International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 3 Issue 1 January 2017

Analysis of Adaptive AIS Based Intrusion Detection System

[1]Rachna Lodhi
[2]Anoop Singh
[1]M-Tech Scholar, [2]Guide and Head of Department
[12]Department of Electronics and communication Engineering, VITS, Bhopal, India

ABSTRACT- As fast increase in unauthorized activities and abuse of computing system by each system internal and external entrant trends to extend the degree of network security. so as to extend network security numerous technique has been projected however having a deficiency over IDS system in a number of things i.e. if correlation alarm isn't precise, reduction and interference of false positive and false negative is high , ultimately having shy activity of pattern recognition. So as to beat of this deficiency from IDS, system over network, we propose a completely unique twin detection of IDS supported AIS that group action the DCA and DBT .The DCA helps us to unravel the matter of correlation and DBT theory resolves the matter of unknown and chop-chop evolving harmful attacks. The simulation results shows that the projected technique has improved the accuracy rates, minimizing false +ve and false –ve alarm generation and to extend the potency and accuracy of the IDS system.

KEYWORDS: HIDS, NIDS, SVM, DCA, DBT

I INTRODUCTION

Computer security is an important issue to all users of computer systems. The rapid growth of the internet, computer attacks are increasing and can easily cause millions of dollar damage to an organization. Detection of these attacks is an important issue of computer security. Intrusion Detection Systems (IDS) technology is an effective approach in dealing with the problems of network security.The main goal of Intrusion Detection System is to detect unauthorized use, misuse and abuse of computer systems by both systems insiders and external intruders. There are several methods used to implement intrusion detection such as statistical analysis expert systems, and state transition approaches etc., and these several approaches is based on the immune system were proposed in recent years[2].

Now a day's development of any country or origination is depending upon its information technology system and all the information whether it's confidential, personal or public is shared through internet or network. So any country or organization needs to develop their information sharing network throughout the world with rapid speed. There is a rapid development in making such types of networks which available worldwide and have confidential information. But some time the intruder can attack over network where network based or client based firewall not capable enough to provide complete security against these types of threads [1].

In order to provide complete security against these word wide thread IDS system play a key role. IDS system identifies the unauthorized activity that compromise the integrity, confidentially and availability of confidential information [2].

Conventional IDS is based on continuous monitoring of well know attack by their extensive knowledge of signature to detect intrusion. This method based on pattern recognitions of various audit streams and detect intrusion by comparing their pattern provide by human expert. The pattern has been manually revised for a new type of intrusion whenever discover. The basic limitation of this pattern based Method is cannot detect emerging cyber thread.

Artificial Immune System is an emerging technology in order to fine the intruders or making the IDS. Recently AIS is a new bio-inspired model, which is applied for solving various problems in the field of information security, genetic algorithms, neural networks, evolutionary algorithms and swarm intelligence [4]. As one of the solutions to intrusion detection problems, AIS have shown their advantages. To improve the correlation factor and minimizing the false alarm generation we used the concept of AIS and Dempster-Belief theory (DBT) to identify the intrusion in the system.

II LITERATURE SURVEY

Muhammad Asif Manzoor et al. proposed, [25] Network intrusion detection is critical component of network management for security, quality of service and other purposes. These systems allow early detection of network intrusion and malicious activities; based on this detection, appropriate actions can be applied to manage these attacks. Several network intrusion detection systems are proposed and evaluated and many of them are currently in use to provide better security. Currently, computer networks are generating high volume of data traffic which cannot be analyzed by most network intrusion detection systems. This situation

requires new techniques that can handle huge volume of real time data traffic and it must maintain the high throughput. We have proposed to network intrusion system based on support vector machine in this work. We also propose to use Apache Storm framework; which is a real-time distributed stream processing framework. This network intrusion system is tested for KDD 99 network intrusion dataset.

J. M. Vidal et al proposed, [26] this paper presents an alert correlation system for mitigating the false positives problem on network-based intrusion detection, when anomalous detection techniques are applied. The system allows the quantitative assessment of the likelihood that an alert issued because an anomaly becomes a real threat. To do this the differences between the characteristics of the model representing the habitual and legitimate network usage are taken into account, as well as the most representative features of the traffic that generated the alert.

