

Attack Sample Generation Algorithm Based on Dual Discriminant Model in Industrial Control System

Wen Zhou¹, Xueying Cao², Xiaoming Li¹, Yun Sha²*, Jianping Chen², Yong Yan², Xuejun Liu², and Xiangmin Kong²

¹ Information technology and network security research and development center of China Aviation Oil Group Co., Ltd., 2 Madian Road, Haidian District, Beijing, China
² Beijing Institute of Petrochemical Technology College of Information Engineering Shayun, 19 Qingyuan North Road, Daxing District, Beijing, China

*E-mail: shayun@bipt.edu.cn

Abstract. The research of intrusion anomaly detection in industrial control system is facing the problem of few attack samples. This paper proposes an attack data sample generation algorithm based on dual discriminant model. Firstly, a few attack samples are generated by multiple attacks based on the original data set. Secondly, the sparse matrix algorithm is used to expand the data set, and the original data features are distributed to each extended data to ensure the authenticity of the seed data. Finally, a large number of attack samples are generated by the dual discriminant model to complete the sample expansion. The experimental results of Mississippi SCADA natural gas pipeline data set and an industrial control system data set show that, based on keeping the data in a reasonable range, the algorithm can obtain an effectively expanded sample data set. SVM, Random Forest and XGBOOST are used to classify the dataset. The results show that AUC index is better than the negative sample data set generated by traditional GAN algorithm, and is similar to the initial negative sample index.

1. Introduction

More and more industrial control systems and equipment access to the Internet, industrial control systems are facing greater security challenges. The traditional intrusion detection system mainly focuses on the network intrusion protection level, which can not meet the current requirements. Once the firewall is broken, the intruder directly enters the business layer to tamper with the business data, which will cause huge losses. The abnormal detection of industrial operation data is mainly used to identify the abnormal data during operation, which is the last defense line of safety. In 2010, Iran's "seismic network" virus directly manipulated the SCADA system after it invading the nuclear facilities, causing damage to several nuclear centrifuges [1]. According to the white paper on industrial control network situation in 2018 [2], the number of industrial control vulnerabilities has increased significantly after 2010. In 2018, Siemens PLC, SCADA and other industrial control systems exposed two high-risk vulnerabilities, and the U.S. power grid, nuclear power plant and water supply facilities were attacked, which caused huge losses and had a wide impact. Therefore, it is very important to establish an efficient and high-quality attack sample generation method for anomaly detection of underlying business data in industrial control system.

In the active fields of artificial intelligence applications, such as machine vision, natural language processing, etc., the source of negative samples is manually labeled images or text. However, most of
the data in the field of industrial control in the normal operation of safety production are positive samples, and negative samples can only be generated based on business data analysis. For example, the pressure value in the industrial control system is tampered with (from high to low), and there is no alarm when the alarm should have been given, which may lead to system shutdown, parts failure and even explosion and other serious consequences.

According to incomplete statistics, there are more than 30 kinds of data sets related to industrial control. One of the main intrusion attacks is against general protocol and server. However, there are very few negative samples to attack the underlying business data, which seriously limits the development of anomaly detection algorithms for underlying business data. At present, the existing negative sample sets for bottom business are: c-town water distribution data set based on model method and network packet capture proposed by network security research center of Singapore University of science and technology [3], and SCADA natural gas pipeline data set proposed by key infrastructure protection center of Mississippi State University in 2014 [4], which simulate actual attacks and operations on natural gas pipelines Member activities generate data. However, the domestic data set in this area is extremely scarce, so the generation method of attack samples for underlying business data is an urgent problem to be solved.

Attack sample generation in industrial control can be roughly divided into three types: deviation attack, surge attack and geometric attack [5]. Different data in industrial control system have different consequences after being attacked, which needs to be analyzed according to its business. Therefore, the attack method mentioned above should be rooted in the business analysis of industrial control data. A part of negative samples can be generated manually by business analysis, and a certain scale of negative samples need to be generated by algorithm.

