Immune Inspired Concepts Using Neural Network for Intrusion Detection in Cybersecurity

Adeniji O.D. & Ukam, J.J
Department of Computer Science
Faculty of Science
University of Ibadan
Ibadan, Nigeria
E-mail: od.adeniji@ui.edu.ng,sholaniji@yahoo.com.

ABSTRACT

The most prominent artificial immune systems algorithms majorly inspired by the way in which the biological immune system of the human body treats and responds to pathogens are, the negative selection algorithm, the clonal theory, and the immune network are amongst the first-generation algorithms that have found numerous applications in computer security. In this paper, a novel algorithm was designed that employed techniques from AIS with ANN and applied to intrusion detection. Experimental results showed that the developed system; NNET NSA (Neural Network Negative Selection Algorithm) out performed two other classifiers; SVM and Naïve Bayes.

Keywords: Artificial Immune System, Artificial Neural Network, Clonal theory, intrusion detection, Negative Selection, Biological Immune System.

iSTEAMS Multidisciplinary Conference Proceedings Reference Format
Adeniji O.D. & Ukam, J.J (2019): Immune Inspired Concepts Using Neural Network for Intrusion Detection in Cybersecurity. Proceedings of the 20th iSTEAMS Multidisciplinary Trans-Atlantic Conference, KEAN University, New Jersey, United States of America. 10th – 12th October, 2019. Pp 119-126. www.isteams.net/usa2019 - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V20N1P10

1. INTRODUCTION

Several attempts have been made by various authors in the definition of what the security of a computer system really mean. [1] has defined computer security as the protection of computing systems against threats to confidentiality, integrity, and availability. In another approach, its counterpart cybersecurity has been seen by CISCO to be the practice of protecting systems, networks, and programs from digital attacks**.** Also Cybersecurity according to ISO [2] has been defined as the preservation of confidentiality, integrity and availability of information in the cyberspace", with an accompanying definition of cyberspace as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it".

Several immune inspired ideas have been useful in both the design and implementation of algorithms deployable in intrusion detection systems. Algorithms like the negative selection, clonal theory, immune networks have all been studied and applied in various problem domain.

2. RELATED WORKS

Amongst several functions the Human Immune System performs, one of it is outstanding; protecting the body against various forms of pathogens like viruses, bacteria, parasites. [3] has clearly noted that the regulation of immune responses can broadly be divided into two branches - the humoral immunity which is mediated by B cells and their products, and the cellular immunity mediated by T cells. Both branches follow a similar sequence of steps for defense - proliferate, activate, induct, differentiate and secrete, attack, suppress, and memorize; however, they do this in different ways.

Notably, are two fundamental functionalities when it comes to the biological immune system; the innate immunity primarily responsible in responding to threats and the adaptive system which responds to attacks not previously encountered [4]. AIS has been applied in numerous field by several researchers like [5] developed an algorithm for solving a multi-criteria customer allocation problem in supply chain environment, [6] developed an IDS based on the concept of an AIS. In addition to this, AIS seem to have found more suitable application in computer security problems. This has thus necessitated a broader application areas outlined by [7] to have included clustering/classification, Bio-informatics Anomaly detection, Image processing, Computer security, Control, Numeric function optimization, Robotics, Combinatorial optimization, Virus detection, Learning, Web mining, fraudulent transactions or hardware faults, etc