ManjariJha, Raj Acharya proposed paper, [27] the immune system is built to defend an organism against both known and new attacks, and functions as an adaptive distributed defense system. Artificial Immune Systems abstract the structure of immune systems to incorporate memory, fault detection and adaptive learning. We propose an immune system based real time intrusion detection system using unsupervised clustering. The model consists of two layers: a probabilistic model based T-cell algorithm which identifies possible attacks, and a decision tree based B-cell model which uses the output from T-cells together with feature information to confirm true attacks. The algorithm is tested on the KDD 99 data, where it achieves a low false alarm rate while maintaining a high detection rate. This is true even in case of novel attacks, which is a significant improvement over other algorithms.

Priyanka Suyal et al. proposed paper, [28] Information and communication technology inflate day by day, due to rapid improvement in technologies has increased the need of effective IDS (Intrusion Detection System). Here, Intelligent Intrusion Detection method that is Rough Set based approach presented for performance evaluation of classifier abnormal behavior. Rough Set Theory is used to reduce the input data space, from complex databases and find minimal decision rules or redact, through this we can manage complexity of system and manage huge network traffic. Rough set based effective classification models namely Rule based classifier algorithm with discretization, Decomposition tree algorithm and Decomposition tree with discretization have been applied to find reduced decision rules and classify problem. Comparison of classification results also have perform with various evaluation criteria and recognize best suited classifier for intrusion detection system dataset.

Latifur Khan et al. proposed that, [29] whenever an intrusion occurs, the security and value of a computer system is compromised. Network-based attacks make it difficult for legitimate users to access various network services by purposely occupying or sabotaging network resources and services. This can be done by sending large amounts of network traffic, exploiting well-known faults in networking services, and by overloading network hosts. Intrusion Detection attempts to detect computer attacks by examining various data records observed in processes on the network and it is split into two groups, anomaly detection systems and misuse detection systems. Anomaly detection is an attempt to search for malicious behavior that deviates from established normal patterns. Misuse detection is used to identify intrusions that match known attack scenarios. Our interest here is in anomaly detection and our proposed method is a scalable solution for detecting network based anomalies. We use Support Vector Machines (SVM) for classification. The SVM is one of the most successful classification algorithms in the data mining area, but it's long training time limits its use.

III PROBLEM STATEMENT

The enormous growth of computer network increasing the importance of network security.The central challenge with computer security is to develop systems which have the ability to correctly identify an intrusion which represents potentially harmful activity. Therefore, the role of IDS is as special-purpose devices to detect and prevent the anomalies and illegal access of data.In current scenario, users look for the complete security of data at any cost, since security of data become prime requirement for everyone.The new challenge requires several changes in existing IDS system in order to improve the correlation of alarm; the detection and prediction of false positive and false negative rate must be low. Recently, using biological models such as neural networks and genetic algorithms in modelling and solving computational problems has been spectacularly successful. Lots of traditional IDS techniques are only able to detect and prevent known intrusions and mostly are static. They are not able to recognize unknown intrusions. The biological models has some features such as self-organized, automated, distributed etc., which are now IDS starve for. So

AISTheory for detecting intrusion becomes a new immerging approach in security research.

IV METHODOLOGY

IDS focus on exploiting attacks, or attempted attacks, on networks and systems, in order to take effective measures based on the system security policies, if abnormal patterns or unauthorized access is being suspected. A lot of methods and techniques have been proposed for the effective designing of IDS. But all technique suffered common problem that problem is detection and prediction of false positive and false negative rate is high. Due to this problem the given methodologies are not used in generalize form. So we modified one of the existing second generation AIS algorithm called Dendritic Cell Algorithm for controlling a generation of false alarm generation and also improve classification rate of data more accurately. The Dendritic Cell Algorithm categories efficiently into the normal and abnormal data and Dempster-Belief theory is used to compute the probability of evidences that indicate support the attack or normal class. The use of Dempster Belief theory steadily spreads out, mostly because it is used to cope with large amounts of uncertainties that are inherent of continuously changing environment.

Proposed Framework

The proposed architecture contains various modules each defined with a specific purpose and connected together to identify the exact intruder in the given system. Figure 4.1 shows the architecture for the proposed new methodology for intrusion detection that is based on one of the algorithm of artificial immune system called the Dendritic Cell Algorithm (DCA) and Dempster–Belief Theory (DBT).

