Enhanced AIS Based Intrusion Detection System Using Natural Killer Cells

B. J. Bejoy[1] and S. Janakiraman[2]

[1]*Department of CSE, Christ (Deemed to be University), India*
[2]*Department of Banking Technology, Pondicherry University, India*
E-mail: bejoybj@gmail.com; jana3376@yahoo.co.in
[*]*Corresponding Author*

Received 04 June 2019; Accepted 09 September 2020;
Publication 06 February 2021

Abstract

Intrusion detection system is used to monitor the system and network activities to identify anomalies and attacks so that integrity, availability, and confidentiality can be preserved. Here an intrusion detection system based on Artificial Immune System is proposed based on Natural Killer (NK) cells with immunological memory. NK cells are created and each NK cells detection radius is determined using the negative selection algorithm and is trained to detect various attacks. Effective cells with high fairness values are proliferated and distributed to the network using clonal selection algorithm. In this paper, two types of NK cell are used-a Heavyweight NK cell (HWNK) and a number of Lightweight NK cells (LWNK). The incoming data is vectorized and Major Histocompatibility Complex Class I (MHC1) is created. Then based on this MHC1, any of the receptors i.e. Activating Receptor or Inhibiting Receptor is activated. If it is the signature of an attack, Activating Receptor is activated. Activating receptor activation results in either cytokine release or apoptosis. Here cytokine release means an alarm is generated informing the administrator and apoptosis stands for dropping of the packet. If Inhibiting Receptor is activated, it's a normal packet there is no action

Journal of Cyber Security and Mobility, Vol. 9_4, 515–534.
doi: 10.13052/jcsm2245-1439.942

taken. The technique proposed yields high accuracy, better detection rate and quick response time.

Keywords: Intrusion, IDS, anomaly detection, AIS, natural killer cells.

1 Introduction

The growth of the internet and its universal usage has been the boom of the decade. All the fundamentals amenities are currently depending upon the internet. These circumstances lead to a sudden increase in assaults on these amenities by hackers and intruders. Even top-secret military sites and banking sector are in danger of attack by these malicious users. An intrusion is some malicious activity that happens in a network that affects the integrity and availability of the network. Intrusion Detection Systems (IDS) [1] are used to monitor the networks and detect such type of intrusions. IDS along with firewalls and antivirus provide an important security system for the network.

The human immune system(HIS) in the body fight against a wide variety of pathogens, like virus and other harmful agents that can adversely affect the human body. The HIS can also distinguish these pathogens from body self-tissues. The artificial immune system is the use of algorithms that are inspired by human immunology. Artificial immune system (AIS) is a prime contender for designing intrusion detection systems due to the similarity in their behavior [2, 3]. Distributed systems can solve complex problems very easily by the collaboration of distributed agents [4]. Intrusion Detection system is such a complex task. So system using distributed agents based on AIS is fast becoming the part and parcel of IDS design [5].

We are designing a hybrid method for intrusion detection system that combines both misuse detection and anomaly detection. Misuse detection has a disadvantage that anything that is a new cannot be detected.ie it is considered as normal, whereas anomaly detection has high false positive rates. That is identifying a normal case as an attack. To overcome the limitations of both techniques, we combine the two approaches to create a hybrid method for intrusion detection system. We are using distributed autonomous NK cells in this paper.

2 Related Work

Agent-based model changes the face of intrusion detection systems. AIS combine with the agent-based model is an effective tool for designing

accurate intrusion detection system. AIS mainly revolve around the four Algorithms-Danger theory (DT) [6, 7], Clonal Selection (CS) [8, 9], Immune Network (IN) [10] and Negative Selection (NS) [3]. Some works [11] combine two or more above algorithms to design effective IDS. Some new breeds of algorithms like Conserved Self Pattern Recognition Algorithm (CSPRA) [12] have also been proposed in the area of AIS which can be applied to develop an effective intrusion detection system.

Seresht and Azmi [13] proposed a multi-agent approach based on AIS that was implemented on virtual machines. This work used three types of agents-detection, antigen, and orchestra. It used negative selection algorithm to remove and kill weak agents. The clonal selection was used to improve high fitness detector agent population. Immune network algorithm is used to permit collaboration between agents. To maintain the number of agents, the number of agents removed was equal to the number of agents cloned. In this algorithm, immature agents were randomly generated and they learned and mature based on fitness. Agents with high fitness value were chosen for cloning and they migrated to virtual machines and agents with low fitness values were removed. This hybrid algorithm worked in both network and system settings.

Hu et al. [14] proposed a dynamically real-time algorithm where mature agents update dynamically and form a network using immune network algorithm. This concept also used negative selection to do self-tolerance and clonal selection to proliferate agents. Here the detector radius of a mature agent which failed to recognize a non-self was dynamically resized to improve the performance of that agent by detecting new attacks. If a mature agent identifies another agent it gets animated and when an agent is recognized by another agent, it is smothered. Then these dynamically resized specialists were utilized for interruption identification.

Chung-Ming Ou [15] used a danger theory approach in IDS using dendritic cell agents to develop a host-based IDS. This work is based on danger signal emitted by host computers. In this work, four agents namely Antigen agent to parse the dataset, Dendritic cell agent to analyze those antigens, T-cell agent to identify the attack and Responding agent for a response to the attack were used. The coordination of all these agents helps us to identify any intrusion in the host computer.

