Sampled Value Attack Detection for Busbar Differential Protection Based on a Negative Selection Immune System

Jun Mo and Hui Yang

***Abstract*—Considering a variety of sampled value (SV) attacks on busbar differential protection (BDP) which poses challenges to conventional learning algorithms, an algorithm to detect SV attacks based on the immune system of negative selection is developed in this paper. The healthy SV data of BDP are defined as self-data composed of spheres of the same size, whereas the SV attack data, i.e., the nonself data, are preserved in the nonself space covered by spherical detectors of different sizes. To avoid the confusion between busbar faults and SV attacks, a self-shape optimization algorithm is introduced, and the improved self-data are verified through a power-frequency fault-component-based differential protection criterion to avoid false negatives. Based on the difficulty of boundary coverage in traditional negative selection algorithms, a self-data-driven detector generation algorithm is proposed to enhance the detector coverage. A testbed of differential protection for a 110 kV double busbar system is then established. Typical SV attacks of BDP such as amplitude and current phase tampering, fault replays, and the disconnection of the secondary circuits of current transformers are considered, and the delays of differential relay operation caused by detection algorithms are investigated.**

***Index Terms*—Cyberattack, busbar differential protection (BDP), negative selection, self-data-driven detector, sampled value attacks, internal faults.**

I. Introduction

HIGHLY advanced smart grids are characterized by the interconnection of numerous intelligent electric devices (IEDs) through high-speed networks such as Ethernet and Internet, leading to a high-degree integration among physical power systems and cyber systems. Communication systems play a major role in maintaining the reliability and security of power systems. In recent years, the number of malicious attacks on the cyber components of power systems, which result in blackouts, increases globally, and the security of smart grids is facing severe challenges [1]-[3]. Currently, research works on cyberattacks on power systems have focused mainly on wide-area monitoring, protection and control, e.g., supervisory control, data acquisition, and wide-area protection [4]-[8]. This trend is attributed to the fact that wide-area power systems with enormous network architectures are highly vulnerable to cyberattacks and frangible in terms of security [9]. Cyberattacks can be realized by injecting spoofed sampled value (SV) and generic object-oriented event data frames of substation into the communication network at the bay level [10]. For local protection in substations, a private communication structure is typically employed to enhance the security, which prevents external attacks on the protection system. However, internal attacks cannot be stopped. In particular, the IEC 61850 standard, which is widely used in smart grids, increases the convenience of integrating IEDs such as protection IEDs and merging units (MUs) from different vendors. Thus, a great opportunity exists for countries or regional groups to deploy IEDs on target protection systems for political purposes. Protective relays are originally designed to recognize power system faults and do not yet possess the ability to detect false SVs. Once an SV attack occurs, the maloperation may occur. Similarly, if a circuit breaker (CB) IED receives false tripping signals, the component of protected power system is directly cut off. The busbar is one of the most important components in a power system, and a malfunction of its protection due to an SV attack can lead to the outage of all connected lines, which may seriously affect the stability of the power system. Therefore, defending against SV attacks on busbar differential protection (BDP) for the stable operation of power systems is essential.

Currently, the security of relay protection has received considerable attention [11]-[13], but practical algorithms remain limited. One popular algorithm is to use an encryption strategy to ensure the integrity and confidentiality of data [14]. However, the security of encryption algorithms is relative, and complex algorithms increase not only the security but also the decoding time. In [15], an algorithm for detecting anomalous SVs is proposed by checking the sequence number of each SV packet. Yet, this algorithm cannot identify incorrect SV data and is ineffective against internal attacks from legal IEDs. To discriminate false faults from valid faults, a neural-network-based pattern recognition algo-

Manuscript received: May 23, 2021; revised: July 17, 2021; accepted: November 12, 2021. Date of CrossCheck: November 12, 2021. Date of online publication: February 22, 2022.

This work was supported by National Natural Science Foundation of China (No. 51967003) and Guangxi Natural Science Foundation (No. 2016GXNSFBA380105).

J. Mo (corresponding author) and H. Yang are with the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University, Nanning 530004, China (e-mail: mj1232@126. com; yanghuicherish@163. com).

DOI: 10.35833/MPCE.2021.000318

rithm is presented in [16], but this algorithm requires the current data of all lines within a substation. A distributed agent-based decentralized protection system is presented in [17], in which peer-to-peer communication, reputation-based trust, and a data retransmission scheme are utilized to combat malicious attacks. However, the data retransmission is not suitable for SV transmission of relay protection. To distinguish network attacks from power system faults, a distributed multi-agent algorithm using synchrophasor data, relay status logs, and network event-monitor logs is proposed in [18] and [19]. The criterion of the protection relay agent based on the synchrophasor data of a single line is not suitable for identifying busbar faults and attacks. In addition, the use of relay logs and network event-monitor logs may increase the detection time. However, real-time tests are not conducted in the aforementioned studies. In [20], an algorithm to detect false data injection attacks in line-current differential relays is proposed using unknown input observers. This particular algorithm cannot solve the problem of SV attacks on BDP because the dimension of the attack data of line differential protection is much lower than that of BDP. In [21], a machine learning algorithm called a support vector machine (SVM) is used in the transformer differential relay to distinguish internal faults from other situations. In [22], a common path-mining algorithm (CPMA) is developed and used to learn and identify power system faults and network attack patterns. An intelligent algorithm based on a convolutional neural network (CNN) is proposed in [23] to identify various power system events, including normal operation, fault, false data, and load change events. In [21] - [23], various types of samples must be prepared and used to train the corresponding detectors. However, preparing an available attack sample set for busbar protection is very difficult. Currently, no references are available to address the problem of SV attack identification in BDP.

The biological immune system is an effective organic system that protects the body from invasion. To date, artificial immune models based on biological immune system such as the immune network [24], clonal selection theory [25], and negative selection algorithms (NSAs) [26] have received considerable attentions from researchers studying anomaly and change detections [27]. Compared with other immune algorithms, NSAs are more efficient in detecting unknown types of data and have been widely studied and improved in recent years. In [28], a variable radius for self-sample based on affinity density is proposed to overcome the problems of boundary invasion and overlap between samples. However, changing the size of the self-sample without using the correct means of self-verification is risky. To reduce the computational cost, a screening rule for a decreased overlay rate is proposed in [29]. In addition, the detector movement is used to avoid a decreased coverage rate. Considering the deficiency of the random coverage of traditional NSAs, the known nonself is used as the candidate detector to further generate the detector and thereby repair holes [30]. In [31], an adaptive immunoregulation-based real-value NSA is proposed to calculate the self-radius and optimize the location of candidate detectors for different applications. To overcome the challenges of negative selection and multiple NSAs, a hybrid algorithm combining negative and positive selection techniques is proposed to detect the unknown malware in the Internet of Things [32]. Currently, most NSAs are unable to comprehensively address boundary intrusion, detector coverage, and particularly computational costs.

In view of these problems, we present an improved NSA and develop a detection algorithm for SV attacks on BDP. The main contributions of this paper are as follows.

1) Based on the immune system of negative selection, SV attack detection by BDP is developed. Compared with traditional learning algorithms, this algorithm has greater potential to identify unknown SV attacks of differential relays according to the sample deficiency experiment.

2) The results prove that SV attack detection can cause delays in differential relay operations. However, these delays can be reduced by the proposed self-shape optimization (SSO) algorithm by decreasing the confusion between busbar faults and SV attacks.

3) A self-data-driven (SDD) detector algorithm is proposed to generate optimal detectors and overcome the difficulty of boundary coverage in traditional NSAs.

II. Attack Model of BDP

A bus is a critical power component in a substations, whose primary protection typically employs current differential relay with restraint characteristics. The basic operation principle of current differential relay is:

$$I_d \geq I_t = \max\left\{ I_{set,\min},\ K_{res}\sum_{i=1}^{n}\left|\dot{I}_i\right| \right\} \tag{1}$$

where I_d is the differential current; I_t is the threshold current; $I_{set,\min}$ is the minimum threshold current, which can be 50% to 150% of the maximum rated value of the current transformers (CTs); K_{res} is the restraint coefficient with a typical range of 0.3-0.7; I_i is the line current; and the restraint current is equal to $\sum_{i=1}^{n}\left|\dot{I}_i\right|$, where n is the number of lines connected to the protected bus.