The dendritic cell algorithm help us to solve the problem of correlation and Dempster–Belief Theory resolve the problem of unknown and rapidly evolving harmful attacks.

Component of Proposed Framework

1. **Intruder Data:**It is a data set available online in order to perform research work. It is a raw data on which the proposed algorithm will work. In our proposed work use KDD cup 99 dataset,Which are explain to later on chapter 5.
2. **DCA over intruder data:** This part of the proposed model takes the intruder data as a input and apply the DCA algorithm and send the result to further process. Before sending it to different stages it will found the normal and abnormal feature.
3. **Dempstershafer Belief function:**This step is use to calculate the degree of belief of the selected data set. It helps to collect the evidence.
4. **Entropy:**In this part of our work the classification and optimization has performed using support vector machine.

The detail explanation of working steps involved in proposed methodology:

Step1: With the help of Dendritic Cell Algorithm we categorized data, whether the data is normal or affected with anomaly or we can say, abnormal [1].

The algorithm operates in two steps:

Firstly it identifies whether anomalies occurred in the past based on the input data,

Secondly it correlates the identified anomalies with the potential causes, generating an anomaly scene per suspect.

After applying the algorithm, we categorize the data into five category namely Normal, Denial of service attack (DOS),user 2 root attack, remote 2 local attack and probing .

Step2: Dempster-Belief theory is used to compute the probability of evidences that indicate support the attack or normal class .The use of Dempster- Belief steadily spreads out, mostly because it is used to cope with large amounts of uncertainties that are inherent of natural environments. This new approach considers sets of propositions and assigns to each of them an interval [Belief, Plausibility] [2].

Step3.After the classification we calculate the entropy of the attack treated as signal. For the calculation of entropy let us consider set having possible event .Each of which we assumed, occurs some numbers of times. Thus if there are n distinct possible event X1,X2,.....Xn , and the event occurred at frequency N1,N2,.....Nn. Now measure of the probability of event is

$$P(xi) = \frac{ni}{\sum_{j=1}^{N} nj} \quad \text{.....} \quad (1)$$

Now measured entropy, represented by H(x) is calculated with the help of given formula [16]:

$$H(x) = \sum_{i=1}^{N} P(xi)\log(\frac{1}{pi})$$

Bit/message ..... (2)

Where p (xi) the probability of event.

On the basis of calculated entropy we find the intruder. Higher entropy, is regarded as the "intruder", and is generated the alarm. With the help of dual detection technique we can not only minimize the false positive and false negative rate but also improved the correlation technique and improve the intrusion detection rate in the system. So it is a better solution of intrusion detection. In this way we

increase the intrusion detection rate of the system thereby improving the security of the system. However, computational requirement of proposed algorithm also need to be considered.

V RESULT ANALYSIS

Figure 1 shows comparison of the simulation result .It gives the comparison of the degree of Accuracy rate of IDS system by using traditional classification method namely SVM and DCA with our proposed method Hybrid model .Hybrid modal increases the accuracy rate by encapsulating SVM and DCA along with belief function method .As shows in figure 1 SVM & DCA classification algorithm alone having accuracy rate for attack detection never reaches even 92.00% whereas hybrid model having accuracy rate up to 96.00%. The X-axes represents the accuracy rate and the Y-axes indicate detection generating value.

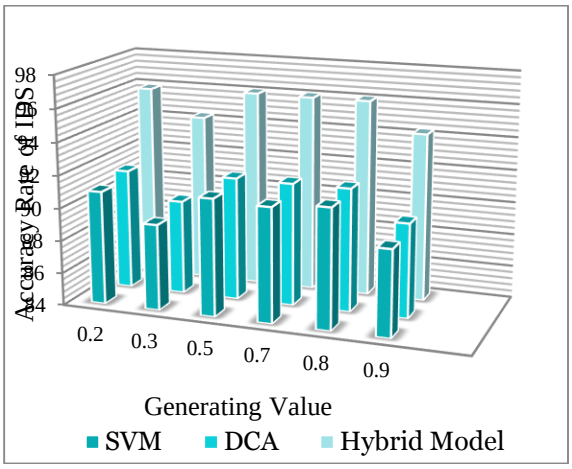

Figure 1 Comparison graph

Figure 2 shows comparison of the true positive rate of IDS system by using traditional classification method namely SVM and DCA with our proposed method Hybrid model. In Hybrid model because of higher degree of filtering minute suspicious data take as abnormal data that's leads to minimizing the true positive rate by encapsulating SVM and DCA along with belief function method .As shows in figure 2 SVM & DCA classification algorithm alone having higher level of true positive rate because of lower level of filtering whereas in proposed hybrid model due to multilevel filtering having lower level of true positive rate. The X-axes represents the true positive rate and the Y-axes indicate detection generating value.