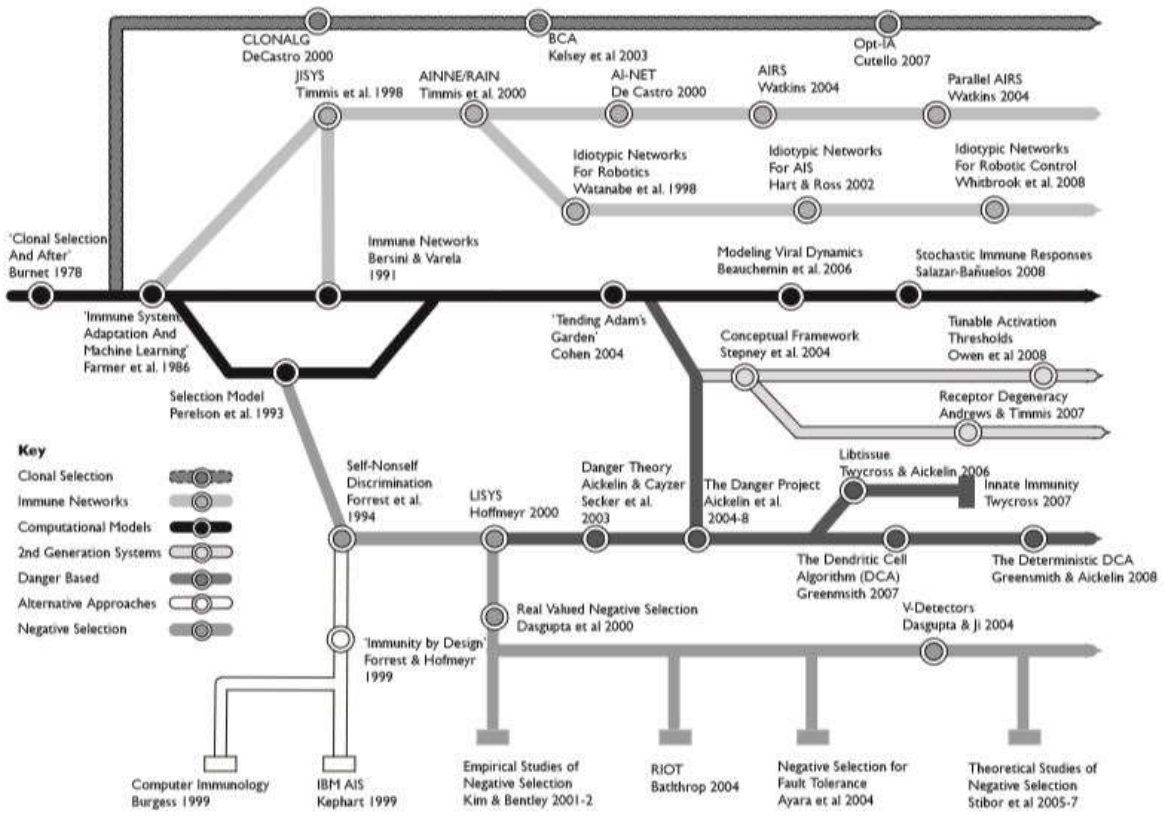

Figure 1: Evolution of AIS from 1978 to 2008 Greensmith (2010)

[8] developed the negative selection algorithm based on the negative selection of immune system process. The negative selection algorithm has according to [9], the following steps:

1. Define self as a set S of elements of length l in representation space U.
2. Generate a set D of detectors, such that each fails to match any element in S. Then, monitor S for changes by continually matching the detectors in D against S.

Several adjustments to date has been made to the negative selection algorithm. For example, NSA using strings representation have been reported in [10] and [11]. As a measure against the time and space consuming factors, [12] developed the linear and greedy detector generation algorithms, with both operating in linear time with respect to the size of the self and detector sets. [13] Introduced binary template with no intention of decreasing the time but rather generating efficient non-redundant detectors. [14] made a performance comparison of the different strings detector generation algorithms. Hofmeyr et al. [15] and later Balthrop et al. [16] developed a network intrusion detection system by applying the Hamming negative selection and the r-contiguous matching rule. In a more recent work, [17] had developed a super base station fault detection mechanism in which the Negative Selection Algorithm and Expert Knowledge Base were combined. An augmented NSA found in [18] featuring detectors that have variable coverage was developed. A boundary aware NSA was developed in [19] which described the continuous self-region defined by the collection of self-data.

A self-adaptive negative selection algorithm used for anomaly detection was developed by [20] to adjust the self-radius and evolve the non-self-covering detectors to build an appropriate profile of the system. To overcome the problem of excessive invalid detectors generation and improve the detection performance of NSA, [21] presented a bidirectional inhibition optimization r-variable negative selection algorithm (BIORV-NSA). Despite all these improvements over NSA, the idea of self-non-self was challenged by Polly Matzinger in 1994 in her proposed Danger Theory. In an interview by Lauren Constable [22], Polly Matzinger confirmed that the danger model makes the prediction that the immune system will respond to molecules that enter the body and do damage, causing the damaged tissues to release immune-stimulating alarm signals. The concept of apoptosis (when cells die normally) and necrosis (cells of the body when a cell dies unexpectedly) became relevant as seen in (Apoptosis).