This paper is based on a small number of negative samples of public data set and a small number of negative samples generated by manual in an industrial control system data set. According to the sample set, the sparse matrix is generated, and then the matrix is filled on the basis of matrix UV decomposition to complete the first step of negative sample expansion, and the initial expansion of negative sample set is obtained. Then, based on the generative confrontation network of dual discriminant model, the second step expansion is carried out to obtain a large number of negative sample data sets.

2. Generative Adversarial Network

For the technology of sample generation, in addition to all kinds of negative samples mentioned above, generative adversarial network is the current technology hotspot of sample generation. The principle of adversarial attack is to cheat the deep neural network through the adversarial sample, so that it can make a wrong decision.

The concept of adversarial sample was proposed by Christian Szegedy [6]. It refers to the input sample formed by deliberately adding subtle interference in the original data set, resulting in the model giving a wrong output with high confidence. Under the background of regularization, the error rate of the original independent and identically distributed test set is reduced by adversarial training, and the network is trained on the anti disturbance training set samples. Antagonism refers to the degree to which the original classifier is confused by the adversarial samples, which can be measured by the accuracy of the classifier. The generation steps are shown in Figure 1.

![Figure 1. Schematic diagram of adversarial sample generation method.](image-url)
Although the existing GAN generation methods have made great progress, there are still deficiencies in practical application, especially in the field of industrial control. According to the attack types, the generating algorithms of generative adversarial can be divided into two categories: 1). White box; 2). Black box. The commonly used white box method is: L_BFGS [7], this method requires that the gradient of model and objective function can be solved; JSMA algorithm [8], model and objective function require gradient solvable; DE [9] algorithm, only for single pixel adversarial sample problem; FGS algorithm [10], although fast, but the similarity of confrontation samples is not very high. The typical representative of black box method is MalGAN [11]. The algorithm emphasizes the accuracy of the whole sample set, and does not care about the similarity of individual samples. Table 1 shows the comparison of the above five methods.

| Method | Attack type | Similarity calculation | Application area | Limitations |
|--------|-------------|------------------------|------------------|-------------|
| L-BFGS | White box   | L2                     | image            | It is required that the gradient of the model and objective function can be solved |
| JSMA   | White box   | L0                     | image            | It is required that the gradient of the model and objective function can be solved |
| DE     | White box   | L0                     | image            | Only for single pixel adversarial sample problem |
| FGS    | White box   | L∞                     | image            | Fast but the similarity of the generated anti sample is not the highest |
| MalGAN | Black box   | TPR                    | malicious software | It emphasizes the accuracy of the whole sample set, but does not care about the similarity of individual samples |

3. Algorithm Principle
In this paper, an attack sample generation method for industrial control business data set is proposed when there are few attack samples in industrial control system. The specific steps are as follows:

- Positive sample is extracted from business data set to form positive sample data set;
- According to the business requirements, attack the positive sample data set. For example, tampering with the pipe pressure (from large to small) will inhibit the effectiveness of the pressure maintaining system, thus causing danger. Here, the attack sample set generated manually according to the service characteristics is called the initial negative sample set;
- In order to generate more initial negative sample data, after the initial negative sample data is generated into the matrix, it is sparse, that is, each element in the matrix is placed in the same column but not in the same row, so as to generate a sparse matrix;
- SGD method is used to fill the sparse matrix to generate the initial attack sample matrix. Each row of the matrix is taken as a sample to generate the extended negative sample set;
- Based on the positive sample set and the extended negative sample set, the final negative sample set is generated by the generative adversarial network based on the dual discriminant model. The flow chart of algorithm steps is shown in Figure 2, in which the key steps are pre-attack sample expansion and dual discrimination model training.
Positive sample is extracted from business data set to form positive sample data set

Attack the positive sample data set and generate the pre attack sample data set

The sparse matrix of pre attack samples is formed by sparse processing of pre attack sample data set

The sparse matrix of pre attack samples is filled to form the initial attack sample data set

Based on the initial attack sample data set, a generative countermeasure network based on double discriminant model is used to form the attack sample generation model

Call attack sample generation model to generate attack sample data set

**Figure 2.** Flow chart of attack sample generation based on dual discriminant model.

### 3.1. Preliminary Expansion of Sparse Matrix

The extended negative sample set is generated by filling the sparse moments formed by the initial negative sample set. The filling method of sparse matrix is based on UV principle of matrix decomposition [12] and SGD method is used.

