INTRUSION DETECTION USING BIOLOGICAL INSPIRED IMMUNE SYSTEM

Ankita Trivedi , Dr. Aumreesh Kumar Saxena, M. Arshad , Mr. Shivendra Dubey and Dr. Sitesh Kumar Sinha

Abstract: Researchers and scientists are always motivated by environment and natural organisms to crack real world problems. Protection of computer systems is no exclusion. For identifying intrusion, artificial immune system motivated from natural defense system works proficiently. In this proposed methodology, we are implementing two levels of defense for computer security. The primary level of defense is Innate Immune system and the secondary is Adaptive Immune system. For Innate immune system, detectors are generated using negative selection algorithm. The result reveals the effectiveness of proposed methodology for detecting intrusion against malicious attacks on the network system

Index Terms: Adaptive immune system, innate immune system, intrusion detection, negative selection algorithm, human immune system. detection rate, network security.

1. INTRODUCTION

The Internet is a large scale open network. With expansion of the Internet and its capability, life is becoming easy for everyone. It is helpful and beneficial for both business organization and individual user. In today's world, most of the work can easily done by Internet like e-business, e-ticket, e-shopping and many more [1]. Now days, Internet connectivity is becoming very important phase. The widespread growth of Internet and increasing easy accessibility of tools, for attacking computer network is one of the major concerns of network administrators and security providers for the security of computer systems [2] and data in it capitalized. Network security is the protection offers to a network from illegal, unwanted access and threats [3]. To take on protective actions for network from security threats, is the responsibility of network administrator. Computer networks [4] that are involved in normal daily dealings and communication within the government, individuals, or business organization require safety of their computer. In past few years, government, our army and business area shows their increased reliability and dependability on Internet for their day to day activity. This has created a major challenge to prevent external attacks and securing the computer network. The main concern is choosing suitable intrusion detection system which is mainly of two types: network intrusion detection (NIDS) [5] and host intrusion detection (HIDS) [6]. These both techniques are very dissimilar from one another. Approach of deployment for both techniques is very different. Both technology is opposite to each other and can't be replaced for one another. Network IDS is placed on the network segment and monitors all the hosts which are on that network segment. In the work [5], they used different techniques to automate intrusion detection.

Host IDS is a completely different from NIDS. It has software application or agents which install on particular hosts which is to be monitored. It examines different types of modification over time on host which may signal safety problems. HIDS examines the actions and activities of a host which is to be monitored and match up to with its normal behavior. Example of HIDS is an intrusion detection system that monitors mainly system files while IDS that explore ongoing network traffic is a part of network intrusion detection system. We can also categorize IDS on basis of detection approach: signature-based detection (detects malware by looking for particular pattern) and anomaly-based detection (detecting variation from a model of normal behavior of system, which often relies on machine learning). In [7], they used hybrid approach using artificial immune system [8] and soft computing. Rough set theory with artificial immune system is used for intrusion detection in NIDS. A higher level artificial immune system [9] is used for process anomaly detection [10, 11], in which artificial cells communicate with each other. Signature-based approach can also be referred as Knowledge-based approach. It refers database for earlier attacks and for known system vulnerabilities. It easily detects known attacks but it is not possible for it to detect attacks that are new to system and unknown for it [12]. Another approach is Anomaly-based which can also be referred as Behavior-based intrusion detection system. It is mainly for detection of new and unknown attacks. It uses the approach of machine learning and prepares a model of normal behavior of system and compare any new pattern against this model .This is effective against previously unknown attacks. For real time systems, memory heat map technique is used in [13]. Researchers and scientists are always motivated by environment and natural organisms to resolve real world troubles. Computer safety is no exclusion in it. Artificial immune system (AIS) motivated from natural immune system [2, 3] works proficiently for identifying malicious attacks and threats in a network. Incremental learning on the basis of population technique [14] and a classifier is used with AIS for detecting intrusion in network. Artificial Immune System is a group of strategies which is motivated by the immune system of human [9, 15]. For solving complex problems, defense system is a motivation for latest innovative methodologies. The main attraction of immune system is its adaptive nature, robustness, self management, self defensiveness, self learning and many more which

- *Ankita Trivedi completed masters degree program in CSE from SIRTS SGI, Bhopal India,. E-mail: ankita_tr09@gmail.com*
- *Dr. Aumreesh Kumar Saxena is Associate Prof in CSE Dept in SIRTS, SGI Bhopal India,. E-mail: aumreesh@gmail.com*
- *M. Arshd is Associate Prof in CSE Dept in SIRTS, SGI Bhopal India,. E-mail: arshadsirt@gmail.com*
- *Mr. Shivendra Dube is AP in CSE Dept in SIRTS, SGI Bhopal India,. E-mail:shivendra.dubey5@gmail.com*

