A Novel Multilayer Artificial Immune System for Network Defense

Mohamed M. K. Elhaj, Hussam Hamrawi, Yahia Abdalla

Abstract—Artificial Immune System is a promising computational intelligence system inspired by human immune system which acts as a natural resistance to diseases using sophisticated mechanisms intended to protect our bodies from invaders which are facing a number of layers of defense, i.e. physical, physiological, innate and adaptive layers. Recently we proposed a multilayer network defense artificial immune system inspired by innate immunity in humans, the outcome of that work showed encouraging results from the innate layer. This paper describes a framework of a multilayered network defense system composed of two main layers, innate and adaptive layers, both layers are described, the innate layer as a first layer of defense which is designed and implemented using fuzzy logic expert system, and adaptive layer as a second layer and shows detailed results from the whole system. The innate layer shows very encouraging results since it has already dealt with 77% of the whole traffic with false positive rate of only 0.0107, this rate could still be reduced when adding more rules to the fuzzy knowledge base.

Index Terms— Artificial Immune System, Innate Immune system, Fuzzy Expert System, Intrusion Detection System, Network Security, Human Immune System, KDD Cup 1999

1 Introduction

FOr a long time nature has inspired solutions for different problems. In computer and network security, the human systems inspired even the names of the problems let alone the solutions. For example, viruses and worms were used to express invasion of foreign entities of the computer or network system. Moreover, human immune system has inspired the defense mechanism of intrusions to these systems.

Artificial Immune Systems (AIS) has been around for decades, they emulate those of humans in order to solve complex problems. This human immune system has several properties of real interest for researchers like uniqueness, anomaly detection, noise tolerance, distributed detection, learning and memory [1][2][3][4]. AIS research has been applied to solve complex computational and engineering problems related to several applications especially in classification, optimization or anomaly detection [5].

One of the most common problems that found intensively in AIS literature is network security due to the characteristic similarities between immune system and network defense systems such as intrusion detection system [3][4][6][7][8][9].

Most AIS research focus has been on the adaptive immune system and only recently innate immunity has been introduced, many applications and frameworks using adaptive immunity are available throughout the literature, and in contrast those using innate immunity can hardly be found [7][10][11].

In [11] and [12] innate immunity is seen as the first line of defense and natural resistance in which the body defends itself from foreign entities.

Early Works in [13], [14], [15] and [16] among many other researches made a potential architecture and the general requirements for an immunity-based intrusion detection system with notable focus on anomaly based IDS, whereas in [9] a general review of various artificial immune system approaches of intrusion detection system development were presented. On one hand, in [17] innate immunity is thought to provide some answers to known problems associated with adaptive immunity, on the other hand, in [18] innate immunity interacts with adaptive immunity in different ways, and the role of the innate immunity as the instigator of the adaptive immunity system was explored.

In [19] a hybrid approach to detect intrusions in a network based on artificial immune system theory was developed with three levels of defense, i.e. surface barrier, innate immune system and adaptive immune system.

Late discoveries in immunology revealed that the central role and high importance of innate immunity in immunology, the significant amount of research carried out has highlighted the interaction of innate immunity with the adaptive immune system [10].

These discoveries also showed how the adaptive immunity works together with innate immunity, it is now known that acquired immunity does not work independently from innate immunity, and they jointly eliminate foreign invaders [11][20][21].

In [22] innate immune mechanism designed to formulate a first layer of defense which categorizes traffic before passing it to adaptive layer, writers used unsupervised learning methods to simulate innate capabilities.

The fact that adaptive and innate immune systems interact together are widely considered as a comprehensive defense mechanism against pathogens [25], the human body in this manner is viewed as integrated system with levels of defense

- *Mr. Mohamed Elhaj is currenlt pursuingPhD degree program in electrical & electric engineering, Sudan University of Science & Technology, Sudan, Khartoum, NTC Tower PO Box: 2869. E-mail:mohamed.elhaj@ntc.gov.sd*
- *Dr. Hussam Hamrawi is currentlyworking as dean of computer engineering faculty in University of Bahri, Sudan, Khartoum, Mohd Najeeb Street, PO Box:1660, E-mail: hussamw@bahri.edu.sd*
- *Dr. Yahia Abdalla is currently working as director general of National Telecommunication Corporation,Sudan, Khartoum, NTC Tower, PO Box:2869, yahia@ntc.gov.sd*

and these levels interact with each other to formulate the comprehensive defense sought to protect such system.