Yang et al. [16] used a distributed and hierarchical framework for IDS. Dynamic evolution of self, mature agent and memory agent were proposed for real time ids which used agents like Sensor agents which search for any misbehavior, Analyzer agent that analyze those misbehaviors, Manager

Agent which manages the overall system, Messages agent which helps in inter-sensor communication and an Alert agent which generates the alarm.

Zhang and Tan [17] proposed a new method called for immune cooperation based learning (ICL) in which the concept of danger zone was considered unnecessary. In this approach, two signals, namely antigen-specific and non-antigen specific signals were used to detect malware. These two signals are collectively taken and their cooperation is used to train the system. In this approach, malware is taken as antigens and benign programs are taken as non-antigen.

Fu et al. [18] coined the idea of utilizing NK Cells to artificial immune systems. In this paper, a host-based IDS based on natural killer cells was designed to detect hidden spyware. Here inhibitory signals were used. The inhibitory signal was activated if normal programs features were exhibited and activating signal was activated if spying behavior was exhibited. These NK cells induce cytokines (baits) so that latent spyware trigger actions that can be detected.

Sobh and Mostafa [19] described an adaptive multi layered system that can change with the changes in environment. In this work a combination of danger theory and self-nonself theory was used. To update the knowledge of the system, a vaccination unit was used. Packets were captured by the help of a sniffer module. The affinity of the captured packets was calculated using the Non-self-detector module. Any deviation from normal was calculated using danger detector module. Decisions were taken by Decision making module and a response module was used to take opt responses for an attack.

Laurentys et al. [20] used AIS concepts in detecting fault using immune theory. It used the concept of negative selection algorithm. This Multi Operational Algorithm for better coverage used a variable radius algorithm for determining detector radius. An algorithm that utilized dynamic radius assigned to a detector was used for overlapped conditions. The movement of the detector continues until the overlap is less. The model was used to detect anomaly in working of a DC motor.

Janakiraman and Vasudevan [21] proposed the concept of using lightweight agents and a heavyweight agent to get good accuracy and high detection rate in their ACO based distributed IDS. The heavyweight agent even though has high computational complexity, but increases the accuracy and reduces the false alarm rate of the system.

The concept of a fully distributed autonomous intrusion detection system is still a hoax. Many works reviewed in the literature lack such a fully autonomous environment. Many ids lack the concept of response time [5]

which is very much important in giving a proper reply for an intrusion. So the proposed paper deals with a design that in fully autonomous in nature and has high accuracy as well as quick response time.

3 Proposed Work

The work proposed in this paper is based on Artificial Immune System. Here we use Natural Killer Cells of the human immune system to accurately identify intrusions in the network. In the first place, we give a presentation about NK cells and then their utilization to plan IDS. A Natural Killer cell is characterized as "An independent immunity based agent that are proliferated into the network". We discuss the IDS based on NK cell that we have designed and then we give the experimental analysis of the approach using NSL KDD dataset. First NK cells are generated using the negative selection algorithm and are trained. Based on its performance these NK cells are cloned and distributed throughout the system. A population control mechanism is used to control the population of NK cells.

3.1 Natural Killer Cells

Natural killer cells (NK) are a type of white blood cells that belong to an innate immune system that is cytotoxic. They provide quick responses to virally infected cells or cancer cells [Figure 1]. NK cell work on missing-self recognition. Natural killer cells have dual surface receptors -Activating and Inhibitory receptors. Based on Major Histocompatibility Complex class I molecules (MHC-1) present in the cell, NK cell works. The downregulating of MHC-1 in a cell is due to virus activity. When the cells with fewer MHC-1 are encountered, activating receptors are activated and those cells are prone to Apoptosis (programmable cell death). When inhibitory receptors are activated, it means that the cell is normal and is allowed to pass through. Natural killer cells (NK) were once considered the backbone of innate immunity, recent studies revealed that they have immunology memory and has a role in adaptive immunity also.

3.2 Artificial Nk Cells

Here Artificial NK cells for network intrusion detection are introduced. Only memory NK cells that have antigen-specific immunology memory is considered. Artificial NK Cells are Independent Immunity based agents

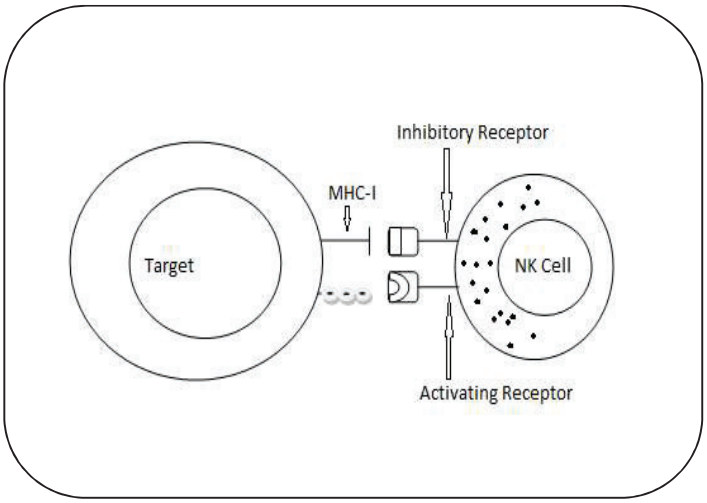

Figure 1 NK cell.