- *Any external attack that aim data of computer systems, and its networks, or private systems by a variety of means of hostile activities generally initiated from an unknown source that either modify, interrupt, or demolish a particular target is called cyber attack. In an effort to prevent unknown cyber attacks, one of the most appropriate solutions is Intrusion Detection System. An intrusion detection system (IDS) is a hardware or software application that examines a network or systems for hostile activity.*

catches attention. Human immune system is full of many strategies which become motivation for large variety of skills and methods [14]. These approaches are negative selection algorithm, artificial immune networks, clonal selection approach, danger algorithm [16], and dendrite cell algorithm [17, 21]. A multilevel immune learning algorithm [18] is used for pattern detection which is motivated from immunological ideology. The negative selection algorithm [19] describes 'self' by defining normal profile patterns of a system, which is to be monitored. The randomly generated patterns are compared with self defined samples. If random pattern matches with patterns which are normal then that pattern can't become detector. If randomly generated pattern is not matched with self then it becomes detector pattern. During monitoring phase, if any new pattern matches with detector then it is consider as anomaly. The remaining paper is structured as: section2 gives background about topic. In this, we are providing overview of negative selection algorithm and human immune system. Section 3 presents the proposed approach. Section 4 is about results and analysis. Then section 5 presents the conclusion drawn from the results. Finally, this paper presents references of this paper.

2 BACKGROUND

2.1 Human Immune system

The immune system is a defense system of our body and it consists of several natural structure and procedure within our body that secures us against infection. Immune system has to detect any outer threats, such as pathogens, viruses, worms and to distinguish these agents from our body's cells and tissues. The immune system can be categorized into two subsystems, the innate immune and the other is adaptive immune system [20]. The innate immune system also recognized as the non-specific immune system. It is an essential part of human immune system which includes cells and processes that protect the body from foreign elements. The innate system recognizes and takes action against any antigen in a common basic manner, but, it does not give lifelong immunity to the human body as the adaptive immune system offers. Innate immune systems provide instant safety against outer threat. Primary layer of defence: Innate ImmunityInnate immune system defends the body against pathogen, malignant cell and virus. It is not specific security system. When an antigen, virus or pathogen get in touch with human body then it play its role without any delay. It involves physical obstacles like skin, cells and tissues of defense system that target outer threats in the body. Chemical properties of antigen trigger the innate immune system."Innate" immunity refers to immunity that is present from the time of birth and not learned. Physical epithelial barriers, phagocyte leukocytes, dendrite cells, a unique form of lymphocyte termed as natural killer (NK) cell, and circulating plasma proteins are important components of this primary defense system. After local injury or infection in the body, its first reaction is inflammation. Injured tissues release chemo attractant histamine for signaling the body about inflammation. Neutrophils are first immune cells that reach at injured part. These are rapid response cells which identify and destroy the antigens and bacteria with process phagocytosis. In this process, cell engulfs and digests another cell or bacteria. Macrophages are also immune cells which are little bigger and have longer lifespan then neutrophils [22]. These are also phagocytizes foreign organism. Natural killer cells [23] are a kind of immune cell which have the ability to detect and target intracellular infection of body cells by viruses. It is a unique kind of lymphocytes which is an essential and key component of innate immunity system that controls numerous types of tumors and other infections by limiting their speed and subsequent tissue damage. Figure 1 show the activation time of innate immunity after infection is some hours i.e. it responds quickly after infection.