Figure 1 shows a typical SV attack tree model for busbar protection, where *DC*, *TC*, *RC* stand for the differential, threshold, and restraint currents, respectively, and DR stands for differential relay. The root node is the differential relay operation determined by the second layer nodes. When the differential current is greater than or equal to the threshold current, and a voltage component such as the zero sequence V_0, the negative sequence V_2, or the phase amplitude V_{ph} exceeds a certain threshold, the busbar protection will operate and send tripping signals to the corresponding CB IEDs. Because the current differential relay is the key to busbar protection, we focus only on the current data attack. The differential relay is assumed to operate when $I_d \geq I_t$. Two common algorithms are used to enable $I_d \geq I_t$: ① increase the differential current by tampering with the SVs through one or more MUs; and ② decrease the restraint current (or threshold current) by tampering with the SVs through one or more MUs during an external fault. SVs can be tampered with by replaying the data and free attacks. A typical SV attack in-

volves the replay of a fault current or saturation current by specific MUs. The free attack can increase or decrease the current amplitude or modify the current angle through one or more MUs. According to the different current data and the combination of attackers, numerous attack samples are available for differential relay. For machine learning algorithms, preparing a sufficient training sample set of attack types is difficult. One advantage of NSAs is that they require only nonattack samples, which can be easily obtained through experiments. Therefore, an NSA is chosen in this paper to design the detection algorithm for SV attacks.

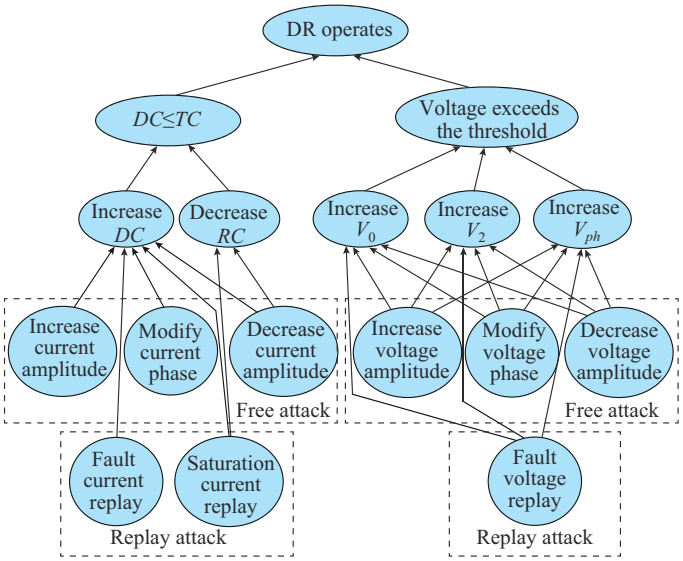


Fig. 1. Typical SV attack tree mode for busbar protection.

III. NSA

NSAs, which imitate the immune tolerance behavior of T-cells in biological immune system (BIS), are first introduced in [33]. In T-cell production, a censoring process is employed in which T-cells that bind to self-molecules are destroyed, whereas those that do not bind are permitted to leave the thymus. This process is known as negative selection. Mature cells that leave the thymus are used to identify foreign cells such as viruses and bacteria. In NSAs, the self and detectors are basic data corresponding to T-cells that bind to self-molecules and those that do not bind, respectively. The self-data model is defined based on the characteristics of the research object. In general, it is a fixed-size entity described by multiple feature attributes. Detectors are the entities that occupy the nonself region and are usually generated using a random algorithm [34]. Each candidate detector must undergo a process known as self-tolerance. In this process, if the detector matches any self-samples, it is eliminated. Eventually, mature detectors remain outside the self-region. The basic steps of an NSA are described as follows.

Step 1: define the self-model according to the characteristics of the SV data, and then obtain the self-set that represents the normal operation of the busbars.

Step 2: generate a set of detectors through the self-tolerance process.

Step 3: monitor the attack behavior by matching the detectors with new data. When an SV data point is covered by a detector, it is regarded as attack data.

The main goal of NSAs is to cover the entire nonself region with detectors. However, the coverage close to the boundary between the self and nonself regions is a difficult problem for current algorithms [35]. In this paper, an SDD detector generation algorithm is proposed to enhance the detector coverage. In addition, to avoid the confusion between internal faults and attacks, an SSO algorithm is considered.

A. Data Model

For differential relay, the synchronous current data for a multiline in the same phase can be divided into three groups: increased, decreased, and unchanged current amplitudes. Correspondingly, the three characteristic attributes used to determine the coordinates of the SV data point in the shape space are defined as follows.

1) Increment attribute A_I. This attribute is determined by the current data with an increased amplitude as:

$$\begin{cases} A_I = \sum [\Delta I_i - K_v I_i(t-\Delta t)] \\ \Delta I_i - K_v I_i(t-\Delta t) > 0 \end{cases} \tag{2}$$

where $\Delta I_i = I_i(t) - I_i(t-\Delta t)$, $I_i(t)$ is the current amplitude at time t for the i^{th} line, and Δt is the time window; and K_v is a constraint parameter used to reduce the proportional error and is equal to the composite error of the CT.

2) Decrement attribute A_D. This attribute is determined by the current data with a decreased amplitude as:

$$\begin{cases} A_D = \sum [-\Delta I_i - K_v I_i(t-\Delta t)] \\ -\Delta I_i > K_v I_i(t-\Delta t) \end{cases} \tag{3}$$

3) Constant attribute A_C. This attribute is used to reflect the steady-state characteristics. It is determined by the current data with an unchanged amplitude as:

$$\begin{cases} A_C = \sum I_i(t-\Delta t) \\ \left|\Delta I_i\right| \le K_v I_i(t-\Delta t) \end{cases} \tag{4}$$

In the aforementioned model, Δt should not be less than the transient time of the fault current to extract as much transient information as possible from the sampled data.

B. Definition, Optimization, and Verification of Self-set

1) Definition of Self-set

A self-set is composed of nonattack samples during various operations, including normal operation during internal and external faults. The self-sample is a sphere with a fixed radius. The normalized self-sample diameter should not exceed the composite error of the CTs for the optimization of the self-set. The coordinates of the sphere center are determined by the three characteristic attributes proposed in section III-A. Self-samples can be easily prepared through a simulation experiment. However, obtaining a perfect self-set for continuous sampling data is impossible. If the space of vacant self-samples, e. g., internal fault samples, is covered by detectors, the corresponding self-samples will be mistaken for attack data, which may cause delay in the operation of differential relay or even maloperations. To address this problem, the self-set is rearranged using an optimization al-

gorithm with the goal of covering the self-space as completely as possible with a minimum number of samples.

2) Optimization of Self-set

SSO is realized by performing multiple proliferation and inhibition operations on the sample set. If a sample set S_m exists prior to the m^{th} proliferation, then sample X_i and its nearest neighbor X_j, both of which belong to S_m, will determine a new sample X_n that satisfies:

$$\begin{cases} D(X_n,X_i)+D(X_n,X_j)=D(X_i,X_j) \\ D(X_i,X_j)\le D(X_i,X_k) \qquad X_k\in S \\ D(X_n,X_i)=0.5D(X_i,X_j) \\ D(X_i,X_j)\le 4R_s \end{cases} \tag{5}$$

where S is the current sample set; $D(\cdot)$ is the Euclidean distance between two data points with three dimensions (characteristic attributes); X_n is a new sample; and R_s is the radius of a self-sample.

An orthogonal mutation cloning strategy is considered to further enhance proliferation coverage. The variant of a new sample X_n is generated on a plane in which any vector is perpendicular to the vector $\boldsymbol{\eta}=\overrightarrow{X_iX_j}$. Let $\boldsymbol{\eta}=[a,b,c]$, where a, b, and c are coordinates, $\boldsymbol{u}=[b,a,0]^{\mathrm{T}}$, and $\boldsymbol{v}=\boldsymbol{\eta}\times\boldsymbol{u}$. Then, the variant coordinates are expressed as:

$$\boldsymbol{C}_n'=\boldsymbol{C}_n+\rho R_s\left(\frac{\boldsymbol{u}}{\|\boldsymbol{u}\|}\cos t+\frac{\boldsymbol{v}}{\|\boldsymbol{v}\|}\sin t\right) \tag{6}$$

where $\boldsymbol{C}_n$ is the coordinate of X_n; t is the time of mutation; and ρ is the probability of variation, which can be calculated by:

$$\rho=1/(p^2-1) \tag{7}$$

where p is the total number of samples intersecting X_n.