that proliferate into the network and detect any misbehavior that affects the confidentiality, integrity, and availability of information. NK cells have two types of receptors -Activating and Inhibitory. If the incoming packet is normal, the Inhibitory receptor is activated. If the packet is abnormal, the activating receptor is activated. When an activating receptor is activated NK cell responds in two ways-releasing cytokines that are releasing an alarm thereby informing the user or to perform Apoptosis (Programmed cell death) that is to drop the packet.

An artificial NK Cell defined in this paper can be articulated as

NK (Type, AR, Fitness, State)

Type: Type defines the type of attack the NK cell is qualified to discover.

Activating Range (Ar): is the distance between the central vector of the particular NK cell and its detection radius.

Fitness: Fairness rate of the NK cell is constructed in accordance with the number of attacks it has detected. The higher the fitness value of NK cell, the better the proliferation or cloning of the cell.

State: Initially all the NK cells are in a passive state until they are activated. An NK cell is activated when the incoming MHC1 is given to it. If the MHC1 is within Ar, at that point the NK cell is in Activating Response (AR), else it

is in Inhibitory Response (IR). If the Fitness assessment is greater than fitness threshold, then the cell is considered as mature. If the total number of cells is less than total population then cell is proliferated. NK cell can be modeled as a DFA as follows:

$$NK = DFA\ (Q, \Sigma, \delta, q_0, F)$$

Where
$Q = \{q_0, q_1, q_2, q_3, q_4, q_5\}$ is the set of states
$\Sigma = \{a, b, c, d, e, f, g, h\}$ is the set of inputs
δ: Q x $\Sigma \rightarrow$ Q as tabulated below:

Table 1 States and inputs

States	Inputs							
	a	b	c	d	e	f	g	h
q_0	q_1	–	–	–	–	–	–	-
q_1	–	q_2	q_3	–	–	–	–	-
q_2	–	–	–	q_4	–	–	–	-
q_3	–	–	–	–	q_0	–	–	-
q_4	–	–	–	–	–	q_0	q_5	-
q_5	–	–	–	–	–	–	–	q_0

Where q_0 is the start state and $F = \{q_0\}$ is the set of final states.

States Description

Table 2 States

State	Description
q_0	Passive
q_1	Active
q_2	Activating Response
q_3	Inhibitory Response
q_4	Mature
q_5	Cloning

Inputs Description

The State diagram of the FA, NK is as given in Figure 2.

Table 3 Inputs

Input	Description
a	MHC1
b	DRin
c	DRout
d	Fitness Threshold
e	Normal
f	MaxPop
g	<MaxPop
h	Cloning Completed

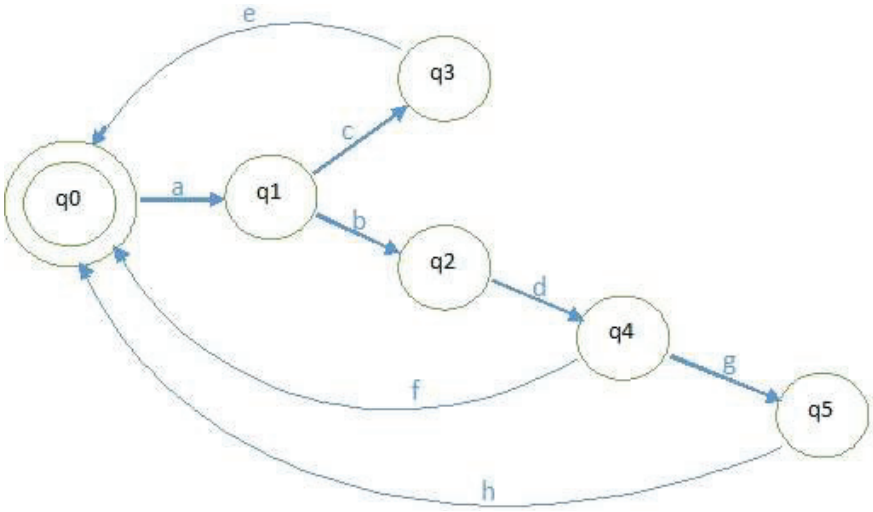

Figure 2 State diagram.

3.3 Working

In preliminary phase, arbitrary NK cells are generated and their detector radius defined. Detector radius of the NK cell is the space where an NK cell detects attacks. The detector radius is determined by the nearest self-space. So detector radius is given by the Equation (1):

$$\mathrm{NKR}_i = \mathrm{Min} \sum_{j=1}^{M} (d_i - r_{ij})^2 \tag{1}$$

where $NK_i = (d_1, d_2, \ldots)$ and $S_j = (r_{1j}, r_{2j}, \ldots)$.

S_j refers to the self -antigens and NK_i refers to NK cells and *d* and *r* are the detectors and self-antigen coordinates respectively. Then based on the detection, each NK cell detector is associated with known attack by the heavyweight NK cell. More than one attacks can be associated with a detector. This helps us to identify the known attack that has occurred.