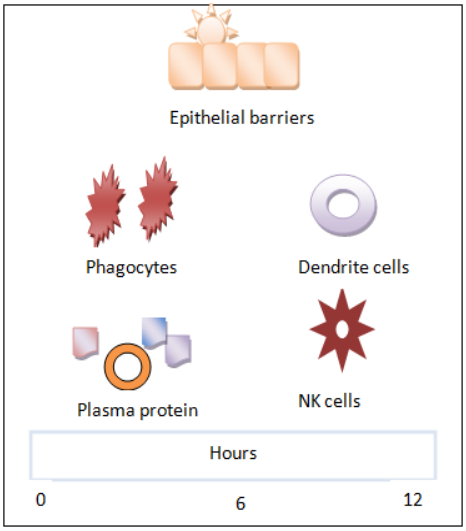

Figure 1 *Activation time of innate immunity after infection*

The main attraction of innate immune system is it responds quickly to various unknown invaders whether they have been encountered before or not. Secondary layer of defence: Adaptive ImmunityIt is termed as antigen-specific or acquired immune system. When any antigen or pathogen attacks our body then that foreign body is first processed and identify by it. Adaptive defence system [24] creates a collection of immune cells to attack detected foreign body. For making upcoming response more effective against specific pathogen it uses "memory". In contrast to innate defence, it is little slow but it provides long lasting safety. It consists of much focused cells, tissues and methods that eradicate antigens and stop their development. It is also termed as acquired defence system or specific defence system which is a part of whole defence system and develops throughout our life time. The main role in adaptive defence response is of white blood cells which are recognized as lymphocytes. Lymphocytes are also of two types T lymphocytes and B lymphocytes. Both type of lymphocytes come from the same stem cells, and are differentiated after their maturation. B-cell is matured in bone marrow while T lymphocytes get mature in thymus. In humeral defence reaction, B lymphocytes play a vital role. On the other hand, in cell-mediated defence reaction T- lymphocytes come in picture. B-cell produces antibodies while T-lymphocyte secretes lymphokines for fighting against pathogen and antigen. Figure 2 represents the activation time of adaptive immunity is in days after infection which shows its slow response against infection. The adaptive T cell aims to that pathogens that have colonized body cells or which have become malignant and B-cell aims to that pathogen that are free in bloodstream or present at mucosal surface.

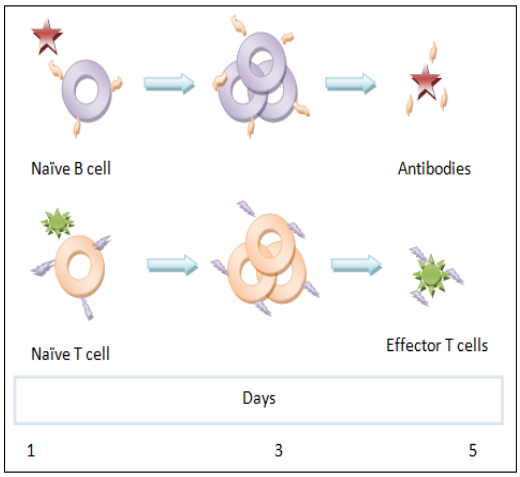

Figure 2 *Activation time of adaptive immunity after infection*

The adaptive system destroys pathogens and the toxic released by them. But sometimes it is unable to differentiate between harmless and harmful foreign body and signals false alarm. Table 1 gives overview of distinction between innate and adaptive immunity on different characteristics.

Table 1 Comparison of innate and adaptive immunity [24]

Properties	Innate Immunity	Adaptive Immunity
Existence	Innate Immunity exists in body from the time of birth.	It is build up in response to any foreign body attacks.
Specificity	Non-specific response	Specific response
Memory cells	Not able to memorize the pathogens	It have memory cells for memorizing pathogens and antigens
Prior Exposure	No need of prior exposure	Only develops when body expose to antigens and pathogen
Range of defense	Restricted	High
Other name	In born Immunity	Acquired Immunity

2.2 Negative Selection Algorithm

Negative Selection algorithm (NSA) has been in demand and most liked algorithm to study and apply in diverse area, because it is simple, less complicated and easy to put into practice. Its detection or recognition phase give good outcome, if detectors are properly generated. NSA [25] differentiates between self and non-self i.e. between normal and intruder. If detector is good then it should not resemble with self patterns defined by the system, thus choosing the approach to generate these detectors is a key decision. The similarity measures which are used for matching regulations should be exactly chosen, so that self patterns should be accurately or closely the same. The main idea behind negative selection algorithms is to distinguish between self and non-self. It consider self as normal and non-self as intruder or abnormal to the system. This is done by T-cells [26] in our body which is born in bone marrow and then goes to thymus for maturation. In maturation phase, T-cells are being trained to learn the self or normal sample. Self patterns are defined and other patterns which are not in self are termed as Non-self for system. After training phase, when they become mature, they are ready to begin recognition process [25-26]. Figure 3 explain the generation of detector set using NSA in training phase.

In the same manner, in intrusion detection system, a pattern is defined which symbolize the normal behavior or self. Patterns which do not match the self are termed as detectors in training period. After completion of training mode, they enter into detection phase where they detect and recognize anomalous activity.

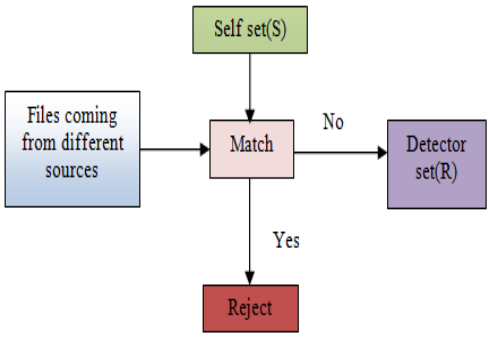

Figure 3 *Generation of detector set using NSA*

3 Proposed Methodology

The proposed methodology is inspired by immune system of human. In this we detect external threats by the mechanism as followed by human body to protect our body from pathogens and antigens. It incorporates AIS using innate and adaptive immune system for intrusion detection. We use negative selection algorithm. NSA defines self and non- self to the system. Figure 4 illustrate the procedure of proposed methodology in terms of block diagram.

