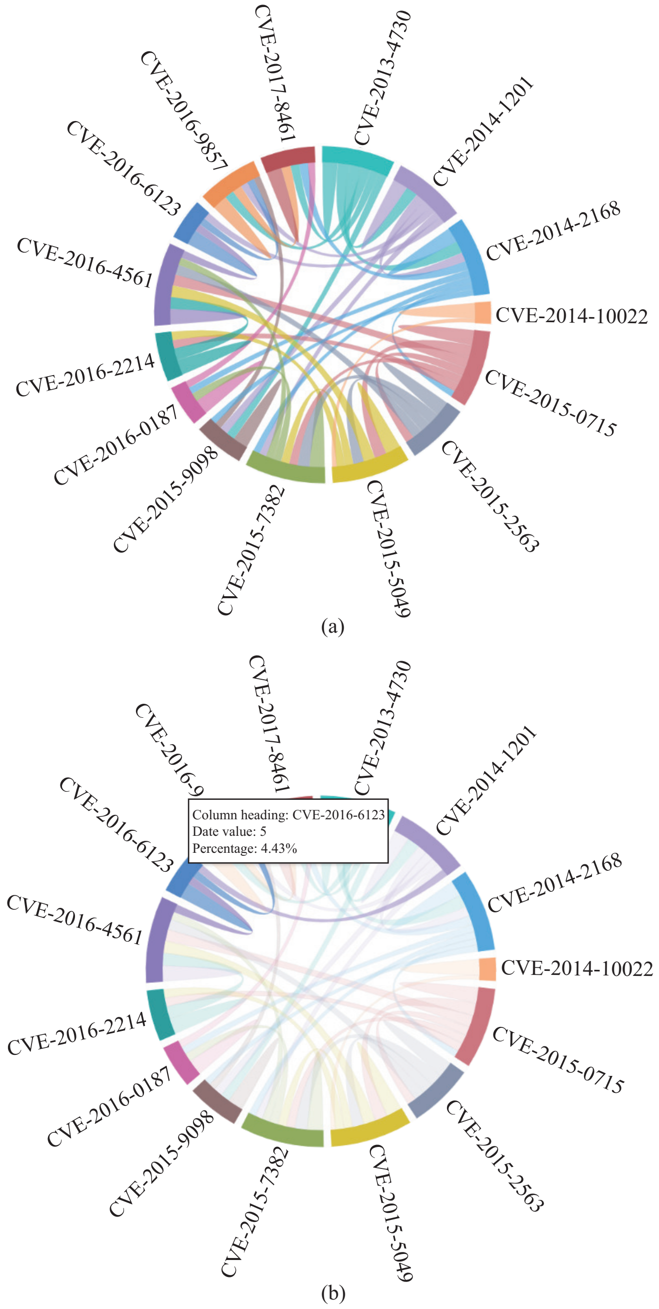


Fig. 11. Parallel vulnerability discovery interactive radiation pattern. (a) Overview. (b) Details.

