The Integrated Artificial Immune Intrusion Detection Model Based on Decision-theoretic Rough Set

Rui-Hong Dong, Dong-Fang Wu, Qiu-Yu Zhang
(Corresponding author: Qiu-Yu Zhang)

School of Computer and Communication, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
(Email: zhangqylz@163.com)
(Received Aug. 16, 2016; Revised and accepted Dec. 7 & 25, 2016)

Abstract

The intrusion detection methods used in the industrial control network generally have a higher false positive rate. Considering this issue and improving the detection performance of intrusion behaviors, an integrated artificial immune intrusion detection model based on decision-theoretic rough set was proposed in this paper. Firstly, by the approach of decision-theoretic rough set attributes reduction algorithm (DTRSA), attributes reduction was finished. And the rule set was obtained from the training data which has the binary string form. Secondly, taking into consideration of the negative selection algorithm (NSA), the rule set produced the corresponding detector sets. Vaccine mechanism was added into the model. Finally, real time dendritic cell algorithm (rtDCA) analyzed the environment and antigen information. The antigen matching threshold was obtained. Considering the intrusion behaviors and antigen matching threshold, the dynamic increases of rule set was achieved. Experimental results show that the proposed model obtained the lower false positive rate (FP) and the true positive rate (TP) reached to 95.5%. And both known and unknown intrusion detections had the high performance.

Keywords: Decision-theoretic Rough Set; Detector; Integrated Artificial Immune; Intrusion Detection System; Rule Set

1 Introduction

Industrial control system (ICS) is widely used in many national critical infrastructures. According to the statistics, more than 80% national critical infrastructures use ICS to achieve the automation of the industrial production. Therefore, the security of ICS can affect the national security and economy development directly. At the beginning of ICS development, the design of industrial control network didn't consider the security requirements. Following the disappearances of the network physical closure, the "Stuxnet" and "Flame" security events happen on the industrial control area. The security situation of industrial control network becomes worse. The main information security problem of ICS is closely related to the security of industrial control network. As the vital technique in the network security, intrusion detection approaches in industrial control network attach more focus from the researchers.

For the improvement of intrusion detection system (IDS), many approaches included probability statistics, neural network, support vector machine, genetic algorithm and artificial immune system [7, 10, 11], were proposed to research the network intrusion detection. According to the different intrusion detection objects, intrusion detection methods are divided into two types. One is named as anomaly detection which is used in the detection of the unknown intrusion. And, the other is called misuse detection that is used to detect the known intrusion. Both of them have advantages and disadvantages [14]. In [6], the simulation experiments and analysis of the integrated scheme for the anomaly and misuse detection were achieved. By the combination of structural features and behavioral characteristics two detection measures, the integrated system obtained the good detection performance. But, the experimental data has the high dimension of the condition attributes, which leads to the high time complexity. In this condition, for the real-time of system, the attributes reduction approach was recommended. According to [19], the above mentioned integrated scheme for two methods was also adopted. By the rough set algorithm (RSA), the rule set was obtained from the training data. And the corresponding detectors which actively participated in the intrusion detection were produced. Using vaccine mechanism, the producing process of detectors was optimized. But, as Figure 4 shown, comparing with the rough set, the decision-theoretic rough

set has a better characterization degree of domain. The characterization speed of domain is also faster.

In the artificial immune intrusion detection researches, Forrest, Castro and Greensmith [3, 8, 9] make more contributions. In [18], an improved artificial immune intrusion detection method was introduced. To obtain the superior antibodies, by the using of rough set and fuzzy set, a scheme of antibody based on the rough set was proposed. And the speed of intrusion detection was kept. According to [17], for the low detection performance of clone selection algorithm (CSA), a features selection method was used in the improvement of CSA. With the clone and mutation of some objects which have excellent characteristics, the classification ability of classifiers and algorithm performance were improved. In [12], the negative selection algorithm (NSA) included the fixed and variable r-contiguous bits two kinds matching methods, was introduced. The performance of NSA was improved via the real-time adjustment of binary string matching length. According to [15], in the process of features selection, using the filter approach, the result of attributes reduction was input into the dendritic cell algorithm (DCA). As the experiment shown, the performance of DCA was improved and the requirement of calculation ability was low.

Considering the shortcomings of the above researches, an integrated artificial immune intrusion detection model based on decision-theoretic rough set (DTRSIAI-IDM) was proposed in this study. By the DTRSA, the attributes reduction of experimental data was achieved. And the complexity of condition attributes was efficiently decreased. Meanwhile, self and nonself rule set was obtained from the training data. The corresponding nonself detectors which were used in the misuse detection were produced. To overcome the disadvantages of randomly producing detectors, vaccine mechanism was added into the NSA. Then, the real time dendritic cell algorithm (rtDCA) real-timely captured the antigen and environment information. The abnormal judgment was made via the computing of antigen abnormal index and matching threshold. To improve the speed of intrusion detection, the abnormal behaviors real-timely gave feedbacks to the rule set and detector sets. Finally, as the simulation experiments shown, comparing with the traditional rough set algorithm, the DTRSA got a better description of the positive domain and a lower complexity of experiment data. And the quality of detectors could be guaranteed. By the above proposed integrated scheme, the artificial immune model got a high true positive rate and a lower false positive rate.