Inhibition operations are performed after the proliferation operations. For any three samples X_i, X_j, and X_k, if the Euclidean distance between any two samples is less than $2R_S$, the samples covered by the minimum sphere tangent to the triangle determined by the three samples can be deleted. Let the center of the minimum sphere be X_o; then, its radius r_o can be solved by:

$$\begin{cases} r_{\mathrm{o}}=\dfrac{\left|\overrightarrow{X_iX_o}\times\overrightarrow{X_iX_j}\right|}{\left|\overrightarrow{X_iX_j}\right|}=\dfrac{\left|\overrightarrow{X_jX_o}\times\overrightarrow{X_jX_k}\right|}{\left|\overrightarrow{X_jX_k}\right|}=\dfrac{\left|\overrightarrow{X_kX_o}\times\overrightarrow{X_kX_i}\right|}{\left|\overrightarrow{X_kX_i}\right|} \\ \begin{vmatrix} \overrightarrow{X_oX_i}\overrightarrow{X_oX_i} & \overrightarrow{X_oX_i}\overrightarrow{X_oX_j} & \overrightarrow{X_oX_i}\overrightarrow{X_oX_k} \\ \overrightarrow{X_oX_j}\overrightarrow{X_oX_i} & \overrightarrow{X_oX_j}\overrightarrow{X_oX_j} & \overrightarrow{X_oX_j}\overrightarrow{X_oX_k} \\ \overrightarrow{X_oX_k}\overrightarrow{X_oX_i} & \overrightarrow{X_oX_k}\overrightarrow{X_oX_j} & \overrightarrow{X_oX_k}\overrightarrow{X_oX_k} \end{vmatrix}=0 \end{cases} \tag{8}$$

The aforementioned proliferation and inhibition operations are executed alternately and terminated when a stable status is reached.

3) Verification of Self-set

For optimization, the self-set should be divided into three classes associated with normal operation, internal faults, and external faults. In the proliferation operation, new samples must be verified to avoid false negatives, which decrease the detection rate. In BDP, power-frequency fault components can be used to increase relay sensitivity. A common power-frequency fault-component-based differential protection criterion is expressed as:

$$\begin{cases} \left|\sum_{i=1}^{n}\Delta\dot{I}_i\right|>\Delta I_{set} \\ \left|\sum_{i=1}^{n}\Delta\dot{I}_i\right|>K'_{res}\sum_{i=1}^{n}\left|\Delta\dot{I}_i\right| \quad 0<K'_{res}<1 \end{cases} \tag{9}$$

where $\Delta\dot{I}_i$ is the power-frequency fault component of the current for the i^{th} line; ΔI_{set} is a set value that should be greater than or equal to the minimum line current at full load; and K'_{res} is the restraint coefficient of the power-frequency fault component.

Since $\left|\sum_{i=1}^{n}\Delta\dot{I}_i\right|=\left|A_I-A_D\right|$, (9) can be used to determine whether the samples are types of internal faults.

The sequence-component-based differential protection is not considered because the positive-, negative-, and zero-sequence components cannot be calculated based on the characteristic attributes.

According to (9), the judgment equations for an external fault and normal operation can be expressed as:

$$\begin{cases} \left|\sum_{i=1}^{n}\left|A_I-A_D\right|\right|>\Delta I_{set} \\ \left|\sum_{i=1}^{n}\left|A_I-A_D\right|\right|\le K'_{res}\sum_{i=1}^{n}\left|A_I-A_D\right| \end{cases} \tag{10}$$

$$\left|\sum_{i=1}^{n}\left|A_I-A_D\right|\right|\le\Delta I_{set} \tag{11}$$

C. Detector Generation

Detector generation can be implemented by using random generation algorithm, a genetic algorithm, or a deterministic algorithm. The random generation algorithm is simple but has difficulty in covering a narrow region due to blind generation, and the genetic algorithm is too complicated for a 3D model. The proposed SDD algorithm is a deterministic algorithm for generating spherical detectors. In this algorithm, each self-sample determines a set of detectors that are tangential to the outer surface of the self-sample. The tangency points are uniformly distributed on the surface of the self-sample to ensure the coverage in each direction. As shown in Fig. 2(a), 12 detectors exist, which are driven by the self-sample located at the bottom left of the shape space. The narrow region between the self-sample and the border of the shape space shows good coverage. The unique advantage of the proposed SDD algorithm is that the coverage rate of the nonself space increases with the number of self-samples. Figure 2(b) shows the distribution of detectors driven by two self-samples, which provide a larger coverage area than that driven by a single sample. The number of detectors increases with the number of self-samples. However, the available coverage increases with the number of detectors. Therefore, the proposed SDD algorithm can be used for complex self-structures.

According to the proposed SDD algorithm, the detector generation for a self-sample in 3D space includes the following three steps.

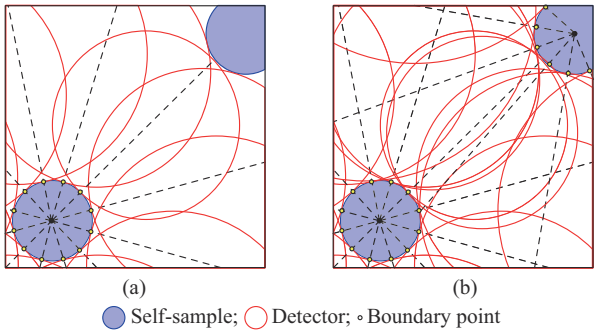


Fig. 2. Distribution of detectors. (a) Single-sample driven. (b) Two-sample driven.

Step 1: determine the boundary points of the detectors around the self-sample. First, randomly select a plane crossing the center of the self-sample, and then determine m boundary points with a rotation step of θ ($\theta=360/m$) on the circle section. Finally, rotate the m points around a local axis from 0° to 180° with a rotation step of θ.

Step 2: validate the self-tolerance. Eliminate the boundary points that fall in any self-sample. Checking all self-samples for a boundary point is not necessary because removable boundary points exist only at the intersections between the self-samples. Only samples close to the driven self-sample must be considered.

Step 3: solve the radius of the detector. Assume that the center and boundary point of a detector are X_c and X_b, respectively. Thus, the radius of the detector can be expressed as $r_d=D(X_c,X_b)$. The optimal radius of the detector is the maximum value when the detector remains outside the self-set. In other words, we can obtain:

$$\begin{cases} \max\ r_d=D(X_c,X_b) \\ \text{s.t. } D(X_c,X_b)+D(X_z,X_b)>R_s+r_d \quad \forall z\in S \\ \quad D(X_c,X_z)\ge D(X_c,X_b)+R_s \quad \forall z\in S \\ \quad D(X_c,X_b)+D(X_b,X_v)=D(X_v,X_c) \\ \quad \arccos\dfrac{\overrightarrow{X_vX_b}\,\overrightarrow{X_vX_z}}{\left|\overrightarrow{X_vX_b}\right|\left|\overrightarrow{X_vX_z}\right|}<\dfrac{\pi}{2} \\ \quad D(X_c,X_b)\le L_h \end{cases} \tag{12}$$

where X_z is the center of the reference sample z; S is the self-set; X_v is the center of the self-sample v on which X_b is generated; and L_h is the size of the data space.

With a blind search, the efficiency of the aforementioned model is very low for numerous samples, which is a common shortcoming of deterministic generation algorithms. Thus, we introduce a self-boundary heuristic (SBH) that uses the boundary information of historical records as the current search guide. We then define the subdomain model, i.e., the minimum grid cell of the data space, and the number is written as:

$$g=\varphi(x,y,z) \quad x,y,z\in W_g \tag{13}$$

where W_g is the data space set of subdomain g; (x,y,z) are 3D coordinates; and $\varphi(\cdot)$ is the mapping function that satisfies the following conditions.

$$\begin{cases} \varphi(x_1,y_1,z_1)\ne\varphi(x_2,y_2,z_2) \\ x_1,y_1,z_1\in W_i \\ x_2,y_2,z_2\in W_j \\ i\ne j \end{cases} \tag{14}$$

where W_i and W_j are the data space self of subdomains i and j, respectively.

The optimal reference sample of the boundary point of the self-sample is recorded in the corresponding number of subdomain models. The optimal reference sample model of boundary point b of self-sample v is:

$$\min\left\{\frac{D(X_v,X_z)}{2\cos<\overrightarrow{X_vX_b},\overrightarrow{X_vX_z}>}\right\}-R_s \quad z\in S \tag{15}$$

The solution process of the optimal detector based on SBH is shown in Fig. 3. For a given boundary point of the self-sample, the information about the reference sample in the corresponding subdomain is first examined, which usually becomes the current global optimal reference because it is the optimal information of the adjacent nodes. Even if it is not the optimal, the self-samples covered by the subdomain can be used as reference samples to solve the optimal detector.

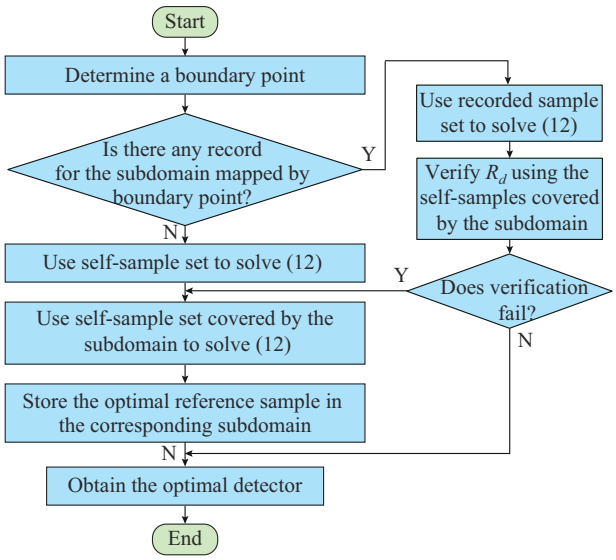


Fig. 3. Solution process of optimal detector based on SBH.

