Survey of DCA for Abnormal Detection

Lei Ding
School of Information Science and Engineering, Jishou University, Jishou 416000, China
E-mail: yylxdinglei@126.com

Fei Yu[1], Zhenghua Yang[2]
[1]Jiangsu Provincial Key Laboratory for Computer Information Processing Technology,
Soochow University, Soochow 215006, P. R. China
[2]School of Information Science and Engineering, Jishou University, Jishou 416000, China
Email: hunanyufei@126.com

***Abstract*—As a latest immune algorithm, dendritic cell algorithm (DCA) has been successfully applied into the abnormal detection. First, this paper reviewed the research progress of DCA from the following aspects: signal extraction technology, DCA signal processing technology, the decision method for load anomaly judgment, and the application research of DCA. Next, the corresponding solving thoughts for the main problems existing in the DCA were proposed in this paper. Finally, the future research trends of DCA were presented in this paper.**

***Index Terms*—Immune algorithm; DCA; abnormal detection; developing process of DCA**

I. INTRODUCTION

Intrusion detection system (IDS) means a system that can detect the intrusion by analyzing the data related to the system safety. Generally speaking, IDS consists of three parts, signal extraction module, analysis and process module for DCA signal, and the decision module. According to the detection method, IDS can be categorized into two main approaches: misuse detection and anomaly detection [1].

Misuse detection system detects the intrusion events using pattern matching algorithm based on feature matching. The feature set consists of the features extracted from the known intrusion. The detection results will be determined according to the matching degree between the current sampled data and the features. If the matching degree is greater than a given threshold, then IDS can detect the intrusion attacks and give a warning. The misuse detection has high measuring accuracy. However, the misuse detection can't find the unknown attacks. Anomaly detection also known as the behavior-based detection system detects the intrusion events according to the behavior characteristics. The anomaly detection compares the network behavior with the normal behavior. If the current behavior deviates from normal behavior, then IDS can detect the intrusion attacks. The normal behavior patterns are constructed through some statistics related to the system behavior. The abnormal detection can detect unknown attack. However, it is hard to get the statistics and give the preset anomaly threshold. In addition to this, the anomaly detection has a high false alarm rate.

All kinds of artificial cases based on the mechanisms of immune system or the theory of immunology are collectively called the artificial immune system (AIS). At present the artificial immune system has been successfully applied into a number of fields, such as the intrusion detection, optimization, and classification, etc., and a series of artificial immune algorithm has been presented since 1990s. The traditional immune system consists of three basic algorithms: negative selection algorithm (NSA) [2], clone selection algorithm (CSA) [3], and immune network algorithm (INA) [4].

With the development of immunology, a new theory called danger theory was presented in 1994 [5]. This danger theory doesn't rely on self-nonself discrimination mechanism, and only reacts to the danger signal which will do harm to health. The danger theory can deal with some problem which can't be resolved by the traditional immune algorithm. For example, the bowels have millions of bacteria, but the immune system doesn't reject these bacteria. The scientists can't explain this phenomenon with the traditional immune theory. However, this phenomenon can be interpreted with the danger theory, namely the immune system only reacts to the danger signal which will do harm to health. In 2003, Aickelin et al. first introduced the danger theory into the artificial immune system [6]. In this paper, the danger theory was translated into the realms of computer security, namely creating AIS which doesn't rely on self-nonself discrimination. In 2005, Greensmith presented dendritic cell algorithm (DCA) based on danger theory, and applied it to the abnormal detection [7].

Dendritic cells are the presently known most powerful professional antigen presenting cells (APC). DCA imitates the process of the dendritic cells, namely discriminating health tissue and infected tissue. The input signal will be abstracted from the input antigen signal, and the output signal will be acquired through the signal processing module. Then, IDS can estimate the dangerous level of the antigens, and can determine whether the intrusion behavior occurs or not [8]. In 2006, Greensmith et al. substantiated the claims that DCA has the ability to detect the intrusion behavior [9]. In this paper, a port scan detection is performed.

Compared with the traditional artificial immune algorithm, DCA is the latest artificial immune algorithm,

doi:10.4304/jsw.8.8.2087-2094

and is more suitable for anomaly detection. In addition to this, DCA has the following advantages: simpleness and rapidness. So, DCA is an important developing direction of artificial immune algorithm. However, the time is not long since DCA emerged, and a lot of subjects need further research.

The remainder of the paper is organized as follows: Section 2 introduces the principle of DCA. Section 3 discusses the development situation of DCA from four aspects as followed: signal extraction technology, signal processing technology, and the decision method for anomaly judgment. In section 4, the problems existing in the DCA is discussed according to the above analysis, and the corresponding solving thoughts are proposed. Conclusions are presented in section 5.

II. THE PRINCIPLE OF DCA

The anomaly detection mechanism relies on the discrimination of normal behavior and anomaly behavior. The observed behavior will be determined to anomalous behavior if it doesn't match the normal profile. This mechanism can detect the novel intrusion behavior. However, the anomaly detection has a high false alarm rate.