The rest of the paper is organized as follows: Section 2 introduces the model and workflow of the integrated artificial immune intrusion detection approach. Section 3 describes all the algorithms included in the model and analyzes the complexity. In Section 4, firstly, it introduces the preprocessing of the data and analysis of the detectors length. Secondly, it discusses the merits and demerits of rough set (RS) and decision-theoretic rough set (DTRS). Thirdly, it analyzes and compares the detection performance of the proposed model. Finally, we conclude our paper in Section 5.

2 DTRSIAI-IDM

According to the research of Common Intrusion Detection Frame (CIDF) [19], as Figure 1 shown, an integrated intrusion detection model is designed. The model includes three function modules: rule set module (thymus), rule matching module (tissue) and analysis center module (lymph gland). By the preprocessing of KDD99 data, the experimental data translates into binary string form. Then, the data set, as the information of antigen, is input into the rule matching module and participates in the detection.

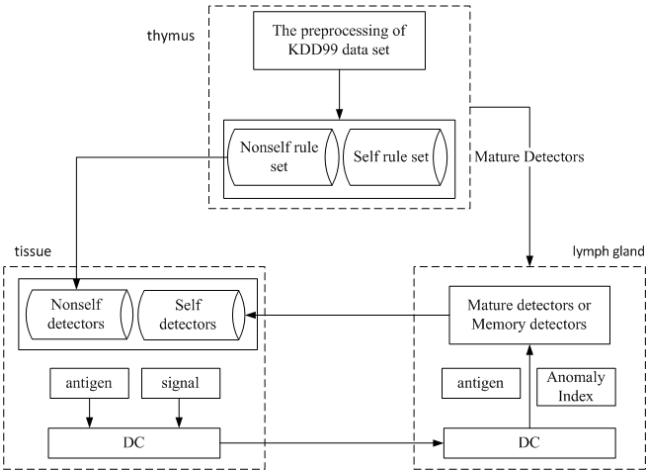

Figure 1: DTRSIAI-IDM integrated model

DTRSIAI-IDM includes four algorithms: integrated artificial immune algorithm based on decision-theoretic rough set (DTRSIAIA), DTRSA, NSA and rtDCA. By the using of the DTRSA approach, the data is processed and the rule set is obtained. According to the rule set, NSA produces the detector sets which meet the demands of detection system. For the undetected antigens, dendritic cell model captures the antigen and environment information. According to the metastasis threshold of dendritic cells, the states of dendritic cells are real-timely updated. And the match threshold is also computed. Then, the rule matching module receives the feedbacks from the anomaly detections. There is the general workflow of the model, as shown in Figure 2.

3 The Proposed Model

3.1 DTRSIAIA

In [6], the conception of matching threshold was mentioned. In the integrated artificial immune system, combining the dynamic anomaly index of antigen, the ap-