D. Detection of SV Attacks

In the detection of SV attacks, if an SV data point is covered by a detector, it is regarded as attack data. We used a grid-based detector searching algorithm to quickly find the matching detector. Figure 4 shows the grid model for detector searching. The node has 3D coordinates (x,y,z) that must have an integer index. The standardized characteristic attributes of the detector, which are usually less than 1 and more than 0, are mapped onto the grid space by multiplying by an integer that depends on the memory space. In the power system, each node stores the detectors that cover it.

The process of searching for a matched detector is as follows:

1) Convert the SV data into the characteristic attribute data and determine the coordinates in the power system.

2) Identify the node nearest the SV data coordinates as the center and sequentially search the memory detectors from the vertices of eight adjacent subcubes.

3) If the Euclidean distance between the data point and the center of the detector is less than the detector radius, the SV data are regarded as attack data.

The proposed matched detector searching algorithm employs mapping table technology. In the worst case, only 27 nodes must be checked for a data point.

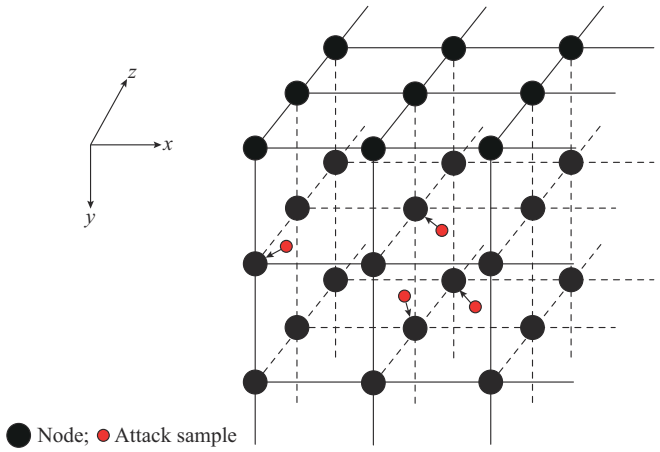


Fig. 4. Grid model for detector searching.

IV. Results

To verify the performance of the proposed NSA, we first conduct a comparison test on a benchmark dataset and then implement the NSA for double-bus protection. Finally, we build an online testbed to investigate the performance of the NSA by considering various conditions including normal operation, external faults, and internal faults.

A. Performance Comparison of Up-to-date NSAs on a Benchmark Dataset

The compared algorithms include the real-valued negative selection algorithm (RVNSA) [28], improved negative selection algorithm (INSA) [29], known nonself (KN) [30], and adaptive immunoregulation negative selection algorithm (AINSA) [31]. It is assumed that 40% of the nonself set is known and used for INSA and KN to optimize the detector distribution. The constant self-radius is 0.05 for the SDD, INSA, and KN. These algorithms all utilize the same self-set. Considering the data attribute characteristics of the BDP, Haberman's survival dataset [36] is selected for the test. The dataset contains 306 postoperative patient records, of which 225 survive, and the remaining 81 die. Each record includes three attributes as in the BDP data model. We define the data of dead and surviving patients as self (negative) and nonself (positive), respectively. Table I lists the true positive rates (TPRs) and false positive rates (FPRs) of each algorithm for 20% and 80% of the known self-set. When the known self-proportion is 20%, RVNSA has the smallest TPR (81.33%) due to random detector generation and INSA has the highest FPR (79.01%) because the self-coverage is not optimized. Our algorithm proves its superior in terms of self-repair and detector coverage and has the highest TPR (98.22%) and the lowest FPR (19.75%). When the known self-proportion is 80% (this case is similar to that of BDP), the FPR of SDD is 3.7%, which is still the smallest. However, the TPR is reduced to 96.89%, which is slightly lower than the AINSA value of 97.78%. This is due to the fact that when the self is sufficient, the proposed SSO technique will cause some self-data to invade the nonself area to a minimal extent. In addition, the self-verification is not used in this example because the self-verification algorithm proposed in this paper is only applicable to BDP. However, the proposed NSA still ensures that the FPR is as small as possible, which is critical to the reliability of relay protection.

TABLE I
Performance Comparison of Up-to-date NSAS on Haberman's Survival Dataset

Algorithm	20% of known self-set		80% of known self-set	
	TPR (%)	FPR (%)	TPR (%)	FPR (%)
SDD	98.22	19.75	96.89	3.70
RVNSA	81.33	38.27	84.89	7.41
INSA	86.22	79.01	86.22	17.28
KN	85.44	76.54	85.44	16.05
AINSA	97.33	28.40	97.78	6.17

B. Implementation of NSA for BDP

The test case is a 110 kV double busbar system, as shown in Fig. 5. For simplicity, in the simulation model, all feeders have the same maximum load current, and the total maximum load current is 1.2 kA. The differential protection of the double busbar consists of a large differential relay (LDR) and two small differential relays (SDRs) associated with bus bar 1 and busbar 2. For the LDR and SDRs, the minimum operation current threshold $I_{set,\min}$ is set to be 900 A, and the restraint coefficient K_{res} is 0.5. In the self-verification model, the power frequency fault component threshold ΔI_{set} is 67 A, and the restraint coefficient K'_{res} is 0.5. For the current measurement, it is assumed that all CTs have the same ratio of 600 A/5 A and a composite error of 5%. The sampling rate for relay protection is 2400 Hz.

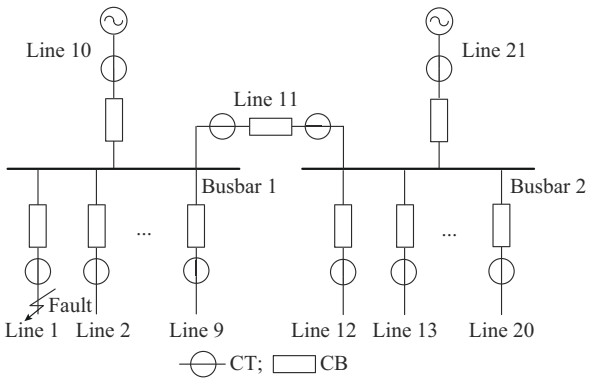


Fig. 5. 110 kV double busbar system.

In the proposed NSA, considering the composite error of the CT, the normalized self-radius is set to be 0.025, and the

rotation step is 30°. The time window Δt in the SV data model is a fundamental cycle. Characteristic attribute data are normalized using:

$$y = x/(x + I_{res,\max}) \tag{16}$$

where $I_{res,\max}$ is the maximum restraint current of differential relay under normal operation.

1) Preparation of Self-samples

Self-samples are selected from the recorded data of a power system based on a PSCAD simulation conducted at a sampling rate of 2400 Hz. The feeders adopt a stochastic load model that is evenly distributed between the two sources. The fault sample set mainly consists of various metallic short-circuit faults such as single-line-to-ground faults (1-LGF), double-line-to-ground faults (2-LGF), three-line-to-ground faults (3-LGF), and line-to-line faults (LLF). The sampling time for the fault samples spans from the moment of fault occurrence to the relay operation moment. In total, 5327 self-samples are prepared for the LDR and SDRs.

Figures 6-8 show the distributions of self-samples for normal operation, external faults, and internal faults, respectively. To illustrate the shapes more effectively, the self-samples are shown in several different colors. Many cracks can be observed in the original self-shape due to lack of samples associated with load current and various nonmetallic faults. Following SSO, the distribution of the self-samples is improved so that the mature detectors cannot enter the cracks.

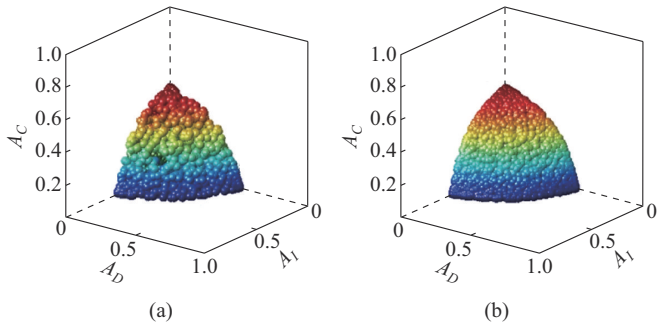


Fig. 6. Distributions of self-samples for normal operation. (a) Without SSO. (b) With SSO.