The danger theory proposed by Matzinger relies on the detection of endogenous danger signals which arises as the result of damage emerging the tissue cells. The key point of danger theory is that the immune system only reacts to the danger signal which will do harm to health. The dendritic cell Algorithm is an immune-inspired algorithm originally based on the function of natural dendritic cells. The dendritic cells belong to a family of cells known as macrophages, and can act as the professional antigen presenting cells. As a professional antigen presenting cell, the dendritic cell can control the activation state of T-cells in the lymph nodes. The dendritic cells have three different states, namely immature state (iDC), semi-mature state (smDC) and mature state (mDC). The decisive immunogenic signal is the release of proinflammatory cytokines from the DCs.

Immature state is in DCs' initial maturation state, and its primary function is to collect and remove the debris. Mature DCs can activate naive T-cells. For an iDC to become a mDC, the iDC has to be exposed to a greater quantity of signals, namely either PAMPs or danger signals than safe signals. Conversely, an iDC will become a semi-mature DC (smDC). The smDCs can also present antigen, yet they can't activate T-cells. The DCs differentiation mechanism can be represented graphically in Fig.1 [10]. CKs denote cytokines in Fig.1.

Let the input signals be categorized either as PAMPs (P), safe signals (S), danger signals (D) or inflammatory cytokines (IC), then the input signals are transformed to output concentrations of costimulatory molecules (csm), smDC cytokines (semi) and mDC (mat) cytokines [10]. The signal processing function is calculated as Equ.1, where C_{csm}, C_{semi}, and C_{mat} are the input concentration, and w_P, w_D, and w_S are the weight. The weight is presented in Table I.

$$C_{[csm,semi,mat]} = (1+IC)(w_P * S_P + w_D * S_D + w_S * S_S) \quad (1)$$

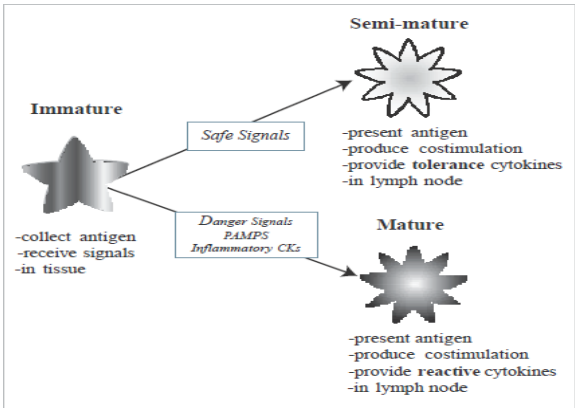

Fig.1. The iDC, smDC, and mDC behaviours and signals required for differentiation

TABLE I.
SUGGESTED WEIGHTING VALUES FOR THE SIGNAL PROCESSING FUNCTION BASED ON DC MATURATION RATIOS

w	*csm*	*semi*	*mat*
PAMPs(*P*)	2	0	2
Danger Signals (*D*)	1	0	1
Safe Signal (*S*)	2	3	-3

Form TABLE I, we have

$$\begin{aligned} C_{csm} &= (1+IC)(2*S_P + 1*S_D + 2*S_S) \\ C_{semi} &= (1+IC)(3*S_S) \\ C_{mat} &= (1+IC)(2*S_P + 1*S_D - 3*S_S). \end{aligned} \quad (2)$$

Then, the corresponding output signals can be depicted as:

$$\begin{aligned} O_{csm}(j) &= O_{csm}(j-1) + C_{csm} \\ O_{semi}(j) &= O_{semi}(j-1) + C_{semi} \\ O_{mat}(j) &= O_{mat}(j-1) + C_{mat}, \end{aligned} \quad (3)$$

where j means the j^{th} iteration, j=1, …, n, $O_{csm}(0)$=0, $O_{semi}(0)$=0, and $O_{mat}(0)$=0.

After each iteration, the value of output signals will be updated. The DC will stop sample antigens and be removed from the tissue if the value of O_{csm} is greater than the given preset threshold. If the value of O_{semi} is greater than the value of O_{mat}, the immature DC becomes a semi-mature DC, conversely, a mature DC.

III. THE RESEARCH PROGRESS OF DCA

A. Signal Extraction Technology

How to extract the corresponding signals such as PAMP, danger signal, safe signal, and inflammatory cytokines is vital to DCA. At present, there are three main signal extraction technologies, namely the

correlation-analysis-based feature selection method, the information-gain-based feature selection method, and the principal component analysis method.

Greensmith et al. applied information-gain-based method to select the DCA signals [11]. In the same way, Chen et al. applied information-gain-based method to select the DCA signals [12]. In this paper, 10 features in KDD 99 set are selected as the signals of DCA, and the 10 features are classified PAMP, danger signals, and safe signals. The features 25, 26, 29, 38 and 40 are classified to PAMP, the features 23 and 24 are classified to danger signals, and the features 12, 31 and 32 are classified to safe signals. In this paper, the value of features is normalized to a range of 0~100, and the average value of each kind of signal is use to represent the value of the signal.

