Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Dendritic Cell Algorithm and Dempster Belief Theory Using Improved Intrusion Detection System

Neha Singh **Prof. Yogadhar Pandey**

Abstract: - There are several methods used to implement intrusion detection such as statistical analysis expert 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. To minimize false alarm rate we proposed novel dual detection of IDS based on Artificial Immune System that integrating the Dendrite Cell Algorithm and Dempster Belief theory in our work fuzzy logic techniques, state transition approaches, Rule-based Detections, Pattern Structure, and these several approaches is based on the immune system were proposed in recent years. But false alarm rate was still high. This work will solve the problem of correlation and will resolve the problem of unknown and rapidly evolving harmful attacks. Our simulations show that the proposed technique has improved the correlation factor, minimizing false +ve and false –ve alarm generation and to increase the efficiency and accuracy of the IDS system.

Keywords- Intrusion detection system, dempster belief theory, dendritic cell algorithm, fuzzy logic technique, correlation factor.

I. Introduction

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 [2]. 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.

II. The Dendritic Cell Algorithm

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. DCs have the ability to combine a multitude of molecular information and to interpret this information for the T-cells of the adaptive immune system, to induce appropriate immune responses towards perceived threats. Therefore, DCs can be seen as detectors for different policing sites of the body as well as mediators for inducing a variety of immune responses [6].

a) Similarities of AIS and IDS

There are similarities between AIS and IDS both of them use pattern recognition and anomaly detection to prevent system which depends on them security-based failures. And that is the reason that IDS can be designed based on AIS Both Artificial immune system and intrusion detection system use signature and anomaly detection The Signature detection part detects the known intrusions and the anomaly detection part is used to detect new types of intrusions [3].

III. 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 1.1 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) [4].

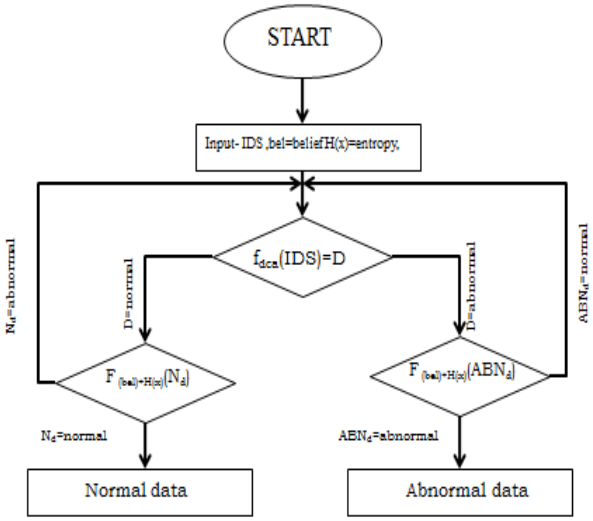


Figure 1.1 Flow chart of Proposed Architecture

Step1: With the help of Dendritic Cell Algorithm we categorized data.
Step2: Dempster-Belief theory is used to compute the probability of evidences that indicate support the attack or normal class.
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 [7].

IV. Proposed Algorithm

Input : S = set of data items to be labelled safe or dangerous. **Output**: D = set of data items labeled classes DBF= dendritic belief function
Begin Create an initial population of dendritic cells (DCs), D Create a set to contain migrated DCs, M For **all** data items in S do Create a set of DCs randomly selected from D, P
For all DCs in P do Add data item to DCs collected list, Update danger, PAMP and safe signal concentrations, Update concentrations of output cytokine, Migrate the DC from D to M and create a new DC in D if concentration of co-stimulatory molecules is above a threshold
End, end if entropy(bad && good) bad=high, good=low, pass DBF(bad) **for all** DCs in DBF do Set DC to be semi-mature if output concentration of semi-mature cytokines is greater than mature cytokines, otherwise set as mature end **for all** data items in S do Calculate number of times data item is presented by a mature DC and a semi-mature DC Label data item a safe if presented by more than semi-mature DCs than mature DC's, otherwise label as dangerous Add data item to labeled set M end.

a)KDD Cup 99 Data Sets

The data set used in the experiments is ‘‘KDD Cup 1999 Data’, which is a subversion of DARPA (Defense Advanced Research Projects Agency) 1998 dataset