During the testing phase when a detector detects an attack its fitness value is incremented. Then high fitness agents are cloned and migrated to the entire network. There is a population control system to maintain the number of agents in the system. Based on the occurrence of attack after training, most occurred attack agents are cloned more and less occurred are cloned less. These agents thus deployed on the network monitors the packet flow and identify known attacks.

3.3.1 Working of individual NK Cells Agent

An MHC1 is generated centered on the approaching packet. MHC1 is defined as an information vector that can be extracted from the IP packets which may include the IP address, port number, protocol types etc. The incoming vectorized MHC1 is used by the NK cell agents as either activating signal or inhibitory signal [Figure 3]. If it's the activating receptor, then Apoptosis (programmed cell death) is performed. That means it is an attack and either message is sent to admin that an attack is detected. In future work, there will be a packet dropping mechanism. If it's the inhibitory receptor signal, then it's a normal packet. Functions of each Nk cells are sensing, analyzing and response. The sensing function selects particular features from a packet based on what attack the NK cell is trained to detect. The analyzing function compares the detection radius of the NK cell and used it to activate the activating receptor or inhibitory receptor. The response function is used to give a response based on the output of analyzing function.

3.4 NK cell-based IDS Architecture

NK cell-based Intrusion detection system involves two types of NK Cells. - Light Weight NK cells (LWNK) and a Heavyweight NK cell (HWNK). Each LWNK has an NK cell at the beginning and based on the performance that NK cell is proliferated. The design also has a HWNK which can detect all the attack and normal packets. If the attack does not belong to any known attacks or normal, a new NK cell is created by HWNK for the new attack. NK cell based design is portrayed in Figure 4.

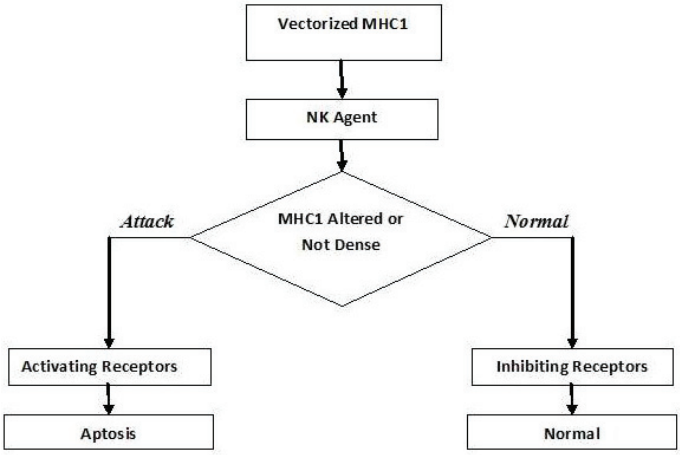

Figure 3 Working of each agent.

The system architecture consists of Sensors, LWNK and HWNK cells. Sensors collect the traffic data and supply it to the NK cells. As the NK cells are deployed in promiscuous mode rather than the inline mode, so we use passive sensors, i.e. a copy of actual traffic is given to NK cells rather than the original packet. The sensors collect the information and LWNK cells work in parallel thus reducing the processing time.

Each LWNK has an analyzer and an NK cell at the beginning. The NK cell is at passive state at the start of the deployment. The analyzer is responsible for extracting particular features from the packet and supplying it to the NK cells. At the start of the deployment, each LWNK cell has one NK cell to process the packet. As the NK cell detect more attacks, its fitness rate surges. When the fitness rate touches a particular threshold, the NK cell is flourished. When the proliferated NK cell reaches a high fitness value, it is also proliferated. The proliferation continues until a maximum population is reached. The analyzer also performs load balancing that is directing which NK cell should process the packet. It uses a round robin method for load balancing. The use of LWNK cells reduces the processing time and the response time of the IDS system.

The Heavy Weight NK cell (HWNK) also has an analyzer and an NK cell that can detect all the attacks as well as normal packets. The heavyweight agent first analyses whether it is a normal packet. If its normal no further processing is done i.e. inhibitory response is there. If it's not, the packet is checked for possible attack scenarios. This helps the HWNK to detect new

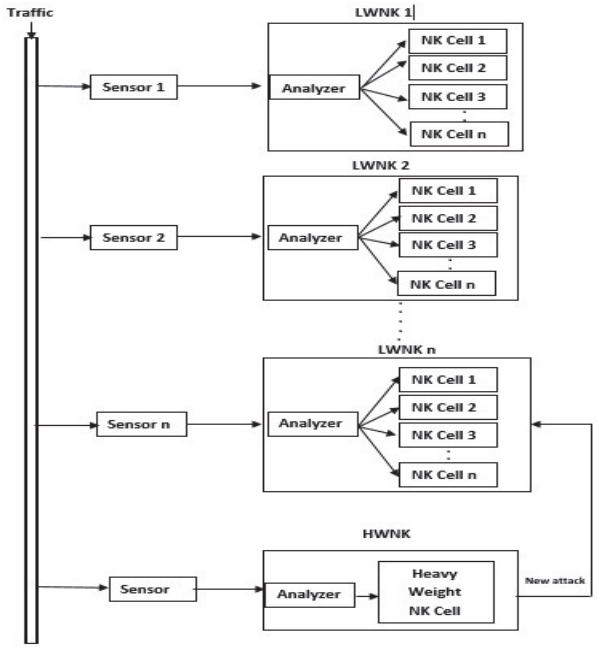

Figure 4 An NK cell-based IDS architecture.

attacks. If a new attack is detected.it updates its own repository as well as create a new LWNK cell and deploy it in the system. Even though there is an increase in complexity due to the usage of HWNK cells but it gives better accuracy to the system as well as to detect new attacks.