This paper is about this kind of comprehensive structure of defense, a multilayered defense mechanism that takes onboard both innate and adaptive immunity. The multilayer defense framework was first proposed and developed in our previous work [23].

In this paper, the model is further developed and experiments to evaluate the framework are presented. In section two the multilayer defense system architecture is explained and the overall system view is presented. In section three the innate immune layer is described with detailed explanation of the use of fuzzy systems to model the behavior of innate immunity. In section four the adaptive immune layer used in this system is described and the choice of the particular adaptive system is justified. In section five the experiments made to verify the assumptions about the multilayer immune system is presented and their results are discussed. Finally in section six a conclusion is drawn with suggested further work.

2 Multilayer Network Defense System

This paper proposes a multilayer network defense framework that simulates AIS capabilities; the proposed framework is composed of two main layers, innate and adaptive layers. As shown in Fig. 1 captured network traffic will be entered into the input unit in which the following processes will be accomplished:

- Loading data into database;
- Extract features from the captured traffic;
- Add rules to the knowledge base;
- Prepare data to be entered into innate layer in a data set format;
- Prepare parameters and variables for the fuzzy software;
- Delete duplicated records of the dataset (for test purposes only).

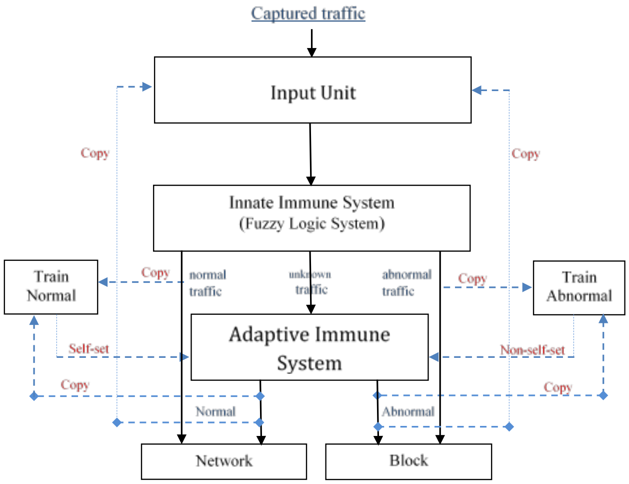

Fig. 1. Multilayer network defense system

The input unit then passes traffic to the innate immune system as first layer of defense in a dataset format. The innate layer uses fuzzy expert system to categorize traffic into three categories i.e. normal, abnormal and unknown traffic, the normal traffic will be ignored and allowed to pass to the network without further delay or investigation, the abnormal traffic will be blocked and not allowed to reach network. The third category is unknown traffic, in other words, the traffic that the innate system could not judge whether it is normal or abnormal traffic, and here the innate layer calls the adaptive layer of the immune system for further investigation.

The innate layer categorization and decision making is performed in a fast manner and preserve the feature of the innate mechanism in increasing the speed of the overall network defense performance.

As mentioned above, traffic considered unknown will pass to the second layer of defense, the adaptive layer, in our early experiments [23] only 30% of whole traffic reached adaptive layer for further inspection, this will definitely reduce overhead of the adaptive layer, and since the adaptive detection mechanism is totally different from the innate way of defense this will help catching different attacks.

The adaptive layer discriminates self sets from non-self sets, self sets will be ignored and allowed to enter network and copy of this traffic will be used as trained data to produce more self sets, whereas the non-self sets will be blocked and denied to access network and copy of this traffic will be used as trained data for producing antibodies for non-self sets. The training process for both normal and abnormal traffic is being conducted offline and could be in any other separated system.

