2011 3rd International Conference on Signal Processing Systems (ICSPS 2011)
IPCSIT vol. 48 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V48.15

Principle and Application of Dendritic Cell Algorithm for Intrusion Detection

Xufei Zheng [1] and Yonghui Fang [2]

[1] College of Computer Science, Sichuan University, Chengdu, China
[2] School of Electronic and Information Engineering, Southwest University, Chongqing, China
Email: zxufei@163.com; fyhui@swu.edu.cn

Abstract. The Dendritic Cell Algorithm (DCA) is inspired by the function of the dendritic cells of the human immune system. In nature, dendritic cells are the intrusion detection agents of the human body, policing the tissue and organs for potential invaders in the form of pathogens. This paper describes biological mechanisms of dendritic cells, presents the principle of DCA and its development, introduces the applications of DCA in intrusion detection field, assesses the performance of DCA with other similar methods based on standard KDD 99 data-set, and points out some problems of DCA.

Keywords: Artificial immune system; Danger theory; Dendritic cell algorithm; Intrusion detection

1. Introduction

Artificial Immune Systems (AIS) are computer systems inspired by Human Immune System (HIS), which are applied to solve real world problems. Since AIS are designed through mimicking the detection mechanism for intruders, obvious Intrusion Detection can be the principal applications of AIS. Currently, the major AIS encompass two different types of immune inspired algorithms, Negative Selection Algorithm (NSA) and Clonal Selection Algorithm (CSA), and which have solved some problems in the past decade [1, 2, 3, 4]. But there are still numerous problems exists, such as scaling issues, detector coverage problems and the generation of excessive undesirable false positives [5, 6]. In response to this situation, Matzinger put forward Danger Theory (DT) in 1994, and the focus of AIS began to shift from the adaptive immune system mechanism study to the innate immune system [7]. In 2003, Aickelin et al. outlined a project named "danger theory" which describes the application of a novel immunological theory, the DT to Intrusion Detection Systems (IDS) [8]. In 2005, Greensmith et al. design and implement the DCA for intrusion detection according to the mechanism of dendritic cell of HIS [9].

In this paper, we introduce the principle and applications of DCA, generalize the development of DCA, and discuss some problems of DCA from theoretically and technically. Our major contributions are firstly we review the principle and application of DCA; secondly we compare the DCA with some other AIS algorithms and analyze the DCA from theoretically and technically; and finally we discuss some possible improvement of DCA for intrusion detection.

The paper is organized as follows. In section 2 we introduce the danger theory and compare with traditional strategy of AIS. In section 3 we discuss the bio-mechanism of dendritic cell of HIS, the design and implement of DCA, and the development of DCA. In section 4 we enumerate some typical applications of DCA for intrusion detection. In section 5 we compare the DCA with some other method of AIS, and analyze the DCA from theoretically and technically. The conclusions are given in section 6.

2. The Danger Theory Approach

The danger theory, proposed by immunologist Matzinger, emphasizes the crucial role of the innate immune system for guiding the adaptive immune responses [7]. She stated that the only pathogens detected are the ones that induce necrosis and cause actual damage to the host tissue, not the detection of antigen structures or bacterial products. Unlike detecting exogenous signals, the DT rests on the detection of endogenous signals, which arise as a result of damage or stress to the tissue cells themselves. It is suggested that DCs have the capability to combine signals from both endogenous and exogenous sources.

Figure 1 depicts how we might picture an immune response according to the DT. A cell in distress sends out an alarm signal, whereupon antigens in the neighbor are captured by Antigen Presenting Cells (APCs), which then present the antigens to lymphocytes. Accordingly, the danger signal establishes a danger zone around itself. Thus B cells producing antibodies that match antigens within the danger zone get stimulated and undergo the activation process. Those antibodies do not get stimulated that do not match antigens or outside the danger zone.