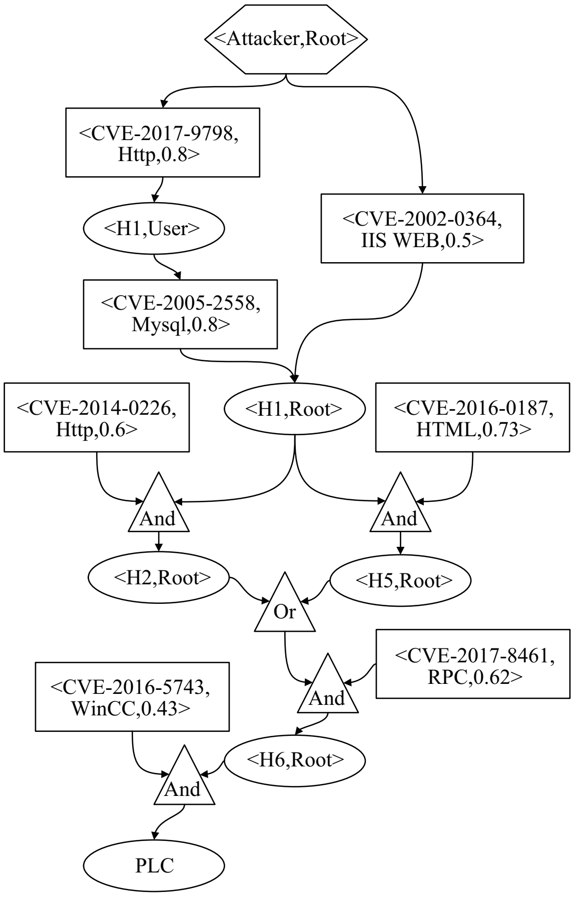

<Attacker,Root>
<CVE-2017-9798, Http,0.8>
<CVE-2002-0364, IIS WEB,0.5>
<H1,User>
<CVE-2005-2558, Mysql,0.8>
<CVE-2014-0226, Http,0.6>
<H1,Root>
<CVE-2016-0187, HTML,0.73>
And
And
<H2,Root>
Or
<H5,Root>
<CVE-2017-8461, RPC,0.62>
<CVE-2016-5743, WinCC,0.43>
And
<H6,Root>
And
PLC

Fig. 12. The attack graph of the exploit relationship.

types of vulnerabilities, which affected the normal operation of the PLC.

As shown in Fig. 12, the possible attack paths include: 1) H1 −> H2 −> H6; 2) H1 −> H5 −> H6.

C. Defender Experiment Results

The attack scenarios include remote tripping command injection, relay setting change and data injection. The remote tripping command injection to remotely open one relay or two relays (R1, R2, R3, R4 respectively). The data injection attempts to simulate an effective fault by changing the measurement value, and then sends an illegal trip command to the relay of the transmission line between CB1 and CB2, CB3 and CB4. The relay setting change imitates the influence of illegal control measures to the disabled relays during a fault on the line connected to those relays (R1, R2, R3, R4 respectively).

The defender trains the intrusion detection model based on the physical layer data from the Power System Datasets and the GCPS platform. Some of the data features, such as R4-PA: Z have missing data (the missing rate in the training set is 7.93% and the missing rate in the test set is 7.65%). In order to solve this problem, the whole data set is first processed by the elimination method. The data distribution of 8 features is presented in the form of a scatter graph matrix, as shown in Fig. 13.

Then, rank each feature of the dataset. Because of too many features, only the information gain is shown here as the result of the evaluation method. In reality, 50% of all the features provide 96% of the information. Figure 14 shows the results of using the information gain to rank the features, which are displayed in graph for the top 60 features. In Fig. 14, the abscissa ID represents the serial number of the feature value, and the ordinate IG represents the information gain value of the feature. It can be clearly shown that the features with the highest information gain are the 115, 114, 86, 85, 57, 56, 28, 27 features, which correspond to the PA: ZH and PA: Z attributes of each relay, and the information gain values range from 0.74 to 0.76. The values of the voltage phase angle, current phase angle, voltage amplitude and current amplitude are also relatively high (the information gain value is between

