Analysis of Dendritic Cell Algorithm in Intrusion Detection System by Using Dempster Belief Theory

Neha Singh
Student of MTech SIRT College, RGPV University Bhopal

Abstract: *latest immune algorithm, dendritic cell algorithm (DCA) has been successfully applied into the abnormal detection. this paper reviewed the research progress of DCA from the following aspects: signal extraction 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 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.Prevention of security breaches completely using the existing security technologies is unrealistic. As a result, intrusion detection is an important component in network security. many current intrusion detection systems (IDSs) are signature based systems The rate of false positives is small to nil but these types of systems are poor at detecting new attacks, variations of known attacks or attacks that can be masked as normal behaviour.*

Keywords: intrusion detection system, human immune system, danger theory, negative selection algorithm, Dempster–Belief theory, Artificial Immune System, DCA,

I INITIALLY ARTIFICIAL IMMUNE SYSTEMS

Initially Artificial Immune Systems were based on simple models of the human immune system. The first generation of artificial immune system algorithms including negative selection and clonally selection do not produce the same high quality performance as the human immune system [14]. These algorithms, negative selection in particular, are prone to problems with scaling and the generation of excessive false alarms when used to solve problems such as network based intrusion detection. The resulting algorithms are believed to encapsulate the desirable properties of immune systems including robustness, error tolerance, and self-organization. One such "second generation" AIS is the Dendritic Cell Algorithm (DCA), inspired by the function of the dendritic cells (DCs) of the innate immune system. It incorporates the principles of a key novel theory in immunology, termed the "danger theory". This theory suggests that DCs are responsible for the initial detection of invading microorganisms, in addition to the induction of various immune responses against such invaders. An abstract model of natural DC behavior is used as the foundation of the developed algorithm.

- **Self-Organized**: A self-organizing IDS provides adaptability and global analysis. Without external management or maintenance, a self-organizing. IDS automatically detect intrusion signatures which are previously unknown and/or distributed, and eliminate and/or repairs compromised components. Such a system is highly adaptive because there is no need for manual updates of its intrusion signatures as network environments change. Global analysis emerges from the interactions among a large number of varied intrusion detection processes.
- **Lightweight**: A lightweight IDS supports efficiency and dynamic features. A lightweight IDS does not impose a large overhead on a system or place a heavy burden on CPU and I/O. It also dynamically covers intrusion and non-intrusion pattern spaces at any given time rather than maintaining entire intrusion and non-intrusion patterns.
- **Multi-Layered**: A multi-layered IDS increases robustness. The failure of one

layer defense does not necessarily allow an entire system to be compromised.

- **Disposable**: Disposable IDS increases robustness, extendibility and configurability. A disposable IDS does not depend on any single component. Any component can be easily and automatically replaced with other components.

II 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 [13].

- **PAMP**: A measure that increases in value as the observation of anomalous behavior. It is a confident indicator of anomaly, which usually presented as signatures of the events that can definitely cause damage to the system.
- **Danger**: A measure indicates a potential abnormality. The value increases as the confidence of the monitored system being in abnormal status increases accordingly.
- **Safe**: A measure that increases value in conjunction with observed normal behavior. This is a confident indicator of normal, predictable or steady-state system behavior. Increases in the safe signal value suppress the effects of the PAMP and danger signals within the algorithm, as per what is observed in the natural system. The primary components of a DC based algorithm are as follows [13]:

1. Individual DCs with the capability to perform multi-signal processing.

2. Antigen collection and presentation.

3. Sampling behavior and state changes.

4. A population of DCs and their interactions with signals and antigen.

5. Incoming signals and antigen, with signals pre-categorized as PAMP, danger, safe or inflammation.

6. Multiple antigen presentation and analysis using 'types' of antigen.

7. Generation of anomaly coefficient for various different types of antigen.

The DCA is a population based algorithm, with the population consisting of a set of interacting objects, each representing one cell.

III INTRUSION DETECTION SYSTEM

Intrusions can be divided into basic six main types are as follow.

1. Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints.
2. Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints.
3. Penetration of the security control system, which are detected by monitoring for specific patterns of activity.
4. Leakage, which is detected by atypical use of system resources.
5. Denial of service, which is detected by atypical use of system resources.
6. Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

Anomaly Detection : Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities: (1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are). This is a dangerous problem, and is far more serious than the problem of false positives. The main issues in anomaly detection systems thus become the selection of threshold levels so that neither of the above 2 problems is unreasonably magnified, and the selection of features to monitor. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics in Figure 1.

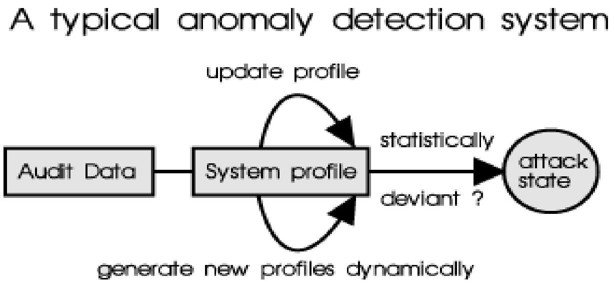


Figure 1.IDS

Misuse Detection: The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. Means that these systems are not unlike virus detection systems -- they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior.

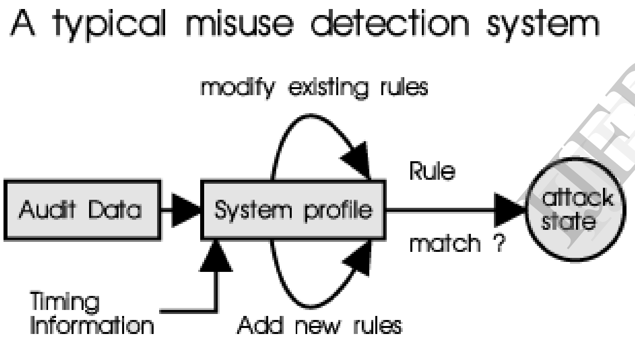


Figure 2.IDS

IV 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 (respectively body and computer network) from 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. We can identify positive selection, negative selection and clonally algorithms as some pretexts for artificial immunity system [10].

The most popular AIS models which used to design IDSs are negative selection models. An ID which is based on AIS would be multilayered. This means that an intruder cannot be successful by crossing only one layer of IDS. Several layers will monitor one specific point of the computer network while each and every of them has a different architecture which makes it harder for intruder to attack. Furthermore, a successful intrusion on one or more host will not help the intruder to get access to all hosts and by this means; the speed of the attack will be reduced. Also an AIS based IDS would be disposable. It means that it is not dependent on a single component and its components can be replaced easily by other component.

V LITERATURE REVIEW

Chung-Ming Ou , and Yao-Tien Wang, proposed Agent-based artificial immune system (ABAIS) to apply over intrusion detection systems (IDS). A multi agent-based IDS (ABIDS) inspired by the danger theory of human immune system.

Li Rui, LuoWanbo states, in the Intrusion technique for detection of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies,

YUAN Hui, LIU Jian-yong, proposed methodology integrating the concept of AIS and Danger theory (DT). It provides the Dynamic equation of the ripe cell and memory cell, and sets up a kind dynamic match Algorithm.

By Lei Deng De-yuanGao proposed Immune based Adaptive IDS Model (IAIDSM) is using Enhanced Fast Adaptive Clustering Algorithm and Algorithm of Mining Fuzzy Associate. The Immune based Adaptive IDS Model.

Junmin Zhang,Yiwen Liang proposed a traditional negative selection, clonal selection algorithms predefine one part of antigens to be self (the training set) in intrusion detection applications, but in practice the self is difficult to define and can change over time.

Haidong Fu , Xiuo Yuan , Liping Hu , introduces a four-layer model based on Danger Theory (DT) and AIS for IDS, which consists of four layers, each of them works independently and interacts with each other. In the third layer-IRL a mechanism of reasoning with uncertainty is presented to increase the detection accuracy.