3 Innate Immune System

The innate immune layer has been formulated using fuzzy expert system with the aim of taking decisions based on predetermined expert knowledge that can incorporate uncertain information. The system is designed to fulfill the well known biological innate immune system properties which are divided into two main groups, the first group is related to general attributes of the innate system and can be found in [5][9][10][18][20][23], whereas the second one is describing how innate responds to the antigen and can be found in [9][10][13][21][23][24][25][26].

The properties related to general attributes are:

- First layer of defense;
- Triggers adaptive system to start its response;
- Not adaptable system;
- Has no memory, although some researchers suggested that innate system could have immunological memory [25].

The properties related to innate response are:

- Non-specific response;
- Responds according to general properties;
- Immediate maximal response;
- Responds rapidly;
- Responds the same way every time;
- Not long lasting response.

The proposed innate layer response is highly reflects the properties of the human innate system in responding to antigen stimulus actions, it acts as a first responder to antigen to formulate the first layer that defend human body, it is also designed to classify attacks according to general properties and to network behavior. The system deals with non-fuzzy inputs as well as uncertain connections using fuzzy expert system abilities to translate uncertain expert knowledge base into a decision making process and its known capabilities of converting human rules into mathematical formulations to be easily designed and implemented using computer programs [27].

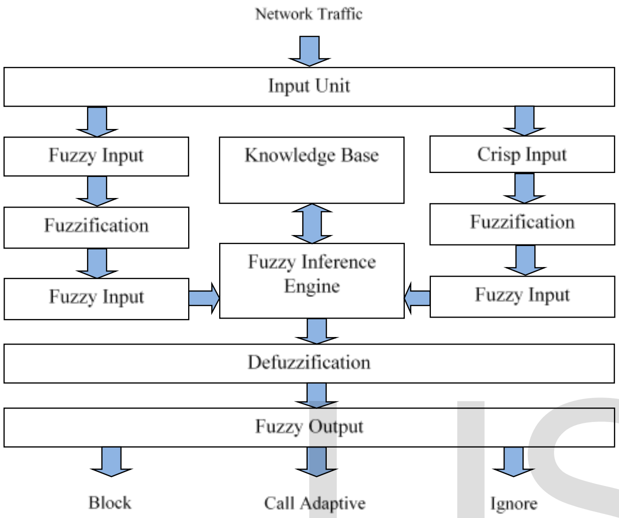

Fig. 2. Innate immune layer using fuzzy expert system

As shown in Fig. 2 the input unit classifies network traffic into either crisp or fuzzy inputs, both inputs go through fuzzification process where fuzzy sets are defined and a degree of membership for crisp inputs are defined as well, then when passed through inference engine fuzzy rules will be evaluated and output for each rule will be produced using rules stored in the knowledge base, those rules are collected and generated using network security experts knowledge and general traffic observations.

In the defuzzification process the output decision will be taken after combining all outputs of all rules, the system will have one of three decisions ignore, block or call adaptive component.

In order to construct a fuzzy set different methods can be used i.e. taking expert opinion, a panel of experts then using some statistical method to choose points, using a statistical survey for non-experts, or using methods that make use of old data if available. All of these methods can lead to different areas of research and in this paper a simple and straight forward expert opinion is used to construct fuzzy sets.

Many fuzzy set shapes can be used i.e. triangular, rectangular, bell-shaped, gaussian, shoulder shaped, etc., in this paper triangular fuzzy sets are used for simplicity. Using other shapes can be the area of study for further research. Table I shows the fuzzy sets for 22 chosen features and how lingual expressions like short, very short and long are mathematically described.