3.1 Architecture

In the proposed approach, IDS is positioned at each host computer. Each host based computer has two layer of defense. The primary layer referred as innate immune detection system and secondary layer of defense referred as adaptive immune detection system.

3.2 Methodology

System uses negative selection algorithm by defining self set(S) or normal file extensions like .txt, .word, .doc, .pdf, .xml, .xls,. Number of files comes from different sources are compared to self set. It also has detector set (R) which describes abnormal pattern. If file matches with self set or normal extensions then it does not become detector pattern. If file extensions are not matched with self set then it becomes detector pattern and added in detector set. In monitoring stage, file extensions matched with detector pattern termed as anonymous file extensions. In monitoring phase, the innate immune detection system monitors each file that is accepted by host computer. The extension of file can be of any type. When file arrives at host computer, the primary layer of defense (innate immune detection system) is activated. It checks the file, whether it is of the extension type matched with detector set like .exe, .bash, .dos or .bat. If file extension is matched with detector then it is marked as anonymous files and if it does not belong to detector pattern then it is accepted and considered as normal file. Anonymous files are sends to secondary layer of defense that is adaptive immune detection system by changing their extension to .doc or .txt. By changing the file properties the susceptibility of file to multiply or reside in the hard disk is minimized. As the file extension is changed from original, B-cell activation module which is a part of

adaptive immune detection system is invoked. This module checks the vulnerability of file. If file is found malicious after parsing by B-cell activation module, T-cell activation module is invoked. T-cell activation module is also a component of adaptive immune detection system. It deletes the file, which founds malicious after file parsing by B-cell module and it also generates alert and sends mail to the administrator.

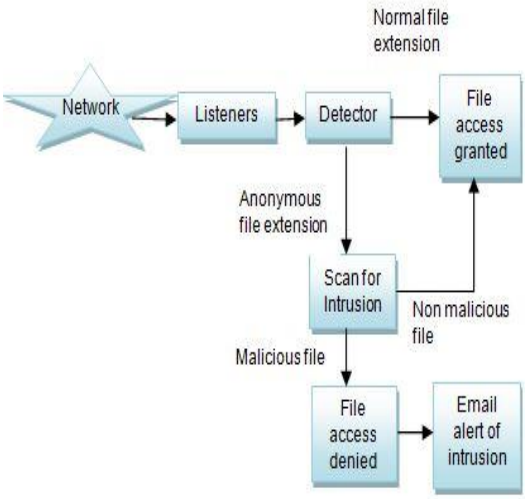

Figure 4 *Block diagram of proposed methodology*

3.3 Proposed Algorithm

Figure 5 gives general idea of training phase and detection phase of proposed algorithm. In training phase, samples are classified as self and non-self on the basis of negative selection algorithm. In monitoring or detection phase, new samples are compared with negative samples by anomaly detection function, for identification of normal and anomalous file extensions. Training Phase

Step1: Specify the normal file extensions i.e. self set for system which are .txt, .word, .pdf, .xml.

Step2: System also declares the detector set which defines abnormal patterns or anonymous extensions.

Step3: When the file comes from network and its extension are compared with self set, defined by the system.

Step4: If file extension not matched with normal or self set then it becomes detector and added in detector set.

Step5: During monitoring stage any file extension that matches with detector pattern, then it is termed as anonymous extension.

Monitoring Phase

Step 1: Accept the file from network to host based computer. File can be of any extension.

Step 2: Store the file details in Master table like file name, extension, date of arrival, original path.

Step 3: Detect the file extension whether it is of detector set like .exe, .bash, .dos or .bat. If file have these extension the file marked as anonymous file.

Step 4: If file is found anonymous in step 3 then file is renamed and duplicate filename, modification date, duplicate path is entered in master table.

Step 5: Accept the file in B-cell table (transaction table) if it is found anonymous in step 3 and store its detail in B-cell table like original file name, original path, duplicate filename, duplication path, date of modify, status, date of delete.

Step 6: Accept the file from B-cell table for parsing.

Step 7: Identify the virus, worm or malware if any present in anonymous invalid file.

Step 8: If file is found malicious then file access denied otherwise file access granted.

Step 9: If file type is found to be malicious then alert is generated to the server and mail is sent to the administrator.