Let the sparse matrix be generated by multiplying the sum of two vectors, and then iterate based on SGD optimization method to get the sparse value. This step is mainly to expand the initial negative sample set, so as to make the expanded pre attack samples more reasonable.

Let $p_u$ and $q_i$ be the $u$-th and $i$-th components of vectors $P$ and $Q$, respectively, and $r_{ui}$ is the element value of the $u$-th row and $i$-th column of the matrix $R$. For all $u$ and $i$, the following conditions are satisfied:

$$r_{ui} = p_u \times q_i \quad \text{(1)}$$

The constraint conditions are satisfied:

$$\min \sum_{r_{ui} \in R} (r_{ui} - p_u \times q_i)^2 \quad \text{(2)}$$

For formula (2), calculate the partial derivatives of $p_u$ and $q_i$, respectively:

$$\frac{\partial f_{ui}}{\partial p_u} = \frac{\partial}{\partial p_u} (r_{ui} - p_u \times q_i)^2 = -2q_i(r_{ui} - p_u \times q_i) \quad \text{(3)}$$

$$\frac{\partial f_{ui}}{\partial q_i} = \frac{\partial}{\partial q_i} (r_{ui} - p_u \times q_i)^2 = -2p_u(r_{ui} - p_u \times q_i) \quad \text{(4)}$$

The process of SGD optimization method is as follows:
• All \( p_u \) and \( q_i \) are initialized randomly;
• Repeat the following steps for a given number of times.

For all known \( r_{ui} \), repeat the following steps:
Update \( p_u \) and \( q_i \):
\[
p_u = p_u + \alpha \times q_i (r_{ui} - p_u \times q_i) \tag{5}
\]
\[
q_i = q_i + \alpha \times p_u (r_{ui} - p_u \times q_i) \tag{6}
\]
where \( \alpha \) is the learning rate.

At the end of the iteration, \( p_u \) and \( q_i \) are obtained, and the value of the sparse position is obtained. The initial attack sample data set is obtained.

3.2. Generative Adversarial Network Model Based on Dual Discriminant Model
Based on the preliminary expansion of negative sample data set, a generative adversarial algorithm based on dual discriminant model is proposed to generate large scale negative sample set. Different from the traditional generative adversarial network, in order to make the generated negative samples in a reasonable range, the algorithm makes full use of the existing positive samples and extended negative samples, and satisfies two conditions in the iterative process: 1. Ensure that the generated samples have certain intrusion ability; 2. Be similar to the current negative samples. The model modifies the attack discrimination model of generative adversarial samples and adds an intrusion discrimination model.

3.2.1 Attack Discrimination Model. The attack discrimination model is called \( F \). On the basis of learning positive samples, \( F \) makes the generated attack samples become more real attack samples. It needs two constraints:
• The loss rate of the positive sample needs to be minimized, as shown in formula (7):
\[
\min(L(F(x), y)) \tag{7}
\]
where \( x, y \) denote the extended negative sample and its label.
• The loss rate of negative samples generated needs to be maximized. Since it is very difficult to maximize a certain data, the logarithm of the attack sample is taken and a negative sign is added. In this way, the problem becomes a minimum value that is easier to solve. See formula (8):
\[
\min(-\log(L(F(x^\ast), y^\ast))) \tag{8}
\]
where \( x^\ast \) and \( y^\ast \) are pre-attack samples and their labels. In order to ensure that the order of magnitude of the positive sample data is consistent with that of the attack sample, the logarithm of formula (8) is also required, as shown in formula (9):
\[
\min(\log(L(F(x), y))) \tag{9}
\]