TABLE I. Fuzzy Sets for chosen features

Feature Name	Fuzzy Sets
Duration	short<0,100,200>; average<100,250,400>; long<300,450,600>; vlong<500,800,1000>; xlong<900,1200,4000>; xxlong<1500,10000,…>
src_bytes	vfew<0,75,100>; few<75,100,200>; average<150,250,300>; many<275,500,800>; xmany<600,1200,2000>; xxmany<1600,3000,….>
dest_bytes	vfew<0,100,300>; few<200,350,500>; average<400,1000,3000>; many<2000,4000,6000>; xmany<5000,10000,…>
Count	vfew<0,25,50>;few<35,80,120>;average<100,200, 300>; many<280,350,400>; xmany<375,450,520>
srv_count	vfew<0,25,50>;few<35,80,120>;average<100,200, 300>; many<280,350,400>; xmany<375,450,520>
serror_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
srv_serror_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
rerror_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
srv_error_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
same_srv_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
diff_srv_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
srv_diff_host_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
dst_host_count	few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>
dst_host_srv_count	few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>
dst_host_same_srv_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>
dst_host_diff_srv_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>
dst_host_same_src_port_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
dst_host_srv_diff_host_rate	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>

To explain how these fuzzy sets are constructed, the first feature *duration* is taken as an example. It describes the duration a connection takes and is measured in milliseconds. Expert opinion shows that duration can be described using six different time ranges i.e. short, average, long, very long, extremely long, and extremely long to infinity. The fuzzy sets are called short, average, long, vlong, xlong, and xxlong respectively. Experts are asked to set the scale and the parameters of the triangle that represent each fuzzy set, the parameters are the first, middle, and last points of the triangle.

4 Adaptive Immune System

The adaptive immune system is a distributed detection system with high abilities of learning, classification and pattern recognition, it consists of two kinds of lymphocytes B- and T-cells as a main actors of the acquired immune response, these white blood cells are responsible basically for recognizing pathogens and neutralize and eliminate them [8][13].

B- and T-cells express proteins on their surfaces acting as detectors capable of interacting with specific antigen types. T-cells are protecting the body from attacking its own cells using negative selection algorithm, in this algorithm immature detectors are compare to self patterns, those which respond to own cells of the body will be killed, others are start to be a mature detectors [8][28][29].

Antibodies are continuously compared to non-self patterns; those which match with high affinity will be cloned, detectors not match with antigen for certain time will be destroyed. To ensure diverse type of detectors for better coverage, antibodies copy themselves with minor differences, this process called clonal selection algorithm [28]. Antibodies matching enough number of antigens in its life time will be added to memory cells database; this will help adaptive immune system to better respond to the same attacks in the future.

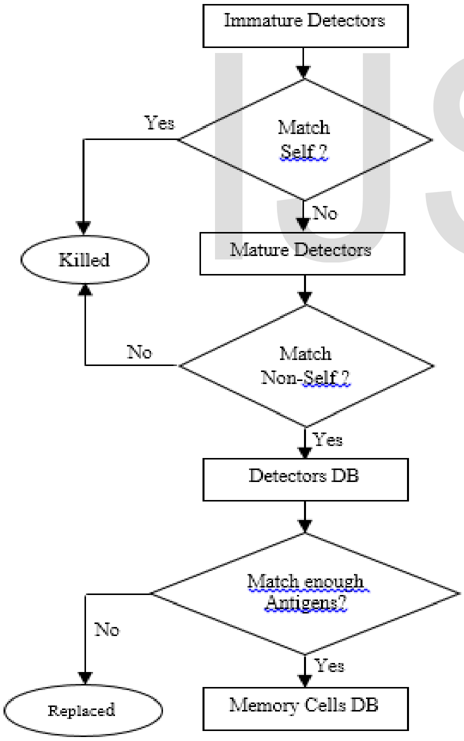

Fig. 3. Detectors generation process

In our proposed adaptive immune system shown in Fig.3 we first generated immature detectors sets through random selection, these immature detectors pass through negative selection algorithm, if the detector matches self sets, it will be discarded and otherwise it will be added to a mature detectors database.

The antigen and antibody sets are constructed as fixed length binary strings extracted from the Internet Protocol packet in a network environment and consist of main features like port number, protocol type, flags, packet length, etc. Self and non-self sets are collected from normal and abnormal network traffic respectively during training. The length of these string sets are subject to more research since long sets produce more accurate results but needed bigger resources [6][13][30].

It has to be mentioned that we have applied a typical adaptive immune system structure which being adopted widely for instance in [6][15][31] and described in details in [30].