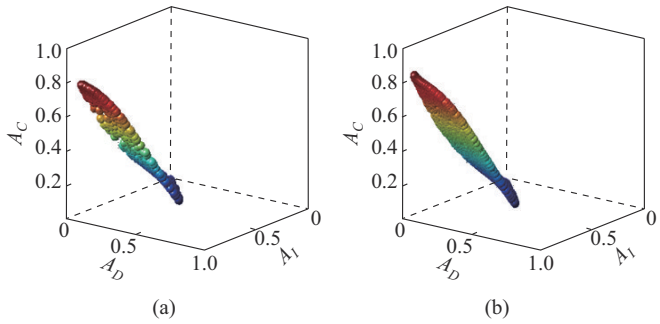


Fig. 7. Distributions of self-samples for external faults. (a) Without SSO. (b) With SSO.

2) Preparation of Attack Samples

According to the attack tree model, many possibilities exist for data attack against differential relay. We illustrate several types of data attacks that can be easily performed by attackers. However, our proposed algorithm can be applied to other attack types.

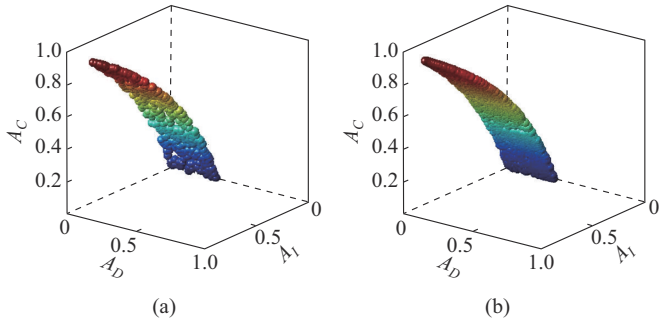


Fig. 8. Distributions of self-samples for internal faults. (a) Without SSO. (b) With SSO.

The SV attacks studied include the following six types:

Class 1 (C1): the MU corresponding to the CT on line 10 replays the SV data of the CT on line 10 for a 3-LGF on bus 1 during normal operation.

Class 2 (C2): the MU corresponding to the CT on line 11 replays the SV data of the CT on line 11 for an LLF on bus 2 during normal operation.

Class 3 (C3): the MU corresponding to the CT on line 9 replays the SV data of the CT on line 9 for a 1-LGF on line 9 during normal operation.

Class 4 (C4): the MU corresponding to the CT on line 11 reduces the line current to mimic a disconnection fault of the secondary circuit of the CT when a 1-LGF occurs on bus 2.

Class 5 (C5): the MU corresponding to the CT on line 11 modifies the current phase angle through a rotation of 180° when a 1-LGF occurs on bus 2.

Class 6 (C6): the MU corresponding to the CT on line 11 replays the saturation current data of the CT on line 11 when a 1-LGF occurs on bus 2.

Figure 9 shows the measurement data for SV attack. We fabricate 50 instances for each attack class based on a stochastic load model, in which the load current obeys a uniform distribution. In each instance, the attack current is injected at 0.02 s, and the samples are extracted from 0.02 s to 0.036 s at a sampling rate of 2400 Hz.

3) Detector Generation

In NSAs, generating a large number of detectors is typically time-consuming because each generated detector must undergo self-tolerance and be checked against the existing detectors to remove redundancies. To verify the performance of the proposed algorithm, the same initial self-set is used with other algorithms, including RVNSA [28], INSA [29], KN [30], and AINSA [31]. The average increment of each round of candidate detectors is 100, and the maximum number of detectors is 58292, which is the total number of detectors generated by the proposed algorithm. We use the attack sample set to check the nonself coverage rate of the detector generation algorithms at certain intervals. Figure 10 shows the curves of nonself coverage rate with the time for up-to-date NSAs on a 2.93 GHz computer. The proposed algorithm utilizes an SBH to guide optimal detector generation. The advantage is that it does not require many repeated

checks. Therefore, compared with other algorithms, it has a shorter computation time (99% nonself coverage in 13 s). Although many improvements have been made to NSAs, they are still based on random generation. In particular, KN also uses the existing attack samples (mature detectors) to generate candidate detectors, which helps speed up the algorithm, and the time to reach 99% nonself coverage is 212 s. However, due to lack of heuristic technology, the computing costs of the other three algorithms rise considerably as the number of detectors increases. As the number of detectors increases from 50000 to 58000, the computation cost for the verification is $\sum_{i=0}^{7999}(50000+i)(i+1)>1.6\times1012$. This redundant processing presents great challenges to the computer. However, BNSA also adds the detector movement operation, resulting in the lowest coverage index.

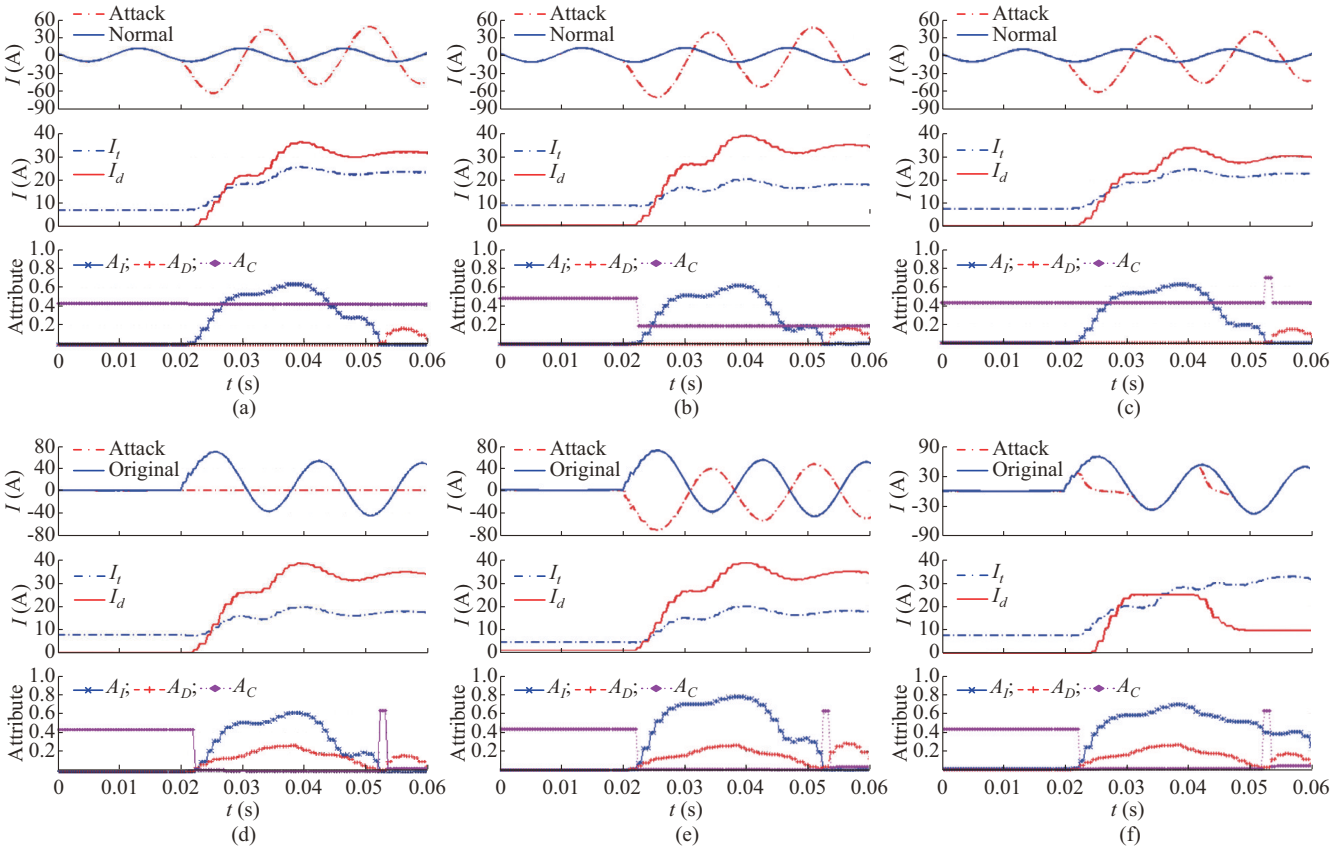


Fig. 9. Measurement data for SV attack. (a) C1. (b) C2. (c) C3. (d) C4. (e) C5. (f) C6.

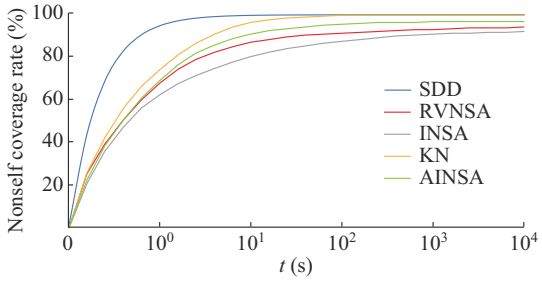


Fig. 10. Curves of nonself coverage rate with time for up-to-date NSAs.