The Dendritic Cell Algorithm (DCA) was developed as part of the Danger project by [23] and it's based on a model of the function of dermal dendritic cells of the human body and their ability to discriminate between healthy and infected tissue. Various application areas can be found in [24] and a recent improvement over DCA called dDCA (Deterministic Dendritic Cell Algorithm) can be found in [25]. On the other hand, an Artificial Neural Network is based on a collection of connected units or nodes called artificial neurons, which loosely model the neurons in a biological brain. Each connection, like the synapses in a biological brain, can transmit a signal from one artificial neuron to another. Techniques from ANN has found widespread application in stock market prediction, [26], and both credit rating and credit scoring [27].

3. PROCEDURE

Ideas from how the negative selection algorithm worked were abstracted with a combination of the r-chunk matching rule in the design of this work. The dataset used was the NSLKDDCup1999 dataset publicly available at the MIT Lincoln laboratory. The detailed analysis of this dataset can be found here [28] and its improvement found here [29] using various machine learning approaches. Furthermore, the algorithm was coded in the R programming language and experiments performed in the Rconsole and further validated with RapidMiner as a tool. For accuracy purpose, the average error rates, weighted averages and confusion matrix was built and revalidated using the WEKA framework.

4. RESULT ANALYSIS

The following section shows some of the result obtained and their implication.

Figure 1 below shows the matching of antigen to create corresponding antibodies. There are altogether seven major nodes displayed here and corresponding twenty seven minor nodes with respect to the attributes of the dataset used. Each of this node has am equivalent weight assigned to them. This result helps us further understand where intrusions will likely take place.

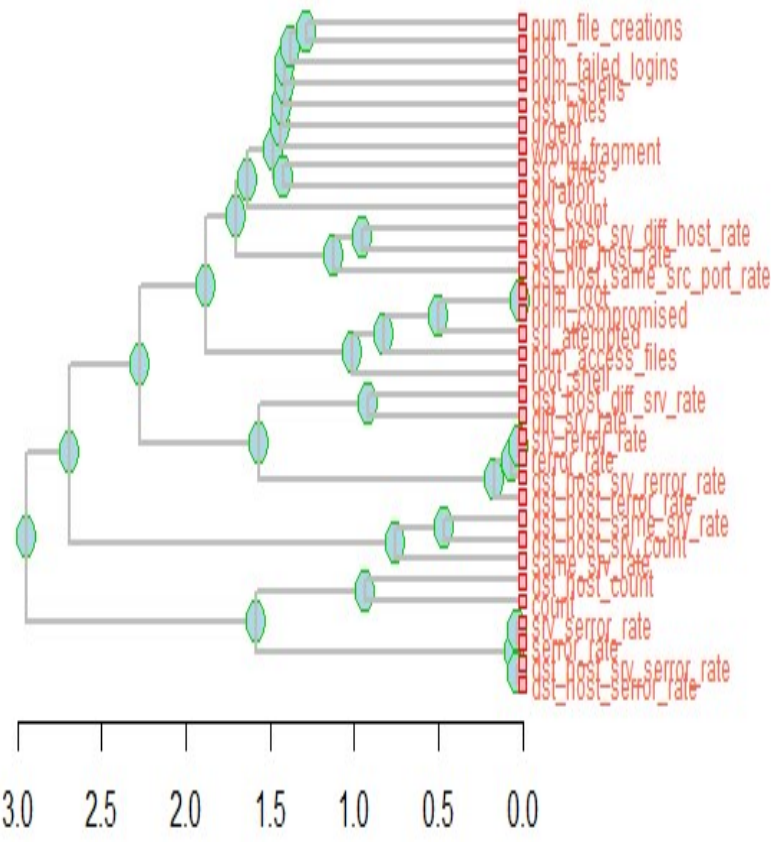

Figure 2: Matching of antigenes to create antibodies

The Pearson discriminant coordinate was used to generate the antibodies from the above antigen matched as illustrated in figure 3 below