To reduce dimension and noise, the principal component analysis is applied to obtain the signals of DCA [13]. In addition to this, the principal component analysis can realize the automatic classification of input data. The results of the above three feature selection methods has demonstrated that compared with the information-gain-based method and the correlation-analysis-based method, the principal component analysis method has the best feature selection effect [14]. However, this paper pointed that the feature selection method based on PCA has some main shortcomings. For example, the principle of PCA is that the original high dimensional data is mapped to a low dimensional data, and the problem to be resolved should be a linear problem in theory. In addition to this, the variance should fully reflect the principal character of the problem to be resolved. However, the process of practical networks is very complex, and hardly satisfies the above condition. So this paper suggests that the kernel PCA method may be used to extract the signals of DCA.

In 2012, Chelly et al. presented a new DCA feature selection and categorization method using Rough Set Theory (RST) [15]. In this paper, the RST CORE and REDUCT concepts are applied into the feature selection and the categorization processes. Results show that compared with PCA, RST is more convenient for data preprocessing and yields much better accuracy.

From the above analysis, the conclusion can be drawn that the feature selection needs further research due to the complexity of the network.

B. Signal Processing Technology

The prototype of DCA is presented in [7], and the experiment results show that the DCA is suitable to the anomaly detection. An improved DCA was proposed in [9] based on the prototype of DCA presented in [7]. In this paper, each DC acts as an independent agent, which processes the input signals and antigens. The process of tissue and cell updating components can be represented graphically in Fig.2 [9]. In [16] Greensmith et al. compared the performance of the DCA and a Self-Organizing Map (SOM) in the detection of SYN port scans. In this paper, experiment results show that a SOM is an ideal candidate for comparison as it shares similarities with the DCA due to the employed data fusion method. Furthermore, the anomaly detection experiment results show that the DCA has the same standard as an established technique. In [17] Oates et al. demonstrated that the DCA has an emergent filtering mechanism. The reason is that the manner in which the cell accumulates its internal variables caused the mechanism. Experiments showed the migration threshold of the cells relates to the transfer function of the algorithm. Furthermore, they proposed a tuning methodology and revisited a robotic application published previously using the new tuning technique.

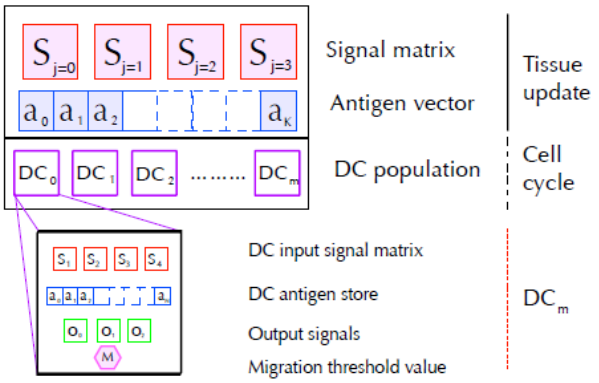

Fig.2. Tissue and cell update component

To deal with the highly randomness, a large amount of parameters, and the difficulty to analyze the original DCA, a deterministic DCA (dDCA) is proposed in [18]. In this paper the deterministic DCA is implemented and tested using a port scan dataset. Experiments show that the dDCA is a controllable system, and the time windows and the variation on the number of cells have the influence on the algorithm. In addition to this, the dDCA introduces a novel metric to assess the algorithms output. Experiments show that the new introduced metric is more sensitive than the metric of the original DCA. Gu et al applied the DCA to a standard data set, namely the KDD 99 data set [19]. In this paper, they reported the results of different versions of the DCA, including antigen multiplier and moving time windows. Experiment results suggested that the DCA is suitable to KDD 99 data set, and the antigen multiplier and moving time windows have a little effect on the DCA due to this particular data set.

In [20] Gu et al. used the duration calculus method to specify a simplified single-cell model of the DCA. In this paper each individual cell of DCA acts as a detector in real-time. Furthermore, they used the real-time analysis component to replace standard DCA, and performed the periodic analysis of real-time detection. In [21] Gu et al developed a real-time analysis component to replace the offline analysis. Firstly, the segmentation is applied to the DCA, namely segmenting the output into slices and performing the analysis. Then, two segmentation approaches of the antigen based segmentation and the time based segmentation were introduced and tested. Experiments showed that compared with the standard DCA, the DCA with segmentation has significantly better results in some cases and is suitable for the real-time

analysis. In [22] Stibor et al. examined the DCA (DCA) from the mathematical perspective. In this paper the dot product is used to represent the signal processing phase, and the signal processing element can be represented as a collection of linear classifiers. Furthermore, they found that these classifiers have the drawback due to the parallel decision boundaries, and limits the applications of DCA. In this paper an expanded view of an example boundary region can be shown in Fig.3. Form Fig.3, the conclusion can be drwan that the classification distribution of DCA is not gradiated, but varies significantly only for minor changes in input signal. Experiment results demonstrated their viewpoint. So they suggested a nonlinear signal process model should be developed. However, this paper didn't give the concrete solution.