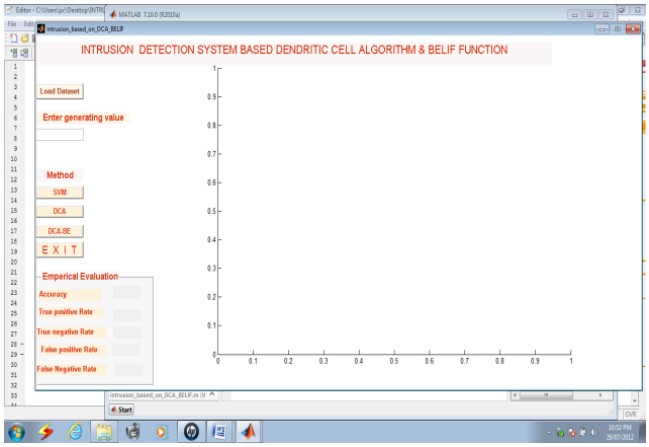


Figure 1.2shows that main window of proposed IDS system

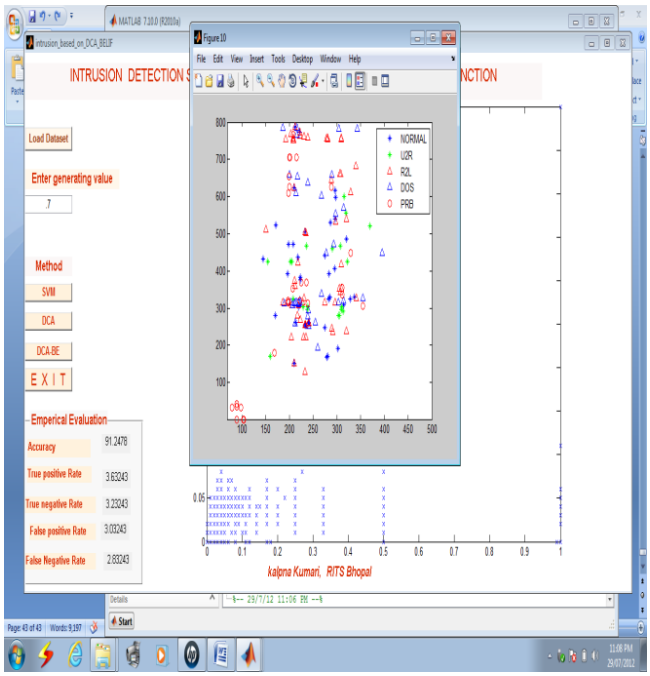
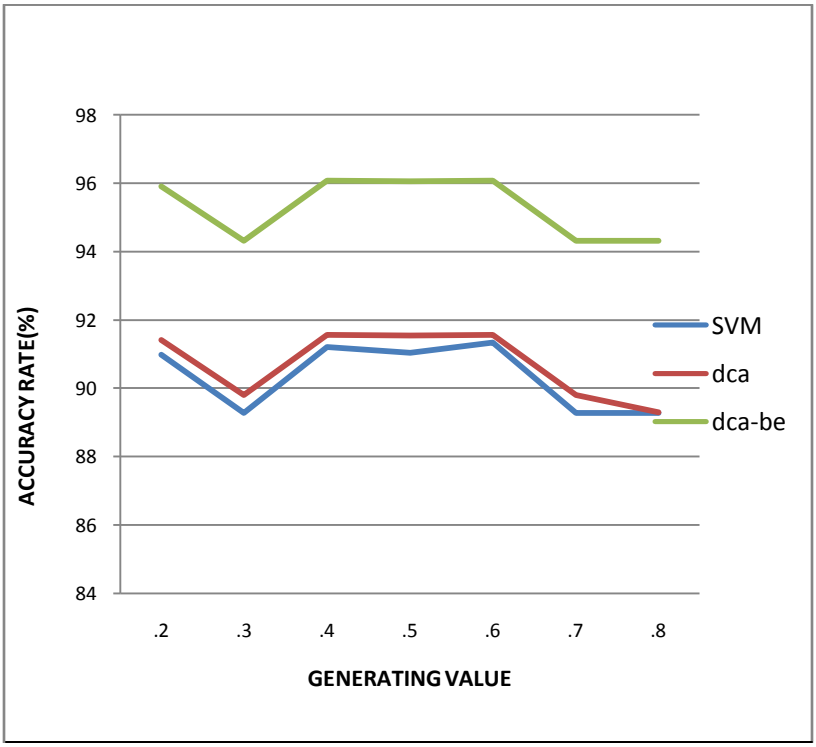


Figure 1.3 shows that classification windows and rate of detection of data set with Svm method

b) Result analysis with the help of Graphs

The comparison of the simulation result is given in Fig. 1.2. It gives the comparison of the Accuracy rate for the classification of attack using the traditional method namely SVM and DCA with our proposed method DCA-BE. In simulation the generating function also called the activated threshold value was set to 1. The maximum accuracy rate of our algorithm is possible only by using DCA –BE method .Fig.1.3 shows when using SVM & DCA classification of the accuracy of attack never reaches even 92.00% but by using DCA-BE approaches the accuracy rate reaches 96.00%. The X-axes represents the accuracy rate and the Y-axes indicate detection generating value.