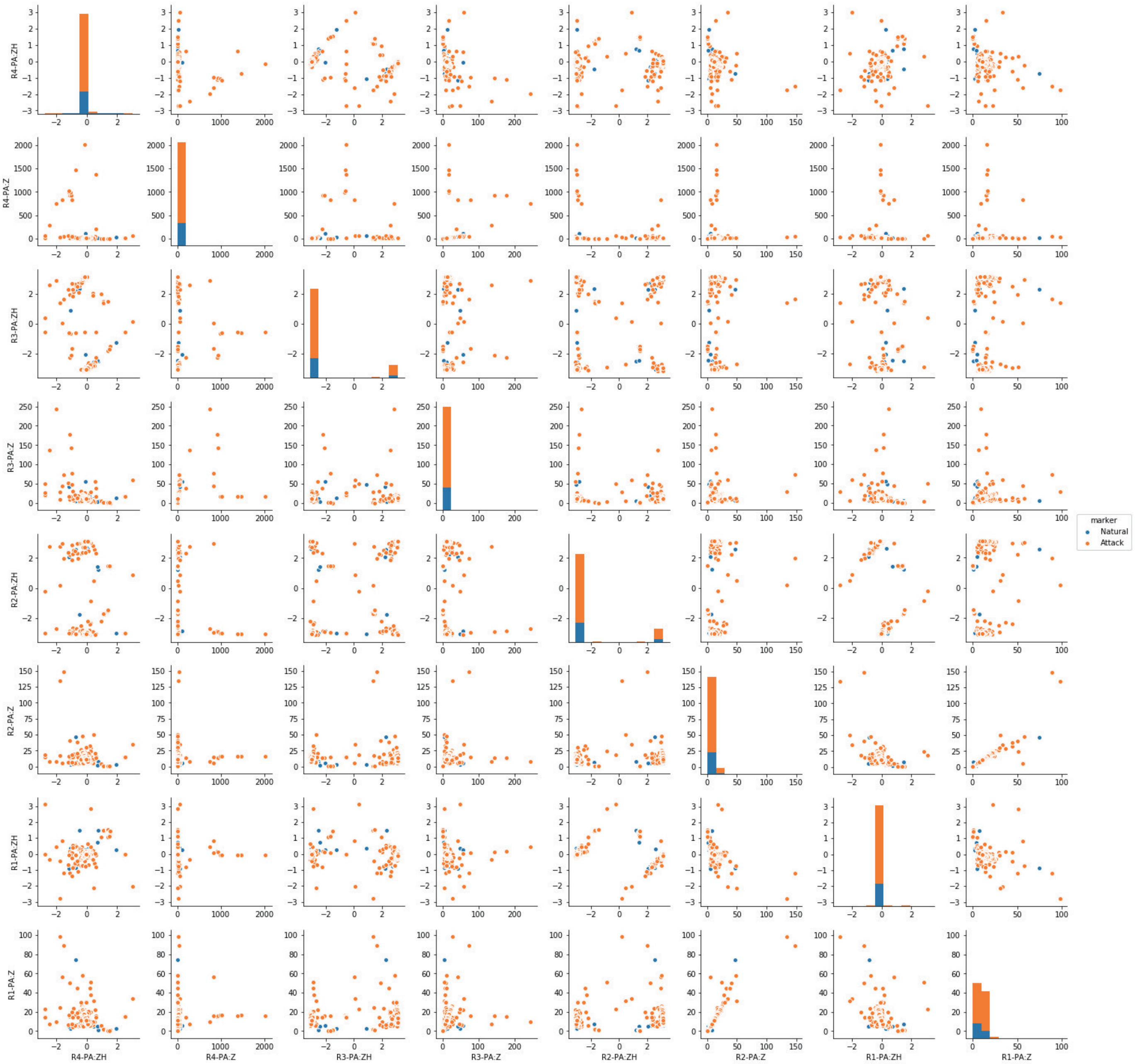


Fig. 13. The scatter graph matrix distribution of the intrusion detection data set.