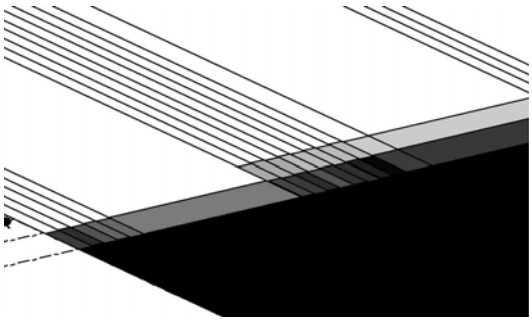

Fig.3. An expanded view of an example boundary region

In [23] Musselle et al. investigated the antigen sampling component of the dDCA. They proposed a model to produce synthetic data for two temporal correlation problems. They explored to use a multi-agent population to sample the antigens, and suggested that the capacity of antigen pool should be variable. In [24] Chen proposed an improved DCA which was called real-time dendritic cell algorithm (rtDCA), which can perform online analyzing, outputting dynamic anomaly metrics. The rtDCA redefines the concept of lifespan of DCA, and the total lifespan of DCA is divided into two phases, namely the lifespan of tissue and the lifespan of lymph. The lifespan of tissue is determined by the threshold, and the relationship between the lifespan of tissue and the lifespan of lymph can be expressed as

$$I_2 = 1 + \beta I_1 \ , \qquad (4)$$

where I_1 and I_2 are the lifespan of tissue and the lifespan of lymph respectively, and β is the apoptosis factor. The data structure of rtDCA can be shown in Fig.4 [24]. The DC with bigger migration threshold will sample more signals and antigens in the tissue, and its lifespan of lymph will be prolonged to take full advantage of its information. Next, the random replacement mechanism is used to limit the capacity of lymph in the rtDCA. Experiment results showed that rtDCA can get high detection rate and low false alarm rate, and the value of immigration threshold should fully consider the response speed and robustness at the same time.

In [25] Gu et al. proposed an improved DCA, which introduced adjuvants to DCA. This improved DCA can increase the immunogenicity of stealthy malware and accelerate the reaction of DCs. Experiments showed that the improved DCA can improve the detection rate for stealthy malware as well as the hidden malware. In [26] Silva et al. documented the development of the models for engineering systems from the transitional view aspect. In [27] the signals and antigens of DCA are more explicitly redefined based on the outputs of the change point detecting subspace tracker developed for detecting key change points across multiple data streams. Experiment results demonstrated the redefinition for antigens is meaningful. In [28] Gu et al. use the set theory and the mathematic functions to define the deterministic DCA (dDCA), and analyze the runtime of the standard algorithm and the one with additional segmentation. Experiments show that the introduced segmentation changes the algorithm's worst case. Furthermore, for further development, two runtime variables are formulated to understand its runtime behaviours.

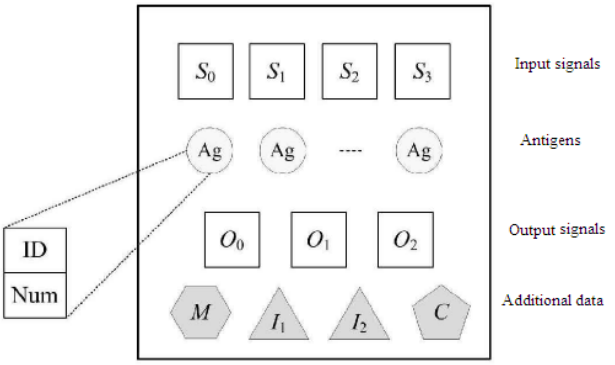

Fig.4. Data structure of rtDCA

From the above analysis, we can see that the immigration threshold has an important influence on the detection rates. However, no paper illustrates how to set the immigration threshold in theory.

C. Decision Method for Load Anomaly Judgment

In [10] Greensmith gave the concept of MCAV, namely it is mean value of context per antigen type, and MCAV can be expressed as

$$\text{MCAV of antigen type} = \text{mature count / antigen.} \qquad (5)$$

Then the value is closer to one, it is more likely that the majority of the antigens are a set of signals. When the value of MCAV is larger than a preset threshold, the detection system will generate alarm signal.

In [29] Al-Hammadi et al. proposed the MCAV Antigen Coefficient (MAC) , it is can be expressed as

$$MAC_x = \frac{MCAV_x * Antigen_x}{\sum_{i=1}^{n} Antigen_i} \ , \qquad (6)$$

where $MACV_x$ means the value of $MCAV$ of the x^{th} type of antigen, and $Antigen_x$ means the number of the x^{th} type of antigen.