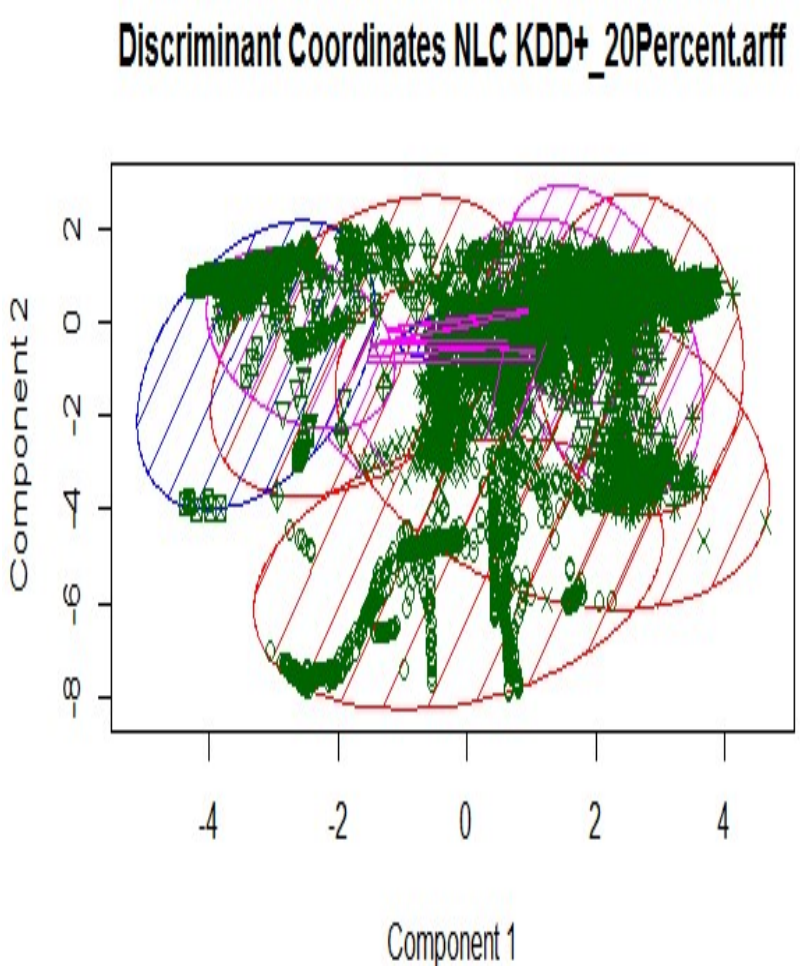

Fig 3: Antibodies generated from r-chunk matching of the antigens.

Further results showed that our model performed optimally wen when compared with other two classifiers; Naïve Bayes and Support Vector Machine as seen in the table 1 below:

Table 1: Summary of results obtained using NNET NSA and other classifiers

Algorithm	Classification Accuracy	Computation Time
Naive Bayes	81.66%	100.15s
SVM	65.01	215.81s
NNET NSA	90.1%	15.00s

5. CONCLUSION AND FUTURE WORK

We have been able to develop a novel system called NNET NSA that combined the strength of both AIS and ANN with application to network intrusion detection. Although some level of result has been achieved with respect to our system, our future direction will be to explore the time complexity of our system and experiment further with other standard intrusion detection datasets and synthetic dataset.

REFERENCES

[1] Abraham, A., Grosan, C., & Chen, Y. (2005). Cyber Security And The Evolution Of Intrusion Detection Systems. *I-Manager's Journal On Future Engineering And Technology*, *1*(1), 74-82. doi: 10.26634/jfet.1.1.968

[23] Aickelin, U., Bentley, P., Cayzer, S., & Kim, J. (2004). Danger Theory: The Link between AIS and IDS?. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2832042

[7] Aickelin, U., Bentley, P., Cayzer, S., & Kim, J. (2004). Danger Theory: The Link between AIS and IDS?. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2832042

[14] Ayara, M., Timmis, J., Lemos, R. de, Castro, L. N. de, & Duncan, R. (2014). Negative selection : How to generate detectors. *ICARIS*, *1*(January 2002), 89–98.

[16Balthrop, J., Forrest, S., & Glickman, M. Revisiting LISYS: parameters and normal behavior. *Proceedings Of The 2002 Congress On Evolutionary Computation. CEC'02 (Cat. No.02TH8600)*. doi: 10.1109/cec.2002.1004387

[27] Credit Scoring Model. *Springerreference*. doi: 10.1007/springerreference_1160

[21] Cui, L., Pi, D., & Chen, C. (2015). BIORV-NSA: Bidirectional inhibition optimization r-variable negative selection algorithm and its application. *Applied Soft Computing*, *32*, 544-552. doi: 10.1016/j.asoc.2015.03.031