Baoyi Wangs ,Zhang , proposed the algorithm of generating variable-radius detectors to generate detectors. Analyze different effects on detection results by choosing different radii. Test samples need to compare with all detectors to detect intrusions

VI 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 5 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).

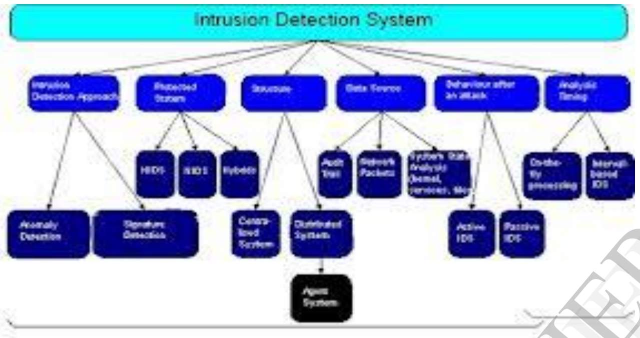


Figure 3 Proposed Architecture

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.

KDD Cup 99 Data Sets

The data set used in the experiments is ‘‘KDD Cup 1999 Data’’ [18], which is a subversion of DARPA (Defense Advanced Research Projects Agency) 1998 dataset.

The KDD cup 99 dataset Includes a set of 41 features [21] derived from each connection and a label which specifies the status of connection records as either normal or specific attack type.

VII RESULTS

Proposed Work has implemented in MATLAB 7.8.0 framework .Figure 5 shows the main window of proposed IDS system. first Load data set by the user, second for the generating function value and third to select the particular methods SVM, DCA and DCA-BE(proposed method) for the classification .

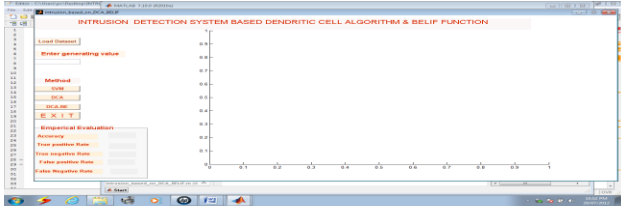
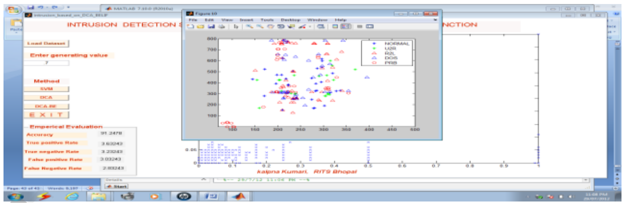


Figure 4 shows that main window of proposed IDS system

Figure 4 shows classification windows for Support Vector Machine (SVM) .In the Svm method the accuracy for the classification of data for generating function .7 is 91.2478%.

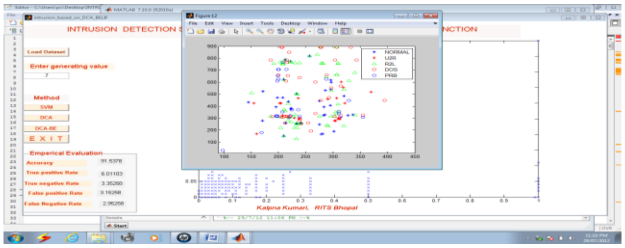


Enter generating value: 7

Emperical Evaluation
Accuracy 91.2478
True positive Rate 3.63243
True negative Rate 3.23243
False positive Rate 3.03243
False Negative Rate 2.83243

Figure 5 shows that classification windows and rate of detection of data set with Svm method

Whereas Figure 5 shows classification windows with DCA method, in which accuracy for generating function .7 is 91.5378%.