However, *MCAV* and *MAC* are the static abnormal index, and can't reflect the dynamic index. Then Chen proposed the dynamic index, namely dynamic *MCAV* and dynamic *MAC* [24], and the dynamic MCAV and the dynamic *MAC* can be expressed as Equ.7. In Equ.7 V_a and C_a mean the dynamic *MCAV* and dynamic *MAC*, respectively, a means the antigen type, m_a means the mature number of the a^{th} type of antigen, A_a is the total number of the a^{th} type of antigen.

$$V_a = \frac{m_a}{A_a}$$
$$C_a = \frac{V_a A_a}{\sum_{i=1}^{A} A_i}, \tag{7}$$

In [30] Chelly et al. proposed a fuzzy dentritic cell method (FDCM) within the framework of fuzzy set theory. The method uses the fuzzy set theory to smooth the abrupt separation between normality and abnormality. Experiments show that the improved DCA has a better accuracy than DCA. In [31] Kumari et al. proposed a novel intrusion detection method, which combines the DCA with dempster-belief theory. Experiments show that the proposed method can improve the detecting rates and decrease the false alarm rates. In [32] Li et al. proposed a network malicious code DCA based on fuzzy weighted SVM. This method applies the coefficient of variation method to determine the values of the weights.

In [12] Chen et al. proposed an integrated artificial immune system (IAIS), which combined DCA with negative selection algorithm (NSA). The DCA was employed to detect behavioral features, and the NSA was employed to detect structural features. Experiments showed that compared with single detection model, the integrated detection model can increase the detection rates and decrease the false alarm rates.

From the above analysis, we can see that the decision methods for load anomaly judgment are appearing the trend of integration model.

D. Application Research of DCA

To detect the worm intrusion, Kim et al. proposed a cooperative automated worm response and detection immune algorithm by simulating the interaction mechanism between DCs and T-cell. This paper explained the three central T-cell processes, namely T-cell maturation, differentiation and proliferation. However, this paper only proposed the blueprint, and didn't test it practically [33]. Greensmith et al. implemented the DCA using an immune inspired framework, libtissue, and applied the DCA to the real-time port scan detection [34] and the SYN scan detection [35]. Port-scan detection shows that DCA can be applied to the anomaly detection, and discriminate between normal behaviour processes and abnormal behaviour processes. SYN scan detection shows that DCA can be applied to detect anomaly intrusion in the complicated condition. Wallenta et al. illustrated the process of the DCA detecting an attack on a sensor network using two separate implementations, namely a J-sim simulation and an TinyOS implementation for the T-mote Sky sensor. In addition to this, this paper also introduced an interest cache poisoning attack and a series of the detection processes [36]. Oates et al. applied the DCA to a robotic classification problem. An investigation on the effects of the different migration threshold median of the cell population is carried out when the DCA was implemented on a real robot. Experiments showed that the DCA can be employed as a classifier within the field of robotic security [37]. Mokhtar et al. proposed a modified DCA to detect the robotic system online. First, the DCA was implemented on both simulated robotic units and an online micro-controller with constrained resource, and the errors brought by micro-controller can be transmitted into the robotic unit [38]. According to the task scheduling in real-time embedded systems (RTES), Lay illustrated more detailed general applicability of the DCA than precious work in [39]. Lay deemed that the examination of the results of the DCA was related to the overall problem difficulty. Furthermore, he presented a detailed understanding of how the DCA can clearly identify the difficultly detected anomalies [40]. Kim et al. claimed that the ideas of AIS can be applied into the sensor networks, and illustrated that the danger theory especially the DCA can closely match the structure and functional requirements of sensor networks. In addition to this, Kim et al. illustrated that the DCA can be applied to detect a new sensor network attack which is called an Interest Cache Poisoning Attack [41]. Wallenta et al. investigated a method to use the danger theory based Artificial Immune System, such as the DCA to detect an attack of a sensor network, namely using J-sim to simulate and using TinyOs to implement the T-mote Sky sensor, respectively. Furthermore, they investigated how the DCA detected the interest cache poisoning attack in a series of experiments [42].

Al-Hammadi et al. firstly illustrated the behavioural attributes correlation between the key logging and the packet flooding behaviour. Then, they used the spearman's rank correlation algorithm and DCA to detect the existence of a single bot, irrespectively. Experiments showed that compared with the spearman's rank correlation algorithm, the DCA has a better accuracy [43]. In [44] Yuan et al. proposed a real-time analysis algorithm, which can immediately output and assess an antigen presented by sufficient DCs. In this paper, sufficient assessments are used to reduce the influence brought by the errors, and the antigen and signal pool of temporal correlation can eliminate the mutual interference of the antigens and signals. Experiment results showed that the real-time analysis algorithm can obtain ideal accuracy.

To deal with the unordered data set in anomaly detection, Yuan et al. proposed a multiple and merging DCA. First, the data set is multiplied n times. Next, each instance is assessed. Finally, the n assessments for each type of antigens are merged, and the corresponding results are obtained [45]. Yang et al. used the DCA to detect and analyze web server aging. Experiments show that DCA is beneficial to improve the quality of service in web server systems [46]. Lee et al. used the

mechanisms of migration and maturation of DCA to search the pareto optimal solutions of complex problems. In this paper they further studied the applicability of DCs within DC-mediated Signal Cascading Framework. For example, they studied the ability of convergence of the Pareto Front [47]. Nigam et al. analyzed many applications, such as the strengthening of protein coding regions using CSA, data mining of proteins using NSA & DCA, and clustering of micro-array using multi-objective AIS. Experiments showed that the above applications further validate the algorithms. Therefore, the corresponding conclusion can be drawn that AIS can be applied to model and predict for the most of the important domains of bioinformatics [48].