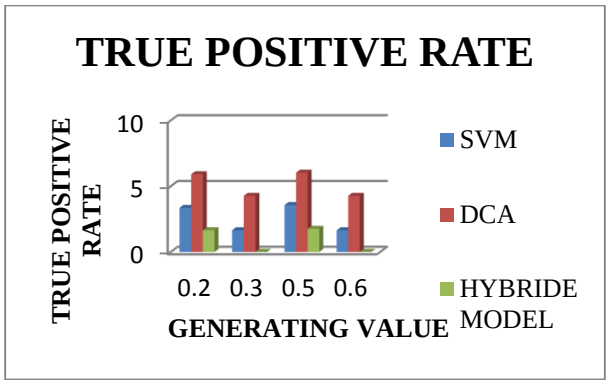

Figure 2: Comparison graph of true positive rate

Figure 3 shows comparison of the true negative rate of IDS system by using traditional classification method namely SVM and DCA with our proposed method Hybrid model. Here same as true positive rate because of multilevel filtering or verification Hybrid modal having lower true negative rate .As shows in figure 3 SVM & DCA classification algorithm alone having higher level of true negative rate because of lower level of filtering whereas in proposed hybrid model due to multilevel filtering having lower level of true negative rate. The X-axes represents the true negative rate and the Y-axes indicate detection generating value.

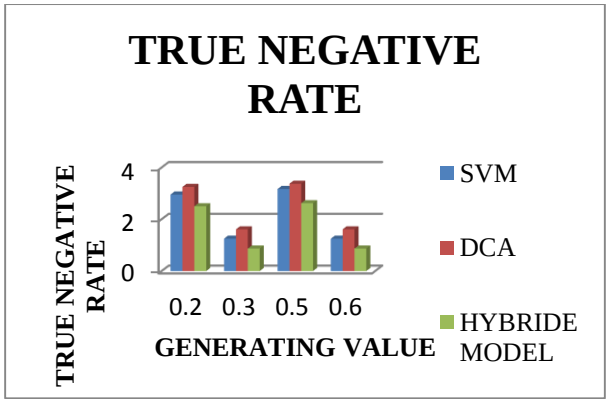

Figure 3: Comparison graph of true negative rate

False positive means if any data is abnormal and our system take it as normal ,higher FPR leads lower level of accuracy. Figure 4 shows comparison of the false positive rate of IDS system by using traditional classification method namely SVM and DCA with our proposed method Hybrid model. As per requirement Hybrid modal minimizing the false positive rate by encapsulating SVM and DCA along with BE method that's trend to lead higher accuracy

rate . The X-axes represents the false positive rate and the Y-axes indicate detection generating value.

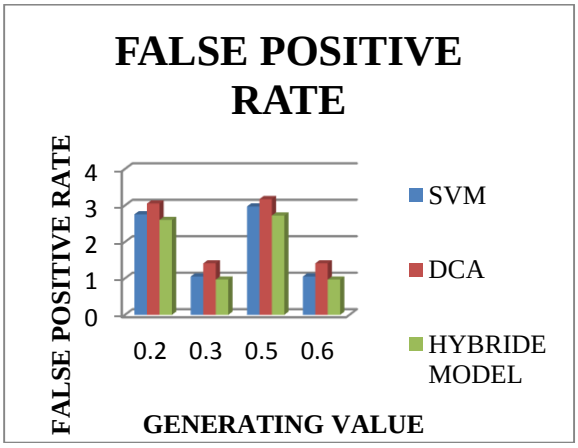

Figure 4: Comparison graph of false positive rate

False negative means if any data is normal and our system take it as abnormal. Figure 5 shows comparison of the false negative rate of IDS system by using traditional classification method namely SVM and DCA with our proposed method Hybrid model. Here same as true positive rate and true negative rate because of multilevel filtering or verification Hybrid modal having lower false negative rate .As shows in figure 5 SVM & DCA classification algorithm alone having higher level of false negative rate because of lower level of filtering whereas in proposed hybrid model due to multilevel filtering having lower level of false negative rate. The X-axes represents the false negative rate and the Y-axes indicate detection generating value.