These mature detectors sets will be entered to clonal selection algorithm, in which they will be compared with non-self sets, if they match with high affinity they will clone themselves and produce new sets with minor changes. If mature detector matches with enough antigens in a certain period of time then it will be added to memory detectors which have smaller threshold value and longer life cycle, if not, this detector will be subject to replacement soon. To calculate the affinity in negative selection and clonal selection algorithms we used hamming distance which efficiently calculates bit differences between two binary strings.

Traffic passes from innate layer will be compared to detectors generated from the above process, matches traffic will be blocked and copy of these data will be used to help produce more non-self sets in a training unit, others will be passed directly to the network.

5 Experiments

As illustrated in Fig. 4, five Windows based operating system machines were used to test the system, all with duo processor 2.5 GHz, 500 GB Hard disk and 8 GB of RAM, these computers are connected in a separate LAN network using 8 ports switch. Machine (1) is used as an Input Unit in which network traffic in different formats prepared to be entered into innate layer.

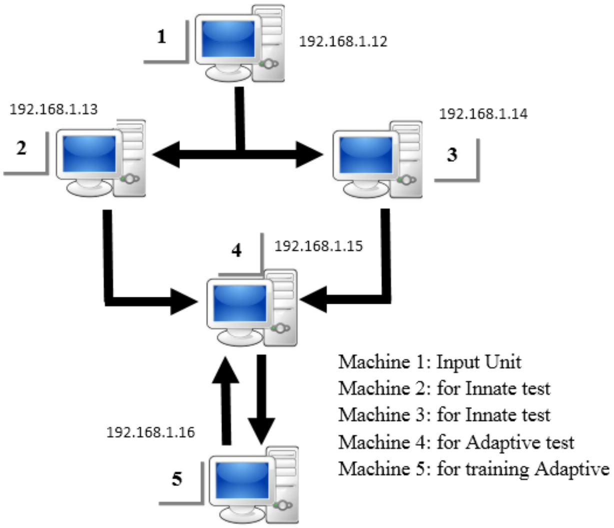
1
192.168.1.12
192.168.1.13
2
192.168.1.14
3
4
192.168.1.15
192.168.1.16
5
Machine 1: Input Unit
Machine 2: for Innate test
Machine 3: for Innate test
Machine 4: for Adaptive test
Machine 5: for training Adaptive

Fig. 4. Network configuration used in experiments

Machines (2) and (3) were used for testing innate immune layer using KDD training dataset as initial input. Machine (4) is being used for testing adaptive immune layer while Machine (5) is for constructing detectors in adaptive response. Three software programs are developed by writers using PHP and installed in 4 PCs, which are Machine (2), (3), (4) and (5).

TABLE II. DETECTION RATE OF THE KDD CORRECTED DATASET ATTACKS

No	Attack Name	KDD Corrected Dataset	Sample Dataset	Detected Instances	True Positive Rate %
1	Apache2	794	500	420	84.00
2	Back	1098	500	401	80.20
3	BufferOverflow	22	22	10	45.45
4	Ftp_write	3	3	1	33.33
5	GuessPassword	4367	500	405	81.00
6	Httptunnel	158	158	104	65.82
7	Imap	1	1	1	100
8	IPsweep	306	306	245	80.06
9	Land	9	9	5	55.55
10	Loadmodule	2	2	1	50.00
11	Mailbomb	5000	500	434	86.80
12	Mscan	1053	500	419	83.80
13	Multihop	18	18	11	61.11
14	Named	17	17	9	52.94
15	Neptune	58001	500	426	85.20
16	Nmap	84	84	66	78.57
17	Perl	2	2	1	50.00
18	Phf	2	2	1	50.00
19	Pod	87	87	45	51.72
20	Portsweep	354	354	256	72.31
21	Processtable	759	500	410	82.00
22	Ps	16	16	8	50.00
23	Rootkit	13	13	7	53.84
24	Saint	736	500	412	82.40
25	Satan	1633	500	369	73.80
26	Sendmail	17	17	10	58.82
27	Smurf	164091	500	412	82.40
28	Snmpget	7741	500	401	80.20
29	Snmpguess	2406	500	390	78.00
30	Sqlattack	2	2	2	100
31	Teardrop	12	12	7	58.33
32	Udpstorm	2	2	2	100
33	Warezmaster	1602	500	380	76.00
34	Worm	2	2	1	50.00
35	Xlock	9	9	6	66.66
36	Xsnoop	4	4	3	75.00
37	Xterm	13	13	6	46.15
Attacks Connections		**250436**	**7655**	**6087**	**79.52%**