From the above analysis, we can see that the DCA has been successfully applied into various fields. However, compared with the traditional immune algorithm, the application studies for DCA are not profound enough, and need further study.

IV. SUGGESTED SOLUTION FOR THE PROBLEMS EXISTINBG IN DCA

From the above analysis, we can see that the main problems existing in the DCA can be summarized as follows:

- The signal variance of networks is a very complicated process, and the original data sampled by DCs is not linearly separable. So the original datum should be transformed into a linearly separable datum before extracting the features in DCA.
- The immigration threshold will influence the maturation time of DCs. Too small immigration threshold of DC will lead to a premature, and the DCs will become more sensitive to external environment. Conversely, too big immigration threshold of DCs will lead to plethora accumulation information, and the DCs can't reflect the external situation. However, there are no papers which give the theory evidence to preset the immigration. According to all the known literature, the immigration threshold is given randomly or experiencedly. So it is necessary to study the theory evidence for the immigration threshold.
- At present, the decision method for load anomaly judgment is based on the ratio between the presented mature DCs and the total presented DCs. So it is necessary to study the cooperation between the mature DCs to restrain the innocent bystander phenomenon and improve the detection rates.

The corresponding solution thought for the above problems existing in the DCA can be described as follows:

- According to the non-linearly separable character of the original data sampled by DCs, the kernel method will be employed to map the original datum into the high-dimensional space, and the original data will be transformed into a linearly separable data. Then, the PCA or RST may be employed to extracting the features of DCA.
- To study the theory evidence for the immigration threshold, the lifespan will be introduced into the DCA. Then the relationship model between the immigration threshold and the changing trend of type and number of antigens sampled by DCs at different ages will be build. Finally, the theory evidence will be acquired through the relationship model.
- The variance with time of each type of antigen can be observed through the cooperation mechanism of the DCs mature in different ages. Then the number of those antigens easily misclassified into anomaly antigens due to the innocent bystander phenomenon will be decreased through the cooperation mechanism.

V. CONCLUSIONS

This paper surveyed the progress of DCA for abnormal detection. This paper reviewed the research progress of DCA from the four aspects, and proposed the corresponding solving thoughts for the main problems existing in the DCA.

From the above analysis, we can see that it is hard to get the statistics data in DCA. So the future development of DCA is that the DCA should be integrated with other artificial immune algorithm which is used for misuse detection.

ACKNOWLEDGMENT

This Project is supported by Hunan Provincial Natural Science Foundation of China (No. 13JJ6058), Hunan Province Science and Technology Plan Foundation of China (No. 2010 GK3018), Scientific Research Fund of Hunan Provincial Education Department (No. 12C0290), Scientific Research Fund of Ethnic Affairs Commission (No. 12JSZ002), and National Natural Foundation of China (No. 61262032).

REFERENCES

[1] L.Q. Xie, F. Yu, C. Xu. Distributed Firewall with Intrusion Detection System[J]. Journal of Computers, Vol 7, No 12 (2012), 3110-3115

[2] S. Forrest, A.S. Perelson, L. Allen, et al. Self-nonself discrimination in a computer [C]. Proceedings of the 1994 IEEE symposium on research in security and privacy. Los Alamos, CA: IEEE computer society, 1994: 202-209.

[3] L.N. de Castro, F.J. Von Zuben. The clonal selection algorithm with engineering applications [C]. Proceedings of the genetic and evolutionary computation conference. Las Vegas, USA: ACM, 2000: 36-37.

[4] L.N. de Castro, F.J. Von Zuben. An evolutionary immune network for data clustering [C]. Proceedings of the IEEE Brazilian symposium on artificial neural networks. Rio de Janeiro, Brazil: IEEE computer society, 2000: 84-89.

[5] P. Matzinger. Tolerance, Danger and the Extended Family. Annual Review of Immunology, 12(1), 1994: 991–1045.

[6] U. Aickelin, P. Bentley, S. Cayzer, et al. Danger theory: The link between ais and ids [C]. Proceedings of the Second International Conference on Artificial Immune Systems (ICARIS-03), Edinburgh, 2003:147–155.

[7] J. Greensmith, U. Aickelin, S. Cayzer. Introducing

Dendritic Cells as a Novel Immune inspired Algorithm for Anomaly Detection [C]. Proceedings of the 4th International Conference on Artificial Immune Systems, Alberta, 2005:153–167.

[8] M.B. Lutz, G. Schuler. Immature, semi-mature and fully mature dendritic cells: which signals induce tolerance or immunity [J]. Trends in Immunology, 23(9), 2002: 445-449.

[9] J. Greensmith, U. Aickelin, J. Twycorss. Articulation and clarification of the dendritic cell algorithm [C]. Proceeding of International Conference on Artificial Immune System (ICARIS 2006). Oeiras, Portugal: Springer Verlag, 2006:404-417.

[10] J. Greensmith. The Dendritic Cell Algorithm [D]. Thesis of Doctor of Philosophy, University of Nottingham, 2007.