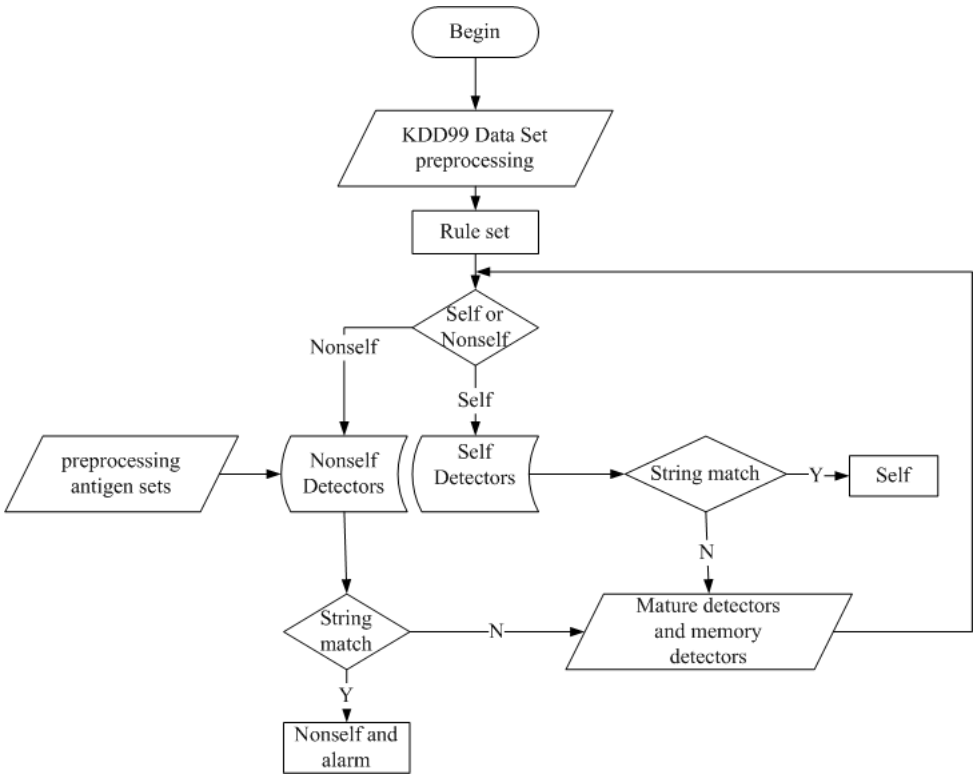

Figure 2: The workflow of the DTRSIAI-IDM

proach of computing matching threshold between detectors and antigen is proposed.

$$Y_\alpha = (L - \varepsilon)e^{-a(X_\alpha - \delta)}. \quad (1)$$

where the Y_α is the matching threshold of α type antigen. And, a is a constant. For the memory detectors, $a = -1$. In rtDCA, δ is the anomaly threshold. L is the length of detectors. And, $L = 24$. In the binary space, ε is self-radius which decides the coverage area of detectors. According to the Equation (2), when the anomaly degree is higher, the matching threshold is lower. And, when the anomaly degree of antigen is decreasing, the matching threshold is increasing. X_α is the dynamic anomaly index of α type antigen.

$$X_\alpha = \frac{m_a}{\sum_{i=1}^{A} A_i}. \quad (2)$$

where α is the antigen set which has the same value. And, the number of α type mature antigens is m_a. A_i is the total transformation number of i type antigens. The total number of all the types is A.

3.2 DTRSA

As the Ref. [16] describes, the study introduces the follow definitions: decision-theoretic rough set, α-positive domain, positive domain reduction and α-positive domain global significance.

Algorithm 1 DTRSIAIA

```
Input: Antigen and preprocessing information flow
Output: The detected anomaly antigens
while input data do
    if Semi ≤ Mat then
        Add the input antigens to the self-set
    end if
    Check and produce the detectors (NSA)
    Using rtDCA to deal with the antigens and the environment information
    According to Equation (2), real-timely analyze the input data and obtain the dynamic anomaly index
    According to Equation (1), when we know the anomaly index, computing the matching threshold
    Using detectors to detect the antigens
    Produce the alarm signals
end while
```

Definition 1. *(Decision-theoretic Rough Set) A decision-theoretic table is following tuple:*$DT = \{U, A_t = \{C \cup D\}, \{V_a | a \in A_t\}, \{I_a | a \in A_t\}\}$, *where* $U = \{x_1, x_2, .., x_m\}$ *is a finite nonempty set of objects.* A_t *is a finite nonempty set of all condition attributes.* $A_t = C \bigcup D$ *, where* C *is the condition attributes set and* D *is the decision-theoretic set. And,* V_a *is a nonempty set of values of* $a \in A_t$*.* $I_a : U \to V_a$ *is an information function that maps an object in* U *to exactly one value in* V_a*.*

Definition 2. *(α-positive domain) Given a decision-*

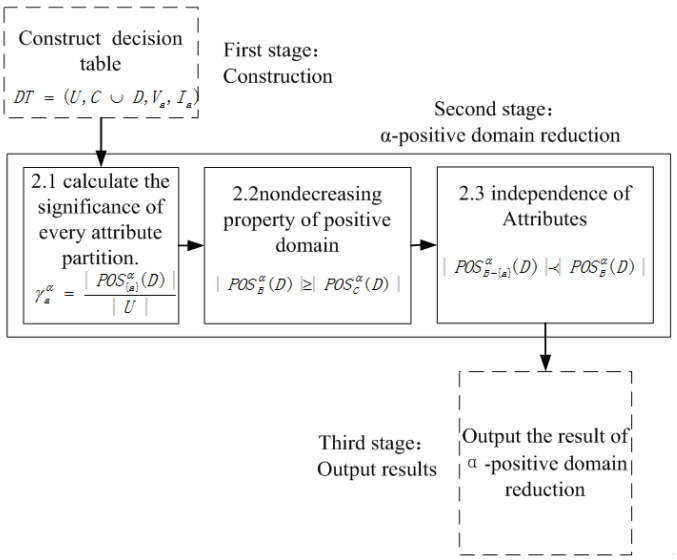

Figure 3: The attributes reduction model for DTRSA

theoretic table is following tuple: $DT = \{U, A_t = \{C \cup D\}, \{V_a|a \in A_t\}, \{I_a|a \in A_t\}\}$. *The decision-theoretic rough set is related with decision attributes and condition attributes. The* α*-positive domain is defined as:*

$$POS_B^\alpha = \bigcup_{X \in \frac{U}{D}} \underline{apr_C^\beta}(X). \tag{3}$$

where $\underline{apr_C^\alpha}(X)$ *is the* α *approximations of* X, $\underline{apr_C^\alpha}(X) = \{x \in U|P(X|[x]_c) \geq \alpha\}$.