[12] D'haeseleer, P., Forrest, S., & Helman, P. An immunological approach to change detection: algorithms, analysis and implications. *Proceedings 1996 IEEE Symposium On Security And Privacy*. doi: 10.1109/secpri.1996.502674

[6] Dutt, I., Borah, S., & Maitra, I. (2016). Intrusion Detection System using Artificial Immune System. *International Journal Of Computer Applications*, *144*(12), 19-22. doi: 10.5120/ijca2016910496

[8] Forrest, S., Perelson, A., Allen, L., & Cherukuri, R. Self-nonself discrimination in a computer. *Proceedings Of 1994 IEEE Computer Society Symposium On Research In Security And Privacy*. doi: 10.1109/risp.1994.296580

[10] Forrest, S., Somayaji, A., & Hofmeyr, S. A. (1997). Comput Immu. *Communications of the ACM*, *40*(10).

[25] Greensmith, J., & Aickelin, U. (2009). Artificial Dendritic Cells: Multi-Faceted Perspectives. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2827957

[15] Hofmeyr, S., & Forrest, S. (2000). Architecture for an Artificial Immune System. *Evolutionary Computation*, *8*(4), 443-473. doi: 10.1162/106365600568257

[20] Jinquan, Z., Xiaojie, L., Tao, L., Caiming, L., Lingxi, P., & Feixian, S. (2009). A self-adaptive negative selection algorithm used for anomaly detection. *Progress In Natural Science*, *19*(2), 261-266. doi: 10.1016/j.pnsc.2008.06.008

[2] Lunt, B., & Ekstrom, J. (2008). The IT model curriculum. *Proceedings Of The 9Th ACM SIGITE Conference On Information Technology Education - SIGITE '08*. doi: 10.1145/1414558.1414560

[11] Majd, M., Shoeleh, F., Hamzeh, A., & Hashemi, S. (2010). Towards Efficient and Effective Negative Selection Algorithm: A Convex Hull Representation Scheme. *Lecture Notes In Computer Science*, 45-54. doi: 10.1007/978-3-642-17298-4_4

[26] Pei-Chann Chang, Chin-Yuan Fan, & Chen-Hao Liu. (2009). Integrating a Piecewise Linear Representation Method and a Neural Network Model for Stock Trading Points Prediction. *IEEE Transactions On Systems, Man, And Cybernetics, Part C (Applications And Reviews)*, *39*(1), 80-92. doi: 10.1109/tsmcc.2008.2007255

[5] Prakash, A., & Deshmukh, S. (2011). A multi-criteria customer allocation problem in supply chain environment: An artificial immune system with fuzzy logic controller based approach. *Expert Systems With Applications*, *38*(4), 3199-3208. doi: 10.1016/j.eswa.2010.09.008

[28] Ravipati, R., & Abualkibash, M. (2019). Intrusion Detection System Classification Using Different Machine Learning Algorithms on KDD-99 and NSL-KDD Datasets - A Review Paper. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3428211

[29] Revathi, S., & Malathi, A. (2013). A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. *International Journal of Engineering Research and Technology (IJERT)*, *2*(12), 1848–1853.

[4] Sarafijanovic, S., & LeBoudec, J. (2005). An Artificial Immune System Approach With Secondary Response for Misbehavior Detection in Mobile ad hoc Networks. *IEEE Transactions On Neural Networks*, *16*(5), 1076-1087. doi: 10.1109/tnn.2005.853419

[9] Stibor, T., Bayarou, K., & Eckert, C. (2004). An Investigation of R-Chunk Detector Generation on Higher Alphabets. *Genetic And Evolutionary Computation – GECCO 2004*, 299-307. doi: 10.1007/978-3-540-24854-5_31

[3] Timmis, J., Knight, T., de Castro, L., & Hart, E. (2004). An Overview of Artificial Immune Systems. *Natural Computing Series*, 51-91. doi: 10.1007/978-3-662-06369-9_4

[13] Wierzchon, S. T. (2000). Discriminative power of the receptors activated by k-contiguous bits rule. *Journal of Computer Science and Technology*, *1*(3), 1–13.

[17] Ye, G., Wang, Y., & Sun, Q. (2019). Super Base Station Fault Detection Mechanism Based on Negative Selection Algorithm and Expert Knowledge Base. *IOP Conference Series: Materials Science and Engineering, 490*, 072019. doi:10.1088/1757-899x/490/7/072019