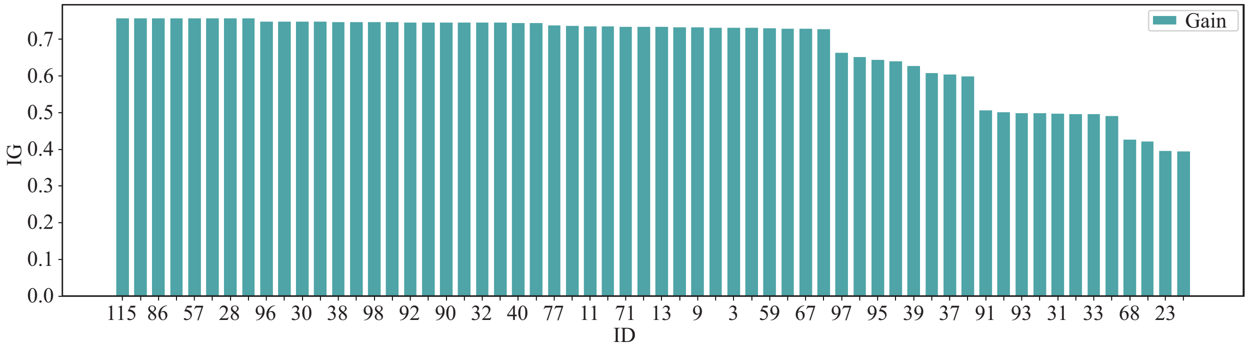
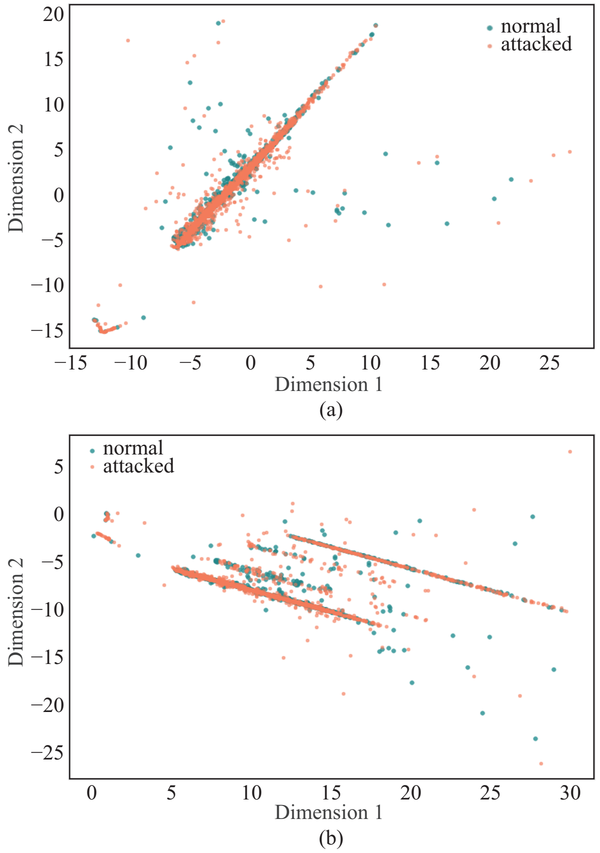


Fig. 14. The information gain ranking of features.

TABLE III
THE BASELINE PROJECTION MATRIX AND THE INTERACTIVE ADJUSTED PROJECTION MATRIX

Conversion coefficients	$\boldsymbol{x}_1$	$\boldsymbol{x}_2$	$\boldsymbol{x}_3$	$\boldsymbol{x}_4$	$\boldsymbol{x}_5$	$\boldsymbol{x}_6$	$\boldsymbol{x}_7$	$\boldsymbol{x}_8$
α	-2.77×10^{-4}	9.99×10^{-1}	1.60×10^{-4}	2.02×10^{-2}	-9.47×10^{-6}	-4.59×10^{-4}	9.32×10^{-6}	-4.41×10^{-4}
β	-7.67×10^{-3}	-2.02×10^{-4}	3.99×10^{-2}	1.30×10^{-1}	3.42×10^{-2}	8.84×10^{-1}	-1.23×10^{-2}	4.47×10^{-1}
α'	-1.19×10^{-5}	5.42×10^{-1}	5.97×10^{-1}	2.09×10^{-1}	3.93×10^{-1}	3.85×10^{-1}	-5.94×10^{-5}	5.77×10^{-2}
β'	-2.17×10^{-1}	-7.75×10^{-1}	5.27×10^{-1}	6.13×10^{-2}	1.16×10^{-1}	1.13×10^{-1}	-2.01×10^{-1}	6.41×10^{-2}

0.72 and 0.74). These together make up the top 40 features.



(a)

(b)

Fig. 15. The comparison graph of data distribution mapped to a two-dimensional plane through the projection matrix. (a) Data distribution under the baseline projection matrix. (b) Data distribution after interactive adjustment of projection matrix.

The intrusion detection samples after feature selection are mapped to a two-dimensional plane through the baseline projection matrix. But there is a large area of overlap between normal samples and attack samples, which brings some difficulties to the classification process. Increase the α and β (α and β are conversion coefficients, used to project the K dimensional data after feature selection to two-dimensional space) values corresponding to R4-PA: Z and R4-PA: ZH by typing in the table. After continuous adjustment, the projection matrix composed of α' and β' is obtained through the Schmidt orthogonal transformation. The projection matrix after interactive adjustment is shown in Table III. At this point, the normal sample and the attack sample have been separated, and the remaining few overlapped parts can be further adjusted and optimized according to the weight corresponding to the features. The interactive optimization effect is shown in Fig. 15. It is verified by the SVM algorithm that the accuracy of the optimized training set increased from 70.85% to 73.97%, and the accuracy of the intrusion detection of the test set increased from 78.33% to 80.54%.