4 Results and Discussion

We are testing our proposal on 10% of NSL KDD Dataset [22]. The NSL Kdd data set is a popular benchmark dataset for IDS available. It is a corrected version of KDD Cup 99 Dataset where the inherent problems of the old dataset are solved [23]. The dataset was preprocessed and normalized to reduce redundant information as well as produce stocktickerMHC1 value. The training dataset is used to train the NK cells and then are given the testing dataset. This helps us to improve the learning of NK cells. The dataset was divided into five classes namely Normal, Probe, DoS, U2R and R2L. The Second dataset to be used for the evaluation of our approach is the CCIDS 2017 Dataset [24]. We are preprocessing our dataset using the techniques

```
Begin
        Randomly create NK cells and calculate the radius based on nearest self-antigen.
        Eliminate self-identifying NK cells.
        Deploy it in network
        NK. State=Passive;
        Incoming traffic is vectorized to create MHC1.
        MHC1 is given to NK Cell
        NK. State=Active;
        If Incoming MHC1<>Dr (Detection Radius)
                        NK. State=AR    //Activating Response
                        F++;
                        Send a message to the Administrator.
                        If F>=T(Threshold)
                                NK. State=Mature;
                                If N (No of NK cells) <P(Population)
                                Proliferate the NK Cell;
                                End
                        End
        Else NK. State=IR;              //Inhibitory Response
        Consider the MHC1 as normal
        End
        NK. State=Passive;
End
```

Figure 5 Algorithm for NK cell-based IDS.

used in. Then we apply min-max normalization and convert those to training and testing datasets. Only the following data from Table 4 CCIDS 2017 dataset is considered.

Table 4 CCIDS 2017 dataset

Attack Type	Number
Benign	200
Heartbleed	11
SQL Injection	21
XSS	652
Brute force	1507

We are comparing our work with that of [20] and [21]. Janakiraman and Vasudevan [21] introduced the concept of heavy weight agent along with an individual agent and [20] used the concept of detector moving for better coverage. The parameters used in this comparison are accuracy, detection rate, false alarm rate. For NSL KDD we are considering a parameter Response delay that is very much important if the following work should be upgraded

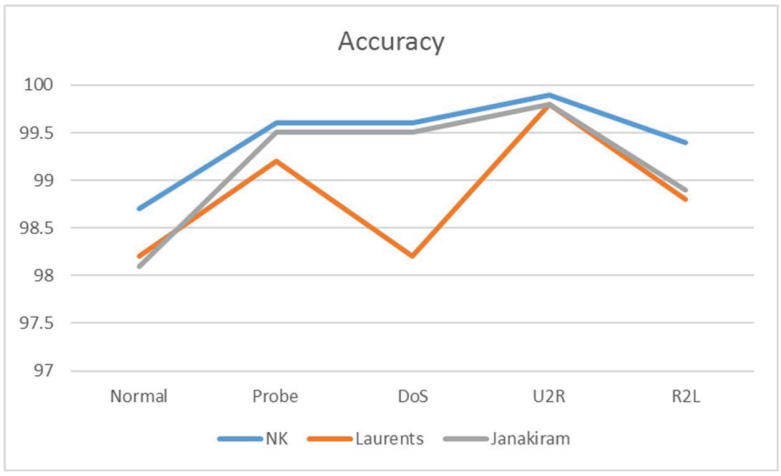

Figure 6 Accuracy (NSL KDD).

to an Intrusion Prevention System.

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{TN} + \text{FP} + \text{FN}) * 100 \quad (2)$$

$$\text{Detection Rate} = \text{TP}/(\text{TP} + \text{FN}) * 100 \quad (3)$$

$$\text{False Alarm Rate} = \text{FP}/(\text{FP} + \text{TN}) * 100 \quad (4)$$

4.1 Results with NSL KDD Dataset

The approach using NK Cells give an Average Accuracy of 99.44% whereas [21] and [20] have an Average Accuracy of 99.16% and 98.84% respectively [Figure 6]. So a higher accuracy means the system detects the attack correctly.

The average detection rate for [21] and [20] are 95.62% and 95% respectively whereas the NK cell-based approach outperforms them with an average detection rate of 96.68%. The detection rate of U2R is higher than the compared work but considering other types of attack it is the lowest. This may be due to a minimum number of samples available in the dataset for these types of attacks.

False alarm rate is an important parameter in intrusion detection system. The smaller the false alarm rate the better the intrusion detection system. NK cell-based IDs has an average false alarm rate of 0.4 while the other two has a false alarm rate of 0.7 and 1.1 respectively.