C. Online Test

An online testbed based on a real-time digital simulator (RTDS) is established, as shown in Fig. 11, where GOOSE stands for generic object-oriented substation event. Networks 1 and 2 are constructed using a 100-Mbps Ethernet switch. All IEDs such as the protection device, MU, and CB are simulated using industrial computers with 2.93 GHz CPUs. The test algorithm involves modifying the SV messages from the RTDS with specific MUs and sending the messages to network 1, causing the protection IED to send tripping signals to the CB IEDs. The detection program for SV attacks is installed on the protection IED, which can generate a log file for detection and tripping events.

The performance of the detection algorithm is tested by investigating the action of the differential relays for busbar 1 under SV attacks during normal operation and external faults and the effects on protection during internal faults. To verify the advantages of the proposed algorithm, common algorithms including CNN [21], CPMA [20], and SVM [19] as well as a V-detector-based improved NSA (KN [30]) are used for comparison. To ensure the fairness, under normal operation and external fault experiments, all algorithms use the same original measurement data. KN has the same self-radius and number of detectors with SDD and has 99% coverage by training. For the other three algorithms, all prepared attack samples are used for training.

Figure 12 shows the normal operation under SV attacks. The output of the detection program should be SV attacks or

nonattacks. For the SV attack, the protection operation will be blocked for a time of $3/f$, where f is the sampling rate, and the fault counter will be reset to be zero. If the relay is not locked, the tripping signals are sent when three successive fault samples that satisfy (1) are detected.

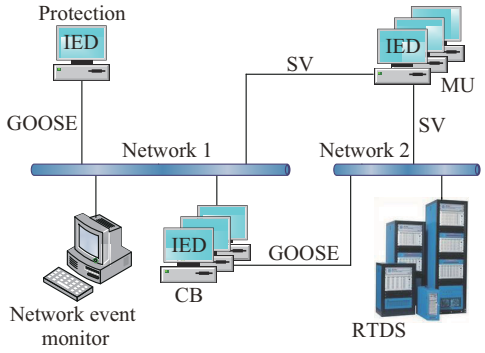


Fig. 11. Online testbed for SV attack detection.

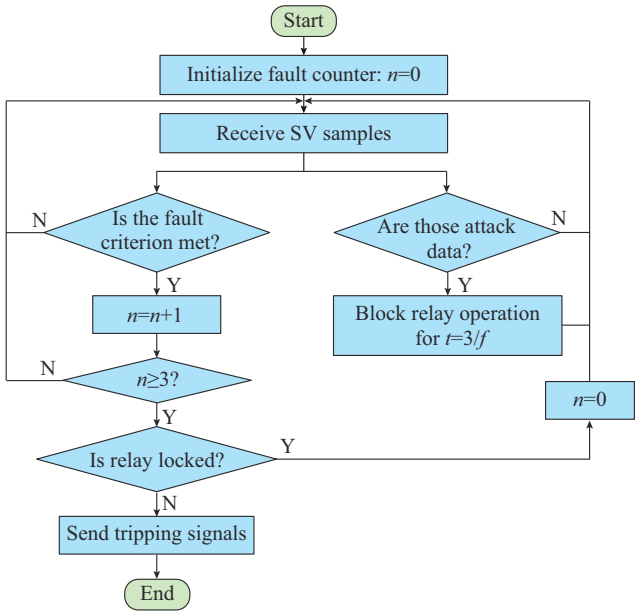


Fig. 12. Normal operation under SV attacks.

1) Normal Operation Under SV Attacks

Under normal operation, the maloperation rates under SV attacks are shown in Fig. 13. With a low load, the detection performance of the KN is the worst because of the poor boundary coverage, and the maximum maloperation rates of the LDR and SDR appearing under the no-load condition, i.e., the boundary point, are 23.4% and 23.4%, respectively. In addition, as the boundary coverage is greatly enhanced, the maloperation rates of the LDR and SDR provided by SDD are 13.2% and 13.4%, respectively, which are slightly higher than those of the other learning algorithms. However, when the load is relatively high, e.g., greater than 10%, SDD exhibits the best performance in reducing the maloperation rates for the two relays. Because traditional learning algorithms are essentially based on the principle of similarity, their performance is not affected by the load, and fluctuations in maloperation rates are relatively small. Table II shows the average TPRs and FNRs of the LDR and SDR for each algorithm. In this paper, TPR denotes the detection rate, which is equal to the ratio of detected attack instances to total attack instances. Thus, FNR is the maloperation rate of the differential relays. For the LDR, the lowest average maloperation rate provided by SDD is 7.42%, and the average maloperation rates by the other algorithms are greater than 8%. Similar results are obtained for the SDR.

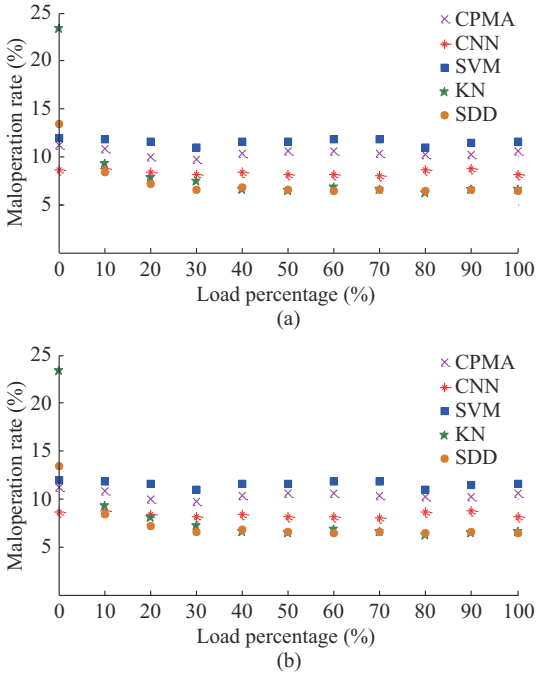


Fig. 13. Maloperation rates under SV attacks. (a) LDR. (b) SDR.

TABLE II
AVERAGE TPRS AND FNRS OF LDR AND SDR FOR EACH ALGORITHMS

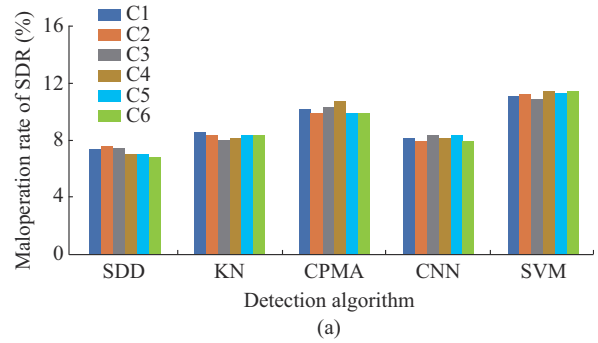
Algorithm	LDR		SDR	
	TPR (%)	FNR (%)	TPR (%)	FNR (%)
CPMA	89.58	10.42	89.56	10.44
CNN	91.51	8.49	91.60	8.40
SVM	88.47	11.53	88.44	11.56
KN	91.49	8.51	91.51	8.49
SDD	92.58	7.42	92.60	7.40

It should be noted that the aforementioned results rely on the known training samples. In fact, BDP may encounter unknown attacks, which should be the focus of our study. Figure 14 shows the maloperation rates of SDR for various detection algorithms with and without the training by the corresponding attack samples. Only the results of the SDR are provided because of the similarity of the results of the two relays. Without training, the performances of CNN, CPMA, and SVM significantly decrease. In particular, for C5, the maloperation rates for CPMA, CNN, and SVM are 85.2%, 80.6%, and 81.6%, respectively. In contrast to C5, the other attack classes show some similarities that can compensate for insufficient training samples. For example, CT saturation, disconnection line, and current amplitude reduction show

similar current amplitude variations. Thus, when only C2 is learned, the attacks with C4 and C6 can be detected with a certain probability.

2) External Faults Under SV Attacks

Currently, the maloperation of the differential current relay caused by the secondary circuit disconnection of CT or core saturation during the external faults may occur. Thus, investigating the defense against the attacks with C4 and C6 on external faults is of great significance. In this experiment, the external fault is set at point *f* on line 1 close to busbar 1. And for each type of fault, the number of C4 instances is 11, which is related to the disconnection of phase A CTs on the lines connected to busbar 1. The number of C6 instances is 50, corresponding to different saturation degrees of CT for line 1. Table III lists the maloperation rates of the SDR under SV attacks during external faults. For the secondary circuit disconnection of CT, all algorithms can block the protection operation, whereas for CT saturation, the learning algorithms including CNN, CPMA, and SVM fail. In this paper, all detection algorithms are based on the fundamental root mean square of the current, which cannot fully reflect the CT saturation characteristics such as the inrush harmonic component or waveform feature. Therefore, even after sufficient training, the learning algorithms cannot distinguish SV attacks from CT saturation.