Definition 3. *(positive domain reduction) Given a decision-theoretic table is following tuple:* $DT = \{U, A_t = \{C \cup D\}, \{V_a|a \in A_t\}, \{I_a|a \in A_t\}\}$. $\alpha \in [0, 1]$, *when the attributes subset* $B \subseteq C$ *has the following characteristics:*

1) *Positive domain no decreasing property:* $|POS_B^\alpha(D)| \geq |POS_C^\alpha(D)|$

2) *Independence of attributes:* $\forall \alpha \in B, |POS_{B-\{a\}}^\alpha(D)| < |POS_B^\alpha(D)|$

Definition 4. *(*α*-positive domain global significance) Given a decision-theoretic table is following tuple:* $DT = \{U, A_t = \{C \cup D\}, \{V_a|a \in A_t\}, \{I_a|a \in A_t\}\}$.*Let the condition probability threshold* $\alpha \in [0, 1]$, $a \in C$, *a is one attribute. The* α*-positive domain global significance is defined as follow:*

$$\gamma_a^\alpha = \frac{|POS_B^\alpha(D)|}{|U|}. \tag{4}$$

Attention, in reduction algorithm, there is one low time complexity belongs to positive domain global significance. In DTRSA, a heuristic reduction algorithm is adopted. The α-positive domain global significance, as the heuristic function, is selected to compute positive domain reduction. As shown in Figure 3, that is the basic thought of the DTRSA.

Algorithm 2 DTRSA

1: Input: The decision-theoretic table $DT = \{U, A_t = \{C \cup D\}, \{V_a|a \in A_t\}, \{I_a|a \in A_t\}\}$ and the *condition probability threshold* $\alpha \in [0, 1]$
2: Output: α attributes reduction
3: Preprocessing the *positive domain* attributes set $r = \emptyset$ $M \times N$
4: According to Equation (3), computing the *positive domain* of attributes. According to Equation (4), computing the *significance* of every condition attributes.
5: Obtain the global significance list γ, and show in descending order.
6: **while** $|POS_B^\alpha(D)| < |POS_C^\alpha(D)|$ **do**
7: Let $a = P(i)$, add a to α-positive reduction attributes set,$R = R \bigcup \{a\}; i = i + 1$
8: **end while**
9: **while** R does not meet this property **do**
10: $\forall a \in R$,
11: **if** $|POS_{B-a}^\alpha(D)| \geq |POS_B^\alpha(D)|$ **then**
12: $R = R - \{a\}$
13: **end if**
14: Using detectors to detect the *antigens*
15: **end while**

3.3 NSA

NSA includes two parts: producing the detectors and anomaly detection. By the DTRSA approach, the rule set is obtained. According to the affinity, NSA randomly produces some detectors which meet the self-radius. In [5], by the Equation (5), the affinity between detectors and self-samples is computed.

$$affinity = \sqrt{\sum_{i=1}^{L}(x_i - y_i)^2}. \tag{5}$$

where x_i is the i feature bit and y_i is the i feature bit.

When the detector sets cannot meet the demands of model, NSA producing detectors randomly and computing the affinity. When the affinity is less than matching threshold, the antigen sample is abnormal.

Algorithm 3 DTRSA(Produce the detectors)

```
Input: Self set, Self-radius, Detector length and the number of required detectors
Output:Detectors set
while the number of current detectors ≤ the number of required detectors do
    Randomly produce some fixed length detectors
    for every self-sample do
        According to Equation (5), computing the affinity between detectors and self-sample
        if candidate detectors are not in the self-radius range then
            Add the candidate detectors into the detectors set
        end if
    end for
end while
```

Algorithm 4 DTRSA(Anomaly detection)

```
Input: Anomaly detection output the unknown antigens and self-detectors set
Output:Detection results
while input date do
    for every detector do
        Computing the affinity between antigen and detectors
        if affinity less than matching threshold then
            Abnormal antigen
        else
            Normal antigen
        end if
    end for
end while
```