[11] F. GU, J. GREENSMITH, U. AICKELIN. Further exploration of the dendritic cell algorithm [C]. International Conference on Artificial Immune Systems, Phuket, Thailand, 2008:142-153.

[12] Y.B. Chen, C. Feng, Q. Zhang, C.J. Tang. Integrated artificial immune system for intrusion detection [J]. Journal of communications, 2012, 33(2): 125-131.

[13] F. Gu, J. Greensmith, R. Oates, et al. PCA 4 DCA: the application of principal component analysis to the dendritic cell algorithm [C]. Proceeding of the 9th Annual Workshop on Computational Intelligence, Nottingham, UK, 2009.

[14] F. Gu. Theoretic and empirical extensions of the dendritic cell algorithm [D]. Thesis of Doctor of Philosophy, University of Nottingham, 2011.

[15] Z. Chelly, Z. Elouedi. RC-DCA: A New Feature Selection and Signal Categorization Technique for the Dendritic Cell Algorithm Based on Rough Set Theory [J]. Artificial immune systems, 2012, 7597:152-165.

[16] J. Greensmith, U. Aickelin, J. Feyereisl. The DCA-SOMe comparisons: a comparative study between two biologically-inspired algorithms [J]. Evolutionary Intelligence: Special Issue on Artificial Immune System, 2008, 1(2):85-112.

[17] R. Oates, G. Kendall, J.M. Garibaldi. Frequency analysis for dendritic cell population tuning [J]. Evolutionary Intelligence: Special Issue on Artificial Immune System, 2008, 1(2): 145-157.

[18] J. Greensmith, U. Aickelin. The deterministic dendritic cell algorithm [C]. Proceedings of International Conference on Artificial Immune Systems (ICARIS 2008). Phuket, Thailand: Springer Verlag, 2008: 291-302.

[19] F. Gu, J. Greensmith, U. Aickelin. Further exploration of the dendritic cell algorithm : antigen multiplier and time windows [J]. Artificial Immune Systems, 2008, 5132: 142-153.

[20] F. Gu, J. Greensmith, U. Aickelin. Exploration of the dendritic cell algorithm using the duration calculus [C]. Proceedings of International Conference on Artificial Immune Systems (ICARIS 2009). York, UK: Springer Verlag, 2009: 54-66.

[21] F. Gu, J. Greensmith, U. Aickelin. Integrating real-time analysis with dendritic cell algorithm through segmentation [C]. Proceeding of Genetic and Evolutionary Computation Conference. Montreal, Canada: ACM, 2009: 1203-1210.

[22] T. Stibor, R. Oates, G. Kendall, et al. Geometrical insights into the dendritic cell algorithm [C]. Proceedings of the 11th Annual Conference on Genetic and Evolutionary Computation. Montreal, Canada: ACM, 2009:1275-1282.

[23] C.J. Musselle. Insights into the antigen sampling component of the dendritic cell algorithm [C]. Proceeding of International Conference on Artificial Immune System (ICARIS 2010). Edinburgh, UK: Springer Verlag, 2010: 88-101.

[24] Y.B. Chen. Study on artificial immune system for intrusion detection [D]. Thesis of Doctor of Engineering, University of defense technology, 2011.

[25] J. Fu. H. Yang. Introducing adjuvants to dendritic cell algorithm for stealthy malware detection [C]. Fifth International Symposium on Computational Intelligence and Design (ISCID), 2012:18-22.

[26] G.C. Silva, R.M. Palhares, W.M. Caminhas. A Transitional View of Immune Inspired Techniques for Anomaly Detection [J]. Intelligent Data Engineering and Automated leaning, 2012, 7435: 568-577.

[27] C. Musselle. Rethinking Concepts of the Dendritic Cell Algorithm for Multiple Data Stream Analysis Artificial Immune Systems, 2012, 7597: 246-259.

[28] F. Gu, J. Greensmith, U. Aickelin. Theoretical formulation and analysis of the deterministic dendritic cell algorithm [J]. Biosystems, 2013, 111(2): 127-135.

[29] Y. Al-Hammadi, U. Aickelin, J. Greensmith. DCA for bot detection [C]. Proceedings of International Congress on Evolutionary Computation (CEC 2008), Washington, DC: IEEE Computer Society, 2008:1807-1816.

[30] Z. Chelly, Z. Elouedi. FDCM: a fuzzy dendritic cell method [C]. Proceeding of International Conference on Artificial Immune System(ICARIS 2010), Edinburgh, UK:Springer Verlag, 2010:102--115.

[31] K. Kumari, A. Jain, S. Dongre, A. Jain. Improving dendritic cell algorithm by dempster belief theory [J]. International journal of Computer Engineering & Technology 2012, 3(2): 415 – 423.

[32] P. Li, R. Wang, Y.T. Zhou, Q.Y. Dai. Research on Network Malicious Code Dendritic Cell Immune Algorithm Based on Fuzzy Weighted Support Vector Machine [J]. Advances in wireless sensor networks communications in computer and information science, 2013, 334:181-190.