Graph 1.1Comparison of the SVM & DCA and DCA-BE

Generating value	SVM	Dca	Dca-be
0.1	89.27	89.29	94.3
0.2	90.9697	91.4	95.9
0.3	89.27	89.79	94.3
0.5	91.19	91.55	96.06
0.7	91.024	91.53	96.04
0.8	91.33	91.55	96.06
0.9	89.27	89.79	94.3

Figure 1.4 shows the Comparison

DCA and DCA-BE . In experiment 2 we calculate the TPR,TNR,FPR and FNR parameter for the different methods SVM,DCA,DCA-BE separately. From this experiment 2 we conclude that our approach gives better method for the classification of the data as well minimum TPR, TNR, FPR and FNR.

V. Conclusion

As rapid increase in unauthorized activities and abuse of computer system by both system insider and external intruder trends to increase the degree of network security. In order to increase network security various technique has been proposed but having a deficiency over IDS system in some of the situation if correlation alarm is not precise, reduction and prevention of false positive and false negative is high , at last having insufficient measurement of pattern recognition. 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.

VI. Future Work

Feature reduction process of KDD dataset takes large amount of time. Therefore in future work for modify feature reduction optimization for the better selection of feature in KDD dataset can be attempted.

References

[1] FarhoudHosseinpour,Kamalrulnizam Abu Bakar,AmirHatamiHardoroudi,NazaninsadatKazazi, "Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems" 2010 International Conference on Intelligent Networking and Collaborative Systems, pp 158-189.

[2] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in 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", 2011 IEEE International Conference on Fuzzy Systems ,pp 115 -122.

[4] Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser bikas,"an implementation of intrusion detection System using genetic algorithm" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, pp109-121.

[5] M. Bishop. Computer Security: Art and Science. Addison-Wesley Professional, New York, NY, USA, 2002.

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

[7] ArefEshghiShargh, "Using Artificial Immune System on Implementation of Intrusion Detection Systems", 2009 Third UKSim European Symposium on Computer Modeling and Simulation,pp164-169.

[8] ArefEshghiShargh, "Using Artificial Immune System on Implementation of Intrusion Detection Systems", 2009 Third UKSim European Symposium on Computer Modeling and Simulation,pp164-169.

[9] Xuanwu, Zhou, "Evolutionary Algorithm and its Application in Artificial Immune System", 2008 Second International Symposium on Intelligent Information Technology Application,pp.33-38.

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

[11] Julie Greensmith, Jamie Twycross and UweAickelin, "Dendritic Cells for Anomaly Detection", 2006 IEEE Congress on Evolutionary Computation Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada July, 2006,pp16-21.'

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

[13] Lu Hong, "Immune Mechanism Based Intrusion Detection Systems," nswctc, vol.2,pp.568571,2009InternationalConferenceonNetworksSecurity,WirelessCommunications and Trusted Computing, 2009.

[14] Wei Hu, Jianhua Li QiangGao, "Intrusion Detection Engine Based on Dempster-Shafer's Theory of Evidence", 2006 IEEE,pp1627-1632.

[15] Dasgupta, "Immunity-based intrusion detection system: a general framework, Proceeding of the 22nd NationalInformation Systems Security Conference (NISSC)", Arlington, Virgina, pp.147-160, 1999

[16] Matzinger. P, (1994) "Tolerance, Danger and the Extended Family", Annual Review in Immunology, vol.12,2004, pp. 991-1045.

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

[18] Dasgupta and Gonzalez, "An Immunity-Based Technique to Characterize Intrusions in Computer Networks",IEEE Trans on Evolutionary Computation, pp.281-291, 2002.

[19] Guo Chen ,Peng Shuo ,Jiang Rong ,Luo Chao, "An anomaly detection system based on dendritic cell algorithm", 2009 Third International Conference on Genetic and Evolutionary Computing,pp192-195

[20] Li Rui , Luo Wanbo , "Intrusion Response Model based on AIS", 2010 International Forum on Information Technology and Applications,pp-86-96.

[21] YUAN Hui, LIU Jian-yong, "Intrusion Detection Based on Immune Dynamical Matching Algorithm", 2010 International Conference on E-Business and E-Government-pp-1342-1346.

[22] Lei Deng, De-yuan Gao, "Research on Immune based Adaptive Intrusion Detection System Model", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing pp-488-492.

[23] Junmin Zhang, Yiwen Liang, "A Novel Intrusion Detection Model Based on Danger Theory", 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application,pp-867-872.

[24] Haidong Fu , Xiuo Yuan, Liping Hu , "Design of a Four-layer Model Based on Danger Theory and AIS for IDS", 2007 IEEE,pp-6337-6341.

[25] Baoyi WANG , Shaomin ZHANG , "A New Intrusion Detection Method Based on Artificial Immune System", 2007 IFIP International Conference on Network and Parallel Computing – Workshops ,pp-91-99

[26] G. Shafer, A Mathematical Theory of Evidence, Princeton, University Press, Princeton, NJ, 1976.