3.4 rtDCA

DC can capture three kinds of information: PAMP signal, Danger Signal and Safe Signal. In [2], the preprocessing scheme of data was researched. Receiving the input information, by the Equation (6), dendritic cell produces the output information and the dynamic anomaly index. The output information includes: Co stimulation signal (Csm), Semi mature signal (Semi) and Mature signal (Mat). The equality about the information can be written as follows:

$$O_j = (1 + I_{in}) \sum_{i=0}^{I} \omega_{ij} S_i. \quad (6)$$

where S_i is input information and O_j is output information. I_{in} is inflammatory signal. Let ω_{ij} be the transformation weight. I is the number of signal types. S_0, S_1, S_2 are separately corresponding to PAMP signal, Danger Signal and Safe Signal. O_0, O_1, O_2 separately represent three signals: Csm, Semi and Mat. Table 3 describes the signal transformation rule.

Algorithm 5 rtDCA

```
Input: Antigen flow and preprocessing signal flow
Output: Dynamic anomaly index of antigens
(Tissue)
Initialization of dendritic cell population
while input the data do
    Update the antigen structure and signal matrix
    for dendritic cell do
        Capture and store antigen
        According to Equation (6), processing the signal
        if Csm ≥ Migration threshold then
            if Mat ≥ Semi then
                cell context = 1
            else
                cell context = 0
            end if
            Dendritic cell migrate into lymph gland
            Add a new dendritic cell into the tissue
        end if
    end for
end while
(T cell population)
for dendritic cell do
    Computing the anomaly index of every kinds antigen
end for
```

Dendritic cell not only capture the antigen and environment information, but produce the output information. Dependent on concentration of input information, the environment information can be obtained. Then, computing the antigen anomaly index and responding the abnormal feedbacks.

3.5 Algorithm Complexity Analysis

The analyses for the above discussed algorithms were made, as the Table 1 shown. In the DTRSA, let M be the number of condition attributes. The number of decision-theoretic attribute is 1. Let the training set be N_1. And, let the number of undetected antigens be N. After the misuse detection, N_2 is the number of antigens. And, let the number of self-detectors is K. Let K_1 be the number of nonself detectors. And L is the length of detectors. Let $R(R < M)$ to express the number of α-positive domain objects. The time complexity of DTRSA is $O((N_1+1)*2^{R+1}+2*(R+M)N_1)$. And the space complexity is $O((MN_1KL)$. Comparing with the RSA mentioned in [10], the time and space complexities of DTRSA are equivalent with RSA. In the NSA, the time complexity

is $O(LN_2K)$. And, the space complexity is $O((L+1)K)$. For the rtDCA, the time complexity is $O(MN_2^2)$ and the space complexity is $O(N_2(L+1))$. The time complexity of DTRSIAIA is $O(NL(N_2+NK))$ and the space complexity is $O(MN_1K_1L)$.

Table 1: Analyses of algorithm complexity

Algorithm	Time complexity	Space complexity
DTRSA	$O((N_1+1)*2^{R+1}$ $+2*(R+M)N_1)$	$O((MN_1KL)$
NSA	$O(LN_2K)$	$O((L+1)K)$
rtDCA	$O(MN_2^2)$	$O(N_2(L+1))$
DTRSIAIA	$O(NL(N_2+NK))$	$O(MN_1K_1L)$

4 Experiments and Analysis

In intrusion detection, considering the security problems of industrial control network, true positive rate (TP), false positive rate (FP) and the speed of detection are the main evaluating indicators for the intrusion detection system. By the above indicators, the real-time and effectiveness of the system can be analyzed. As the input data, KDD99 data participates in the experiments and verifies the performance of DTRSIAIA. The simulation experiment is finished in the windows 7 system.

4.1 Date Set

For intrusion detection systems, KDD 99 is a standard test data which includes connection and attack items. There are almost 38 kinds of attacks which include smurf, nmap and rootkit. The dimension of KDD99 data is 41. According to the demands of experiments, preprocessing of data can be finished. In [6], the preprocessing approach of the data was proposed. On the one hand, antigen expresses the structural features. On the other hand, signals represent the behavioral characteristics.

1) Antigen

In Table 2, transform the selected attributes into the corresponding binary strings and construct the new antigen.

2) Input Information

According to the information gain attributes selection approach [19], divide 10 selected attributes into three kinds of signals.

- PAMP Signal: attributes 25, 26, 29, 38 and 40
- Danger Signal: attributes 23 and 24
- Safe Signal: attributes 12, 31 and 32

Let x to express the value of attribute. When $x \in [m,n]$, this domain can be divided into PAMP signal or Danger signal. Otherwise, it is the Safe signal. The normalization of the data can be processed by the following equation.

$$f(x) = \left\{ \begin{array}{l} 0, x \in [0,m) \\ \frac{100x}{n-m}, x \in [m,n] \\ 100, x \in (n,+\infty) \end{array} \right\}. \quad (7)$$

For the attribute 12, the numerical range is $[0, 0.99]$. According to $[min, max]$, the numerical range is constructed. The mean value express the condition of this kind of signal.