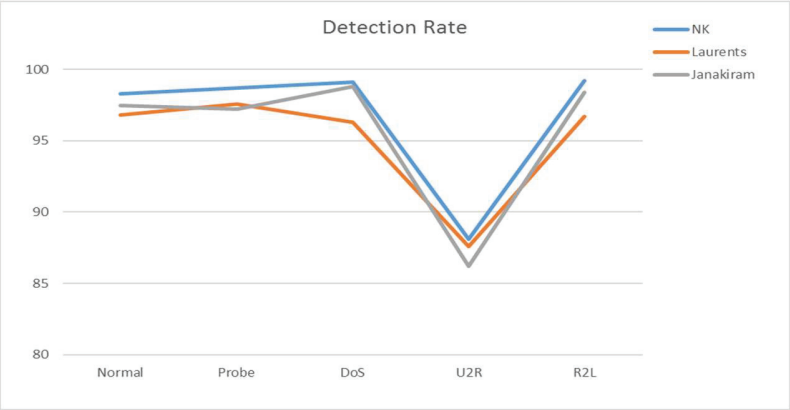

Figure 7 Detection rate (NSL KDD).

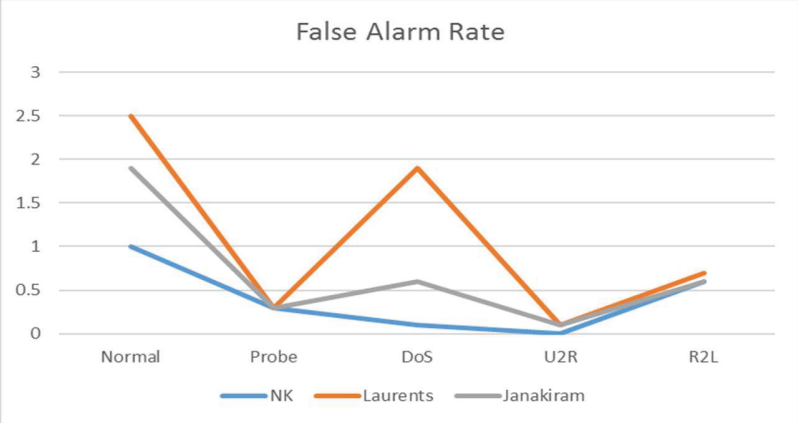

Figure 8 False alarm rate (NSL KDD).

Here we are using a parameter Response Time in this proposed work [Figure 9].

Detection Delay (D_d): The delay between the actual occurrence of attack and the original detection by the intrusion detection system.

$$D_d = \sum_{i=1}^{N} D_i \tag{5}$$

Detection delay contains N delays like packet capture, feature selection, processing, queuing delay if any etc.

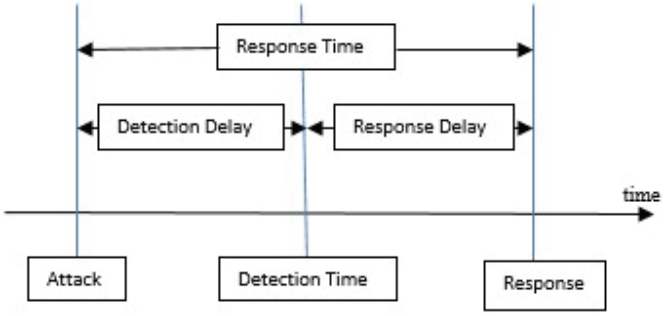

Figure 9 Response time.

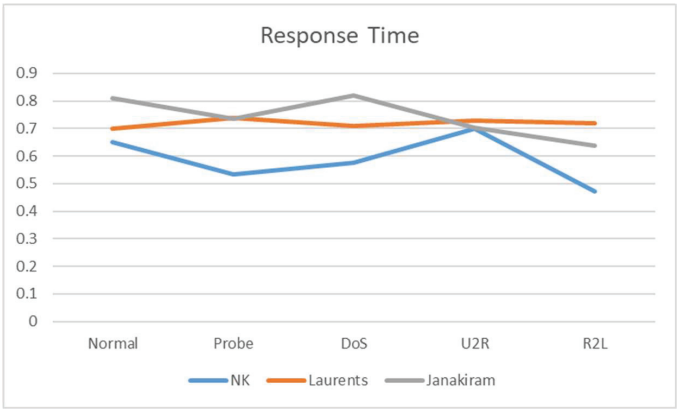

Figure 10 Response time.

Response Time(R_t)-The total time that is needed by the ids to respond to a detected attack.

$$R_t = D_d + D_r \tag{6}$$

Where D_r represents the response delay of the system. The smaller the R_t, the more efficient the intrusion detection system will be.

Nk cell-based IDS shows a much reduced and quick response time when compared to other two approaches shown in Figure 10.

4.2 Results using CCIDS 2017 Dataset

For CCIDS 2017 dataset also we are considering the three parameters i.e. accuracy, detection rate, false alarm rate that are very much important in design of IDS from the literature.