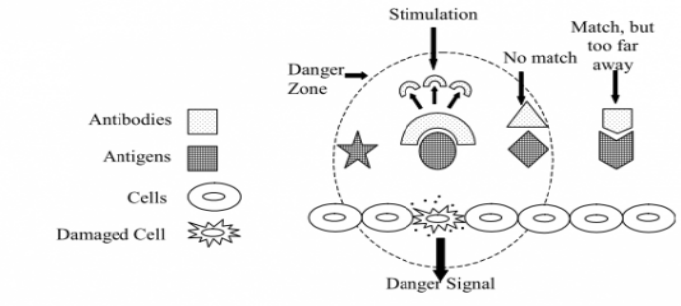

Fig.1. The Danger Theory Model

The central idea in the DT is that the immune system does not respond to non-self but to danger, this is the essential difference to the self-nonself (SNS) pattern. Compared to the SNS pattern, the DT approach can bring two major benefits: firstly the DT approach does not require the removal of all non-self antigens but dangerous ones, and take immune tolerance to those non-self antigens but not dangerous, thereby reducing the false positive; and secondly the DT approach does not distinguish between self and non-self, but only respond to harmful antigen in the danger zone presented by APCs (but all antigens in SNS pattern), thereby reduce the calculation and improve detection efficiency.

3. Dendritic Cell Algorithm

3.1. Biological Mechanism of DC

DCs are white blood cells, which have the capability to act in two different roles - as macrophages in peripheral tissues and organs and as a vehicle for antigen presentation within the secondary lymphoid organs. The DCs' initial function is to collect debris from the tissue inclusive of antigen. The DCs migrate from the tissue and presents any collected debris as antigen to T-cells, causing activation immune response. In addition, the DCs deal with environmental elements and release of specific cytokines to influence T cell differentiation process, in which facilitate the immune response of T cells.

There are 3 states of DC: immature DC (iDC), semi-mature DC (smDC), and mature DC (mDC). Essentially, the DC is a biological anomaly detector [10] that combines a variety of input signals, process a large number of antigens to provide health-related environmental signals for T cells and tissues.

When a DC meets Pathogen-Associated Molecular Pattern (PAMP) or the danger signals from dying cells, the DC matures from iDC to mDC, and secrets IL-12 besides present antigen to the effector T-cells. Conversely, signals collected as a result of apoptotic death causes the DC to change from iDC to smDC and secrets IL-10. The smDC cannot activate T- cells, but cause presentation of antigens in a tolerogenic context, vital to the prevention of autoimmunity. When the concentration of IL-12 is higher than IL-10, it means that the antigens presented are in the abnormal environment, and vice versa it means normal. Inflammation can affect a DC by acting as an amplifier for the potency of all additionally received signals. The smDC and mDC

both secret CD80/86, they migrate from the tissue to lymph node and drive the immune response or immune tolerance of T cells when the concentration higher than the threshold.

3.2. Apply DCs to AIS

DCs have the ability to combine signals from apoptosis, necrosis and PAMPs and to use this information to instruct the immune system to respond appropriately. As stated in [11], DCs are treated as processors of both exogenous and endogenous signal processors. Input signals are categorized either as PAMP Signals (PS), Danger Signals (DS), Safe Signals (SS) or Inflammatory Signals (IS) and represent a concentration of signal. They are transformed to output concentrations of co-stimulatory molecules (CSM), smDC cytokines (semi-mature) and mDC (mature) signals. The signal processing function described in Equation 1 is used with the empirically derived weightings presented in Table 1. This function is used to combine each of the input signals to derive values for each of the three output concentrations, where C_x is the input concentration and W_x is the weight.

$$C_{[CSM,semi-mature,mature]} = \frac{(W_{PS} * C_{PS}) + (W_{DS} * C_{DS}) * (1 + IS) + (W_{SS} * C_{SS})}{W_{PS} + W_{DS} + W_{SS}} * 2 \quad (1)$$

$$CSM_n = DS_n + SS_n \quad (2)$$

Where CSM_n, DS_n and SS_n are the current sample of the danger signal, the safe signal, and CSM value.

Table1.Weighting values for the signal processing function based on DC maturation ratios

Signals	CSM	semi-mature	mature
PAMP Signals (PS)	2	0	2
Danger Signals (DS)	1	0	1
Safe Signals (SS)	2	3	-3

3.3. Design and Implementation of DCA

Greensmith et al. study the physiological function and role of DC and design the DCA based on DC behavior modeling [10]. The DCA is a population-based algorithm, designed for tackling anomaly-based detection tasks. It is inspired by functions of natural DCs of the innate immune system, which form part of the body's first line of defense against invaders.