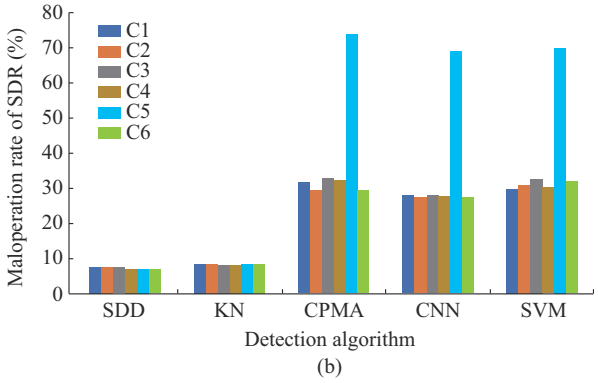


Fig. 14. Maloperation rates of SDR for various detection algorithms. (a) With training. (b) Without training.

The average maloperation rates provided by the CNN, CPMA, and SVM are 71%, 53%, and 67%, respectively. In contrast to normal operation, CT saturation during external faults is very similar to internal faults for differential relay. Therefore, the learning algorithms may regard SV attacks as internal faults, which reduces the detection performance. In the absence of training, the average maloperation rates provided by the learning algorithms reach 90% or higher, whereas for SDD and KN, differential relay remains silent. Regarding the surface area of the self, the external fault is smaller than that of the normal operation, which means that the probability of the boundary effect is smaller. Thus, the immune algorithms perform better against external attacks.

TABLE III
MALOPERATION RATES OF SDR UNDER SV ATTACKS DURING EXTERNAL FAULTS

Algorithm	Training or not	Attack class	Maloperation rate (%)			
			1-LGF	2-LGF	LLF	3-LGF
SDD	Yes	C4	0	0	0	0
		C6	0	0	0	0
	No	C4	0	0	0	0
		C6	0	0	0	0
KN	Yes	C4	0	0	0	0
		C6	0	0	0	0
	No	C4	0	0	0	0
		C6	0	0	0	0
CNN	Yes	C4	0	0	0	0
		C6	68	72	70	72
	No	C4	0	0	0	0
		C6	90	96	92	94
CPMA	Yes	C4	0	0	0	0
		C6	52	50	52	56
	No	C4	0	0	0	0
		C6	92	96	94	92
SVM	Yes	C4	0	0	0	0
		C6	66	64	68	68
	No	C4	0	0	0	0
		C6	94	98	96	96

The aforementioned results show that the detection performance of learning algorithms for unknown attacks will be greatly reduced due to the absence of training, whereas that of immune algorithms is not affected. In addition, to detect the attacks with complex characteristics, learning algorithms underperform compared with the proposed algorithm because of the limitations of the data model.

3) Internal Faults with SV Attack Detection

To investigate the influence of the detection algorithm on the protection operation, many simulations with differential protection for various faults on busbar 1 have been previously conducted. The FPR can reflect the failure rate of a relay and is defined as the ratio of the number of internal fault instances detected as an attack to the total number of internal fault instances. Table IV shows the FPRs of each algorithm for SDR during bus faults. The FPRs provided by SDD and KN with SSO are higher than those provided by the other three algorithms at the same sampling rate. However, when SSO is not adopted, the NSAs will perform poorly. For example, at a sampling rate of 4800 Hz, the FPRs derived

from SDD and KN are 10.58% and 10.46%, respectively, whereas those of the other three algorithms are lower than 6%.

TABLE IV
FPRs Provided by Each Algorithm for SDR During Bus Fault

Algorithm	Adopt SSO or not	FPR (%)		
		f=1200 Hz	f=2400 Hz	f=4800 Hz
SDD	Yes	3.69	3.82	4.02
	No	10.44	10.51	10.58
KN	Yes	3.69	3.81	4.02
	No	10.19	10.35	10.46
CNN		4.83	4.96	5.12
CPMA		5.17	5.28	5.29
SVM		5.36	5.54	5.82

In the case of busbar faults, false positives in SV samples will cause protection action delays. In Fig. 15, the tripping signal delay caused by NSA without an SSO is shown when a 1-LGF occurs on busbar 1. The 1st, 4th, 5th, 6th, and 8th fault samples are identified as the attack data. Because the relay will be blocked for three sampling intervals when detecting an attack sample, the blocking signals retain 10 sampling intervals. The tripping signals are not presented until three successive fault samples are detected. Therefore, the total operation delay of the SDR is 13 sampling intervals (approximately 2.7 ms for a sampling rate of 4800 Hz). In other algorithms, increased protection operation delays are also observed. We test the maximum protection operation delays of the SDR, as shown in Table V. For each algorithm, the delays of relay operation for LLF are higher than those for 1-LGF, and increased sampling rates lead to decreased delays in the relay operation. The worst case for the immune algorithms appears at a sampling rate of 1200 Hz for the three LGFs when the delay of the relay operation provided by SDD is 9.21 ms. By contrast, the delays provided by the other three learning algorithms are less than half a cycle (8.33 ms). In the case of an incomplete self-set, the detectors generated by the NSA tend to cover the missing internal fault samples, which cause the proposed algorithm to underperform compared with the learning algorithms. With the help of the SSO, the relay operation delays provided by the SDD and KN are greatly reduced. With the 1-LGF taken as an example, at a sampling rate of 1200 Hz, the maximum operation delay of the relay using SDD is 1.72 ms (reduced by 66%), which is determined by the normal samples (close to the threshold of the differential relay operation) that are regarded as the SV attacks according to the condition of the operation and prevention of differential relay. Whereas the maximum operation delays provided by CNN, CPMA, and SVM are 3.34, 4.17, and 5.02 ms, respectively, which are three times greater than the sampling interval and are therefore caused by the internal fault samples regarded as SV attacks. At a sampling rate of 1200 Hz, SDD and KN show nearly the same operation delays for various faults. However, at the other sampling rates, SDD still provides greater relay operation delays. One reason for this is that the detectors generated by the SDD cover the self-samples of normal operation that have not been recovered. In fact, the adoption of SSO to detect SV attacks of the BDP is risky. In this paper, to improve the detection performance of SV attacks, the optimized self does not cross the actual boundary between self and nonself, which is a conservative strategy. In other words, if the self exceeds the actual boundary, the relay operation delays will decrease as the maloperation rate of the protective relays increases.

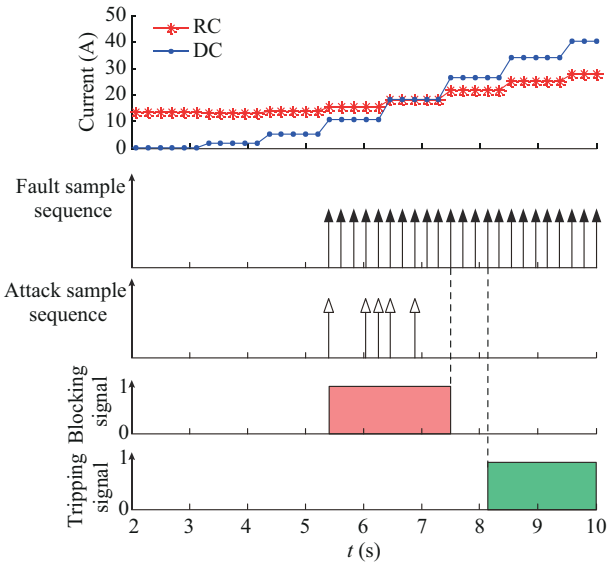


Fig. 15. Recording data of SDR with SDD at a sampling rate of 4800 Hz.