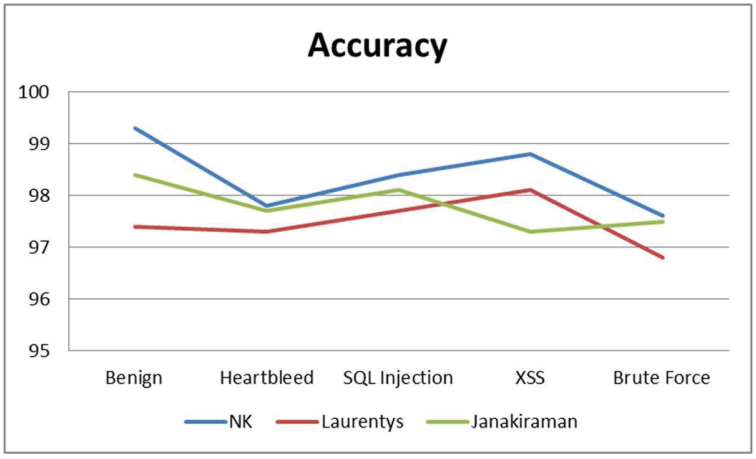

Figure 11 Accuracy (CCIDS 2017).

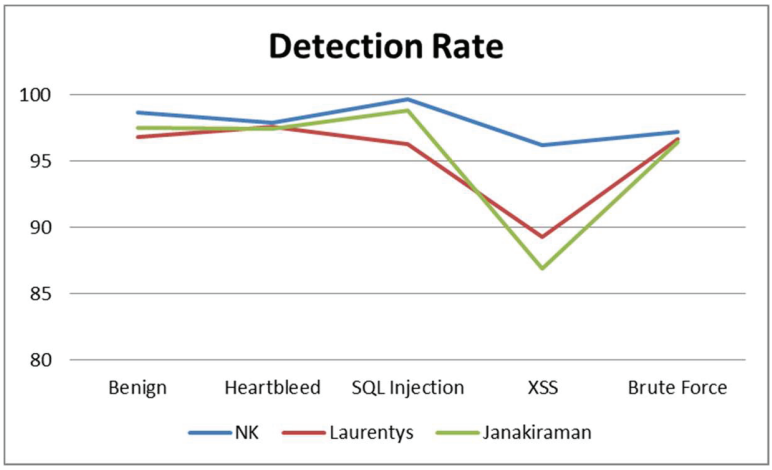

Figure 12 Detection rate (CCIDS 2017).

The average detection rate of NK cell based approach is 98.38% where Laurent's and Janakirman have an average detection rate of 97.46% and 97.8% respectively (Figure 11).

NK cell based approach has an average detection rate of 97.94% whereas Laurent's and Janakiraman have 95.34% and 95.4% respectively (Figure 12).

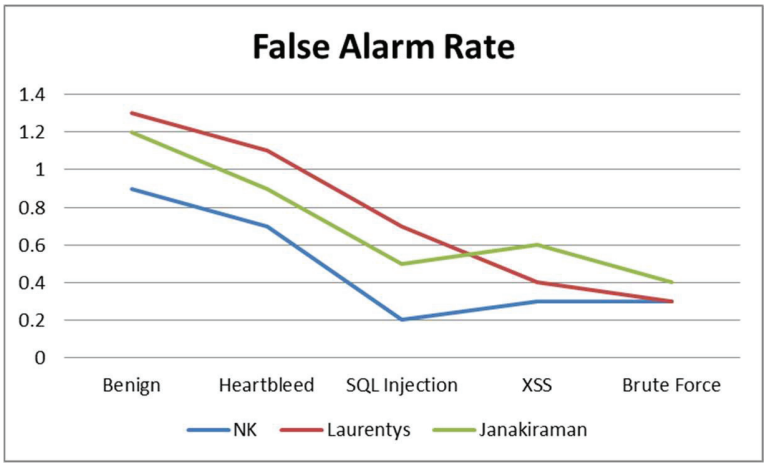

Figure 13 False alarm rate (CCIDS 2017).

5 Conclusion

An intrusion detection system which is based on NK cells is proposed. The system deployed has high accuracy, better detection rate, low false positive rate and quick response time when compared with other IDS compared in the work. As the approach used here is based on Anomaly based detection, so there is no bias of the proposed system towards attacks if there number is less. But certainly the less number of attacks can affect the creation of mature NK cells when the system is upgraded to NK cell based Intrusion Prevention System. The reduced false positive rate and quick response time of the proposed work facilitate it to be used as an Intrusion Prevention System. Even though the use of heavyweight agent increases the complexity of the proposed work, but it is mitigated by increased accuracy and ability to detect new attacks on the proposed system. The future work depends on using high fairness NK cell to migrate to an Intrusion Prevention System that is connected inline to the network traffic where Apoptosis happens by dropping the packets from a known attacker.