The DCA correlate the data streams of antigen and different signals (including PAMPs, danger, safe signals and inflammation), the output information indicates that abnormal level of antigens. The DCA is not a classification algorithm, which does not indicate whether the abnormal of antigens, but the abnormal degree. The abnormal degree is express as Mature Context Antigen Value (MCAV) which is the percentage of the antigens presented in mature context to total antigens as described in Equation 3. By comparison of the value of MCAV with the threshold to determine whether there is an anomaly. It provides information representing how anomalous a group of antigens are, not simply if a data item is anomalous or not.

$$MCAV = o_1/(o_1 + o_2) \quad (3)$$

Where o_1 is the count of mDCs, and o_2 is the count of iDCs as well as smDCs.

The signal processing performed in the form of a weighted sum equation, bypassing the modeling of any biologically realistic gene regulatory network or signal transduction mechanism. In the generic algorithm, the only crucial component of this procedure is the ability of the end user to map raw input data to one of the four categories of input signals. The general form of the signal processing equation is shown in equation 4, where PS_n, DS_n, SS_n are the input signal value of PAMP signals (PS), danger signals (DS) and safe signals (SS), PS_w, DS_w, SS_w are the related weights, and IS represents the inflammation signal.

$$Output = \left(\sum (PS_n * PS_w) + \sum (DS_n * DS_w) + \sum (SS_n * SS_w)\right) * (1 + IS) \quad (4)$$

Figure 2 shows the overflow information process of DCA, in which DCA as a classifier to effectively handle all kinds of input signals come from DCs' differentiation process.

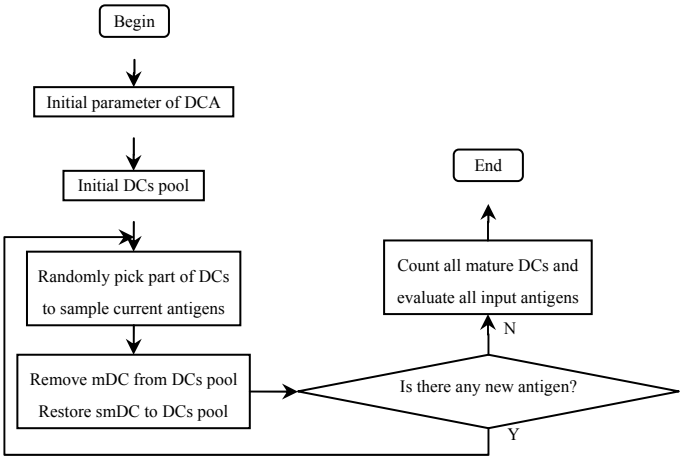

Fig.2. The Algorithm Process of DCA

To illustrate the signal processing capabilities of DCA, Greensmith et al. have designed and implemented a simple prototype system [10]. They use the standard UCI Wisconsin Breast Cancer data-set, containing 700 items, each with nine normalized attributes. Two experiments are performed using the standard Breast Cancer machine learning data-set. This data is divided into class 1 (240 items) and class 2 (460 items). Experiment 1 uses data on a class by class basis. Experiment 2 uses 120 data items from class 1, all 460 items of class 2 followed by the remaining 120 items from class 1. Figure 3 shows that the two experiments' high detection rate, which indicating that the DCA with anomaly detection capability.