TABLE V
The Maximum Operation Delay of SDR for Each Algorithm

Algorithm	Adopt SSO or not	The maximum operation delays of SDR (ms)											
		f=1200 Hz				f=2400 Hz				f=4800 Hz			
		1-LGF	2-LGF	LLF	3-LGF	1-LGF	2-LGF	LLF	3-LGF	1-LGF	2-LGF	LLF	3-LGF
SDD	Yes	1.73	2.54	2.55	3.37	1.72	2.56	2.56	2.98	0.48	1.11	1.10	1.31
	No	5.06	8.41	8.42	9.21	3.81	7.11	7.11	7.95	3.18	4.43	4.42	7.01
KN	Yes	1.72	2.56	2.55	3.37	1.31	2.14	2.14	2.56	0.27	0.89	0.89	1.10
	No	4.24	7.53	7.54	8.35	2.98	5.47	5.46	7.14	2.35	4.01	4.01	6.52
CNN		3.34	4.17	4.17	5.01	2.12	2.94	2.94	3.35	1.49	2.32	2.32	2.73
CPMA		4.17	5.01	5.01	5.84	2.95	3.77	3.77	4.52	1.69	3.14	3.14	3.35
SVM		5.02	5.85	5.85	6.68	3.35	4.59	4.59	5.01	2.52	3.97	3.97	4.18

V. Conclusion

Identifying SV attacks of BDP is difficult because of high dimensionality. In this paper, a detection algorithm based on an NSA is developed to identify SV attacks of BDP. Two improvements are proposed: ① recovering the self-data of differential relay using shape-space optimization algorithm; and ② generating the detectors by self-driven algorithm to enhance the boundary coverage. Compared with up-to-date NSAs, our detector generation algorithm has a shorter computation time and higher nonself coverage. The online test results show that the traditional learning algorithms suffer from a decreased detection performance due to lack of training samples, whereas the performance of SDD is not affected by training samples. Therefore, our detection algorithm has great potential for detecting unknown SV attacks of BDP. Compared with fully trained learning algorithms, the proposed algorithm also has some advantages. For example, during normal operation, when the load is not too small, SDD exhibits stronger performance in preventing a differential relay operation. For busbar faults, the delays of differential relay operation using SDD and KN are significantly higher than those of the learning algorithms, indicating that NSAs are still deficient in distinguishing busbar faults from SV attacks. After SSO, the delays of the differential relay operation are greatly reduced, and SDD outperforms the traditional learning algorithms. However, compared with KN, the delays of differential relay operation are still slightly higher. The comparison between SDD and KN proves that the detection performance of SV attacks is improved and the conflict for the delays of differential relay operation is reduced. To ensure the rapid action of BDP, developing an optimization scheme is necessary, which aims at the maximum detection rate of SV attacks and is constrained by differential relay operation delays. The development of this type of scheme is the future research goal.

References

[1] O. Kosut, L. Jia, R. J. Thomas *et al*., "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[2] X. Yu and Y. Xue, "Smart grids: a cyber-physical systems perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016.

[3] J. Yang, C. Zhou, and S. Yang, "Anomaly detection based on zone partition for security protection of industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4257-4267, May 2018.

[4] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389-1407, Jul. 2017.

[5] C. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[6] J. Gao, J. Liu, B. Rajan *et al*., "SCADA communication and security issues," *Security and Communication Networks*, vol. 7, no. 1, pp. 175-194, Jan. 2014.

[7] Y. Yang, K. McLaughlin, S. Sezer *et al*., "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092-1102, Jun. 2014.

[8] S. Soltan, M. Yannakakis, and G. Zussman, "Power grid state estimation following a joint cyber and physical attack," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 499-512, Mar. 2018.

[9] A. Alireza, S. Arman, and F. Parisa, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951-7962, Sept. 2020.

[10] V. S. Rajkumar, M. Tealane, A. Ştefanov *et al*., "Cyber attacks on power system automation and protection and impact analysis," in *Proceedings of IEEE PES Innovative Smart Grid Technologies Europe*, Hague, Netherlands, Oct. 2020, pp. 247-254

[11] X. Liu, M. Shahidehpoer, Z. Li *et al*., "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 572-580, Mar. 2017.

[12] R. Bulbul, Y. Gong, C. Ten *et al*., "Impact quantification of hypothesized attack scenarios on bus differential relays," in *Proceedings of Power Systems Computation conference*, Wroclaw, Poland, Aug. 2014, pp. 1-7.

[13] P. Wang, A. Ashok, and M. Govindarasu, "Cyber-physical risk assessment for smart grid system protection scheme," in *Proceedings of IEEE PES General Meeting*, Denver, USA, Jul. 2015, pp. 1-5.

[14] F. Wang, H. Wang, D. Chen *et al*., "Substation communication security research based on hybrid encryption of DES and RSA," in *Proceedings of 9th IEEE Intelligent Information Hiding and Multimedia Signal Processing*, Beijing, China, Jul. 2014, pp. 437-441.

[15] J. Hong, C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643-1653, Jul. 2014

[16] S. Sheng, W. Chan, K. Li *et al*., "Context information-based cyber security defense of protection system," *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1477-1481, Jul. 2007.

[17] K. J. Ross, K. M. Hopkinson, and M. Pachter, "Using a distributed agent-based communication enabled special protection system to enhance smart grid security," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 1216-1224, Jun. 2013.

[18] M. S. Rahman, A. M. T. Oo, M. A. Mahmud *et al*., "A multi-agent approach for security of future power grid protection systems," in *Proceedings of IEEE PES General Meeting*, Boston, USA, Nov. 2016, pp. 17-21.

[19] M. S. Rahman, M. A. Mahumd, A. M. T. Oo *et al*., "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 436-447, Apr. 2017.

[20] A. Ameli, A. Hooshyar, E. F. El-Saadany *et al*., "An intrusion detection method for line current differential relays," *IEEE Transactions on Information and Forensics and Security*, vol. 15, pp. 329-344, May 2019.

[21] V. Dave and A. Sharma, "Operation of differential relay for power transformer using support vector machine," in *Proceedings of IEEE PES Transmission & Distribution Conference & Exposition*, Chicago, USA, May 2008, pp.1-8.

[22] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104-3113, Nov. 2015.

[23] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *International Journal of Electrical Power and Energy Systems*, vol. 107, pp. 690-702, May 2019.

[24] H. Xiong and C. Sun, "Artificial immune network classification algorithm for fault diagnosis of power transformer," *IEEE Transactions on Power Delivery*, vol. 22, no. 2, pp. 930-935, Apr. 2007.

[25] W. Tang, X. Yang, X. Xie *et al*., "Avidity-model based clonal selection algorithm for network intrusion detection," in *Proceedings of 18th IEEE International Workshop on Quality of Service*, Beijing, China, Aug. 2010, pp. 1-5.

[26] E. Alizadeh, N. Meskin, and K. Khorasani, "A negative selection immune system inspired methodology for fault diagnosis of wind turbines," *IEEE Transactions on Cybernetics*, vol. 47, no. 11, pp. 3788-3813, Nov. 2017.

[27] D. Dasguptaa, S. Yua, and F. Ninob, "Recent advances in artificial immune systems: models and applications," *Applied Soft Computing*, vol. 11, no. 2, pp.1574-1587, Mar. 2011.

[28] F. Selahshoor, H. Jazayeriy, and H. Omranpour, "Intrusion detection systems using real-valued negative selection algorithm with optimized detectors," in *Proceedings of 5th Iranian Conference on Signal Processing and Intelligent Systems*, Shahrood, Iran, Dec. 2019, pp. 1-5.

[29] Y. Ren, X. Wang, and C. Zhang, "A novel fault diagnosis method based on improved negative selection algorithm," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1-8, Oct. 2020

[30] Z. Li and T. Li, "Using known nonself samples to improve negative selection algorithm," *Applied Intelligence*, doi: 10.1007/s10489-021-02323-4

[31] H. Deng and T. Yang, "A negative selection algorithm based on adaptive immunoregulation," in *Proceedings of 5th International Conference on Computational Intelligence and Applications*, Beijing, China, Jun. 2020, pp. 177-182.

[32] H. Alrubayyi, G. Goteng, M. Jaber *et al*., "A novel negative and positive selection algorithm to detect unknown malware in the IoT," In *Proceedings of IEEE Conference on Computer Communications Workshops*, Vancouver, Canada, May 2021, pp. 1-6.

[33] S. Forrest, A. S. Perelson, L. Allen *et al*., "Self-nonself discrimination in a computer," in *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, USA, May 1994, pp. 202-212.

[34] J. Zhou and D. Dasgupta, "V-detector: an efficient negative selection algorithm with 'probably adequate' detector coverage," *Information Sciences*, vol. 179, no. 10, pp. 1390-1406, Apr. 2009.

[35] J. Zhou, "A boundary-aware negative selection algorithm," in *Proceedings of 9th IASTED International Conference on Artificial Intelligence and Soft Computing*, Benidorm, Spain, Sept. 2005, pp. 12-14.

[36] Lim T-S. (2021, Jan.). Haberman's survival data set, UCI machine learning repository. [Online]. Available: https://archive-beta.ics.uci.edu/ml/datasets/haberman+s+survival

Jun Mo received the B.Sc. and Ph.D. degrees from the School of Electrical Engineering, Guangxi University, Nanning, China, in 2006 and 2014, respectively. Currently, he is an Assistant Professor at the School of Electrical Engineering, Guangxi University. His current research interests include power system protection, electricity markets, and renewable energy systems.

Hui Yang received the B.S degree from Liren College of the Yanshan University, Qinhuangdao, Hebei, China, in 2019. He is currently pursuing the M. S degree at the School of Electrical Engineering, Guangxi University, Nanning, China. His current research interests include power system reliability analysis, electricity markets, evolutionary game theory, and random mutation theory.