KDD Cup 1999 dataset is a benchmark dataset well defined, organized and labeled to precisely evaluate the performance of intrusion detection systems, this dataset is based on the DARPA 1998 raw dump traffic including payload captured over a period of nine weeks on a local area network in Information System Technology (IST) group of Lincoln Laboratories at MIT University [32].

In a period of two weeks three tests were conducted; two for the innate immune layer using corrected KDD Cup 1999 dataset and generated dataset for the added attacks, the third test is for the adaptive layer using innate output traffic.

KDD Cup 1999 dataset has a number of inherent problems, as illustrated in [33] and [34] the dataset is imbalance since two attacks Smurf and Neptune made up more than 70% of it, and these two attacks plus normal connections made up to 98% of the training dataset; KDD dataset is outdated and misses many of the new attacks [33][35][36] and also many connections of the dataset are duplicated (78% of the training set and 75% of testing set are exactly the same) [33][36][37].

In our test we have used corrected version of the KDD Cup 1999 dataset, unlike in 10% KDD, corrected KDD cup 1999 dataset has more balance attacks distributions and has bigger number of attacks, i.e. 37 attack types [38]. To have more balanced traffic and to reduce the memory usage in the test we tested only 500 connections or less for each attack type and 5000 connections for normal connections, those sample connections are randomly selected after the input unit eliminate duplicated traffic to overcome one of the KDD cup dataset drawbacks. The system changes selected samples each time we conduct a test, the results showed later are the average rates from different tests generated.

We first tested the innate component by entering connections from the 37 attacks in the corrected KDD cup dataset; the detailed results are illustrated in Table II above. Although the innate system concerns only about general characteristics of the connection and is not responding specifically to attack but still we conducted this test to compare the detection abilities of the system for each individual attack.

To guarantee realistic results we have carefully studied the behavior of 144 attacks including KDD attacks then we added tens of rules to the knowledge base extracted from attacks behaviors.

In the second test we added 1000 connections constructed in lab, the majority of these connections are new attacks and normal new internet traffic.

Results of the innate layer for both KDD dataset and added dataset samples are illustrated in Table III, the results showed that the system can deal with more than 77% of the connections, as the system being able to deal with more traffic this will help reduce the amount of storage and processing needed for the adaptive layer, the results also suggested that the false positive rate of only normal traffic tested is 0.013, while the

TABLE III. RESULTS OF THE INNATE LAYER TEST

Data Types	KDD Corrected		True Positive		False Positive	
	All	*Used*	#	%	#	*Rate*
Normal	60593	5000	3673	73.46	65	0.0130
KDD Attacks	250436	7655	6087	79.52	72	0.0094
Added Attacks	1000	231	769	76.90	9	0.0090
All	312029	13655	10529	77.11	146	**0.0107**

average false positive rate of all traffic including attacks of KDD dataset and generated attacks are 0.0107. Although those results are quite acceptable, even better results can be achieved when correcting errors and adding more rules to the knowledge base.

The third conducted test is for the adaptive layer, the input for this test is the connections considered unknown from the innate layer test. Detectors, self-sets and non-self-sets are collected and constructed during the two weeks training period. Results of this test are shown in Table IV below.