3.2.2 Intrusion Discrimination Model. In order to ensure that the negative samples generated have certain invasiveness, an intrusion discrimination model \( R \) is designed to help the newly generated attack samples to "cheat" the discrimination model and make them look like positive samples. In this model, attack samples need to be classified into positive samples to maintain their aggressiveness. Therefore, it is necessary to minimize the loss function in the case of modifying its label, as shown in formula (10):
In addition, for the generative adversarial network, it is necessary to ensure that the new attack sample has sufficient similarity with the old one. The second attack sample is optimized by expanding the distribution of negative sample data set. See formula (11):

$$x_{\text{new}} \sim F(m, \mu)$$  \hspace{1cm} (11)

where $m$ is the mean of $x^*$ and $\mu$ is the variance of $x^*$.

According to the attack discriminant model $F$ and intrusion discriminant model $R$, the negative sample generation model is formed by combining the positive sample data set and the extended negative sample set. The above three constraints restrict each other, so that the generated samples can be discriminated as negative samples by discriminant model $F$ and positive samples by discriminant model $R$. The final attack sample set is obtained by iteration.

4. Experiment and Result Analysis

4.1. Experimental Setup

The experimental environment is set as follows: Windows 10 operating system, Intel (R) core (TM) i5-8250u CPU @ 1.60hz 1.80GHz, debugging environment is python3.5.2, tensorflow 1.4.0, torch 1.3.0.

In order to verify whether the negative sample data generated is reasonable, this paper does three verification work:

- Whether the generated negative sample is sufficiently similar to the original negative sample;
- When the negative sample is missing from the original sample, the classifier is used to test the sample and calculate various evaluation indexes. Using the traditional GAN model to generate negative samples, the generated negative samples and the original positive samples are trained and classified, and the same evaluation index is used to evaluate them; after generating negative samples according to the algorithm in this paper, the classifier is trained again and its classification is evaluated.
- Comparing the results of the three experiments, if the evaluation index of the third experiment is better than the first two experiments, it shows that the negative sample generated improves the accuracy of the classifier.

The evaluation indexes include accuracy rate, accuracy rate, recall rate, F1 and AUC [13] values.

4.2. Similarity Evaluation between the Generated Negative Sample and the Original Negative Sample

4.2.1. Public Datasets. For Mississippi SCADA gas pipeline data set. Firstly, 100 original real negative samples are selected, and based on the UV principle of matrix decomposition, sparse matrix is constructed and filled to obtain the preliminary expanded sample set; under the premise of the same iteration times, 100 samples are extracted from each of the negative samples generated by GAN model and the dual discriminant model in this paper to form the distribution comparison sample set. The comparison chart of sample distribution is shown in Figure 3.
Figure 3. Comparison of sample set distribution.

The graph shows that the negative sample generated by GAN model fluctuates greatly, and the trend is quite different from the original sample. However, the negative sample generated by the dual discriminant model in this paper tends to the original real negative sample. For quantitative analysis, discrete trend distribution formulas such as maximum, minimum, median, mean and variance are used to calculate each column. The results are shown in Table 2. The Manhattan formula is used to calculate the similarity of the two models.

Table 2. Calculation of distribution value of comparative samples.

|                       | Original true negative sample | Gan generated samples | Sample generation by dual discriminant model |
|-----------------------|------------------------------|-----------------------|---------------------------------------------|
| Maximum               | 1.2977                       | 1.5468                | 1.5531                                      |
| Minimum               | 1.0031                       | -0.3462               | 0.1670                                      |
| Median                | 1.1677                       | 0.7885                | 0.9549                                      |
| Mean value            | 1.1596                       | 0.7999                | 0.9533                                      |
| Variance              | 0.0075                       | 0.1705                | 0.1732                                      |

According to the Manhattan distance formula:

$$\text{dist}(X, Y) = \sum_{i=1}^{n} |x_i - y_i|$$  \hspace{1cm} (16)

The smaller the Manhattan distance, the higher the sample similarity. According to formula (16), the Manhattan distances between the GAN model and the original real negative samples can be obtained, which are 44.08 and 39.40, respectively, which indicates that the negative samples generated by the dual discriminant model are more similar to the original real negative samples.