3) Experimental Parameters

The sum of dendritic cells is 10. The range of migration threshold is $[50, 400]$. Let the abnormal threshold $\delta = 0.35$. For the approach of NSA, the length of detector is 24. For the memory detectors, let $a = -1$. And, for the general detectors, let $a = -1/2$. The following Table 3 is an advised threshold value.

Table 3: Threshold value

Weight	Csm Signal	Semi Signal	Mat Signal
PAMP Signal	2	0	2
Safe Signal	1	0	1
Danger Signal	2	3	-3

4.2 Length of Detector

In the experiment, comparing with the monotonicity of rough set, the decision-theoretic rough set has the non-monotonicity. Select 1,000 message records, increase one attribute every time and record the description of the positive domain. As Figure 4 shown, the sum of attributes is 10.

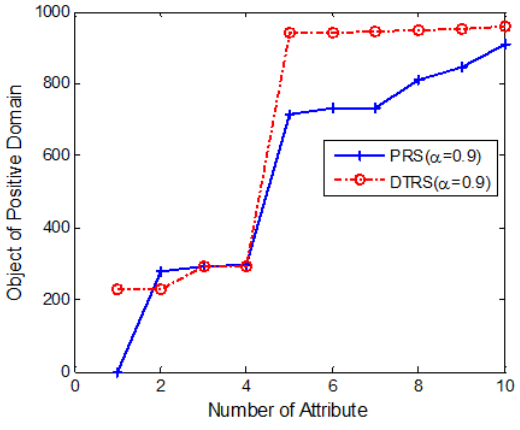

Figure 4: Attributes reduction description of the positive domain

In Figure 4, the dashed line describes the change situation of decision-theoretic rough set α positive domain.

Table 2: The construction of antigen

Attribute number	Transformation	Length
2	TCP,UDP and ICMP expressed by 00,01,10	2
3	Transform the number of the value into binary form	7
4	Transform the number of the value into binary form	4
5	Low, Middle, High and highest expressed by 00,01,10,11	2
6	Low, Middle, High and highest expressed by 00,01,10,11	2
12	Expressed by 0 or 1	1
28	Low, Middle and High expressed by 00,01,10	2
30	If the value equal to 1, expressed by 1, or 0	1
31	If the value equal to 1, expressed by 1, or 0	1
36	Low, Middle, High and highest expressed by 00,01,10,11	2

And, the dashed line does not meet the strict monotonicity. The solid line describes the change situation of the rough set. The dashed line is mostly on the upper of the solid line. And, account for the change situation of the positive domain, decision-theoretic rough set has a better description of the domain objects, as Figure 4 shown.

When $\alpha = 0.7, 0.8, 0.9$, Figure 5 describes the significance situation of attributes. When the value of α is decreases, the significance of attributes is increasing. And, in the decision-theoretic rough set, several attributes can mostly describe the whole positive domain which originally needs all condition attributes to represent. The message record includes 41 attributes. According to [4], the result of attributes reduction is $D = \{2\ 3\ 4\ 5\ 6\ 12\ 28\ 30\ 31\ 36\}$. Therefore, according to Table 2, the length of detector is 24. From the following Table 4, after the attributes reduction, the rule set is obviously decreasing. Add the rule sets into the self or nonself rule sets.

Table 4: The situation of DTRSA attributes reduction

Rule number	Before reduction	After reduction
PAMP Signal	8000	149
Safe Signal	2000	117

4.3 Self-radius

Researching the intrusion detection problems of industrial control network, the ROC (Receiver Operating Characteristic Curve) can be used to express the TP and FP of the detection. Adjust the self-radius continually, record the TP and FP [1]. Then, the ROC can be obtained, as Figure 6 shown.

Let $r = 0$, antigen completely matches detector sets. And, following the increasing of the self-radius, the TP and FP are also raising. When $r = 9$, the trend of the curve is balanced and the TP is higher than 0.9. For a higher TP and a lower FP, $r = 9$ can be selected to construct the detector sets.

4.4 Comparing the Performance

Compare the performance of DTRSIAIA with immune algorithm, rough set and support vector machine. The Table 5 lists the TP and FP of every approach.