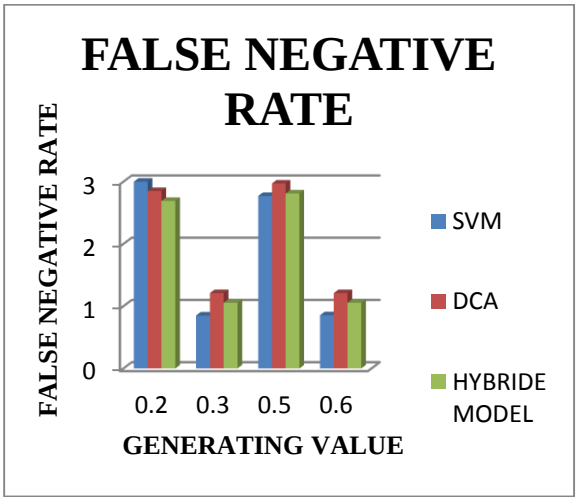

Figure 5: Comparison graph of false negative rate

CONCLUSION

In order to overcome all these deficiency from IDS, system over network ,we propose a novel dual detection of IDS based on AIS that integrating the DCA and DBT .The DCA helps us to solve the problem of correlation and DBT theory resolves the problem of unknown and rapidly evolving harmful attacks.

The simulation results shows that the proposed method has improved the accuracy rates, minimizing false +ve and false –ve alarm generation and to increase the efficiency and accuracy of the IDS system.

REFERENCES

[1]FarhoudHosseinpour, Kamalrulnizam Abu Bakar, Amir HatamiHardoroudi, NazaninsadatKazazi, "Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems" International Conference on Intelligent Networking and Collaborative Systems, IEEE , pp 323-324,Nov-2010.

[2] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.

[3] Chung-Ming Ou, Yao-Tien Wang C.R. Ou , "Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems",International Conference on Fuzzy Systems , IEEE,pp 115 - 122,2011.

[4] SazzadulHoque, Md. Abdul Mukit and Md. Abu Naserbikas,"An implementation of intrusion detection System using genetic algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, pp109-120, March 2012.

[5] Mattew A. Bishop, "Computer Security: Art and Science", Addison WesleyLongman Publishing co., pp:1120, New York, NY, USA, 2002.

[6] William Stallings,"Cryptography &Network Security Principles & Practices", Intrusion Detection (pp.571) (3rd Edition,2003).

[7] EshghiShargh, "Using Artificial Immune System on Implementation of Intrusion Detection Systems", Third UKSim European Symposium on Computer Modelling and Simulation, IEEE, pp164-168, Nov-2009.

[8] Xuanwu, Zhou, "Evolutionary Algorithm and its Application in Artificial Immune System", Second International Symposium on Intelligent Information Technology Application (IITA-08), Vol: 3, pp.32-36, Dec- 2008.

[9] H. Debar, A. Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts", the Fourth workshop on the Recent Advances in Intrusion Detection(RAID), LNCS 2212, pp 85-103,2001.

[10] Julie Green smith, Jamie Twycross and UweAickelin, "Dendritic Cells for Anomaly Detection",IEEE Congress on evolutionary Computation, IEEE, pp664-671,July-2006.

[11] Emma Hart , Jon Timmis, "Application areas of AIS: The past, the present and the future", Applied soft computing science direct,Vol:8,Issue:1,pp191-201,2008.

[12] Lu Hong, "Immune Mechanism Based Intrusion Detection Systems", International Conference on Networks Security, Wireless Communications and Trusted Computing, vol.2,pp.568-571April-2009.

[13] Wei Hu, Jianhua Li QiangGao, "Intrusion Detection Engine Based on Dempster-Shafer's Theory of Evidence", International Conference On Communication, Circuit and System Proceedings, Vol: 3, IEEE, pp1627-1631, June-2006.

[14] D. Dasgupta,"Immunity-based intrusion detection system: a general framework", Proceeding of the 22nd National Information Systems Security Conference (NISSC) , pp.147-160,1999.