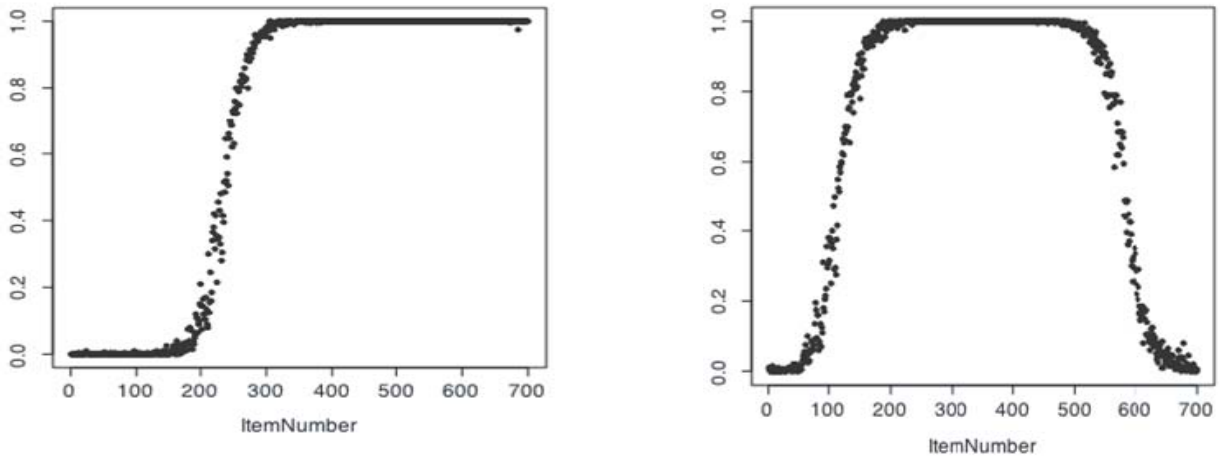

Fig.3. This figure shows the classification of the 700 items. The results for the two different data distributions are presented. The y-axis represents the degree of maturity, from 0 (semi-mature, class1) to 1 (mature, class 2).

3.4. Development of DCA

Theoretical analysis implied that the DCA was simply an ensemble linear classifier, which contradicted some of the claims made previously about the manner by which the DCA functions. In response to this, a large amount of randomness was removed from the algorithm and a simplified version developed, named the deterministic DCA (dDCA) [12]. This DCA variant is predictable in its use; one can follow a single antigen element throughout the system, and given a priori knowledge of the signals used and the antigen's relative position to all other antigen it is possible to predict its classification.

Recently a series of improvements to the original DCA have been made, to respond to some of the criticisms. Firstly, a formal definition of the DCA is given to avoid the potential ambiguities of the algorithm [13]. Secondly, an online analysis component based segmentation approaches is introduced to enable periodic

and continuous analysis [14]. Thirdly, automated data preprocessing methods based on dimensionality reduction and statistical inference techniques for automated signal selection and categorization [15].

4. Applications of DCA for Intrusion Detection

The DCA has been successfully applied to numerous computer security related, more specific, intrusion detection problems, including port scan detection [10, 16], botnet detection [17], a classifier for robot security [18], and malicious behavior detection in wireless sensor networks [19]. According to the results, the DCA has shown not only good performance in terms of detection rate, but also the ability to reduce the rate of false alarms in comparison to other systems.

4.1. Apply DCA to Port Scan Detection

Port scanning is closely related to the attacks of worms and botnets, it will be effectively to prevent later more serious attacks on the early detection of port scan detection. Greensmith et al. use DCA for the detection of port scan, including ICMP scan detection [10] and SYN scan detection [16].

To illustrate the anomaly detection of DCA in ICMP port scanning, Greensmith et al. used different combination of signals and conversion coefficient carry out 4 different experiments, which using nmap tool to produce ICMP scans [10]. The results showed that the algorithm could achieve 100% classification accuracy when appropriate thresholds are used.

The DCA was later on applied to SYN scan detection where the collected dataset consists of over five million data instances [16]. The detection scenario was that the SYN scan was launched from a victim machine, where the DCA is used to monitor the behaviors of the victim. The algorithm produced high true positive rate and low false positive rate, and each experiment could be finished within acceptable time despite the large quantity of data.

4.2. Apply DCA to Botnet Detection

Use either SI (MKS) or CGS as primary units. (SI The DCA was also applied to Botnet detection [17]. Botnets are decentralised and distributed networks of subverted machines, controlled by a central commander, namely “botmaster”. A single bot is a malicious piece of program that can transfer victim machines into zombie machines once installed. This work demonstrated the application of the DCA to the detection of a single bot, to assess its performance on this novel problem area. The results indicated that the DCA was able to distinguish the bot from the normal processes on a host machine.

4.3. Apply DCA to Classifier for Robot Security

The DCA is suitable for time-related data processing, then be used as a classifier for robot [18]. The results indicated that the algorithm performed classification very well without any regulation or training. The author also gave the proposal that how to extend the algorithm to as a classifier for robotic security area.