4.2.2. An Industrial Control Data Set. For the data set of an industrial control system from March to May 2020, 100 negative samples are generated according to the business logic. When generating negative samples, it is assumed that if a certain data in industrial control system is hijacked, the data is tampered by deviation attack to get the initial negative sample data set; then, based on the UV principle of matrix decomposition, sparse matrix is constructed and filled to obtain the initially expanded sample set; finally, negative sample is generated based on the generative adversarial network of dual discrimination model. 200 negative samples generated by GAN model and dual discriminant model in this paper are extracted to form the distribution contrast sample set. Figures 4, 5 and 6 show the distribution of three negative samples generated by sensor bias attack, negative
samples generated by dual discriminant model, negative samples generated by Gan model and original positive sample set.

![A pressure sample distribution comparison chart](image)

**Figure 4.** Distribution of positive and negative samples of a pressure sensor.

When attacking a pressure sensor, the calculation indexes are shown in Table 3.

|                      | Original true negative sample | Gan generated samples | Sample generation by dual discriminant model |
|----------------------|-------------------------------|-----------------------|---------------------------------------------|
| Maximum              | 0.4533                        | 0.8771                | 0.2568                                      |
| Minimum              | 0.1279                        | 0.4911                | -0.3638                                     |
| Median               | 0.2278                        | 0.7542                | 0.2441                                      |
| Mean value           | 0.2502                        | 0.7652                | 0.7651                                      |
| Variance             | 0.0094                        | 0.0064                | 0.0229                                      |

The Manhattan distances between GAN model and dual discriminant model are 116.57 and 103.01, respectively.

![Sample distribution map of attacking a temperature sensor](image)

**Figure 5.** Positive and negative samples of a temperature sensor.
When attacking a temperature sensor, the calculation indexes are shown in Table 4.

**Table 4.** Calculation of distribution value of comparative samples.

|                  | Original true negative sample | Gan generated samples | Sample generation by dual discriminant model |
|------------------|------------------------------|-----------------------|-----------------------------------------------|
| Maximum          | 1.6481                       | 14.0075               | 0.1978                                        |
| Minimum          | -1.0199                      | 12.0149               | -2.5400                                       |
| Median           | 0.8209                       | 13.0256               | -1.3171                                       |
| Mean value       | 0.6582                       | 13.0185               | 13.0183                                       |
| Variance         | 0.5407                       | 0.31416               | 0.3808                                        |

The Manhattan distances between GAN model and dual discriminant model are 2855.13 and 2473.04, respectively.

![Sample distribution of pressure difference](image)

**Figure 6.** Positive and negative examples of pressure sensor difference.

When attacking a temperature sensor, the calculation indexes are shown in Table 5.

**Table 5.** Calculation of distribution value of comparative samples.

|                  | Original true negative sample | Gan generated samples | Sample generation by dual discriminant model |
|------------------|------------------------------|-----------------------|-----------------------------------------------|
| Maximum          | -0.6679                      | 0.2783               | -0.6737                                       |
| Minimum          | -0.71163                     | -0.2540              | -0.9227                                       |
| Median           | -0.6893                      | -0.2361              | -0.7029                                       |
| Mean value       | -0.6894                      | -0.2135              | -0.2135                                       |
| Variance         | 0.0001                       | 0.0054               | 0.0011                                        |

The Manhattan distances between GAN model and dual discriminant model are 50.02 and 47.59, respectively.

The results of two groups of experiments of public data set and industrial control data set show that: (1) compared with negative sample generated by Gan model, the distribution of negative sample set generated by dual discrimination model is closer to the original negative sample; (2) the negative sample generated by the model is different from the original real negative sample, but it can be controlled to a certain extent. The negative sample generated by the model is within the normal range of the point values of the industrial control system, that is, the attack without breaking the value range.
is simulated completely, which will cause damage to the system. Because if the tampered industrial control data exceeds its own range of value, it will easily trigger system alarm. After the system alarm, the hacker attack may have to be interrupted, so the resulting sample is not a successful attack sample.