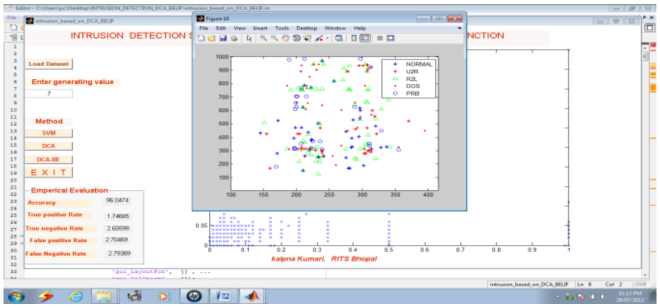


Enter generating value: .7

Emperical Evaluation
Accuracy 91.5378
True positive Rate 6.01103
True negative Rate 3.35258
False positive Rate 3.16258
False Negative Rate 2.95258

Figure 6 shows that classification windows and rate of detection of data set with DCA method

The result of classification of proposed IDS is shown in Figure 6. In the proposed IDS the accuracy for the classification of data for generating function .7 reaches up to 96.0474% with minimum FPR and FNR. Proposed methodology is very effective for the classification of data with maximum accuracy and minimum FPR and FNR.


Editor - C:\Users\pc\Desktop\INTRUSION_DETECTION_DCA_BELIF\intrusion_based_on_DCA_BELIF.m
intrusion_based_on_DCA_BELIF
INTRUSION DETECTION S
NCTION
Figure 10
File Edit View Insert Tools Desktop Window Help
NORMAL
U2R
R2L
DOS
PRB
Load Dataset
Method
SVM
DCA
DCA-BE
E X I T
kalpna Kumari, RITS Bhopal

Enter generating value: .7

Emperical Evaluation

Accuracy	96.0474
True positive Rate	1.74665
True negative Rate	2.60599
False positive Rate	2.70469
False Negative Rate	2.79389

Figure 7 shows that classification windows and rate of detection of data set with DCA-BE method

Result analysis with the help of Graphs

The comparison of the simulation result is given in Fig.5. 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. Figure 8 shows the Comparison of the TPR, TNR, FPR and FNR rates between SVM, 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.

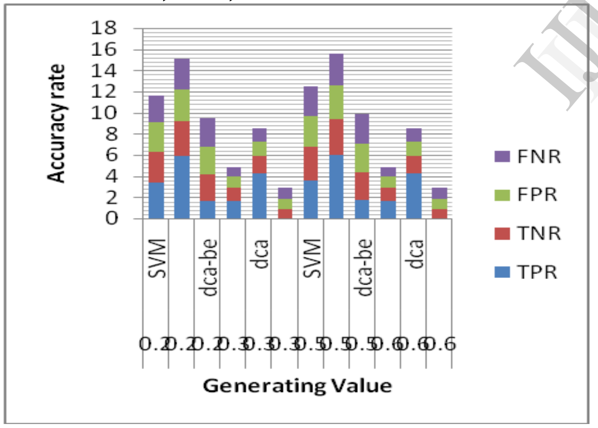


Figure 8 Comparison of the SVM &DCA versus DCA-BE in terms of TPR, TNR, FPR and FNR

In experiment 2, we can easy predicate that by using our proposed approaches the, FPR and FNR is minimal .Whereas with the help of SVM & DCA all the parameters (TPR, TNR, FPR and FNR) shows their maximum value.

Conclusion

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.

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

Future Work

Therefore in future work for modify feature reduction optimization for the better selection of feature in KDD dataset can be attempted.

REFERENCES

[1] FarhoudHosseinpour, Kamalru lnizam Abu Bakar, Amir HatamiHardoroudi, Nazaninsa datKazazi, “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] Li Rui , Luo Wanbo , “Intrusion Response Model based on AIS”, 2010 International Forum on Information Technology and Applications,pp-86-96.

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

[21] Lei Immune 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.

[22] [22] 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.

[23] 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.

[24] 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

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

[26] 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

[27] http://www.mathworks.com/products/matlab/description1.html

[28] R. Shanmugavadivu, “ Network intrusion detection system using fuzzy logic”, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2 No. 1,pp101-121.