4.4. Apply DCA to Malicious Behavior Detection in Wireless Sensor Network

Based on the similarity of wireless sensor network and DCs’ biological mechanisms, the DCA is used to detect the malicious behavior in wireless sensor network [19]. Based on the analysis of the Interest Cache Poisoning attack, Kim proposed a DCA-based attack detection system architecture and defined the signals as well as the antigens. Unfortunately, it is not convincing that the author just gave the application framework but lack of experiments or simulation, even so, which still shows a good sense of the DCA in the wireless sensor network security.

In summary, the DCA has shown reasonable detection accuracy in the past applications, and it has the advantage of not having a training phase shortening the application process and low weight in computation improving detection speed.

5. Comparison and Problems of DCA

5.1. Compare DCA with Other Methods

By comparison with other similar methods, we can better to find the characteristics, advantages and disadvantages of DCA. In [20] it is compared the different DCA with real value NSA and C4.5 decision tree by use of standard KDD 99 data-set. The result indicated that the DCA is more suitable to the data-set in classification. In [21] it is compared the performance of the DCA and of a Self-Organizing Map (SOM) when applied to the detection of SYN port scans, through experimental analysis. Two constructed data sets are produced for this purpose consisting of 13 million data items to classify. It is shown that the results of the two systems are comparable, with the DCA producing a significantly improved performance at detecting the anomalous. It is shown that the DCA can be a competitive intrusion detection algorithm.

The applications of the DCA also indicate the strengths of the algorithm as follows: firstly, the DCA does not require a training phase and the knowledge of normality and anomaly is acquired through basic statistical analysis, so the applications may be less time consuming than other supervised learning algorithms; secondly, the DCA performs linear calculations for its computation, making the system low weight and ideally for intrusion detection tasks. Both strengths make the DCA a suitable candidate for intrusion detection tasks, which mainly require high detection speed.

5.2. Problems of DCA

Much of the work regarding the development of the DCA is still in progress. For example, only static segment sizes applied and tested for the online analysis component of the DCA, more adaptive mechanisms where segment size varies according the situations encountered during detection should be investigated. Additionally, only preliminary work has been performed for the automated data preprocessing of the DCA, more techniques of feature selection and feature extraction and more appropriate mechanisms for signal categorization should be evaluated.

6. Conclusions

In this paper, we review the DCA which combines inspiration from the immune system with principles of information fusion to produce an effective anomaly detection technique. On the other hand, the DCA is a new development in artificial immune systems, and as yet has not been extensively tested. Currently, the fundamental study of computational complexity and parameter sensitivity of DCA is not sufficient yet. In the future, the DCA research may emphasized on the following facets:

1) Thorough investigate the immune mechanism of DCs. In order to construct more efficient algorithm, it is needed in-deep understanding of the immune mechanism. Experience has shown that the discovery of the new mechanism will promote the production of the new algorithm.

2) The mathematical analysis of DCA. The mathematical analysis is a general method for algorithm optimization. By use of common mathematical methods analyze the algorithm and form a rigorous theoretical system, which can provide an effective reference for practical applications.

3) The development of more applications. Applications not only reflect the value of algorithms, but also is the standard to test the merits of algorithms. Although the DCA has been applied in many fields, but these applications are relatively simple, mostly concentrated in the security field, and there is a big gap between the practical engineering application. Therefore, we need more practical applications in the validation of DCA to find the algorithm deficiencies and make improvements.

7. Acknowledgment

This work is sponsored by the Fundamental Research Funds for the Central Universities (XDJK2010C025, XDJK2009C023).

8. References

[1] S. Forrest, A. Perelson, L. Allen, R. Cherukuri. “Self－nonself discrimination in a computer,” Proc. IEEE Symposium on Research in Security and Privacy, 1994, pp. 202-212.

[2] S.A. Hofmeyr, S. Forrest. “Immunity by Design: An Artificial Immune System,” Proc. of Genetic and Evolutionary Computation Conference(GECCO1999), Orlando, USA , 1999, pp. 1289-1296.