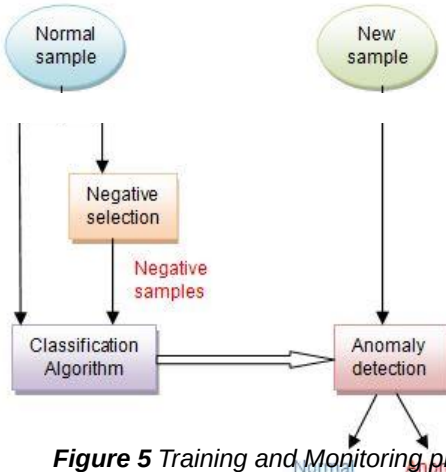

Figure 5 *Training and Monitoring phases*

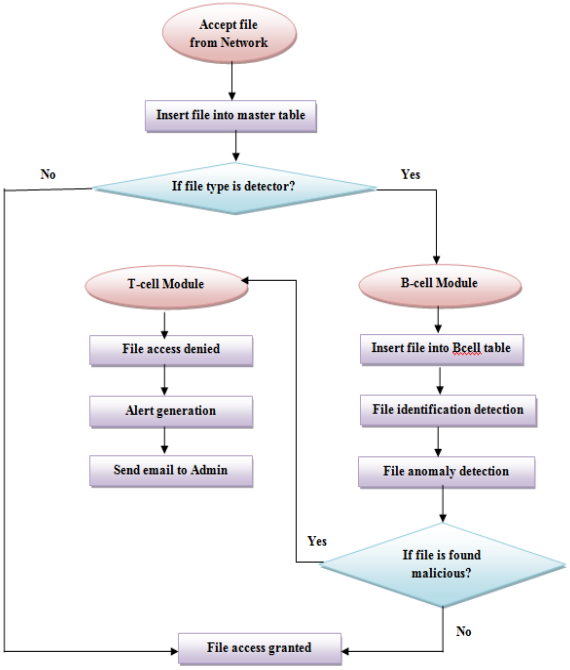

Figure 6 *Flowchart of monitoring (detection) phase*

Figure 6 illustrates the flow of detection phase of proposed approach.

4 RESULTS

Core java 1.7 for dependency injection, spring core 4.1.5 release is used. By using this we eliminate the class to class dependency. Spring integration 4.1.5 release is used for polling data listener, inbound adapter and outbound adapter. Spring mvc is used for controller i.e. for calling backend through Front end. For database connectivity, Hibernate 4.3.8 final is used. For storing data, we used Oracle 10g. Tomcat 8 is used as application server and 200 ok is used as web server. Boot strap is used for Front end directory, so it provides components to front end. There are many measures on which we can compute the performance of intrusion detection system. Major metrics are detection rate, false negative rate, accuracy, false positive rate, effectiveness, efficiency. For

evaluating performance we have to compute the True positive (TP), False positive (FP), True negative (TN), false negative (FN).

•True positive (TP): Intrusions that are recognized by the Intrusion Detection System successfully [27].

•False positive (FP): Normal or non-malicious files that are incorrectly categorize as intrusive by the IDS [27].

•True Negative (TN): Normal or non-malicious files that are correctly marked as normal or non-malicious by the IDS [28].

•False Negative (FN): Intrusions which are failed to spot by the intrusion detection system, and labeled as normal or non-malicious [28].

When the malicious files are induced in the system, the proposed methodology demonstrates the following results as in table 2. The malicious files are induced ranging from 1-1000 as inputs and its corresponding detection rate in % is shown in table 2 and same is demonstrated in form of graph in figure 7.

4.1 Detection Rate (DR)

It is calculated as the proportion between the number of successfully recognized malicious files and the total number of malicious files induced, see equation (1) and (2).

$$DR = \frac{No.\ of\ malicious\ files\ detected\ malicious}{Total\ no.of\ malicious\ files} \quad (1)$$

$$DR = \frac{TP}{TP + FN} \quad (2)$$

As an example, we introduce 100 malicious files and IDS correctly identifies 99 files as malicious. So its detection rate is 99%. And on introducing 1000 malicious files, IDS correctly identifies 993 files as malicious. So its detection rate is 99.3%.

Table 2 Tabular Details of the Number of Malicious Files induced vs. Detection Rate.

No. of malicious files (X-Axis)	Detection rate (in %) (Y-Axis)
1	100
10	100
100	99
1000	99.3

In proposed methodology, we also used NSA with anomaly detection approach. By NSA, detectors are generated. Initially we mark file anonymous, if it have extension .exe and scan it for any malware detection.

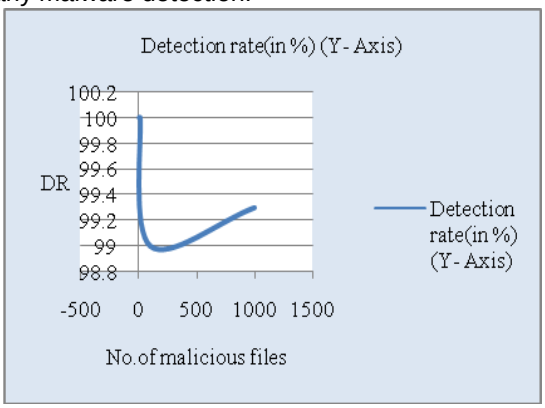

Figure 7 *Represents detection rate according to malicious attack*

Then we increase the count of anonymous extensions (extensions which have the possibility of any malware).