[15] Matzinger. P,"Tolerance, Danger and the Extended Family", Annual Review in Immunology, vol.12, pp. 991-1045,April-1994.

[16] Aickelin U, Cayzer S, "The Danger Theory and Its Application to AIS", 1st International Conference onAIS, pp. 141-148, 2002.

[17] Dasgupta and Gonzalez, "An Immunity-Based Technique to Characterize Intrusions in Computer Networks",IEEE Transaction on Evolutionary Computation, Vol:6,Issue:3, pp.281-291,June-2002.

[18] Li Rui , Luo Wanbo , "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications ,IEEE,Vol:1,pp-86-90,July-2010.

[19] YUAN Hui, LIU Jian-yong, "Intrusion Detection Based on Immune Dynamical Matching Algorithm", International Conference on E-Business and E-Government, IEEE, pp-1342-1345, 2010.

[20] Lei Deng, De-yuan Gao, "Research on Immune based Adaptive Intrusion Detection System Model",International Conference on Networks Security, Wireless Communications and Trusted Computing,IEEE ,pp-488-491,April-2009.

[21] Junmin Zhang, Yiwen Liang, "A Novel Intrusion Detection Model Based on Danger Theory", Pacific-Asia Workshop on Computational Intelligence and Industrial Application, IEEE, Vol: 2,pp-867-871, Dec-2008.

[22] Haidong Fu , Xiuo Yuan, Liping Hu , "Design of a Four-layer Model Based on Danger Theory and AIS for IDS",International Conference on Wireless Communication, Networking and Mobile Computing, IEEE,pp-6337-6340,Sept-2007.

[23] BaoyiWANG ,Shaomin ZHANG , "A New Intrusion Detection Method Based on Artificial Immune System",IFIP International Conference on Network and Parallel Computing – Workshops ,pp-91-98,Sept-2009.

[24] G. Shafer, "A Mathematical Theory of Evidence", PrincetonUniversity Press, Princeton, NJ, 1976

[25] A.P.Dempster, "A generalization of Bayesian inference",Journal of the Royal Statistical Society, Series B pp205-247,1986.

[26] GlennShafer, "Perspectives on the theory and practice of belief functions",International Journal of Approximate Reasoning,Vol : 4,Issue : 5-6,pp323-362,1990.

[27] GlennShafer and Judea Pearl, eds.,"Readings in Uncertain Reasoning", Morgan Kaufmann, Publisher Inc.,pp-768,1990.

[28] GuoChen ,PengShuo ,Jiang Rong ,Luo Chao, "An anomaly detection system based on dendritic cell algorithm", Third International Conference on Genetic and Evolutionary Computing,pp192-195,Oct-2009.

[29]http://www.mathworks.com/products/matlab/description1.html,Access date 15/07/2013,12:33PM

[30] R. Shanmugavadivu, "Network intrusion detection system using fuzzy logic", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1,pp101-111,2011.

[31] MahbodTavallaee, EbrahimBagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", proceeding of the second IEEE SymposiumonComputational Intelligence for Security andDefence Application,IEEE,2009 .

[32] Al-Hammadi, Y., Aickelin, U., &Greensmith,, "DCA for bot detection",Proceedings of the IEEE World Congress on Computational Intelligence (WCCI),IEEE, 2008.

[33] Greensmith, J., &Aickelin, U., "Dendritic cells for SYN scan detection",Proceedings of the Genetic and Evolutionary Computation Conference (GECCO) (pp. 49-56). London, UK,2007

[34] Oates, R., Greensmith, J., Aickelin, U., Garibaldi, J., & Kendall, G. "The application of a dendritic cell algorithm to a robotic classifier", Proceedings of the 6th International Conference on Artificial Immune (ICARIS), (pp. 204–215).,2007

[35] Mokhtar, M., Bi, R., Timmis, T., & Tyrrell, A. M. " A modified dendritic cell algorithm for on-line

error detection in robotic systems", Proceedings of the 11th IEEE Congress on Evolutionary Computation (CEC), (pp. 2055–2062),2009.

[36] Gu, F., Greensmith, J., &Aickelin, U. "Integrating real-time analysis with the dendritic cell algorithm through segmentation",Proceedings of the Genetic and Evolutionary Computation Conference (GECCO), (pp. 1203–1210) , 2009.