[3] F.A. González, D. Dasgupta. “Anomaly Detection Using Real-Valued Negative Selection,” Genetic Programming and Evolvable Machines, vol.4, Springer, 2003, pp. 383-403.

[4] J. Zhou, D. Dasgupta. “V-detector: An efficient negative selection algorithm with “probably adequate” detector coverage,” Information Sciences, vol.179, 2009, pp. 1390 – 1406.

[5] T. Stibor, J. Timmis, C. Eckert. “A Comparative Study of Real-Valued Negative Selection to Statistical Anomaly Detection Techniques,” Proc. of 4th International Conference on Artificial Immune Systems (CARIS2005), Springer, LNCS3627, 2005, pp. 262-275.

[6] J. Greensmith, U. Aickelin, J. Twycross. “Articulation and Clarification of the Dendritic Cell Algorithm,” Proc. of the 5th International Conference on Artificial Immune Systems (CARIS2006), Springer, LNCS4163, 2006, pp. 404-417.

[7] P. Matzinger. “Danger Model: A Renewed Sense of Self,” Science vol.296, 1994, pp. 301-305.

[8] U. Aickelin, P. Bentley, S. Cayzer, et al. “Danger theory: The link between ais and ids,” Proc. of the 2nd Internation Conference on Artificial Immune Systems (ICARIS2003), 2003, pp. 147-155.

[9] J. Greensmith. “The Dendritic Cell Algorithm,” PhD Thesis, University of Nottingham, UK, 2007.

[10] J. Greensmith, U. Aickelin, S. Cayzer. “Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection,” Proc. of the 4th International Conference on Artificial Immune Systems (GECCO2005), Springer, LNCS3627, 2005, pp. 153-167.

[11] T.R. Mosmann, A.M. Livingstone. “Dendritic cells: the immune information management experts,” Nature Immunology, vol.5(6), 2004, pp. 564-566.

[12] J. Greensmith, U. Aickelin. “The Deterministic Dendritic Cell Algorithm,” Proc. of the 7th International Conference on Artificial Immune Systems (ICAIS 2008), Springer, 2008, pp. 291-302.

[13] F. Gu, J. Greensmith, U. Aickelin. “Bio-Inspired Communications and Networking,” IGI Global Press, 2011.

[14] F. Gu, J. Greensmith, U. Aickelin. “Integrating Real-Time Analysis With The Dendritic Cell Algorithm Through Segmentation,” Proc. of the Genetic and Evolutionary Computation Conference (GECCO2009), 2009, pp. 1203-1210.

[15] F. Gu, J. Greensmith, R. Oates, U. Aickelin. “PCA 4 DCA: the application of Principal Component Analysis to the Dendritic Cell Algorithm,” Proc. of the 9th Annual Workshop on Computational Intelligence (UKCI2009), 2009.

[16] J. Greensmith, U. Aickelin. “Dendritic Cells for SYN Scan Detection,” Proc. of the Genetic and Evolutionary Computation Conference (GECCO2007), London, UK, 2007, pp. 49-56.

[17] Y.A. Hammadi, U. Aickelin, J. Greensmith. “DCA for Bot Detection,” Proc. IEEE World Congress on Computational Intelligence (CEC2008), IEEE press, 2008, pp. 1807-1816.

[18] R. Oates, J. Greensmith, U. Aickelin, et al. “The Application of a Dendritic Cell Algorithm to a Robotic Classifier,” Proc. of the 6th International Conference on Artificial Immune Systems (ICAIS2007), Springer, 2007, pp. 204-215.

[19] J. Kim, P. Bentley, C. Wallenta, et al. “Danger Is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm,” Proc. of the 5th International Conference on Artificial Immune Systems (ICAIS2006), Springer, 2006, pp. 390-403.

[20] F. Gu, J. Greensmith, U. Aickelin. “Further Exploration of the Dendritic Cell Algorithm,” Proc. of the 7th International Conference on Artificial Immune Systems (ICAIS2008), Springer, 2008, pp. 142-153.

[21] J. Greensmith, J. Feyereisl, U. Aickelin. “The DCA: SOMe Comparison A comparative study between two biologically-inspired algorithms,” Evolutionary Intelligence, vol.1(2), 2008, pp. 85-112.