Detection Rate with Increasing Number of Detectors

It is calculated same as detection rate but we increase the number of detectors accordingly see equation (3) and (4).

$$DR = \frac{No.of\ malicious\ files\ detected\ malicious}{Total\ no.of\ malicious\ files} \quad (3)$$

$$DR\ with\ increasing\ detectors = \frac{TP}{TP + FN} \quad (4)$$

For example when we only mark 1 file extension as anonymous i.e. 1 detector and introduce 1000 malicious files, it correctly detected 920 files as malicious i.e. detection rate of identifying malicious files correctly by IDS is 92% and when mark 10 file extension as anonymous i.e. 10 detector then out of 1000 malicious files, it successfully detect 960 files as malicious i.e. detection rate of identifying malicious files correctly by IDS is 96%. Table 3 shows the increasing detection rate by increasing no. of detectors i.e. anonymous file extensions and the same is represented in a graph in figure 8.

Table 3 Relation between Number of Detectors and Detection Rate of identifying Malicious Files correctly by IDS.

Table 3 Relation between Number of Detectors and Detection Rate of identifying Malicious Files correctly by IDS

No. of detectors (X-Axis)	No. of malicious files	Detection rate (in %) (Y-Axis)
1	1000	92
10	1000	96
20	1000	97.2
30	1000	97.8
40	1000	98
50	1000	98
60	1000	99.3

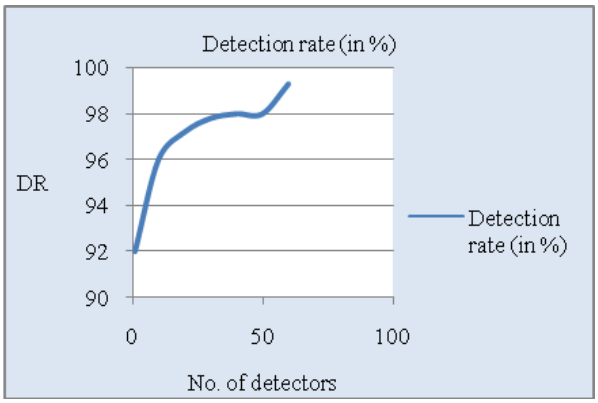

Figure 8 *Depicts detection rate of identifying malicious files correctly by IDS with respect to no. of detectors*

4.2 False Negative Rate (FNR)

It is calculated as the proportion between the no. of malicious files wrongly identified as normal and the total number of malicious files induced, see equation (5) and (6).

$$FNR = \frac{No.of\ malicious\ files\ detected\ normal}{Total\ no.of\ malicious\ files} \quad (5)$$

$$FNR = \frac{FN}{FN + TP} \quad (6)$$

Table 4 represents the decreasing false negative rate by increasing no. of detectors and same is illustrated by graph in figure 9. It is clear that the anomaly IDS that would be developed using our improved algorithm will report less false negative than work previously done [29].For example when we only mark 1 file extension as anonymous i.e. 1 detector and introduce 1000 malicious files, it fails to detect 80 malicious files and mark it as normal i.e. false Negative rate is 8% and when mark 10 file extension as anonymous i.e. 10 detector then out of 1000 malicious files, fails to detect 40 malicious files and mark it as normal i.e. false Negative rate is 4%.

Table 4 Relation between Number of Detectors and False Negative Rate

Number of detectors (X-Axis)	Number of malicious files	False Negative rate (in %) (Y-Axis)
1	1000	8
10	1000	4
20	1000	2.8
30	1000	2.2
40	1000	2
50	1000	2
60	1000	.7

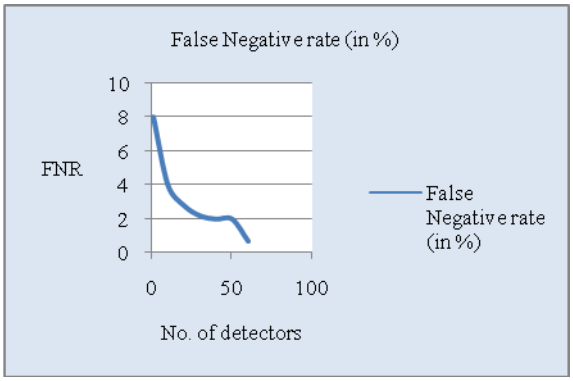

Figure 9 *Depicts false negative rates with increasing no. of detectors*

4.3 False Positive Rate (FPR)

It is calculated as the proportion between the number of normal or non malicious files detected as intrusion and the total number of normal non malicious files, see equation (7) and (8).

$$FPR = \frac{No.of\ normal\ files\ detected\ as\ malicious}{Total\ no.of\ normal\ files} \quad (7)$$

$$FPR = \frac{FP}{FP + TN} \quad (8)$$

Because of negative selection algorithm, FPR is also very less which is shown in table 5 and same is explained by graph in figure 10.