Table 5: Comparing the performance

Name	True positive rate	False positive Rate
RSAI-IID [19]	0.9786	0.0268
SVM [20]	0.931	0.0081
RS-FSVM [13]	0.91	0.1424
rtDCA [6]	0.930	0.025
IAIS [6]	0.9691	0.0321
CSA [17]	0.996	0.1
NSA [12]	0.95	0.01
DTRSIAIA	0.955	0.020

As the Table 5 shown, comparing with other rough set algorithms, DTRSIAIA keeps the higher TP and lower FP. In [6], comparing with rtDCA, the FP is decreasing. And, for the IAIS approach, the proposed approach has a lower FP. In [19], the classifier method based on rough set has a higher TP and FP. The FP of proposed method is

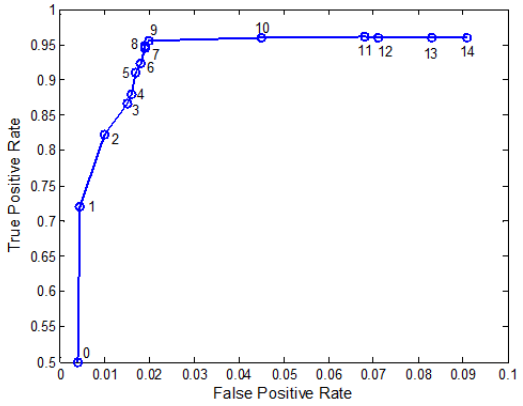

Figure 6: The ROC of the self-radius

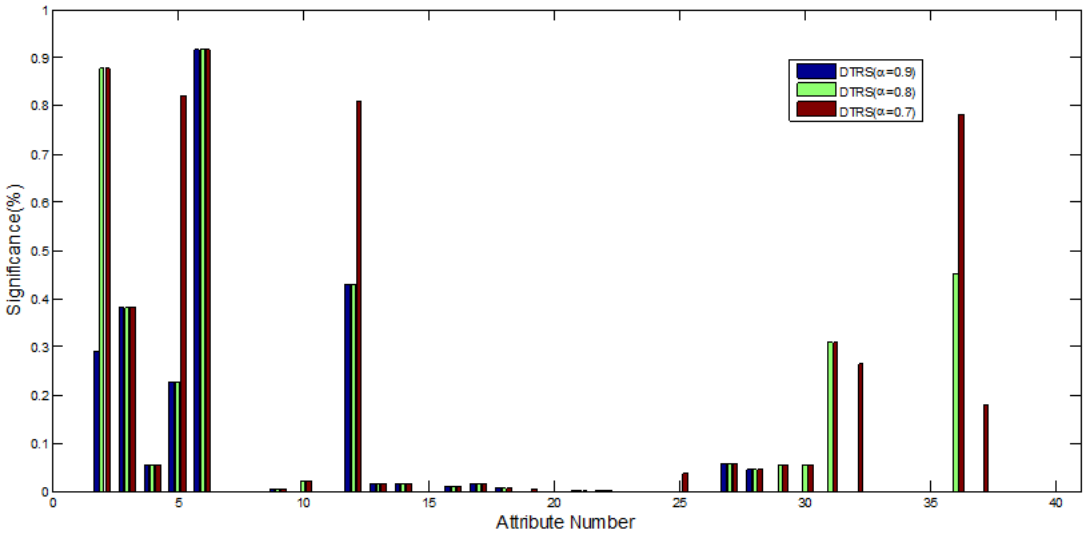

Figure 5: Significances of condition attributes

0.02 and TP is 0.955. In [17], an improved clone selection intrusion detection method was proposed. And the TP is 0.996, but the FP is 0.1. The FP is higher than the approach in this research. In [12], the FP is 0.01, but the TP is also lower. In [20], the FP is 0.0081 and TP is lower. In [13], the DTRSIAIA has a higher TP and lower FP.

According to Figure 6, $r \in [8, 10]$ is suitable for the simulation experiments. And the TP is higher than 0.9. Considering the analysis of algorithm in Section 3.5 , the DTRSIAIA has a lower complexity of algorithm. And, as Figure 4 shown, the DTRSA has a better description of the positive domain.

5 Conclusions

An integrated artificial immune intrusion detection algorithm based on decision-theoretic rough set was proposed. The effectiveness of the proposed intrusion detection method was proved, which deals with the intrusion detection problems in industrial control network effectively. Firstly, by the DTRSA approach, the attributes reduction was finished. Comparing with the RSA, the DTRSA is a better choice for the operation of attributes reduction. Secondly, overcoming the disadvantages of randomly producing detectors, the vaccine mechanism was added into the NSA. Then, the qualified detectors were produced. Finally, using rtDCA to analyze the antigen and environment information, rtDCA real-timely responded the feedbacks to the rule set. By this method, the real-time property was kept. In the experiment, the TP of DTRSIAIA is 0.955 and FP is 0.02. And, with the operation of DTRSA, the result of attributes reduction is obvious. The data complexity is decreasing. However, the time complexity of DTRSA is higher.