4.3. Training and Classification Effect of Anomaly Detection Algorithm for Generated Negative Samples

The ultimate purpose of generating negative samples is to improve the ability of anomaly detection algorithm in industrial control system. In order to make the anomaly detection algorithm recognize the possible attacks in the future, a certain number of negative samples should be generated to improve the ability of anomaly detection.

In the public data set, the positive samples and the existing negative samples are used to train the anomaly detection model, and the negative sample set is tested to get the accuracy of the current anomaly detection model, which is called the first stage of anomaly detection. Based on the method proposed in this paper, the negative sample set is generated; the original positive sample and the negative sample generated by the paper are re used in the anomaly detection model the second stage of anomaly detection is called the second stage of anomaly detection. If the accuracy of the second stage is higher than that of the first stage, it can indirectly show that the negative sample generated is reasonable.

Regarding the anomaly detection model as a classifier, this paper uses three classifiers, including SVM [14], Random Forest [15], XGBOOST [16], respectively, to carry out the first stage and the second stage of anomaly detection for Mississippi SCADA natural gas pipeline data set. The results are as follows:

Firstly, 10000 positive samples and 1000 negative samples are extracted from the Mississippi SCADA natural gas pipeline data set to form a data set. Three classifiers are used to train and test the 11000 samples. Among them, 7700 samples are used for training and 3300 samples are tested. The results are shown in Table 2. For positive samples, the three classifiers all show good results; for negative samples, SVM and random forest have low accuracy, that is to say, they have high false alarm rate. The related results are shown in Table 6.

|               | SVM   | RF   | XGBOOST |
|---------------|-------|------|---------|
| Positive sample accuracy | 99.36% | 100% | 99.97%  |
| Negative sample accuracy  | 98.39% | 0    | 100%    |
| Omission rate           | 1.61%  | 100% | 0       |
| False positive rate     | 0.64%  | 0    | 0.03%   |
| Accuracy               | 99.27% | 91.06% | 99.97% |
| Precision              | 99.36% | 91.06% | 99.97% |
| Recall                 | 99.83% | 91.06% | 100%    |
| F1                      | 99.59% | 91.06% | 99.98%  |
| AUC                     | 0.98   | 0.5  | 0.99    |

Secondly, 10000 positive samples are extracted from the Mississippi SCADA natural gas pipeline data set, and 10000 negative samples are generated by GAN model. The three classifiers are used to train and test the 20000 samples respectively. Among them, 14000 training samples and 6000 test data are used. The results are shown in Table 7.
Table 7. Results of three anomaly detection methods in the second stage.

|                          | SVM    | RF     | XGBOOST |
|--------------------------|--------|--------|---------|
| Positive sample accuracy | 100%   | 69.97% | 100%    |
| Negative sample accuracy | 99.63% | 100%   | 100%    |
| Omission rate            | 0.37%  | 0      | 0       |
| False positive rate      | 0      | 30.03% | 0       |
| Accuracy                 | 99.78% | 84.52% | 100%    |
| Precision                | 99.93% | 68.97% | 100%    |
| Recall                   | 99.63% | 100%   | 100%    |
| F1                       | 99.79% | 81.64% | 100%    |
| AUC                      | 0.98   | 0.84   | 1       |

Finally, 10000 positive samples are extracted from the Mississippi SCADA gas pipeline data set. Then 200 negative samples are selected as the initial sample set, which is expanded to 2000 by using the sparse matrix expansion method in this paper, and 10000 negative samples are generated by the dual discriminant model. The three classifiers respectively train and test the 20000 samples, of which 14000 are used for training and 6000 for test data. The results are shown in Table 8.