Table 5. Tabular details of the Number of Normal Files induced vs. False Positive Rate

No. of Normal files (X-Axis)	False Positive rate (in %) (Y-Axis)
100	0
200	.5
300	.66
400	.75
500	.60
600	.66
700	.71
800	.75
900	.77
1000	.8

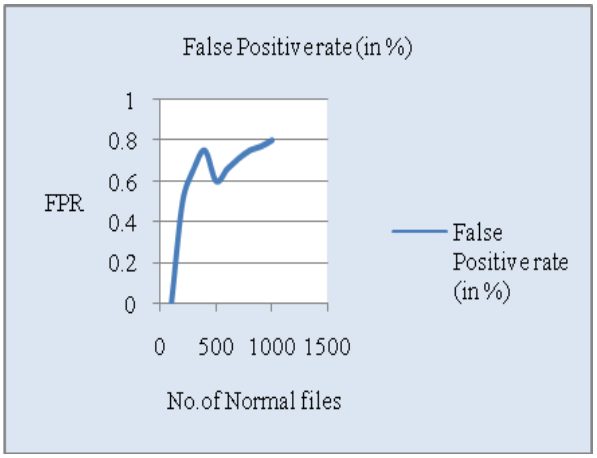

Figure 10 *Represent the False positive rate with normal files induced in the system*

Table 6 shows the parameters detection rate, effectiveness, FNR and FPR, we get improved results as compared to approach proposed earlier [28].

Table 6 Comparison of Implemented Approach with Previous Work

	Detection approach used	No. of Detectors used	Detection Rate	False negative Rate	Effective
Previous work[29]	Signature based and Anomaly based	2	99%	More	Less
Implemented work	Signature based, Anomaly based and Negative Selection based	60	99.3 %	Less	More

4 CONCLUSION

The proposed methodology is inspired by immune system of human. It incorporates artificial immune system using Innate and Adaptive Immune system for Intrusion detection. Negative selection algorithms also applied for generating detectors. Through NSA, in training phase, file extensions which are non-malicious or normal is defined as 'Self' and the extensions which are not matched with 'Self' are added in Detector set. Later, in detection phase, these detector extensions detect anomalous files. The files are accepted from network traffic by host based computer. Then their file extensions are checked for any anomaly. If files are of types like .exe, .bash, .dos, .bat etc i.e. of detector pattern then their properties is changed and it activates the B-cell intrusion detection module. It parsed the anonymous file for threat detection and if it found malicious it activates the T- cell intrusion detection module. If file is found malicious then its access is denied and alarm is generated otherwise file access is granted. The results reveal that the proposed methodology using Negative selection algorithm is more effective and accurate for detecting intrusion in the host-based system. In future, we will convert our IDS into IPS by using another AIS approach and will try to add NIDS architecture.

ACKNOWLEDGMENT

No

REFERENCES

[1] S. Konyeha and E. A. Onibere, "Computer Immunity Using an Intrusion Detection System (IDS)", Advanced Materials Research, Vol. 824, pp. 200-205, 2013

[2] S Forrest, SA Hofmeyr, Aomayaji, 1997 Computer Immunology Communications of the ACM.

[3] D.Dasgupta, 2007 "Immuno-inspired automatic system for cyber defense", Information Security, Tech Rep., Volume12, Issue 4, pp.235-241.

[4] U. Aickelin, D. Dasgupta, 2014 Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques, Artificial Immune Systems, Chapter 13, pp. 1-29.

[5] Carlos A Catania, Carlos Garcia Garino, 2012 "Automatic Network Intrusion Detection. Current techniques and open issue electrical Engineering"

[6] Chung-Ming Ou, 2012 "Host-based Intrusion Detection Systems adapted from Agent-based Artificial Immune Systems", Neurocomputing, Volume 88,pp. 78-86.

[7] Sugata Sanyal, Manoj Rameshchandra Thakur, 2012 "A Multi-Dimensional approach towards Intrusion Detection System", International Journal of Computer Applications (0975 – 888), Volume 48, Issue 5

[8] Junyuan Shen, Jidong Wang, Hao Ai, 2012, "An Improved Artificial Immune System-Based Network", volume4, page 41-47.