VII. CONCLUSION

The paper is oriented to the GCPS security field. Based on the GCPS test platform and visualization technology, an interactive visual analysis method for ADD is proposed. First, based on the GCPS structure, the visual analysis tasks of attackers and defenders are defined. Then the content of knowledge visualization by the attacker and the steps of the defender's interaction optimization of the model are described. For attackers, with the aim of improving the system's vulnerability awareness to assist in determining the attack path, the results of the vulnerability analysis, the relationships between parallel vulnerabilities and the causal relationship between the exploits of the vulnerabilities are visually displayed. For defenders, the PMU data is used to build the attack awareness model. In the process of modeling, interactive means are used to separate the overlap positive and negative sample data, which provides a visual reference for selecting classification algorithms to improve the accuracy of the model. Finally, the effectiveness of the method is verified by experiments and practice. This paper introduces the application of visual analysis methods from a new perspective. Its application value is reflected in the simplification of complex information. It greatly utilizes human view perception ability and cognitive skills, and promotes the dissemination, transformation and understanding of information. It plays a positive role in promoting technical research and ADD in the field of GCPS security.

The scheme proposed in this paper is still worth improving in practice. The following issues should be further considered in a future study: 1) The focus of this article is on the visual interactive analysis method in the field of power offense and defense security. It is necessary to more closely integrate the actual objects of the power grid and consider the differences in data, models, and knowledge in different scenarios of the power grid in order to improve the practicality of the method; 2) Research on the GCPS system can be further carried out to enrich experimental cases to verify the practicability of the scheme in the larger environment With abundant offensive and defensive methods, while the detection model can be considered to identify different types of attacks.

REFERENCES

[1] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[2] G. Q. Liang, S. R. Weller, J. H. Zhao, F. J. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] B. B. Li, R. X. Lu, W. Wang, and K. K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32–41, May 2017.

[4] J. X. Fei, C. C. Shi, X. C. Yuan, R. Zhang, W. Chen, and Y. Yang, "Reserch on cyber attack of key measurement and control equipment in power grid," in *2019 IEEE International Conference on Energy Internet (ICEI)*, Nanjing, China, 2019, pp. 31–36.

[5] D. V. Nga, O. H. See, D. N. Quang, C. Y. Xuen, and L. L. Chee, "Visualization techniques in smart grid," *Smart Grid and Renewable Energy*, vol. 3, no. 3, pp. 175–185, Aug. 2012.

[6] Y. Y. Zhou, P. Li, Y. N. Xiao, A. Masood, Q. C. Yu, and B. Sheng, "Smart grid data mining and visualization," in *2016 International Conference on Progress in Informatics and Computing (PIC)*, 2016.

[7] D. A. Keim, G. Andrienko, J. D. Fekete, and C. Görg, "Visual analytics: definition, process, and challenges," in *Information Visualization*, A. Kerren, J. T. Stasko, J. D. Fekete, and C. North, Eds. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 154–175.

[8] D. Sacha, A. Stoffel, F. Stoffel, B. C. Kwon, G. Ellis, and D. A. Keim, "Knowledge generation model for visual analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 20, no. 12, pp. 1604–1613, Dec. 2014.

[9] M. Panteli, P. A. Crossley, D. S. Kirschen, and D. J. Sobajic, "Assessing the impact of insufficient situation awareness on power system operation," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2967–2977, Aug. 2013.

[10] Q. Sun and L. Yang, "From independence to interconnection — A review of AI technology applied in energy systems," *CSEE Journal of Power and Energy Systems*, vol. 5, no. 1, pp. 21–34, Mar. 2019.

[11] S. X. Liu, X. T. Wang, M. C. Liu, and J. Zhu, "Towards better analysis of machine learning models: a visual analytics perspective," *Visual Informatics*, vol. 1, no. 1, pp. 48–56, Mar. 2017.

[12] Y. Tang, Y. Huang, H. Wang, C. Wang, Q. Guo and W. Yao, "Framework for artificial intelligence analysis in large-scale power grids based on digital simulation," *CSEE Journal of Power and Energy Systems*, vol. 4, no. 4, pp. 459-468, Dec. 2018.