TABLE IV. RESULTS OF THE ADAPTIVE LAYER TEST

	Connections	Detected	TP Rate	FP Rate
Attacks passed from innate	1799	1601	0.8899	0.1101
Normal traffic passed from innate	1327	1020	0.7687	0.2313
All	3126	2621	0.8385	0.1615

As shown in Table IV, about 83% of the traffic passed from the innate layer has been correctly tagged as being attack or normal connection, the initial result shows an average of 0.1615 false positive rate, those error rates could still be enhanced when training more traffic and constructing more self and non-self sets.

6 CONCLUSION

In this paper, we presented a work in progress to model a network defense mechanism inspired by human immune system theory which known of its great protection capabilities. The proposed system is a multilayer system composing of two layers of defense working separately but still in a cooperative way.

The first layer is the innate component, which is the first line of defense, fuzzy expert system used to imitate human innate mechanisms and behavior. The second layer of defense which is starting its mission to detect attacks only after receiving a trigger from the innate system is the adaptive component, which modeled and designed using well known basic theories like negative selection and clonal selection algorithms.

Three different experiments were conducted; two for the innate component testing attacks from Darpa KDD99 and attacks generated in a lab, and the last test is for the adaptive component to have a big picture of the whole system. Innate component results show the ability of the system to deal with more than 77% of the traffic, and left less that 23% to the adaptive component with the false positive rate of 0.0107, and when passing the rest of the traffic to the adaptive component the system recognizes 83.8% of it with false positive rate of 0.1615.

Tests generally show encouraging results for both innate and adaptive components, when adding more accurate rules to the innate knowledge base and allowing more training time slots to the adaptive layer we are being able to have a sustainable and mature multilayer defense system.

ACKNOWLEDGMENT

The authors acknowledge their profound gratitude to Sudan Computer Emergency Response Team (Sudan-CERT) for supporting this project and providing lab facilities. Authors also thank Nile Center of Research and Technology for cooperation and support at every stage of the research.

REFERENCES

[1] Revathi M, Arthi K. “Application of Artificial Immune System Algorithms in Dataset Classification”, 2014

[2] De Castro LN, Von Zuben FJ. “Artificial immune systems: Part I–basic theory and applications”. Universidade Estadual de Campinas, Dezembro de, Tech. Rep. 1999

[3] Cheng Zhang, Jing Zhang, Sunjun Liu, Yintian Liu, "Network intrusion active defense model based on artificial immune system", Fourth International Conference on Natural Computation, IEEE, 2008

[4] Zhang, Qing-Hua, et al. "An Immunity-Based Technical Research into Network Intrusion Detection." Computer Science and Software Engineering, 2008 International Conference on. Vol. 3. IEEE, 2008

[5] Daudi J. An. “Overview of Application of Artificial Immune System in Swarm Robotic Systems”. Advances in Robotics & Automation, 2015

[6] Steven A. Hofmeyr and Stephanie Forrest, "Immunity by design: an artificial immune system", 1999

[7] Twycross, Jamie, Uwe Aickelin, and Amanda Whitbrook. "Detecting anomalous process behaviour using second generation artificial immune systems." arXiv preprint arXiv:1006.3654, 2010

[8] Vijeta, Mr. Vivek Sharma. “A Review on Network Intrusion Detection using Artificial Immune System (AIS)”, International Journal of Engineering Research & Technology (IJERT), vol. 3, 2014

[9] Chauhan P, Singh N, Chandra N. "A Review on Intrusion Detection System based on Artificial Immune System." International Journal of Computer Applications 63, no. 20, 2013

[10] Twycross, J. & Aickelin, U., "Towards a conceptual framework for innate immunity", Artificial Immune Systems, Springer, 2005, 112-125

[11] Krishnan A. ,“Modeling and Simulation of the Innate Immune System”, Master Project Department of Computer Science University of Colorado at Colorado Springs Colorado, USA, 2004

[12] Su, Mu-Chun, Po-Chun Wang, and Yuan-Shao Yang. "A new approach to artificial immune systems and its application in constructing on-line learning neuro-fuzzy systems." Open Artificial Intelligence Journal 2 (2008): 1-10

[13] Somayaji, Anil and Hofmeyr, Steven and Forrest, Stephanie, "Principles of a computer immune system", Proceedings of the 1997 workshop on new security paradigms, 1998