Table 8. The results of three anomaly detection methods in the third stage.

|                          | SVM    | RF     | XGBOOST |
|--------------------------|--------|--------|---------|
| Positive sample accuracy | 100%   | 99.40% | 100%    |
| Negative sample accuracy | 99.64% | 100%   | 100%    |
| Omission rate            | 0.36%  | 0      | 0       |
| False positive rate      | 0      | 0.6%   | 0       |
| Accuracy                 | 99.82% | 99.68% | 100%    |
| Precision                | 100%   | 99.39% | 100%    |
| Recall                   | 99.63% | 100%   | 100%    |
| F1                       | 99.82% | 99.70% | 100%    |
| AUC                      | 0.99   | 0.99   | 1       |

From the experimental results, it can be seen that the performance of the negative samples generated by this method on SVM classifier and RF classifier is better than that generated by GAN, and the false alarm rate is reduced. And the performance of XGBOOST was the same as GAN. Therefore, the negative samples generated by this algorithm are effective.

5. Conclusion
The main purpose of this paper is to solve the problem of less negative attack samples in anomaly detection of industrial control system. Firstly, based on the business data, the deviation attack is used to generate part of the initial attack sample set, and the sparse matrix expansion method is used to expand the data for the first time to generate the pre-attack sample set; Then, the pre-attack sample set is iterated by the generative adversarial network based on the dual discriminant model. Finally, the negative sample set is 50 times of the original initial attack sample set, and the data scale can be further expanded according to the increase of iteration times. Compared with the traditional GAN model, the negative sample generated by this method improves the accuracy of anomaly detection algorithm on the basis of ensuring the similarity with the original sample.

Acknowledgements
Thanks for the support and support of CNAF KJ2019003 and other projects.

References
[1] Miller B, Rowe D 2012 A survey SCADA of and critical infrastructure incidents Conference on Research in Information Technology
[2] Network security team of Northeast University 2018 White paper "R/OL" of industrial control network security situation in 2018 https://www.freebuf.com/articles/ics-articles/196647.html
[3] Taormina R, Tippenhauer N O, Galelli S, Elad Salomons E 2018 The Battle of The Attack Detection Algorithms: Disclosing Cyber Attacks On Water Distribution Network Journal of Water Resources Planning & Management 144(8) 04018065
[4] Nader P, Honeine P, Beausero P 2014 One-classification for intrusion detection in scada systems IEEE Transactions on Industrial Informatics 10(4) 2308-17
[5] C´ardenas A A, Amin S, Lin Z S, Huang Y L, Huang C Y, Sastry S 2011 Attacks against process control systems: risk, as sessment, detection, and response. In: Proceedings of the6th ACM Symposium on Information, Computer and Communication Security. (New York, USA: ACM Press) pp 355–366
[6] Szegedy C, Zaremba W, Sutskever I, et al. 2013 Intriguing properties of neural networks. Computer Science https://arxiv.org/abs/1312.6199
[7] Papernot N, Mcdaniel P, Jha S, et al. 2016 The limitations of deep learning in adversarial settings. In: Proc. of the IEEE European Symp. on Security and Privacy (IEEE, 2016) doi: 10.1109/EuroSP.2016.36
[8] Su J, Vargas D V, Sakurai K 2019 One pixel attack for fooling deep neural networks IEEE Transactions on Evolutionary Computation (Piscataway, NJ: IEEE Press)
[9] Goodfellow I J, Shlens J, Szegedy C 2014 Explaining and harnessing adversarial examples, arXiV preprint arXiV: 1412.6572
[10] Hu W, Tan Y 2017 Generating adversarial malware examples for black-box attacks based on GAN, arXiV preprint arXiV: 1702.05983
[11] Kurakin A, Goodfellow I, Bengio S 2016 Adversarial examples in the physical world, arXiV preprint arXiV: 1607.02533
[12] Koren Y, Bell R, Volinsky C 2009 Matrix Factorization Techniques for Recommender Systems Computer 42(8) 30-7
[13] Zhou Z H 2016 Machine Learning (Beijing: Tsinghua University Press) (in Chinese)
[14] Chen P H, Lin C J, Schlkopf B 2005 A Tutorial on v-support vector machines Applied Stochastic Models in Business & Industry 21(2) 111-36
[15] Breiman L 2001 Random forests Machine Learning 45(1) 5-32
[16] Chen T, Guestrin C 2016 XGBoost: A Scalable Tree Boosting System The 22nd ACM SIGKDD International Conference