Next, the research will pay more attention and time to improve the performance of algorithm and prove the completeness.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61363078), the Natural Science Foundation of Gansu Province of China (No. 1310RJYA004). The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

References

[1] M. H. Aghdam and P. Kabiri, "Feature selection for intrusion detection systemusing ant colony optimization," *International Journal of Network Security*, vol. 18, no. 3, pp. 420–432, 2016.

[2] A. A. Al-Hasan and E. S. M. El-Alfy, "Dendritic cell algorithm for mobile phone spam filtering," *Procedia Computer Science*, vol. 52, pp. 244–251, 2015.

[3] L. N. De Castro and F. J. Zuben, "The clonal selection algorithm with engineering applications," in *Proceedings of the GECCO*, pp. 36–39, Las Vegas, USA, July 2000.

[4] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, 2016.

[5] W. Chen, X. Ding, T. Li, and T. Yang, "Negative selection algorithm based on grid file of the feature space," *Knowledge-Based Systems*, vol. 56, pp. 26–35, 2014.

[6] Y. Chen, Q. Zhang C. Feng, and C. Tang, "Integrated artificial immune system for intrusion detection," *Journal of China Institute of Communications*, vol. 33, no. 2, pp. 125–131, 2012.

[7] B. A. Fessi, S. Benabdallah, N. Boudriga, and M. Hamdi, "A multi-attribute decision model for intrusion response system," *Information Sciences*, vol. 270, pp. 237–254, 2014.

[8] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukur, "Self-nonself discrimination in a computer," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 202–212, Oakland, California, May 1994.

[9] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection," in *Proceedings of the International Conference on Artificial Immune Systems*, pp. 153–167, Banff, Alberta, Canada, Aug. 2005.

[10] C. Guo and Y. Zhou, Y. Ping, Z. Zhang, G. Liu, and Y. Yang , "A distance sum-based hybrid method for intrusion detection," *Applied Intelligence*, vol. 40, no. 1, pp. 178–188, 2014.

[11] K. S. Anil Kumar and V. Nanda Mohan, "Adaptive fuzzy neural network model for intrusion detection," in *Proceedings of the Contemporary Computing and Informatics (IC3I'14), 2014 International Conference on. IEEE*, pp. 987–991, Mysore, India, Nov. 2014.

[12] A. Lasisi, R. Ghazali, and T. Herawan, "Negative selection algorithm: a survey on the epistemology of generating detectors," in *Proceedings of the First International Conference on Advanced Data and Information Engineering*, pp. 167–176, Kuala Lumpur, Malaysia, 2014.

[13] L. Li and K. Zhao, "A new intrusion detection system based on rough set theory and fuzzy support vector machine," in *Proceedings of the International Workshop on Intelligent Systems and Applications*, pp. 1–5, Wuhan, China, May 2011.

[14] S. Qing, J. Jiang, H. Ma, W. Wen and X. Liu, "Research on intrusion detection techniques: A survey," *Journal-China Institute of Communications*, vol. 25, no. 7, pp. 19–29, 2014.

[15] H. A. Le Thi, X. T. Vo A. V. Le, and A. Zidna, "A filter based feature selection approach in msvm using dca and its application in network intrusion detection," in *Proceedings of the the 6th Asian Conference on Intelligent Information and Database Systems*, pp. 403–413, Bangkok, Thailand, Apr. 2014.

[16] Y. Yao and Y. Zhao, "Attribute reduction in decision-theoretic rough set models," *Information Sciences*, vol. 178, no. 17, pp. 3356–3373, 2008.

[17] C. Yin, L. Ma, and L. Feng, "A feature selection method for improved clonal algorithm towards intrusion detection," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 5, 2016.

[18] L. Zhang, Z. Bai, S. Luo, and G. Cui, "A dynamic artificial immune-based intrusion detection method using rough and fuzzy set," in *Proceedings of the Information and Network Security (ICINS'13)*, pp. 1–7, Beijing, China, Nov. 2013.

[19] L. Zhang, Z. Bai, S. Luo, K. Xie, G. Cui, and M. Sun , "Integrated intrusion detection model based on rough set and artificial immune," *Journal on Communications*, vol. 34, no. 9, pp. 166–176, 2013.

[20] H. Zhao, "Intrusion detection ensemble algorithm based on bagging and neighborhood rough set," *International Journal of Security and Its Applications*, vol. 7, no. 5, pp. 193–204, 2013.

Biography

Dong Rui-hong, vice researcher, worked at school of computer and communication in Lanzhou university of technology. His research interests include network and information security, information hiding and steganalysis analysis, computer network.

Wu Dong-fang received the BS degrees in Computer Science and Technology from Northwest University for Nationalities, Gansu, China, in 2015. Currently, he is studying for his masters degree at Lanzhou University of Technology. His research interests include industrial control network security.

Zhang Qiu-yu, researcher/PhD supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research center, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.