[9] Hua Yang, Tao Li, Xinlei Hu, Feng Wang and Yang Zou, 2014, "A Survey of Artificial Immune System Based Intrusion Detection"

[10] Jamie Twycross, Uwe Aickelin, 2008 "An Immune-Inspired Approach to Anomaly Detection", Handbook of Research on Information Security and Assurance, Information Science Reference, Hershey, New York.

[11] Jamie Twycross, Uwe Aickelin, Amanda Whitbrook, 2010 "Detecting Anomalous Process Behaviour using Second Generation Artificial Immune", International Journal for Unconventional Comp., Volume 6, Issue 3–4, pp. 301–326.

[12] Chandrakant Jain, Aumreesh Kumar Saxena " General Study of Mobile Agent Based Intrusion Detection System(IDS)" published in Journal of Computer and Communication (JCC) Vol. 4, No.4, April 2016, Page:93-98, DOI: 10.4236/jcc.2016.44008, ISSN: 2327-5227,.

[13] Man-Ki Yoon, Sibin Mohany, Jaesik Choiz, and Lui Sha, 2015 "Memory Heat Map: Anomaly Detection in Real-Time Embedded Systems Using Memory Behavior", DAC '15, ACM Digital Library, ISBN: 978-1-4503-3520-1.

[14] Meng-Hui Chen, pei-ChannChang, Jheng-LongWu, 2016 "A Population-based Incremental Learning Approach with Artificial Immune System for Network Intrusion Detection", Engineering Applications of Artificial Intelligence", (51)171–181.

[15] Farhoud Hosseinpour, Sureswaran Ramadass, Andrew Meulenberg, Payam Vahdani Amoli and Zahra Moghaddasi, 2013 "Distributed Agent Based Model for Intrusion Detection System Based on Artificial Immune System", International Journal of Digital Content Technology and its Applications (JDCTA)

[16] U Aickelin, P Bentley, S Cayzer, J Kim, and J McLeod. Danger theory: The link between ais and ids. In Proc. of the Second Internation Conference on Artificial Immune Systems (ICARIS-03), pages 147–155, 2003.

[17] J. Greensmith and U. Aickelin, "Dendritic cells for SYN scan detection," in Proceedings of the 9th Annual Genetic and Evolutionary Computation Conference (GECCO '07), pp. 49–56, London, UK, July 2007.

[18] D. Dasgupta, S. Yu, and N. S. Majumdar, "MILA-multilevel immune learning algorithm and its application to anomaly detection," Soft Computing, vol. 9, no. 3, pp. 172–184, 2005.

[19] J Kim and P Bentley. Evaluating negative selection in an artificial immune system for network intrusion detection. Proceedings of GECCO, pages 1330 -1337,July 2001.

[20] Uwe Aickelin, Julie Greensmith, Jamie Twycross, 2004 "A Immune System Approaches to Intrusion Detection".

[21] J. Greensmith and U. Aickelin, "Dendritic cells for real-time anomaly detection," in Proceedings of the Workshop on Artificial Immune Systems and Immune System Modelling (AISB '06), pp. 7–8, Bristol, UK, April 2006.

[22] SA Hofmeyr and S Forrest, Immunity by design: An artificial immune system, Proceedings of Genetic and Evolutionary Computation Conference, pp. 1289-1296, 1999.

[23] U Aickelin, D Dasgupta, Artificial immune systems tutorial, E Burke, G Kendall (Eds.), Search methodologies introductory tutorials in optimization and decision support techniques, Kluwer, pp. 375399, 2005.

[24] J Greensmith, A Whitbrook, U Aickelin, Artificial immune systems, Handbook of Metaheuristics, Springer US, pp. 421-448, 2010.

[25] S Forrest, Self-nonself discrimination in a computer, IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202-212, May 1994.

[26] X Shen, XZ Gao, R Bie, X Jin, Artificial Immune Networks: Models and Applications, International Conference on Computational Intelligence and Security, Vol. 1, pp. 394-397, 2006.

[27] Aumreesh Ku. Saxena ; Sitesh Sinha ; Piyush Shukla "Performance Analysis of Classification Techniques by

using Multi Agent Based Intrusion Detection System" published in IJCNIS Vol. 10, No. 3, Mar. 2018 Pages:17-24 DOI: 10.5815/ijcnis.2018.03.03 ISSN: 2074-9104

[28] Aumreesh Ku. Saxena ; Sitesh Sinha ; Piyush Shukla "Implementation of Mobile Agent Intrusion Detection System Based on Significant Parameters" published in ANUSANDHAN- AISECT University Journal Vol. 06, Issue No. 13, Page: March-2018, E-ISSN 2457-0656

[29] Inadyuti Dutt, Samarjeet Borah, Indrakant Maitra, 2016 "Intrusion detection system using Artificial Immune system", Volume 144-No.12.