[14] Kim, Jungwon, and Peter Bentley. "The human immune system and network intrusion detection." 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany. 1999

[15] Yanbin Z., “Network Intrusion Detection System Model Based On Artificial Immune.” International Journal of Security and Its Applications. 30;9 (9):359-70. 2015

[16] Warrender, Christina, Stephanie Forrest, and Barak Pearlmutter. "Detecting intrusions using system calls: Alternative data models." Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on. IEEE, 1999

[17] Greensmith, Julie, Amanda Whitbrook, and Uwe Aickelin. "Artificial immune systems." Handbook of Metaheuristics. Springer US, 2010. 421-448

[18] Germain, R. N., "An innately interesting decade of research in immunology." Nature medicine, Nature Publishing Group, 2004, 10, 1307-1320

[19] Sanyal S, Thakur MR. “A Hybrid Approach towards Intrusion Detection Based on Artificial Immune System and Soft Computing.” arXiv preprint

arXiv:1205.4457, 2012

[20] Gonzalez, F. & Dasgupta, D. "A study of artificial immune systems applied to anomaly detection." University of Memphis Memphis, 2003

[21] Mishra PK, Bhusry M. "Artificial Immune System: State of the Art Approach." International Journal of Computer Applications; 120(20). 2015

[22] Hämäläinen T. "Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach." 2014

[23] Elhaj, M. M., Hamrawi, H. & Suliman, M., "A multi-layer network defense system using artificial immune system." Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on Computing, Computing, Electrical and Electronics Engineering (ICCEEE), 2013, 232-236

[24] Read, M., Andrews, P. & Timmis, J., "Artificial Immune Systems." 2009

[25] Twycross, J. & Aickelin, U. "Biological inspiration for artificial immune systems." Artificial immune systems, Springer, 2007, 300-311

[26] Fachada, N., Lopes, V. & Rosa, A., "Agent-based modeling and simulation of the immune system: a review." EPIA 2007-13th Portuguese Conference on Artificial Intelligence, 2007

[27] Shanmugam B, Idris NB. "Hybrid intrusion detection systems (HIDS) using Fuzzy logic." INTECH Open Access Publisher; 2011

[28] Luther, K.; Bye, R.; Alpcan, T.; Muller, A. & Albayrak, S., "A cooperative AIS framework for intrusion detection Communications." 2007. ICC'07. IEEE International Conference on, pp. 1409-1416, 2007

[29] Al-Enezi JR, Abbod MF, Alsharhan S. "Artificial Immune Systems-models, algorithms and applications." 2010

[30] Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont, "An artificial immune system architecture for computer security applications." IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, 2002

[31] Benyettou, Noria, et al. "The Multi-Agents Immune System for Network Intrusions detection (MAISId)." Oriental Journal Of Computer Science & Technology 6.4 (2013): 383-390.

[32] H. Günes Kayacık, A. Nur Zincir-Heywood, Malcolm I. Heywood, "Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets." Proceedings of the third annual conference on privacy, security and trust, 2005

[33] Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G. & Vázquez, E., "Anomaly-based network intrusion detection: Techniques, systems and challenges computers & security." Vol. 28, pp. 18-28, 2009

[34] Kayacik, H. Gü. & Zincir-Heywood, A. N., "Using self-organizing maps to build an attack map for forensic analysis." Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, pp. 33, 2006

[35] Salem, M.; Reissmann, S. & Buehler, U., "Persistent dataset generation using real-time operative framework." Computing, Networking and Communications (ICNC), pp. 1023-1027, 2014

[36] Thomas, C.; Sharma, V. & Balakrishnan, N., "Usefulness of DARPA dataset for intrusion detection system evaluation." SPIE Defense and Security Symposium, pp. 69730G 69730G, 2008

[37] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. "A detailed analysis of the KDD CUP 99 data set." In Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications, 2009

[38] Sathya, S. S.; Ramani, R. G. & Sivaselvi, K., "Discriminate analysis based feature selection in kdd intrusion dataset." International Journal of Computer Applications, Vol. 31, 2011