References

[1] Denning, Dorothy, E.: An Intrusion Detection Model, Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986. Author, Article title, Journal, Volume, page numbers (year)

[2] Forrest, S., Hofmeyr, S.A., Somayaji, A.: Computer immunology. Commun. ACM. 40, 8896 (1997).
[3] Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R.: Self nonself discrimination in a computer. Proc. 1994 IEEE Comput. Soc. Symp. Res. Secur. Priv. 202212 (1994).
[4] Yang, J., Liu, X., Li, T., Liang, G., Liu, S.: Distributed agents model for intrusion detection based on AIS. Knowledge-Based Syst. 22, 115119 (2009).
[5] Bejoy B J, Bijeesh TV, S Janakiraman: Artificial immune system based frameworks and its application in cyber immune system: a comprehensive review. JCR. 2020; 7(2): 552–560. doi:10.31838/jcr.07.02.103,
[6] Matzinger, P: The danger model: A renewed sense of self. Science, 296(5566), 301–305 (2002).
[7] Greensmith, J., Aickelin, U., Cayzer, S.: Introducing dendritic cells as a novel Immune-Inspired algorithm for anomaly detection. Lecture Notes in Computer Science, 3627. Berlin, Heidelberg: Springer (2005).
[8] Burnet, F.M.: The clonal selection theory of acquired immunity. Vanderbilt University Press (1959).
[9] De Castro, L.N., Von Zuben, F.J.: Learning and optimization using the clonal selection principle. IEEE Trans. Evol. Comput. 6, 239251 (2002).
[10] Jerne, N.K.: Towards a network theory of the immune system. Ann. Immunol. (Inst. Pasteur), 125C, 373389 (1974).
[11] Luther, K., Bye, R., Alpcan, T., Mller, A., Albayrak, A cooperative AIS framework for intrusion detection. IEEE Int. Conf. Commun. 14091416 (2007).
[12] Yu, S., Dasgupta, D.: Conserved Self Pattern Recognition Algorithm,7th International Conference on Artificial Immune Systems, Phuket, Thailand (2008).
[13] Afzali Seresht, N., Azmi, R.: MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach. Eng. Appl. Artif. Intell. 35, 286298 (2014).
[14] Hu, X., Liu, X., Li, T., Yang, T., Chen, W., Liu, Z.: Dynamically real-time intrusion detection algorithm with immune network. J. Comput. Inf. Syst. 11, 587594 (2015).
[15] Ou, C.M.: Host-based intrusion detection systems adapted from agent-based artificial immune systems. Neurocomputing. 88, 7886 (2012).
[16] Yang, J., Liu, X., Li, T., Liang, G., Liu, S.: Distributed agents model for intrusion detection based on AIS. Knowledge-Based Syst. 22, 115119 (2009).

[17] Zhang, P., Tan, Y.: Immune cooperation mechanism based learning framework. Neurocomputing. 148, 158166 (2015).
[18] Fu, J., Yang, H., Liang, Y., Tan, C.: Bait a trap: Introducing natural killer cells to artificial immune system for spyware detection. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 7597 LNCS, 125138 (2012).
[19] Sobh, T.S., Mostafa, W.M.: A cooperative immunological approach for detecting network anomaly. Appl. Soft Comput. J. 11, 12751283 (2011).
[20] Laurentys, C.A., Ronacher, G., Palhares, R.M., Caminhas, W.M.: Design of an Artificial Immune System for fault detection: A Negative Selection Approach. Expert Syst. Appl. 37, 55075513 (2010).
[21] Janakiraman, S., Vasudevan, V.: Agent-Based DIDS: A Intelligent Learning Approach. International Journal of Intelligent Information Processing, Serials Publications (2009).
[22] http://nsl.cs.unb.ca/NSL-KDD
[23] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani,: A Detailed Analysis of the KDD CUP 99 Data Set, Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), (2009).
[24] https://www.unb.ca/cic/datasets/ids-2017.html

Biographies

B. J. Bejoy is currently working as an Assistant Professor in the Department of Computer Science and Engineering at CHRIST (Deemed to be University) Bangalore. He completed his Ph.D in Banking Technology (An interdisciplinary in CSE and Banking) in thesis titled “Co-operative framework for distributed intrusion detection using Artificial Immune System” from

Pondicherry University in 2019. He completed his ME in Computer Science and Engineering and BTech in Information Technology from Anna University Chennai in 2008 and 2006 respectively. He is a Life Member of ISTE. He has thirteen years of teaching and research experience. His current research areas include Artificial Immune System, Intrusion Detection System, Wireless Sensor Networks, Hardware Trojans Detection, Big Data Analytics and Software Defined Networking.

S. Janakiraman received his Ph.D. (Computer Science and Engineering) degree from the Faculty of Information and Communication Engineering, Anna University, Chennai, Tamilnadu, India in the year 2010. He has obtained both of his Post Graduate degree, M.E. (Computer Science and Engineering) and Graduate degree B.E., (Electrical and Electronics Engineering) from Madurai Kamaraj University, Madurai, Tamilnadu, India. He is currently serving as Assistant Professor, Department of Banking Technology at Pondicherry University, Pondicherry. He has nineteen years of teaching and research experience. He is a Life Member of ISTE, Institution of Engineers (India). He is a reviewer for reputed journals publications which includes IEEE, IET, Elsevier publications. He is serving as a programme committee member and advisory committee member in international/national conferences like IEEE, Springer conferences. His area of research interest is Machine Learning and pattern recognition, Big Data Analytics, Banking Technology, Computer Networks, Security, and Image Processing. He has published more than 36 papers in international journals and presented 44 papers in international and national conferences.