[33] J. Kim, W.O. Wilson, U. Aickelin, et al. Cooperative automated worm response and detection immune algorithm(CARDINAL) inspired by T-cell immunity and tolerance [C]. Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS 2005). Banff, Alberta, Canada: Springer Verlag, 2005:168--181.

[34] J. Greensmith, U. Aickelin. Dendritic cells for real-time anomaly detection [C]. Proceedings of workshop on artificial immune systems and immune system modeling, Bristol, UK, 2006:7-8.

[35] J. Greensmith, U. Aickelin. Dendritic cells for SYN scan detection [C]. Proceedings of the 9th annual conference on Genetic and evolutionary computation. London, England, U.K.: ACM, 2007: 49--56.

[36] C. Wallenta, J. Kim, P.J. Bentley, et al. Detecting interest cache poisoning in sensor networks using an artificial immune algorithm [J]. Applied Intelligence, 2008, 32(1): 1-6.

[37] R. Oates, J. Greensmith, U. Aickelin, et al. The application of a dendritic cell algorithm to a robotic classifier [C]. Proceedings of the 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil: Springer Verlag, 2007:204-215.

[38] M. Mokhtar, Bi R, Timmis J, et al. A modified dendritic cell algorithm for online error detection in robotic systems [C]. Proceeding of 11th Congress on Evolutionary Computation (CEC 2009), Trondheim, Norway: IEEE Computer Society,2009: 2055-2062.

[39] N. Lay, I. Bate. Applying artificial immune systems to

real-time embedded systems [C]. Proceeding of Congress on Evolutionary Computation, Singapore: IEEE Computer Society, 2007: 3743--3750.
[40] N. Lay. Improving the reliability of real-time embedded systems using innate immune techniques [J]. Evolutionary Intelligence: Special Issue on Artificial Immune System, 2008, 1(2): 113--132.
[41] J. Kim, P.J. Bentley, C. Wallenta, et al. Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm [C]. Proceedings of the 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal: Springer Verlag, 2006:390-403.
[42] C. Wallenta, J. Kim, P.J. Bentley, et al. Detecting interest cache poisoning in sensor networks using an artificial immune algorithm [J]. Applied Intelligence, 2008, 32(1): 1-26.
[43] Y. Al-Hammadi, U. Aickelin, J. Greensmith. Performance e valuation of DCA and SRC on a single bot detection [J]. Journal of Information Assurance and Security, 2010, 5:303--313.
[44] S. Yuan, Q.J. Chen. A Dendritic Cell Algorithm for real-time anomaly detection [C]. IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, Hunan, 2012: 448 – 451.
[45] L.Q. Xie, Y. Wang, F. Yu et al. Research on Intrusion Detection Model of Heterogeneous Attributes Clustering[J]. Journal of Software, Vol 7, No 12 (2012), 2823-2831.
[46] H. Yang, S.J. Yi, Y.W. Liang, J. Fu. Dendritic cell algorithm for web server aging detection [C]. International Conference on Automatic Control and Artificial Intelligence (ACAI), Xiamen, Fujian, 2012: 760-763.
[47] N.M.Y. Lee, H.Y.K. Lau. A Cooperative Multi-objective Optimization Framework based on Dendritic Cells Migration Dynamics [J]. Research and Development in Intelligent Systems XXIX, 2012: 201-206.
[48] D. Nigam, V. Kumar. Artificial Immune System: A potential tool to handle bioinformatics issues [J]. International journal of artificial intelligence and knowledge discovery, 2012, 2(1).

Ding Lei was born in 1972. He received the Ph.D. degree in 2012 from central south university. Now he is an associate professor in school of information science and technology of Jishou University. His research interests include computer network, artificial intelligence and industrial process control.

Fei Yu was born in Ningxiang, China, on February 06, 1973. Before Studying in Peoples' Friendship University of Russia, Russia, He joined and worked in Hunan University, Zhejiang University, Hunan Agricultural University, China. He have taken as a guest researcher in State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Guangdong Province Key Lab of Electronic Commerce Market Application Technology, Jiangsu Provincial Key Lab of Image Processing and Jiangsu Provincial Key Laboratory of Computer Information Processing Technology.

He has wide research interests, mainly information technology. In these areas he has published above 90 papers in journals or conference proceedings and a book has published by Science Press, China (Fei Yu, Miaoliang Zhu, Cheng Xu, et al. Computer Network Security, 2004). Above 70 papers are indexed by SCI, EI.He has won various awards in the past.

He served as many workshop chair, advisory committee orprogram committee member of various international ACM/IEEE conferences, and chaired a number of international conferences such as IITA'07, IITA'08;ISIP'08, ISIP'09, ISIP'10, ISIP'11;ISECS'08, ISECS'09, ISECS'10, ISECS'11; WCSE'08, WCSE'09, WCSE'10, WCSE'11, WCSE'12 and ISISE'08, ISISE'09, ISISE'10, ISISE'12.

Zhenghua Yang was born in 1974. He received the Master's degree in 2008 from Jishou university. Now he is a lecturer in school of information science and technology of Jishou university. His research interests include computer network, data mining, knowledge management.