[13] S. S. Liu, D. Maljovec, B. Wang, P. T. Bremer, and V. Pascucci, "Visualizing high-dimensional data: advances in the past decade," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 3, pp. 1249–1268, Mar. 2017.

[14] S. K. Card, J. D. Mackinlay, and B. Shneiderman, *Readings in Information Visualization: Using Vision to Think*. San Francisco: Morgan Kaufmann Publishers Inc., 1999.

[15] A. Kerren and F. Schreiber, "Toward the role of interaction in visual analytics," in *Proceedings of the 2012 Winter Simulation Conference (WSC)*, 2012, pp. 1–13.

[16] J. S. Yi, Y. A. Kang, J. Stasko, and J. A. Jacko, "Toward a deeper understanding of the role of interaction in information visualization," *IEEE Transactions on Visualization and Computer Graphics*, vol. 13, no. 6, pp. 1224–1231, Nov. /Dec. 2007.

[17] D. Sacha, L. S. Zhang, M. Sedlmair, J. A. Lee, J. Peltonen, D. Weiskopf, S. C. North, and D. A. Keim, "Visual interaction with dimensionality reduction: a structured literature analysis," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 1, pp. 241–250, Jan. 2007.

[18] J. G. S. Paiva, W. R. Schwartz, H. Pedrini, and R. Minghim, "An approach to supporting incremental visual data classification," *IEEE Transactions on Visualization and Computer Graphics*, vol. 21, no. 1, pp. 4–17, Jan. 2015.

[19] I. K. Choi, T. Childers, N. K. Raveendranath, S. Mishra, K. Harris, and K. Reda, "Concept-driven visual analytics: an exploratory study of model-and hypothesis-based reasoning with visualizations," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–14.

[20] D. Sacha, H. Senaratne, B. C. Kwon, G. Ellis, and D. A. Keim, "The role of uncertainty, awareness, and trust in visual analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 1, pp. 240–249, Jan. 2016.

[21] X. G. Zhao, Y. Peng, Z. Zhan, Y. Jin, and Y. G. Yao, "Research on parallel vulnerabilities discovery based on open source database and text mining," in *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2015, pp. 327–332.

[22] S. Y. Pan, "Cybersecurity testing and intrusion detection for cyber-physical power systems," Ph. D. dissertation, Mississippi State University, 2014.

[23] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, Denver, CO, 2014, pp. 1–8.

Kehe Wu received the Ph.D. degree in Thermal Engineering from North China Electric Power University, Beijing, China, in 2009. He is a Professor at North China Electric Power University, the director of the Chinese Association for Artificial Intelligence and Beijing Engineering Research Center of Electric Information Technology, and a committee member of the China Electric Power Information Standardization Committee and Professional Electric Power Information Committee of the Chinese Society for Electrical Engineering. His research interests include information security, industrial control system security.

Jiawei Li received the M.S. degree in Software Engineering from Beihang University, Beijing, China, in 2016. He is currently pursuing the Ph.D. degree in Information Security with the School of Computer and Control Engineering, North China Electric Power University, Beijing, China. His main research interest includes the network security defense technology of industrial control systems.

Yayun Zhu received the B.S. degree in Computer Science and Technology from North China Electric Power University (NCEPU), Beijing, China, in 2011, and the Ph.D. degree in Information Security from NCEPU, Beijing, China, in 2018. His research interests include information security, and Big Data in electric power and energy internet.

Siwei Miao received the M.S. degree in Computer Engineering from Nanyang Technological University, Singapore, in 2017. Her Research interests are cyber security, industrial control system security and mobile application security.

Sixun Zhu received the B.S. degree in Automation from Wuhan University of Science and Technology, Wuhan, China, in 2018. She is currently pursuing the M.S. degree in Control Science and Control Engineering with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan, China. Her main research interests include visualization technology and cyber-physical security of industrial control systems.

Chunjie Zhou received the M.S. and Ph.D. degrees in Control Theory and Control Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1991 and 2001, respectively. He is currently a Professor at the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology. His research interests include safety and security control of industrial control systems, theory and application of networked control systems, and artificial intelligence.